NUREG/CR-4387
PNL-5545

Effects of Control System Failures on Transients, Accidents, and Core-Melt Frequencies at a General Electric Boiling Water Reactor

Prepared by W. E. Bickford, A. S. Tabatabai

Pacific Northwest Laboratory
Operated by
Battelle Memorial Institute

Prepared for
U.S. Nuclear Regulatory Commission

NUREG/CR-4387
PNL-5545
RG, R1, R4

Effects of Control System Failures on Transients, Accidents, and Core-Melt Frequencies at a General Electric Boiling Water Reactor

Manuscript Completed: October 1985
Date Published: December 1985

Prepared by
W. E. Bickford, A. S. Tabatabai

Pacific Northwest Laboratory
Richland, WA 99352

Prepared for
Division of Risk Analysis and Operations
Office of Nuclear Regulatory Research
U.S. Nuclear Regulatory Commission
Washington, D.C. 20555
NRC FIN B2386

ABSTRACT

Pacific Northwest Laboratory (PNL) performed probabilistic risk analyses to estimate core-melt frequency and public risk associated with control system failures in a General Electric boiling water reactor. PNL also conducted value/impact analyses of proposed modifications of these control systems to prevent these failures. These analyses were based on failure modes and effects analyses previously performed by the Idaho National Engineering Laboratory (INEL). The control system failure modes identified by INEL and analyzed by PNL fall into three main scenarios: 1) failures that initiate feedwater overfill and also defeat the high level feedwater trip, 2) a failure of the condensate booster pump that results in increased flow to the vessel (overfill), and 3) an inadvertent actuation of the low pressure coolant injection system (LPCI) that also produces an excessive cooldown (overcool). For each of these modes, two failure sequences were postulated. The results of PNL's probabilistic analysis of failure progression to core damage and value/impact analyses of possible resolutions to prevent the occurrence of these failures are presented in this report.

CONTENTS

FIGURES

TABLES

EXECUTIVE SUMMARY

Pacific Northwest Laboratory (PNL) performed a probabilistic risk assessment (PRA) of control system-related failures in light water reactors for the U.S. Nuclear Regulatory Commission (NRC). This work was performed in support of the NRC's Unresolved Safety Issue A-47 program: Safety Implications of Control Systems. This report specifically focuses on control system failures in a representative General Electric boiling water reactor (BWR). The PRA was based on failure modes and frequencies developed for the BWR by Idaho National Engineering Laboratory (Bruske et al. 1985).

In addition, PNL performed value/impact analyses of proposed resolutions to correct these deficiencies identified by the A-47 program. Value/impact analyses are required by the NRC as input into the regulatory decision process to insure that the need for and consequences of cost-effective regulatory actions are identified (NRC 1983a). Cost/benefit analyses are not the sole or even principal basis for decisions, but they do provide one consideration. The purpose here was only to provide a screening tool of potential resolutions.

S.1 GENERAL OVERVIEW

The report discusses the following major topics: 1) control failures identified as being of concern to the A-47 program, 2) the safety implications of failures and progression to core-melt scenarios, 3) risk calculations, 4) resolutions to mitigate or eliminate failures, 5) potential risk reductions with implementation of proposed resolutions, 6) cost of resolutions, and 7) resulting value/impact ratios. These topics will be quickly summarized here, followed by a more detailed summary of the technical analyses and results.

Control Failures of Interest

The A-47 program focused only on those control failures that could result in 1) a more severe plant response than previously predicted in design basis accidents, or 2) failures that could cause plant conditions to exceed operating technical specifications. Using the Browns Ferry plant as a representative General Electric BWR, INEL identified four general failure modes involving feedwater overfill of the reactor vessel, one involving condensate booster pump failure, and one involving low pressure core injection (LPCI) failure. PNL then examined these identified failure modes for safety implications.

With the exception of loss of offsite power, the INEL investigation did not consider events external to the plant, (e.g., seismic events, aircraft crashes, etc). Such events are thus not considered in this report.

Safety Implications

For these analyses, overfill of the reactor vessel was assumed to be initiated by failures in the main feedwater (MFW) control and vessel high water level trip circuits. If not terminated by the operator, this could lead to

water pouring into the steam lines, possibly resulting in steam line damage including major steam line failure. A large uncertainty currently exists concerning this potential, so a high probability of main steam line break (MSLB) given spillover of water into the steam lines was assumed. The remaining failure modes likewise have the potential to introduce water into the steam lines, possibly causing steam line damage. The three main failure scenarios are 1) overfill due to failures in the feedwater contol and vessel high water level trip logic, 2) overfill due to failures of the condensate booster pump, and 3) overfill due to inadvertent actuation of the low pressure coolant injection system (LPCI) pump.

An MSLB in a BWR represents a serious breach of the primary piping, and results in a loss of coolant accident (LOCA). If the flow is not blocked or replaced with injection of additional water, the reactor core uncovers, overheats, and a core-melt occurs. The significance of the control failures identified here then depend greatly on the assumed high probability for MSLB to occur as a result of overfill and spillover of water into the steam lines.

In addition, initiating a transient shutdown in the plant can demand safety systems which in turn have the potential for failure. The initiating events identified by INEL were thus also examined as potential transient initiators both with and without the power conversion system available for decay heat removal.

Risk Assessment Results

The event trees developed for MSLB in the Browns Ferry (NRC 1982a) PRA were used to model the plant response to an MSLB. Three separate responses for small, medium, and large pipe breaks were used. The INEL-predicted initiating frequency was ratioed to reflect the potential for various pipe failure sizes based on their predicted frequencies. The INEL event trees for transient shutdown were also substituted for the initiating frequencies in the PRA. The radionuclide release categories used in the PRA for MSLB and transient core-melt scenarios were also used in this analysis to estimate public risk associated with core-melt.

The net result was an estimate for core-melt for all scenarios of 2.76E-06/py, which is approximately 1 percent of the Browns Ferry PRA core-melt frequency of 2E-04/py. For this study, this was dominated by the contribution from Overfill Sequence 1, which involves failure of the vessel high water level feedwater trip of 2.40E-06/py. The overall risk was put at 18.4 man-rem/py, with 16.2 man-rem/py again associated with Overfill Sequence 1.

The core-melt and risk contributions from failure of the condensate booster pumps (Overfill Sequence 2) and LPCI (Overfill Sequence 3) were lower than for Overfill Sequence 1 by factors of 1000 and 20, respectively. Transient shutdowns also contributed an insignificant amount to the risk.

When compared with the risk estimated for other nuclear safety issues (NRC 1983b), the above estimates of core-melt frequency and risk are small. However, the risk from Overfill Sequence 1 cannot be categorized as an insignificant issue. When the NRC methodology for prioritizing efforts to resolve safety issues is applied, a further examination of costs associated with possible fixes is justified.

Risk Reduction/Cost/Value-Impact

A number of modifications were examined to correct the failure modes that initiate the scenarios defined by INEL. Other modifications included piping upgrades to reduce leaks in the instrumentation line serving the level transmitters, and the addition of another level transmitter for a 2-out-of-4 logic upgrade from the present 2-out-of-3 configuration. Modifications to the control logic and addition of a high water level trip were also examined for the condensor booster pump and LPCI pump failures, respectively.

The upgrade to a 2-out-of-4 configuration was identified as the most effective correction for failure of the high vessel water level trip circuit. This was predicted to lower the initiating frequency by approximately 25 percent, giving a risk reduction of 123 man-rem over 30 years. At a minimum estimated cost of $150,000 for this upgrade, a value/impact ratio of 0.82 man-rem/$1000 was obtained. It was noted, however, that costs in excess of $1,000,000 have been observed for this upgrade in plants needing additional penetrations into containment to add the fourth transmitter. Modifications to plant piping to reduce leaks were estimated to reduce the initiating frequency of overfill by only approximately 4 percent, but costs were estimated to be significantly lower than a level transmitter upgrade. However, the resulting cost/benefit ratio was still lower than that of the transmitter upgrade.

The addition of a high vessel water level trip for the LPCI overfill scenario was estimated to essentially eliminate the potential for that scenario, resulting in a risk reduction of 24.3 man-rem over 30 years. At an estimated cost of approximately $70,000 for such a trip, a value/impact ratio of 0.35 man-rem/$1000 was estimated.

The final conclusion was that risk reductions and value/impact ratios indicate that a more detailed examination of resolutions could be justified for the vessel high water level trip circuit and for inclusion of a high level trip for the LPCI pump. The condensate booster scenario has such little estimated risk that no further examination is likely to be needed.

Finally, it should be noted that control system failures similar to those postulated in this report have occurred in operating BWRs. However, there has been no known progression of such failures to core damage and subsequent release of radioactive material. The accident sequences developed in this report are, therefore, speculative and subject to all the uncertainties and limitations surrounding the use of probabilistic risk assessment for predicting nuclear safety. Again, this value/impact information provides only one small input to the regulatory decision process. This information is expected to be subject to further scrutiny by the NRC, INEL, and by affected utilities, which can bring additional insight and perspective to these results.

S.2 TECHNICAL OVERVIEW

A more indepth technical summary of this report is provided below. The potential control system failures identified by INEL again primarily deals with overfill of the reactor vessel with the potential for water entering the steam

lines. The three main scenarios are 1) overfill due to failures in the feedwater control and vessel high water level trip logic, 2) overfill due to failures with the condensate booster pump, and 3) overfill due to inadvertent actuation of the LPCI pump. The reference plant analyzed is the BWR/4 Browns Ferry class of General Electric BWR.

The control system failure modes identified by INEL fall into three main scenarios: 1) failures that initiate feedwater overfill and also defeat the high level feedwater trip, 2) a failure of the condensate booster pump that results in increased flow to the vessel (overfill) and produces an excessive cooldown of the vessel (overcool), and 3) an inadvertent actuation of the LPCI which results in increased flow to the vessel and which also produces an excessive cooldown (overcool).

The low pressures and temperatures involved with the overcool scenarios (270 psi at 1 percent power) were not considered sufficient to have any credible potential for producing thermal shock-induced failure of the reactor vessel. Further, condensation of the large steam void present in all BWRs makes it physically unlikely that the concurrent high pressures and cooling necessary to induce vessel damage would occur.

Instead, the analyses determined that the primary hazard to plant safety is the potential for water spilling into the steam lines, inducing water hammer, and producing a main steam line break (MSLB). BWR piping performance continues to be the subject of intense review in the industry. Although water hammer and steam condensation have occurred on plant startup and main steam isolation valve lift, no such failures of main steam pipes have ever been observed in actual plant operation. However, to be conservative, this analysis assumed that the probability of MSLB was essentially 1.0, given spillover of water into the steam lines while the plant is operating at power.

The potential for operator intervention in terminating the sequences was also considered. For example, feedwater overfeed while on automatic control generates conflicting level-indicator readings and annunciator alarms. For those situations, the probability of operator error was set at about 50 percent. This estimate conforms to the subjective views of licensing examiners on the potential for operator error. If lower power settings on manual feedwater control or unambiguous instrumentation/alarm readings are assumed, the error probability is thought to be lower.

Frequency and Public Risk Estimates

The core-melt frequency predicted for each of the three failure scenarios is approximately 2.5E-06/py, or 1 percent of the total core-melt frequency calculated in the Browns Ferry PRA of 2E-04/py. The public risk for the three sequences is approximately 18 man-rem/py. This is again primarily due to the MSLB scenario, with 80 percent of the risk associated with BWR release category 2 and 20 percent with release category 3 as defined in the WASH-1400 Reactor Safety Study (NRC 1975). In the Browns Ferry PRA, 20 percent of the dominant transient risk was associated with release category 2 and 80 percent with release category 3. However, the man-rem/event associated with these release categories (Heaberlin et al. 1983) is similar enough (7.1E+06 versus 5.1E+06 man-rem/event) to indicate that the public risk predicted for control system failures is also on the order of 1 percent of overall plant risk.

The control system failures also must be considered in terms of their potential for generating transient shutdown signals. Those transients that disabled the power conversion system (1.73/py) were found in the Browns Ferry PRA to represent approximately 78 percent of the overall plant core-melt frequency of 2E-04/py. A conservative estimate of the impact of control system failures leading to such a transient shutdown resulted in an initiating frequency on the order of 0.001 of that observed for such transients in the Browns Ferry PRA.

The final results are summarized in Table S.1. The additional consideration of control failures that initiate transients increases the total predicted core-melt frequency only slightly to 2.96E-06/py, which is still approximately 1 percent of the overall core-melt frequency of 2E-04/py given in the Browns Ferry PRA. The upper bound on the initiation frequency was not propagated through the calculations. Instead, using the INEL mean value for an initiating frequency, a best estimate of propagation to core-melt was made, giving a net best engineering estimate of the frequency of core-melt due to the particular control system failure.

Value/Impact Assessment

To analyze the value/impact associated with this issue, it was necessary to postulate a number of possible design changes to alleviate the control system failures identified by INEL. Due to the significant interaction of the operator with control systems, training and procedures directed at the operator could possibly reduce the progression of simple control system failures to more serious accidents. The operator's role was considered in the core-melt calculations. However, it is believed that programs set up specifically to deal with operator actions during transients are, in general, better geared to deal with the potential for reducing operator error than the A-47 program; therefore, options for improving operator response are not considered further in this report.

The postulated design changes were directed at reducing the rate of control system failures as identified by INEL. These modifications are shown in Table S.2, along with the associated estimates for reduction in core-melt frequency, public risk, cost, and the resulting value/impact.

As can be seen, the addition of another level transmitter (LT) in a 2-out-of-4 trip logic was found to be the most cost-effective way of counteracting the control system failures identified by INEL for feedwater overfill. This conclusion assumes that a new configuration would be twice as reliable in preventing the overfill, with implementation costs estimated to be about $150,000. Practical considerations indicate that a 2-out-of-4 configuration probably would not achieve such improvements in reliability; furthermore, costs could easily exceed $1,000,000 if substantial modifications were required to implement the level transmitter change. Both uncertainty factors reduce the resulting value/impact ratio significantly.

TABLE S.1. Summary of Control System Failure Induced Core-Melt Frequency and Public Risk for the GE BWR

Sequence Initiator	INEL Accident Initiating Frequency Median (/py)	PNL Core-Melt Frequency Best Estimate (/py)	PNL Public Risk Estimate Best Estimate (man-rem/py)
Reactor Vessel Overfill Sequence 1	6.5E-03	2.40E-06	16.2
Reactor Vessel Overfill Sequence 2	8.2E-05	2.01E-09	0.01
Reactor Vessel Overfill Sequence 3	3.6E-03	1.20E-07	0.81
Overfill Initiated Transient Shutdown			
With Power Conversion System (PCS)	3.40E-04	7.49E-10	3.16E-02
Without PCS	2.87E-03	4.39E-07	2.40E+00
		4.38E-07	2.43E+00
TOTAL		2.96E-06	19.45

TABLE S.2. Proposed Modifications to GE BWRs and Estimated Value/Impact

Modification	Impact	Reductions in Core-Melt 1/py	Reductions in Man-Rem 30 yrs	Cost, $	Value/Impact Man-Rem/$1000
Instrument Line Weld Integrity	Reduce weld failures	1.18E-08	2.4	113,000	0.02
New 316 SS Instrument Lines	Reduce pipe failures	8.89E-08	18	32,220	0.56
New Level Transmitter, 2-out-of-4 trip logic	Reduce high trip failures	6.96E-07	123	150,000	0.82
Modify Isolation Logic for Condenser Flow	Isolate flow from failed valve	2.05E-09	0.3	8,810	0.03
Add LPCI Trip on High Vessel Water Level	Isolate flow from LPCI pump short	1.20E-07	24.3	69,060	0.35

Modifications to the instrument piping to reduce welding or piping ruptures and low level indications are less effective due to the lower initiation frequency for such scenarios and the high cost of annual welding inspections. The alterations to the condenser and LPCI overfill are also significantly less cost-effective, primarily due to the engineered features already built into the plant to prevent false pump actuation signals or electrical short circuits. This is reflected in the low initiation frequencies for these failures. Modifications to these systems may also have negative impacts on the reliability of feedwater delivery during normal operation or LPCI operation during loss of coolant accidents (LOCAs).

The PNL core-melt frequency and public risk estimates are engineering estimates based on the INEL median initiating frequencies. The costs likewise represent a rough engineering estimate. A certain amount of judgment is therefore needed to interpret the value/impact ratio. However, the development of these accident initiators is thought to reflect a conservative approach to estimating their impact on plant engineered safety systems. Cost estimates likewise tend to underestimate the true cost of nuclear plant modifications. These factors, when combined, indicate that the methods used tend to overestimate the value/impact ratios and provide a conservative approach.

Possible plant modifications to reduce overfill frequency can be bounded by comparison to the proposed Safety Goal benefit/cost guideline of $1000/man-rem averted. Assuming a 30-year effective plant life, the total possible risk reduction is (19.45)(30) or approximately 584 man-rem/reactor. If the costs of potential corrective features are compared to the benefits on the basis of $1000/man-rem averted, then an upper bound of approximately $584,000 can be placed on the costs of corrective features.

Areas of Likely Conservatism

Best engineering estimates of failure probabilities were used whenever possible in the analysis of core-melt and risk for the control system failures identified. Some uncertainty does exist, however, in several factors, and the analysis is thought to be conservative. Core-melt frequency and public risk estimates are probably higher than the true values. Among the factors contributing to this conservatism are:

1. Operator Error - The probability assumed for operator failure to diagnose and terminate the scenarios ranged from 0.5 for scenarios with misleading or conflicting information or rapid progression (i.e., overfill in several minutes) to 0.1 for scenarios with non-conflicting information and alarms. Actual operator response might be better, particularly in plants with simulator programs stressing proper diagnosis of failures.

2. Steam Line Break - The probability of MSLB, given spillover into the steamlines at power, was assumed to be 1.0, decreasing to 0.5 for spillover after shutdown. Although several spillover events resulting in support damage have occurred to date in U.S. commercial plants, no steam line failures have occurred. Break location was further assumed to occur above the main steam isolation valves (MSIVs), making isolation impossible. Further information on the probability of break for various overfill scenarios and break location could significantly reduce the resultant risk.

3. Transient Shutdown - The initiating event would cause a transient-induced plant shutdown with loss of the power conversion system (PCS). This represents a serious precursor to core-melt in BWRs. The probability of PCS loss was assumed to be approximately 0.9, but contributed insignificantly to this analysis due to the low initiating frequency.

4. Release Categories - The WASH-1400 (NRC 1975) release categories most representative of these core-melt scenarios were used to estimate risk, with the risk per event as outlined in the Value-Impact Handbook (Heaberlin et al. 1983). Ongoing evaluation of the source terms for various core-melt scenarios indicates that the WASH-1400 release categories may overestimate risk. This will then result in lower risk being attributed to each scenario.

5. Costs - Estimates of the costs associated with modifications in nuclear plants typically underestimate the final costs, even when accompanied by an extensive engineering-cost study. Higher than expected costs would further lower the value/impact ratios estimated here for proposed modifications.

These value-impact calculations are provided only for perspective. The NRC has established the safety goals to be used for evaluation but not for regulatory use during a two-year period. Furthermore, the proposed benefit-cost guideline, even if adopted, would not be the sole or even the principal basis for decisions on safety improvements; rather, it would be one consideration in such decisions. This report presents only a preliminary analysis of the costs and benefits associated with possible design changes to correct control system failures. The purpose of these preliminary estimates is to assist in screening and assessing the options. A more detailed analysis into the possible negative impacts on control system performance would be required before any such modifications could be implemented in existing nuclear plants.

1.0 INTRODUCTION

This analysis 1) evaluates the risks of core damage or core-melt associated with control system failure and vessel overfill in BWRs, 2) estimates the risk reduction represented by possible design modifications, and 3) provides value/impact ratios for these proposed modifications. These results will provide input into the NRC regulatory process for final resolution of Unresolved Safety Issue (USI) A-47.

To accomplish this, transient overfill sequences identified by INEL in a previous study (Bruske et al. 1985) were incorporated into accident sequences that may lead to equipment damage or partial or total loss of function of selected safety systems such as the high pressure coolant injection system (HPCI) or automatic depressurization system (ADS). The three identified failure scenarios are 1) overfill due to failures in the feedwater control and vessel high water level trip logic, 2) overfill due to failures of the condensate booster pump, and 3) overfill due to inadvertent actuation of the LCPI pump.

To be of major safety concern, the transient overfill accident must at some point make a transition from an overfill to an underfill accident such as LCCA or MSLB that could lead to core damage or core-melt. The overfill transient must then be accompanied by damage or failure in systems that would be called on for reactor coolant supply, depressurization, and/or decay heat removal. Because the INEL analysis stopped at onset of overfill, it was necessary to define possible scenarios for progression of the transient. Event sequences were defined that could lead to equipment damage and the potential for partial or total loss of function of selected safety systems such as the high pressure coolant injection (HPCI) or automatic depressurization system (ADS).

The major damage mechanisms that could lead from overfill to an MSLB are assumed to be associated with entrained water in the steam lines leading to possible water hammer, and pipe failures that could result from the static loads caused by water collecting in the steam lines. The water hammer and vibrations of two phase flow might then interfere with valve operation or cause outright damage or pipe breaks.

Given the uncertainty in the potential for pipe damage in an overfill transient, a high probability of MSLB given overfill has been assumed for this report. This can be updated as more specific information concerning the dynamics of overfill becomes available. The overfill events also have been treated as initiators for transient shutdown. Both the MSLB and transient initiators are carried through to core-melt.

Finally, several proposed modifications to correct the identified control system failures are assessed. The cost of implementing such modifications is estimated, along with estimates of the reduction in plant risk associated with improved system performance.

2.0 APPROACH

Overfill transients are the initiating events of interest in this analysis. Failure rates for the systems identified by INEL are translated into failure frequencies on a per reactor year basis.

Typically, operator recovery is not credited in the risk event trees. However, because the initiating events deal with control systems that are normally under operator control, it is thought to be credible to consider the potential role of the operator in recognition of the transient and recovery. To accomplish this, consideration is given to the indications available to the operator at initiation of the transient and as it progresses. This will include positive as well as conflicting readings that could lead to operator error. The probability of operator recognition and correct response is then estimated.

The response of the reactor system to the postulated initiating event will then be examined in detail to determine the various reading, annunciators, and alarms available to the operator for interpreting the transient.

MSLB Event Tree

As mentioned above, the transient must at some point make a transition to a loss-of-cooling event for this issue to impact public safety. To assist in modeling the risk to the public, the approach taken here will be to use the dominant accident sequences and system response identified in the Browns Ferry PRA (NRC 1982a). This PRA concluded that the risks due to pipe break were dominated by breaks occurring inside of containment. Breaks outside of containment were assumed to have essentially the same occurrence frequency, but independent failures of the MSIVs would have to occur before any significant contribution to public risk would result; in the Browns Ferry PRA, this scenario had a very low probability of occurrence because it required two independent failures in addition to the initiating event. In this analysis, however, water in the steam lines might compromise the performance of the MSIVs. The response of the MSIVs to water flow is thus also examined.

Accident Sequences of Interest

The initiating events of interest for this examination are those developed by INEL (Bruske et al. 1985). These events include the following:

Sequence 1: Level indicator and high level trip failure causing feedwater increase
Sequence 2: Valve failure causing condensate flow
Sequence 3: False start of the LPCI.

The initiators for these sequences are discussed in detail in the following sections.

3.0 SEQUENCE 1: LEVEL INDICATION AND HIGH LEVEL TRIP FAILURE

The following initiators for Sequence 1 were identified by INEL as control system failures resulting in a feedwater increase to the reactor vessel and loss of high level trip:

Initiator A: A leak or rupture of the variable leg of the water-level sensing line that is common to two of the three reactor vessel water level sensors.

Initiator B: A common-cause failure of two of the three level sensors or sensor circuitry.

Initiator C: Independent failure of two level sensors or sensor circuitry.

Initiator D: A failure in the control circuit that regulates the feedwater pump speed and failure of two out of three high-level trips.

The last two initiators involve independent failures, and the frequencies were assumed by INEL to be negligible compared to the first two. The overall median frequency for Sequence 1 calculated by INEL was 6.5E-03/py, with an upper bound of 3.0E-02/py.

3.1 SYSTEM CONFIGURATION

For Sequence 1, INEL assumed that the plant is at 68 percent power, and the reactor level control is in automatic.

The BWR/4 can be operated under one-element control using water level in the vessel, or under three-element control using level, feedwater flow and steam flow as the major parameters, with level providing an error correction function.

It will be further assumed that the system is in the three-element control mode, with the control selection switched to the A channel. This is the typical configuration for automatic operation. The individual initiators will now be examined.

3.2 DISCUSSION OF SEQUENCE 1, INITIATOR A

The feedwater system of a GE BWR/4 uses three level transmitters LT(A), LT(B), and LT(C), with LT(A) and LT (C) being on one 2-inch instrument line, and LT(B) being on a separate 2-inch line. This is in reference to the configuration shown in Figure 3.1.

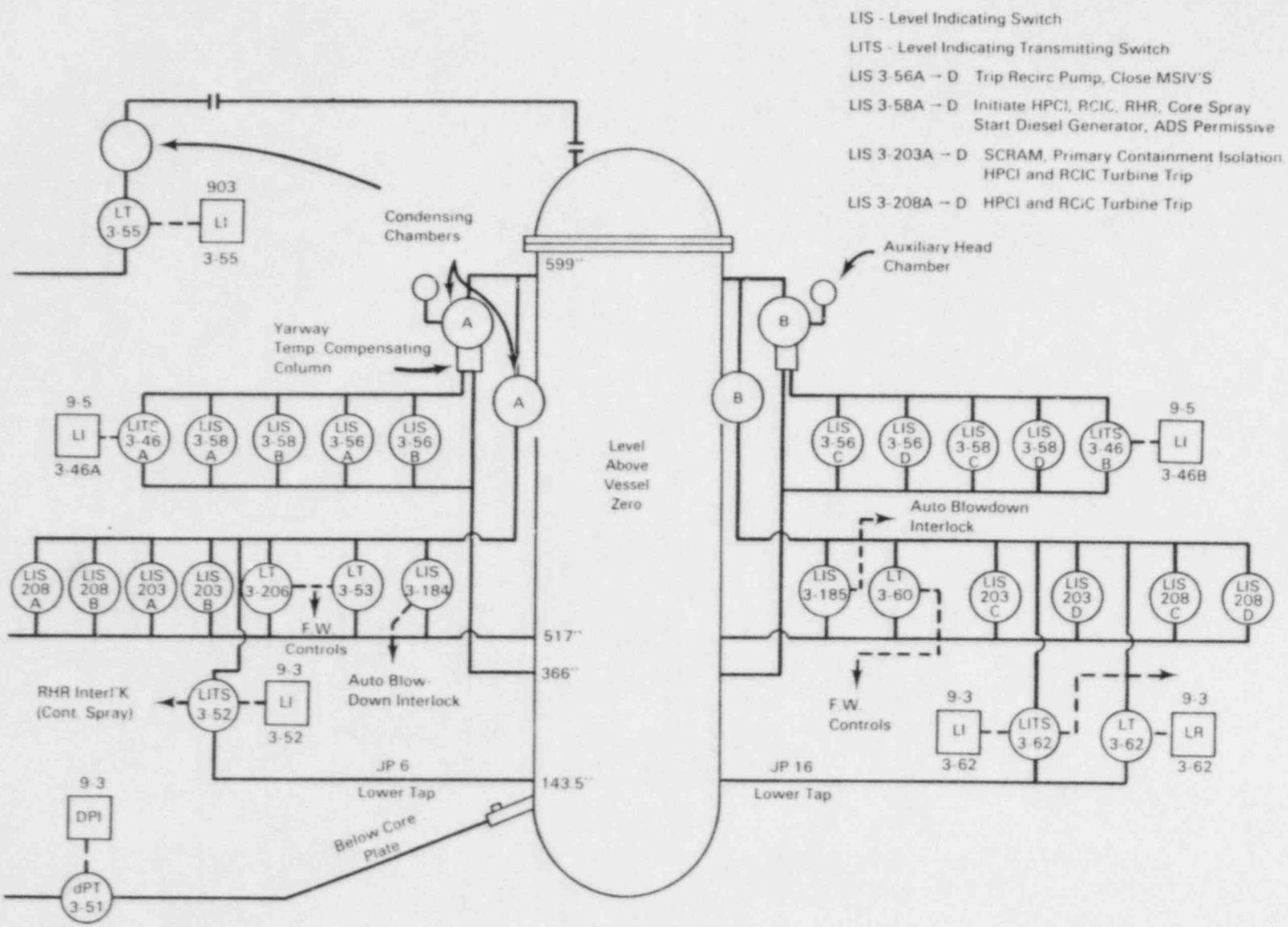


FIGURE 3.1. BWR/4 Reactor Vessel Instrumentation

A leak or rupture of the 2-inch instrument line for the variable leg of level sensors LT(A and C) could occur on the pipe run in the drywell, or on its further extension into the reactor building. Note that a rupture in the drywell could result in steam release and a high pressure indication that could start HPCI. This would produce a reactor SCRAM, but could also aggravate the overfill transient by adding HPCI water flow to the feedwater flow. The HPCI high trips are also located on the same instrument line as the LT(A and C) sensors, and thus might also be defeated with line rupture.

A rupture in the reactor building or leak anywhere along the run, however, may produce no immediate isolation signal. For the purposes of this examination, the failure frequency of both a pipe leak and rupture will be considered, along with the system response.

3.2.1 Failure Rate Information for Sequence 1, Initiator A

The failure rates of interest are for pipe leakages or ruptures, common cause and independent failures for two out of three level sensors, and failures of the control circuit. The failure rates given by INEL used for this analysis are listed in table 3.1.

TABLE 3.1. Pipe Failure Rates

Failure	Failure Rate	Error Factor	Source
Weld Leakage	3.0E-09/hr	10	Wash-1400 (NRC 1975)
Pipe Rupture	1.0E-09/hr	10	NREP Data

The pipe rupture failure rate was further given as the rate per 12 foot section of pipe less than 3 inches in diameter. The error factor of 10 is assumed to apply directly to an upper bound estimate. Assuming 24 hours per day and twelve welds (as did INEL) and 12-foot sections for the variable leg on the yarway back to the reactor vessel, the annual frequencies can be calculated as shown in Table 3.2.

TABLE 3.2. Assumed Failure Rates for BWR Instrument Lines

Failure	Frequency	Upper Bound Frequency
Weld Leakage	3.2E-04/yr	3.2E-03/yr
Pipe Rupture	1.1E-04/yr	1.1E-03/yr
Total	4.3E-04/yr	4.3E-03/yr

3.2.2 System Response to Sequence 1, Initiator A

The three level transmitters provide input into a feedwater trip logic unit that uses a 2 out of 3 indication. If the vessel level increases to level 8 (+ 55 in.), a trip signal is sent. In addition, a summation network compares the

(A-B), (B-A), and (B-C) signals. A difference of 2 inches between the compared levels results in a level failure annunciator alarm in the control room.

The feedwater control system requires a signal selection from transmitter LT(A) or LT(B). This signal is used by the feedwater control circuit. It also provides an additional high water level alarm (level 7, + 40 in.) and low alarm (level 4, + 40 in.), a low level 4 trip for the recirculation control system and feedwater pumps, and a low level 3 (+10 in.) signal to bring the recirculation pumps to slow speed.

Sequence 1.A requires a leakage or rupture of the line with LT(A and C). Line rupture would result in a loss of all pressure on the variable leg side of the level transmitters, resulting in the immediate loss of the high level feedwater trip function (2 out of 3 needed). Assuming that the steam condensation rate in the yarway column remained constant, a leak would also result in a falling level reading, and is likely to result in loss of the high feedwater trip rather than a new equilibrium at a false low reading.

Leakage or rupture would then result in the following:

- Falling or off scale low readings for LT(A) and LT(C) on normal level range
- Signal for increased feedwater flow
- Loss of high level feedwater trips on LT(A and C) level channels
- Signal for interlock on recirculation pump speed (less than 75 percent rated flow) on low level channel A
- SCRAM SIGNAL ON REACTOR PROTECTION SYSTEM (RPS) CHANNEL A (HALF SCRAM) on low level from level indicating switches (LIS) 203-A and 203-B (note that logic requires 1 out of 2 twice, so no RPS SCRAM occurs)
- Loss of high level trip for HPCI and RCIC due to line break and low signal from switches 208-A and 208-B.

Note again that line rupture in the drywell is possible, but is thought to result in SCRAM and MSIV closure before overfill and any other associated system damage could occur. Steam flow to the feedwater turbine would also be terminated with closure of the MSIVs. Sequences which progress to spillover without the initial MSIV closure signal are thought to present the more serious chance for MSLB, and are thus considered here.

3.2.3 Results for Sequence 1, Initiator A

The net result for the estimated frequency of occurrence for Sequence 1, Initiator A then becomes 4.3E-04/yr, with an upper bound of 4.3E-03/yr as was shown in Table 3.2.

3.3 DISCUSSION OF SEQUENCE 1, INITIATOR B

As with Sequence 1, Initiator A, Sequence 1, Initiator B also involves a common mode failure of two out of three indicators. In this case, however, shocks to the system that cause low readings and initiate feedwater flow are of interest. Note that in addition to the pipe leaks and ruptures discussed in 1.A, other sources of common mode failure could include maintenance errors (valving out lines) and calibration errors. However, such errors would be detected during reactor startup with a high level of certainty, and thus are not likely to be of concern here. As a result, shocks are considered as the more dominant common mode failure mechanism (in addition to the pipe rupture considered in 1.A).

3.3.1 Failure Rate Information for Sequence 1, Initiator B

The INEL report presented formulas for common failure from shocks, based on the information in NUREG/CR-3289 (NRC 1983a). This report presented values for the rate at which a specific set of size k assemblies would fail simultaneously in a population of assemblies. However, in the BWR/4 the sensors and switches are in pairs isolated on separate instrument lines. This was not modeled in the INEL calculations. It is uncertain if like sensors on a separate 2-inch instrument line are in fact part of the same population subject to the same shock rates. The conservative assumption is that the shocks are in fact common across instrument lines.

In the BWR/4, two level transmitters (LT) share one 2-inch instrument line, with another on a separate line. These are designated LT(A) and LT(C) on one line, and LT(B) on the other. LT(A) is the controlling feedwater level transmitter in automatic mode. As correctly modeled by INEL, only the LT(AB) and LT(AC) failures would result in feedwater increase and loss of the high level trip. An LT(CB) failure would cause loss of the high level trip, but would not initiate the feedwater increase.

In addition, it is thought that the high level reactor SCRAM, high pressure coolant injection and reactor core isolation cooling (HPCI/RCIC), and isolation functions associated with the level indicating switches (LIS 3-203 A through D) must be defeated if water is to spill past the MSIVs. This does not provide a feedwater trip directly, but early closure of the MSIVs would block steam flow to the feedwater turbine, effectively ending the overfill sequence. In the Browns Ferry BWR/4 two LISs (A and B) operate on safety channel 'A' and share the same 2 inch instrument line with LT(A) and LT(C). The two other switches, LIS(C) and LIS(D), operate on safety channel 'B', being plumbed on the 2 inch instrument line shared with LT(B). Failure combinations that would defeat the one-out-of-two-twice trip function include LIS(AB), LIS(CD), LIS(ACD), LIS(BCD), LIS(ABC), LIS(ABD), and LIS(ABCD). The INEL calculations considered four pairs of two sensors. However, only two pairs are associated with this SCRAM. Another two pairs of LISs on the same instrument line provide another high level trip for the HPCI and RCIC steam driven turbines.

To initiate the sequence, the common shock must satisfy the following fault tree logic of failures:

LLT(AC) or LT(AB)] and LIS(AB) or LIS(CD) or LIS(ACD) or LIS(BCD) or LIS(ABC) or LIS(ABD) or LIS(ABCD).

The INEL report then gave the estimates shown in Table 3.3 of initiating the feedwater transient with loss of the high trip, and losing the 1-out-of-two-twice high trip from the level switches:

TABLE 3.3. INEL Initiating Frequency for Level Sensor and Switch Failure (NUREG/CR-3289)

Component	Failure Mode	Point Estimate	Upper Bound
Level Sensor	Inoperable	2.6E-07/hr	x 3.5
	Reduce capacity	3.1E-07/yr	x 5.2
Level Switch	Inoperable	1.8E-07/hr	x 8
	Reduce capacity	1.2E-06/hr	x 7

These values will be used for comparison, examining the system configuration and response more closely. As correctly modeled by INEL, only the LT(AB) and LT(AC) failures will result in feedwater increase and loss of the high level trip. As mentioned above however, LT(B) is on a separate 2-inch line, and not likely to be subject to the same shocks. Thus the failure rate for a LT(AB) pair failure would be expected to be lower than an LT(AC) failure. Discussions with C. Atwood of INEL regarding assumed instrumentation fault rates indicated that the rate of shocks across instrument lines could be an order of magnitude lower. As a result, the LT(AC) failure alone is likely to be dominant.

The same argument applies to the level indicating switches. Of the failures given above that could cause loss of the one-out-of-two-twice SCRAM, only the LIS(AB) and LIS(CD) failures would be confined to a common shock in an instrument line. And of these two, only the LIS(AB) failure is on the same instrument line as the likely dominant LT(AC) failure.

It is thus thought that the formula and correction factors used by INEL to estimate the rate of failure of this trip (four pairs of two sensors) are likely to be high by a significant margin. The most frequent failure rate sufficient to initiate the sequence of interest is then a common shock to the one instrument line causing failure of LT(AC) and LIS(AB). Other failures which initiate the sequence of interest are possible, but are thought to be significantly less likely. The LT(AC), LIS(AB) failure due to common shock will be used here to arrive at a best estimate of the initiating event frequency, then corrected by an appropriate factor to reflect the non-dominant sequences.

The data in NUREG/CR-3289 are given in Table 3.4 for the failure rate of a specific pair of sensors, corrected for lethal shocks as in Bruske et al. (1985).

TABLE 3.4. Modified Initiating Frequency for Level Sensor and Switch Failure (NRC 1983a)

Component	Failure Mode	Point Estimate	Upper Bound
Level Sensor	Inoperable	1.58E-07/hr	1.18E-06/hr
	Reduce capacity	2.75E-07/hr	9.28E-07/hr
Level Switch	Inoperable	8.5 E-08/hr	3.9E-07/hr
	Reduce capacity	4.16E-07/hr	2.2E-06/hr

A more detailed look at the possible failure modes of the transmitters and switches is provided below.

3.3.2 System Response to Sequence 1, Initiator B

The above probabilities only give a gross indication of the possible failure combinations in the level control system. The level sensors can fail (inoperable) anywhere within their operating ranges as a result of shock. The system response is then very dependent on the false reading after failure. In terms of feedwater control, the level transmitters could become inoperable in any one of five conditions: failing as is, up-scale, high-scale, down-scale, or low-scale. Here, 'high' would mean above the high trip point (54 inches), and 'low' would mean below the low alarm point (10 inches). The INEL analysis did not specify the failure mode of the level transmitters. However, it can be seen that the controlling transmitter (A) must fail in the down scale or low position to initiate a feedwater increase. Indications from PNL experience with reactor operation and operator training are that the transmitters can fail in any position.

For a common mode failure of two level transmitters LIS(AC), the 5 failure modes given above then result in 25 possible failure combinations. However, as indicated above, only 10 combinations would result in feedwater increase (i.e., LT(A) indicating down- or low-scale, LT(C) indicating anything). In addition a high L(C) indication would not defeat the 2-out-of-3 high level trip, as a high indication from LT(B) on overfill would provide the second signal for SCRAM. (Note that two low readings from the feedwater level transmitters would not initiate isolation or safety injection, this being the function of other level switches.)

As a result, only a portion of the possible inoperable failures for two level sensors would provide the necessary conditions for overfill and loss of trip function. If all failure modes are assigned equal probability, only 8/25 or 0.32 of the possible failures would produce the required failure. The shock rate for initiating the sequence would then have to be multiplied by the 0.32 factor.

By the same argument, reduced capacity failures imply a scale drift to a faulty high or low reading, which still changes with changing water level. For this to be an initiating event and knock out two high trips, both LT(A) and LT(C) must drift down-scale. If LT(C) drifts up-scale it will indicate a high reading earlier than normal, and with LT(B) would give the high SCRAM signal.

In addition, the drift down-scale must be of sufficient magnitude that a new high trip signal is not initiated as water approaches the steam lines. The difference between the water height at the steam lines (658 inches) and the high trip (+ 54 inches above the vessel instrument zero of 528 inches, or 582 inches) is 76 inches, implying that the down-scale drift must be at least 76 inches for a reduced capacity failure to block the high trip before overfill occurs. This would require a level reading of 54"-76", or -22 inches below normal instrument zero. A low alarm would sound, but no trip would occur with the level sensors alone.

If only the first order LT(AC) failure is considered, it is apparent that only one of four possible up-/down-scale failure combinations meets the above criteria: a down-scale failure of both LT(A) and LT(C) with both reading at or below -22 inches. Assuming an equal probability between up- and down-scale drift and that a down-scale drift would be to at least -22 inches, the reduced capacity failure rate for the level sensors should be decreased by a factor of 0.25.

For the level indicating switches, inoperable failure implies loss of function, and thus the rate given above needs no correction.

For reduced capacity of the level indicating switches, they also could be subject to up- or down-scale drifts of the trip set point as their likely reduced capacity response to a common shock. Like the level sensors, it is thought that the drift must again be down-scale (and by at least 76 inches) for the dominant LIS(AB) failure to defeat the high trip function. The reduced capacity rates for switches could then also be reduced by a factor of 0.25.

The net result of this consideration for failure rates is given below in Table 3.5, incorporating the appropriate correction factors developed above. The upper error bounds were left unmodified.

TABLE 3.5. Assumed Contribution of Level Sensor and Switch Failure to Initiation of Overfill Transients

Component	Failure Mode	Point Estimate	Upper Bound
LT(AC) Fails Down or Low	Inoperable	5.06E-08/hr	3.78E-07/hr
	Reduce capacity	6.88E-08/hr	2.32E-07/hr
LIS(AB) Fails Down or Low	Inoperable	8.5 E-08/hr	3.9E-07/hr
	Reduce capacity	1.04E-07/hr	5.5E-07/hr

To arrive at the common mode failure rate for both the level transmitters and switches, the values above cannot simply be multiplied together as with a logic 'and' gate, even though both failures are required for the sequence. Because a common cause failure mode is assumed, the bounding case for the point estimate is to simply assume that the larger failure rate of the two represents the rate of the common mode failure. The larger upper bound will be taken as

well. This is highly conservative, but will be used here as a first estimate, as shown in Table 3.6. The rates have also been converted by an assumed (24 hrs/day)(365 d/yr) = 8760 hrs/yr to get the annual frequency.

TABLE 3.6. Assumed Annual Initiation Frequency of Dominant Failure for Overfill Transients

Failure Mode	Point Estimate	Upper Bound
Inoperable	7.45E-04/yr	3.42E-03/yr
Reduced capacity	9.11E-04/yr	4.82E-03/yr
Total	1.66E-03/yr	8.54E-03/yr

Again this failure frequency represents an estimate of the dominant sequence only, involving LT(AC) and LIS(AB). All other combinations of failures that could also initiate the feedwater increase and fail the high level trips require shocks across separate instrument lines. These are again thought to be at least an order of magnitude less frequent. However referring back to the discussion of possible failure combinations, there are 13 others involving the level transmitters and switches that could achieve the necessary combination of failures. As a result, it will be assumed that the non-dominant failure modes contribute at least as much to the total common mode failure frequency as the dominant LT(AC), LIS(AB) failure. The estimates given above will then be doubled to reflect this.

The final estimate for the common mode failure of the feedwater level transmitters and level indicating switches causing feedwater increase and loss of high level trips is then 3.3E-03/yr, with an upper bound of 1.7E-02/yr.

3.4 DISCUSSION OF SEQUENCE 1, INITIATOR C

Sequence 1, Initiator C is the independent failure of two level sensors or sensor circuitry. INEL indicated that the contribution from this term is likely to be insignificant.

Sequence 1.B gives not only the necessary level transmitter failure combinations, but also the failure modes necessary to lead to an overfill. In this case, the failure rates are assumed to be independent. Independent failure rates for individual sensors are likely to be in the range of 1E-06/hr to 1E-07/hr. Even if the highly conservative failure rate of 1E-05/hr is used, the probability that one LT fails and then another fails within an eight-hour period between calibration checks is highly unlikely. This can be quickly verified as given below.

If it is again assumed that LT(C) or LT(B) fails inoperable (anything but high-scale, which is 4 out of 5 possible failure modes) or reduced capacity

(low-scale, or 1 out of 2 possible failure modes) and the probabilities for these failure modes are again assumed to be equal as in Sequence 1.B, a highly conservative estimate of this failure rate is then

$$2 \times (1E\text{-}05/hr)(8760\ hrs/yr)(4/5 + 1/2) = 0.23/yr.$$

However, the LT(A) failure (down- or low-scale) must then occur within an eight hour period between calibration checks of the level indicator. The LT(A) failure can then occur as inoperable (down- or low-scale, or 2 out of 5 possible modes), or as reduced capacity (down-scale, or 1 out of two failure modes), for a total frequency of

$$(1E\text{-}05/hr)(8\ hrs)(2/5 + 1/2)(2.28/yr) = 1.66E\text{-}05/yr.$$

In addition, the level indicating switch high trip must be failed, with the simplest independent failure being LIS(A) and LIS(B). This would further reduce the frequency above, making this contribution of independent failures to the overfill problem insignificant.

If a failure in the LT(A) transmitter is assumed to initiate the feedwater increase first, the available window for failure of LT(C) or LT(B) becomes even shorter, on the order of minutes instead of hours. The likelihood of this would thus be less than that calculated above.

There are also independent failures that could cause loss of high trip given the failure of the feedwater control circuit, designated here as F(CC). To get overfill, this would require:

- Failure of F(CC) and failure of LT(A) up-scale or as is, and LT(B) or LT(C) (inoperative: anything but high-scale; reduced capacity: low-scale), and loss of the high level switch trips: [LIS(A and B) or LIS(C and D) or LIS(A and C and D) or LIS(A and B and C) or LIS(A and B and D) or LIS(A and B and C and D)].

or

- Failure of F(CC) and LT(B) and LT(C), (inoperative, anything but high scale, reduced capacity low-scale), and loss of the high level switch trips: [LIS(A and B) or LIS(C and D) or LIS(A and C and D) or LIS(A and B and C) or LIS(A and B and D) or LIS(A and B and C and D)].

Even if some of these failures are caused by the result of a common mode failure such as a pipe rupture or shock as was presented earlier, one independent failure would still significantly reduce the frequency of the events. The entire Sequence 1.C is thus thought to be insignificant compared to 1.A and 1.B.

3.5 DISCUSSION OF SEQUENCE 1, INITIATOR D

Sequence 1.D calls for a failure of the control circuit that regulates the feedwater pump speed, and a failure of two out of three water level trips.

Letting F(CC) represent the failure of the feedwater pump speed control circuit, the following failures could initiate the sequence:

- F(CC) and common mode failures of 2-out-of-three LT and 1-out-of-2-twice LIS high level trips.
- F(CC) and common mode failures of the LT trips, and independent failures of the LIS trips.
- F(CC) and independent failures of the LT and LIS trips.

The first sequence given is likely the more important, requiring fewer independent failures than the other two. Note that the most likely common mode mechanisms for failing the LT and LIS have already been presented in Sequences 1.A and 1.B. Given the F(CC) failure to initiate feedwater increase, other combinations of LT failure could now be included here as sufficient to cause loss of the 2-out-of-3-twice high level LT trip. This would now include LT(CB) failures which were deleted before, having no impact on feedwater control.

As before, the most important sequences would likely involve failure due to common shock on the same instrument lines. This again would be failure of LT(AC) and LIS(AB). Note, however, that given the feedwater control circuit failure, failure modes for LT(A) which were rejected in Sequence 1.B as not causing feedwater increase can now be included here. For inoperable failures, LT(A) can now fail as is or up-scale. Both LT(A) and LT(C) can still not fail high. This indicates that 16 out of 25 possible failure combinations for LT(A) and LT(C) are now possible. For reduced capacity of level transmitters, it is still thought that they must drift down-scale to avoid eventually reaching a high level trip. Likewise, the consideration of failure modes for the level switches would not be modified from the discussion in Sequence 1.B.

The new estimate for the rate of acceptable LT(AC) failures is then (16/25)x(1.58E-07/hr), or 1.01E-07/hr with an upper bound of 7.55E-07/hr (Table 3.2). Assuming as for Sequence 1.B that the larger failure rate between the LT and LIS failures constituted the common mode failure rate, the assumed initiating frequency for the trip failures for this sequence is shown in Table 3.7 below.

TABLE 3.7. Assumed Annual Initiation Frequency of Dominant Failure Modes for Loss of High Trip

Failure Mode	Point Estimate	Upper Bound
Inoperable	8.86E-04/yr	6.62E-03/yr
Reduced capacity	9.11E-04/yr	4.82E-03/yr
Total	1.80E-03/yr	1.14E-02

Doubling this to account for non-dominant sequences then gives an estimate of the loss of high trip signals as 3.6E-03/yr with an upper bound of 2.3E-02/yr. The failure rate for this portion of the required sequence is thus slightly larger than the whole of Sequence 1.B.

This sequence then requires an independent failure of the feedwater control circuit. Assuming it is as frequent as 0.1/yr, which is considered conservative, the entire sequence frequency could be on the order of 1.8E-04/yr. However, the control circuit failure or common shock causing the loss of the trips would actually have to occur during an eight-hour period between calibration checks. One failure occurring first would also alert the operator to failures in the feedwater control, unless the LT failures were further confined to failures-as-is to avoid the level failure annunciator. The narrow time window actually available for the independent failures to occur would then give a feedwater failure rate on the order of (0.1/yr)/(1 yr/365x24 hrs), this being 1.1E-05/hr or a probability of 9.1E-05 in an 8-hour period.

The frequency of the two required failures would then be on the order of (1.8E-03/yr)(9.1E-05) = 1.6E-07/py. As expected, Sequence 1.D is thus thought to be insignificant compared to 1.A and 1.B.

3.6 SUMMARY OF SEQUENCE 1, OVERFILL INITIATING FREQUENCY

The estimated frequency for Sequence 1 is summarized in the following table. These values do not yet include the probability of operator failure to halt the sequence before overfill begins, which will be discussed in the next section.

TABLE 3.8. Estimated Initiation Frequency of Sequence 1

Sequence	Frequency	Upper Bound Frequency
Sequence 1.a	4.3E-04/yr	4.3E-03/yr
Sequence 1.b	3.3E-03/yr	1.7E-02/yr
Sequence 1.c	-	-
Sequence 1.d	-	-
Total	3.7E-03/yr	2.1E-02/yr

This compares with the estimate made by INEL of 6.5E-03/yr, with an upper bound of 3.0E-02/yr. The PNL estimate of the initiating frequency is thus approximately 1/2 the INEL median estimate, even with a factor of 2 to account for non-dominant sequences. The difference is primarily due to the more detailed consideration of the specific failure modes required for the level transmitters and switches. However, the PNL estimate is well within the bounds given by INEL, and the agreement is considered quite good given the level of uncertainty. The INEL estimate will thus be used in tabulations to follow.

Note that this compares to the overall frequency of feedwater increase at power of 0.2/yr experienced at BWRs (McClymont and Poehlman 1982.) This is about 50 times the frequency predicted here for feedwater increase with the loss of the high level trip.

4.0 SEQUENCE 1: SIGNALS AVAILABLE TO THE OPERATOR

This chapter will examine the signals available to the operator, and estimate the probability of operator termination of feedwater flow before an MSLB occurs. The level failure is assumed to occur, and then the feedwater transient begins to fill the vessel without automatic trip of the feedwater pumps or SCRAM of the reactor. However, further indications are available to the operator:

- Level failure annunciator signalling in the control room due to differential in level transmitter readings from A and B.
- Levels A and C indicators falling in unison, with recording of A.
- Level indicator for B equalling level indicators for Accident Range, Shroud Level Range, and Refueling Range indicators in control room.
- High/Low level alarm occurring on low reading from A and C.

As steam quality begins to degrade, the automatic load following capability of the plant will also provide changing readings in the control room. This will culminate in water pouring into the steam lines, very likely with water hammer. The possible sequence of events after water begins pouring down the steam lines will be developed later.

4.1 OPERATOR RESPONSE TO SEQUENCE 1, INITIATOR A

The operator is most likely to respond in one of several ways under these conditions: do nothing, allowing overfill; interpret the transient as a loss of coolant requiring safety injection and SCRAM the plant; or recognize the level control failure and switch the feedwater control over to channel B. The probability of a correct response cannot be specified exactly, but it is thought that the system response and indicators above make it possible to assign a reasonable probability to the operator response.

The feedwater system is one that the operator uses routinely during plant startup, and malfunctions of the system do occur. Feedwater increase transients are also used routinely in operator training and testing programs. As a result, the operator is very likely to respond in some fashion to the initiator long before plant conditions begin to deteriorate. Based on the indications available, the operator will have a very good indication of a failure in the feedwater level transmitters. Utilizing the other displayed range indicators should provide a reliable indication that the failure has occurred in channel A. If the operator then switches automatic feedwater control to B, the transient will end.

The major sequence analyzed by INEL involved a 125 percent feedwater overspeed with the reactor initially at 68 percent power, this increasing to 90 percent due to reactivity changes (Bruske et al. 1985). This is assumed to be

a worst case analysis. The excess water input is thought to result in spillover into the steam lines in approximately 1 minute. At 100 percent power (1000 psig), such feedwater overspeeds would likely increase power and steam pressure to the high trip set point of 1055 psig. Only lower feedwater overspeeds would then be credible, thus giving more time available for operator action if the transient occurs at 100 percent power.

From PNL discussions with licensed operator examiners, a 50 percent probability of correct operator action in this sequence is felt to be a fair estimate. For the purposes here, this will be further quantified as to operator recognition of a problem, the correct interpretation, and the correct action. The following guidelines were used in calculating the values shown in Table 4.1.

TABLE 4.1. Assumed Operator Error Information

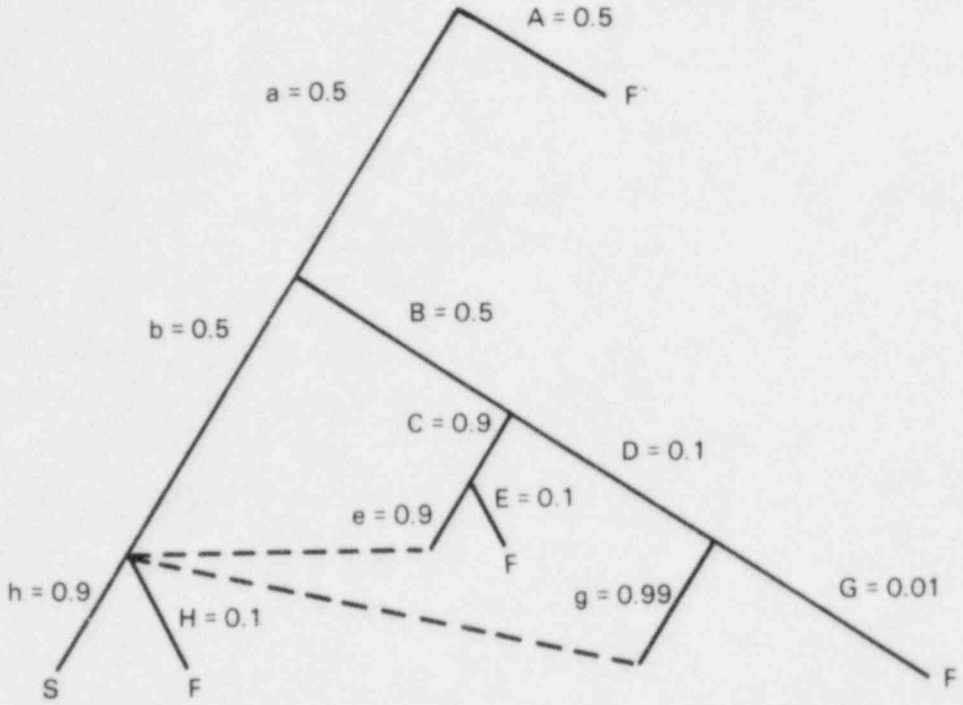
Requirement	Assumed Operator Error Probability
Failure to:	
Respond Correctly to 1 Alarm	0.1
Respond Correctly to More Than 1 Alarm	0.99
Respond Correctly to 1 Annunciator	0.5
Correctly Interpret given no Conflicting Indicators	0.1
Correctly Interpret given Preponderance of Accurate Indicators	0.5
Correctly Interpret given no Accurate Indicators	0.99

Note that the probability of operator failure to correctly respond to an alarm is assumed to be lower than for an annunciator. It was thought that with operator training, operators would be more likely to respond in a correct fashion to an alarm than a simple annunciator. The failure probability is then increased if conflicting signals are present. Note that error rates assumed in previous plant risk studies for operator action under high stress (i.e., an MSLB accident sequence) are typically on the order of 0.1 as opposed to the 0.99 assumed here. The numbers in Table 4.1 are thus conservative.

The resulting estimate for operator error is given in Figure 4.1 in a human reliability analysis (HRA) event tree. Totaling up the failure branches then gives an estimated failure probability of the operator of 0.571. This compares favorably to the previous qualitative estimate of 0.5 made by operator training personnel.

4.2 SIGNALS AVAILABLE TO THE OPERATOR FOR SEQUENCE 1, INITIATOR B

As in Sequence 1.A, an annunciator will light up, indicating level indicator failure for all of the failure combinations considered. In addition, a possible low level alarm will sound if LT(A) fails low.



A - Operator fails to notice annunciator for level failure

B - Operator sees annunciator, but incorrectly interpretes

C - No operator action, letting feedwater continue

D - Operator interpretes falling level indicators as LOCA, responds with HPCI

E - Operator fails to notice lack of response of vessel level to continued feedwater flow

F - Failure and vessel overfill

G - Operator fails to notice lack of response of vessel level to HPCI and feedwater flow

H - Operator fails to switch feedwater level control to level transmitter B

S - Success and vessel overfill prevented

Lower case letters indicate correct operator action in corresponding steps above.

FIGURE 4.1. Human Reliability Analysis Event Tree for Feedwater Overfill

4.3 OPERATOR RESPONSE TO SEQUENCE 1, INITIATOR B

For the purposes of this examination, the possible operator responses will be assumed to be the same as for Sequence 1.A, and depicted in Figure 4.1. The probability of the operator failing to halt the overfill is then 0.517.

For the remaining Sequences 1.C and 1.D, these were again considered relatively negligible.

5.0 SEQUENCE 1: ACCIDENT PROGRESSION TO MSLB

This accident scenario differs from a typical analysis of MSLBs in that the system initially suffers an overfill before the transition to an MSLB. The impact of the overfill on safety systems and their ability to respond later in the accident must then be examined before the Browns Ferry reliability values are used.

The first condition impacted by the overfill is degradation of steam quality. During the onset of the overfill accident, degrading steam quality will impact the performance of the turbine/generator set. There is no doubt that if the accident were to progress to spillover, the turbine would eventually suffer damage resulting in a turbine trip. However, the feedwater control logic is such that feedwater flow would still continue on the receipt of the low water level signal. Thus the turbine trip would not terminate the overfill scenario automatically.

The following observations concerning plant response can then be made:

1. Feedwater turbine damage and trip could occur due to moisture carryover before water begins falling into the steam lines, or shortly thereafter. This would effectively end feedwater flow for the failures outlined in INEL Sequence 1.

2. Main steam turbine damage could occur before water begins falling into the steam lines producing a turbine trip and RPS SCRAM. Feedwater flow, however, would continue.

3. If water begins flowing down the steam lines during operation, the main steam turbine will be damaged, causing a turbine trip and signal for closure of the stop valves. Feedwater flow would continue.

4. The potential exists for an MSLB due to water hammer occurring at the same time as the turbine trip, or shortly thereafter. The cooldown and collapse of steam is the major driving force for water slugs and hammer. An MSLB would generate an MSIV isolation signal on high temperature or pressure in the steam tunnel or drywell. This would generate another RPS SCRAM signal, if turbine trip has not already occurred.

5. It is thought that the potential for a water hammer-induced MSLB is lessened in the case where turbine trip occurs before spillover begins. The reduced steaming rates after shutdown could be assumed to reduce the severity of steam collapse and any water hammer when spillover occurs some time after shutdown.

6. If an MSLB did not occur relatively immediately on overfill as in Step 4, the overfill would then progress, assuming that the feedwater system is still operating. Static overfill of the steam lines could then cause a pipe break due to excessive load, generating an MSIV isolation signal with steam detected in the steam tunnel. However,

the steam collapse and cooldown experienced would likely first generate a low steam pressure signal in the steam lines (less than 825 psi). This is again an MSIV isolation signal, but only when the reactor is in the 'run' mode. This would still be the case even following a turbine trip. The MSIV isolation signal is thus thought likely to occur before a static load failure could occur, further reducing the water flow beyond the MSIVs and limiting the static load experienced by the downstream piping. In any case, pipe break or not, an MSIV isolation signal would be generated. Note, however, that this is ineffective for breaks above the MSIVs. This will be discussed further below under vessel isolation.

Feedwater Turbine

The feedwater turbine in the reference Browns Ferry BWR/4 is a Terry Wheel Turbine, a one piece wheel specifically designed to withstand water slugs that may occur during startup. However, operational experience indicates that the feedwater system is still among the most susceptible to damage (Bush et al. 1982).

Reviews of recent information published on water hammer applicable to the feedwater turbine are contained in NUREG/CR-2781 (NRC 1982b), NUREG-0993 (NRC 1983b), EPRI NP-2590-LD (EPRI 1982a), and NUREG/CR-0927 (NRC 1984). Indications are that PWRs have historically had more feedwater problems than BWRs, but the feedwater systems in both are susceptible. Most problems are caused by steam/water entrainment or steam bubble collapse.

It is uncertain if moisture carryover would be sufficient to cause feedwater turbine failure before water began spilling down the steam lines. At the point of spillover, damage would become more likely. Steam collapse and decreasing steam pressure would also impact feedwater turbine performance.

For the purposes of this analysis, it will be assumed that the probability of feedwater turbine damage before a MSLB occurs is on the order of 0.1. This then gives a 0.9 probability of the accident progressing. The upper bound is a 1.0 probability of the accident progressing; i.e., no feedwater turbine damage occurring before spillover.

Main Steam Turbine

The main steam turbine is more susceptible to damage than the simple feedwater steam turbine. The desire to protect the main turbine is well recognized in the plant design, and is one of the primary reasons for the high level feedwater trips. The turbine also has a protective trip for out-of-balance conditions that would indicate blade failures.

The potential for damage increases greatly under conditions of degrading steam quality. This is particularly true when the water level reaches the driers and moisture carryover becomes significant. The INEL analysis indicates that steam quality could drop to the 60 percent region for some scenarios before spillover actually occurs.

As a result, the potential for preliminary turbine blade damage before water spillover begins is considered to be fairly high. In addition, the potential for massive turbine damage and plant shutdown at the point of spillover is assumed to be essentially 1. This is because the turbine blades are thought to be highly susceptible to damage from steam bubble collapse and entrained water slugs. For the purpose of this examination, it will be assumed that there is a 0.1 probability that a turbine trip will occur before spillover occurs. This is again based on engineering judgment.

However, the feedwater system would continue to attempt feedwater flow as long as no feedwater turbine trip or damage occurred. If the feedwater pumps were not tripped, the degrading steam quality associated with the filling steam lines would significantly reduce the performance of the steam driven feedwater turbine. This would slow progression of the accident, but not halt it.

In addition to the potential for turbine damage and trip, other indications of changing plant conditions will be available to the operator during this period. Primarily, the automated load following controls for the turbine and reactor will respond to the changing conditions caused by the overfill. This includes reactor reactivity and power changes caused by a cooldown, and the turbine response to the degraded steam quality. For the purposes here, it will be assumed that no operator detection or response to these indicators occurs with the plant in automatic operation. Automatic operation is assumed to result in a more conservative estimate of the potential for operator intervention than manual control. Manual control is thought to ensure that the operator would at least be near appropriate panels, and would be more likely to see and correctly interpret the plant parameters displayed.

Main Steam Line Break

The next question is whether a steam line break will occur. The major damage mechanisms are again assumed to be associated with entrained water in the steam lines leading to possible water slugs and hammer, or the static loads possibly caused by water collecting in the steam lines.

Although several events have been suspected of causing overfill at power, there is no real experience for damage under these assumed full power conditions. However, several steam line water hammer incidents have occurred during startup (Bush et al. 1982). In these cases the MSIVs were opened before proper warmup or draining of steam lines, resulting in condensation and liquid flow in the lines. In these cases the entrained water is thought to have impacted the turbine stop valve, resulting in water hammer. Any water slugs forming would then likely be expected to generate impacts at pipe elbows and restrictions, but the end of the run is likely to receive the brunt of the energy. This would again be the main steam turbine that would certainly suffer damage and again cause a reactor trip.

For this particular scenario, the problem will be aggravated at the onset of overfill by water being entrained in the steam flow, and collapsing steam shocks. The question is whether the pipes would suffer damage from water hammer as the steam collapsed and the lines began to fill. A review of past experience

in BWRs (Bush et al. 1982) indicates that pipe leaks have been primarily restricted to those less than 12 inches in diameter. However, cracks have been detected in larger pipes, likely due to inter-granular stress corrosion cracking (IGSCC), which introduces a possible flaw subject to water hammer damage.

A consideration of the static loads was made for PWRs concerning the potential for steam line rupture on overfill following a steam tube rupture.(a) The conclusion was that for the plants examined, the static loads presented by steam lines full of water would not result in any failures. The stress levels would remain within the limits allowed by the ASME code. As a result, the conclusion was that the probability of failure of the main steam line due to overfilling and deadweight loading was not increased. In the absence of a more precise estimate, the probability of failure due to this scenario was valued at 1E-03/overfill event.

Once spillover occurs, damage to the turbine is very likely. The probability of pipe damage during steam collapse is not known. If the accident progresses through this stage to one of simple overfill, the probability of pipe damage can be assumed to go down to 1E-03/event; this is the failure probability due to static load.

Estimate of MSLB Initiation

Two cases are then considered to be important in the progression of the accident: 1) main steam turbine trip before spillover of water occurs, and 2) no initial trip followed by spillover, turbine failure, and trip. The logic to be used is depicted in Figure 5.1. The initiating event frequency is shown, along with the assumed probability of operator error. The probability of feedwater turbine failure ending the sequence is then given, followed by the branch for main turbine trip.

For the first case in which main turbine trip causes SCRAM some time before spillover occurs, it will be assumed that the conditions driving water hammer are reduced. For this assumed less severe case in which early shutdown occurs, the probability of a hammer-induced MSLB will be 0.5. The probability of a static load failure due to continued feedwater flow is then put at 1E-03, for a total MSLB probability of 0.501. Given the assumption of a 0.1 probability of an early turbine trip before spillover results in an effective MSLB probability for this case of 0.05.

For the second case, it will be assumed that the conditions driving steam collapse and water hammer will be more severe if spillover occurs while the plant is operating at full power. The probability of a hammer-induced MSLB will then be assumed to be 1.0. This conservative assumption can be updated as more information becomes available. The contribution from static load induced failure is then ignored. When coupled with the assumption of a 0.9 probability that the turbine would not trip until spillover occurred gives an effective MSLB probability of 0.9.

(a) A-47 Review, ENCLOSURE 2, Responses to Additional Questions from the ACRS Regarding SG Overfill, Draft, July 27, 1984.

The net MSLB probability for the two cases is then 0.95. The assumed initiating frequency of MSLB is then 2.87E-03/py as shown in Figure 5.1. These estimates can be updated as more information becomes available on the response of plant systems to highly degraded steam quality and the potential for water hammer-induced MSLBs.

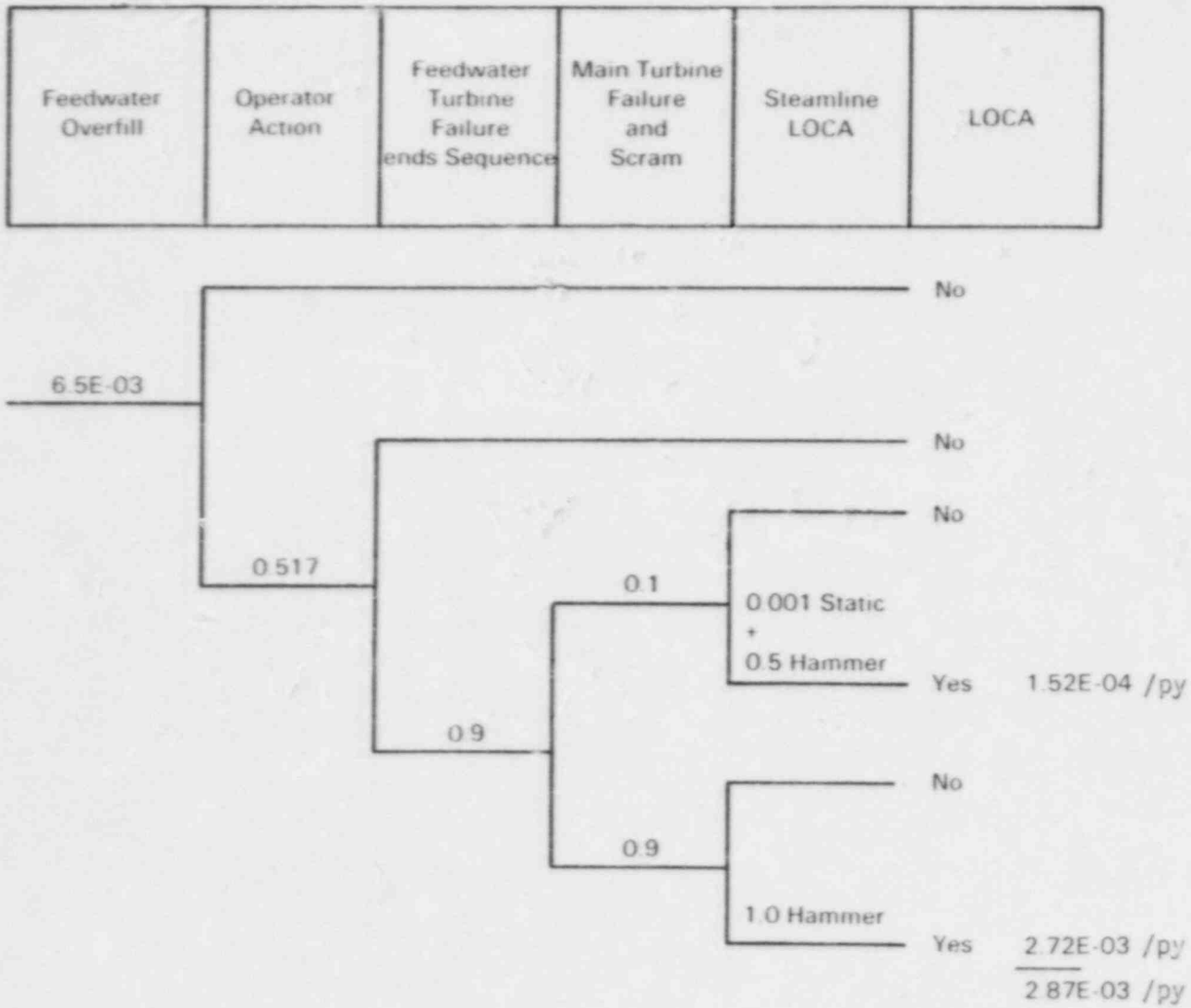


FIGURE 5.1. Sequence 1: Overfill-Induced LOCA Frequency

6.0 SEQUENCE 2: CONDENSATE BOOSTER PUMP FAILURE

The second reactor vessel overfill sequence identified by INEL dealt with failures of the condensate booster pumps. Note that this sequence involves vessel overcool as well.

The three condensate booster pumps in the Browns Ferry reference design suction off the filter/demineralizer outlet of the condensate system and discharge to the low pressure feedwater heaters. Failures involving the pumps and discharge valves could cause the system to deliver water to the reactor vessel. The motor-driven, horizontal, centrifugal pumps have a capacity of 10,830 gpm each, a discharge pressure of 300 psig, and a shutoff head of approximately 350 psig.

The sequence initiators identified by INEL as the cause of booster pump failure to maximum flow include the following:

Initiator A: Any one of three motor-operated feedwater pump discharge valves fails open, allowing an increased flowrate to the reactor vessel.

Initiator B: The air-operated startup feedwater bypass valve used to regulate flow fails open, causing an increased flowrate to the reactor vessel.

Initiator C: The condenser bypass air-operated valve used to recirculate the excess condensate flow back to the condenser fails closed, causing an increased flow rate to the reactor vessel.

The INEL analysis of initial plant response to these initiators assumed that the plant was in a startup mode, with the reactor power at 1 percent, reactor vessel pressure at approximately 270 psia, and the MSIVs closed. This was done primarily due to computer modeling limitations. With the MSIVs closed, mass flow in the system is severely restricted and the potential for water hammer and pipe breaks is thus highly unlikely. Breaks due to overcooling at such reduced temperatures and pressures are also unlikely.

For the purposes of this analysis, it will be assumed that the reactor power has increased to the point of opening the MSIVs, thus introducing a real potential for piping damage if overfill occurs. The sequence of events for reactor vessel overfill as postulated by the INEL is given in Table 6.1.

TABLE 6.1. Sequence of Events for Overfill Sequence

Time, sec	Event Description
0.0	Startup operations. Reactor power is 1 percent, reactor vessel pressure is approximately 270 psia, and the MSIVs are closed. One condensate booster pump fails to maximum flow.
250.0	Steamlines begin to fill.
350.0	Steamlines are liquid full. Cooldown rate has exceeded 100°F/hr (cooldown limit).

Effects of Excessive Cooldown and Thermal Shock

It should be noted that the failure of interest identified by INEL is not the actual steam line break, but that the cooldown rate of the primary system exceeds the technical specification limits. The question is then whether this cooldown presents a significant potential for inducing vessel damage or rupture via thermal shock.

The INEL computer simulations of this cooldown scenario produced a cooldown rate on the order of 0.36°F per second or 1296°F/hr, well in excess of the 100°F/hr allowed by the Technical Specifications. The INEL model was run with the MSIVs closed due to model limitations, with the implication that cooldown rates may actually be higher with the MSIVs open as would be the case during startup. However, the model also assumed constant reactor power where in fact the reactor would respond to the cold water injection with a power increase. Because of the conflicting effects on the cooldown, the INEL results will be assumed to be bounding until further information becomes available.

To model the potential for thermal shock-induced failure of the vessel, a simulation code, VISA-A (NRC 1983c), was run with the INEL cooldown parameters. This code was developed for PWRs, but conceptually can be applied to any pressure vessel. To run the code, a vessel beltline weld with 0.35% Cu and 0.65% Ni was assumed as representative, with a MeV neutron fluence of 2.0E+18 neutrons per square centimeter. The code also contains assumptions of existing vessel flaws which may propagate during the scenario.

When run with the parameters of this failure scenario, the code predicts a zero vessel failure probability. Although the cooldown rates exceed Technical Specifications, the pressures involved are significantly below the design limits so this answer is not unexpected. The real concern in thermal shock is the potential for overcooling while the vessel remains near its design limit (1250 psig operational, 1536 psig hydrostatic test limit for Browns Ferry). In PWRs, this potential exists because the primary system can be solid with water. However, in a BWR, the system operates with a large steam void in the upper regions of the vessel. Excessive cooldown rates, even while at higher power levels than the 1 percent used by INEL, are also accompanied by steam

condensation and rapid pressure drop. The two conditions necessary for thermal shock failure of the vessel, high pressure and rapid cooldown, are thus not present at the same time and the scenario is not of great concern in BWRs.

For this reason, the potential for generating a core-melt path directly as a result of vessel failure given the excessive cooldown must be set to zero at this time. However, a failure probability on the order of 1E-04 could still be significant. Given the low initiating frequency predicted by INEL, the resulting core-melt frequency may be low compared to an overall core-melt frequency for Browns Ferry of approximately 1E-04/py, but could be comparable to the resulting core-melt frequency from Sequence 1 examined in the previous chapter.

The potential for inducing a steam line break given the overfill scenario will be considered below.

6.1 SEQUENCE 2: INITIATING FREQUENCY

The initiating frequencies of this sequence and its subsequent progression to an MSLB are expected to be lower than those for Sequence 1. As a result, it is felt that a less detailed examination of the initiating frequency of this sequence is justified. For the purpose of this analysis, the original frequencies calculated by INEL will be used as a starting point. If the resulting core-melt frequencies are high enough, a more detailed examination of failure mechanisms can then be made.

The initiating frequency of the overall sequence was valued at 8.2E-05/py, with an upper bound of 5.6E-03/py. This was not broken down by the three initiators above in the INEL report. It is assumed, however, that this value is based primarily on the accepted rate for failure-to-open-given-closed, or failure-to-close-given-open of 3E-07/hr. This applies to air- and motor-operated valves. When the 192 hr/yr window for startup and shutdown is considered, the predicted failure rate becomes (3E-07/hr)(192 hr/yr) = 5.76E-05/yr.

However, for Initiator A, the feedwater discharge valves are normally closed during startup, with flow provided by the bypass valve. The proposed failure then requires a normally closed valve to fail open. This failure frequency is lower than that assumed above, implying as it does an inadvertent control signal to open, or an internal rupture of the valve.

For Initiator B, the feedwater regulating bypass valve for the BWR/4 is an air-operated valve with an air-to-close/spring-to-open feature. Loss of air pressure could be assumed to cause the valve to open. However, the air supply incorporates a lock-up feature in case of loss of signal to the voltage/pneumatic converter (less than 1 ma), or loss of air supply (less than 75 psig). Either case will deenergize a solenoid valve which vents the air header of the valve positioner. Air lock valves in each line to the valve operator sense the loss of pressure and lock the air in the operator to prevent valve movement. Loss of air pressure then locks the valve as is. The operator must reset the system after restoring the proper conditions for operation. The frequency of Initiator B is thus also significantly below that of a simple valve failure.

For Initiator C, a condenser bypass valve failure may initially increase the effective pressure from the booster pumps and through the front-end heater trains to the bypass control valve. However, all flow to the vessel is still through the bypass control valve. If the pressure increase is initially reflected as an increase in flow, the control circuit to the positioner for the bypass valve will call for decreased flow. As a result, additional failures would be required in the control circuit to cause an overfill, and the frequency of this sequence is also thought to be lower than a simple valve failure.

However, this frequency includes an estimate of the time per year that the reactor is at or under the output pressure of the condensate booster pumps. This occurs for only a relatively short period of time during startup. Once vessel pressure exceeds 350 psig, the booster pumps do not have sufficient pressure to put water into the vessel, and the accident is no longer credible.

6.2 SEQUENCE 2: ACCIDENT PROGRESSION TO MSLB

The event tree used in modeling this scenario and the plant response to the overfill is given in Figure 6.1 As with Sequence 1, it is assumed that this accident must make a transition to an MSLB to be of safety concern. An overcool in itself is a serious accident requiring a pipe break, valve lift, or challenge of some safety system to represent an accident initiating event. Considering this as a transient initiator, no damage or impairment of RSS or ECCS systems is seen. The specific steps in the event tree and the assumed failure probabilities are discussed further below.

Operator Action

This scenario is postulated to take place during normal startup, at a time when vessel pressure is still low enough to allow input from the condensate booster pumps. The failure is then assumed to occur when flow is from the condensate booster pumps via the startup bypass valve. This mode continues until system pressure reaches 350 psig, with a transition to the main feedwater system. Level control with flow via the bypass valve uses 1 element control only (i.e., level indicators only with no steam or water flow correction), and can be in automatic or manual operation.

During ascent to power, operator attention will typically be focused on vessel water level and feedwater performance. The operator would be able to recognize an overfill condition by the reactor vessel high water level alarm, reactor vessel level indication (strip charts and meters) and increased reactor feedwater flow. All level indicators would also be in agreement, which was not the case in Sequence 1 where level failures had occurred.

The time available to the operator for diagnosis and action estimated by INEL is about 5 minutes before spillover could occur. This is a minimum estimate, with time available for operator action increasing as vessel pressure approaches 350 psig and the pump output goes to zero.

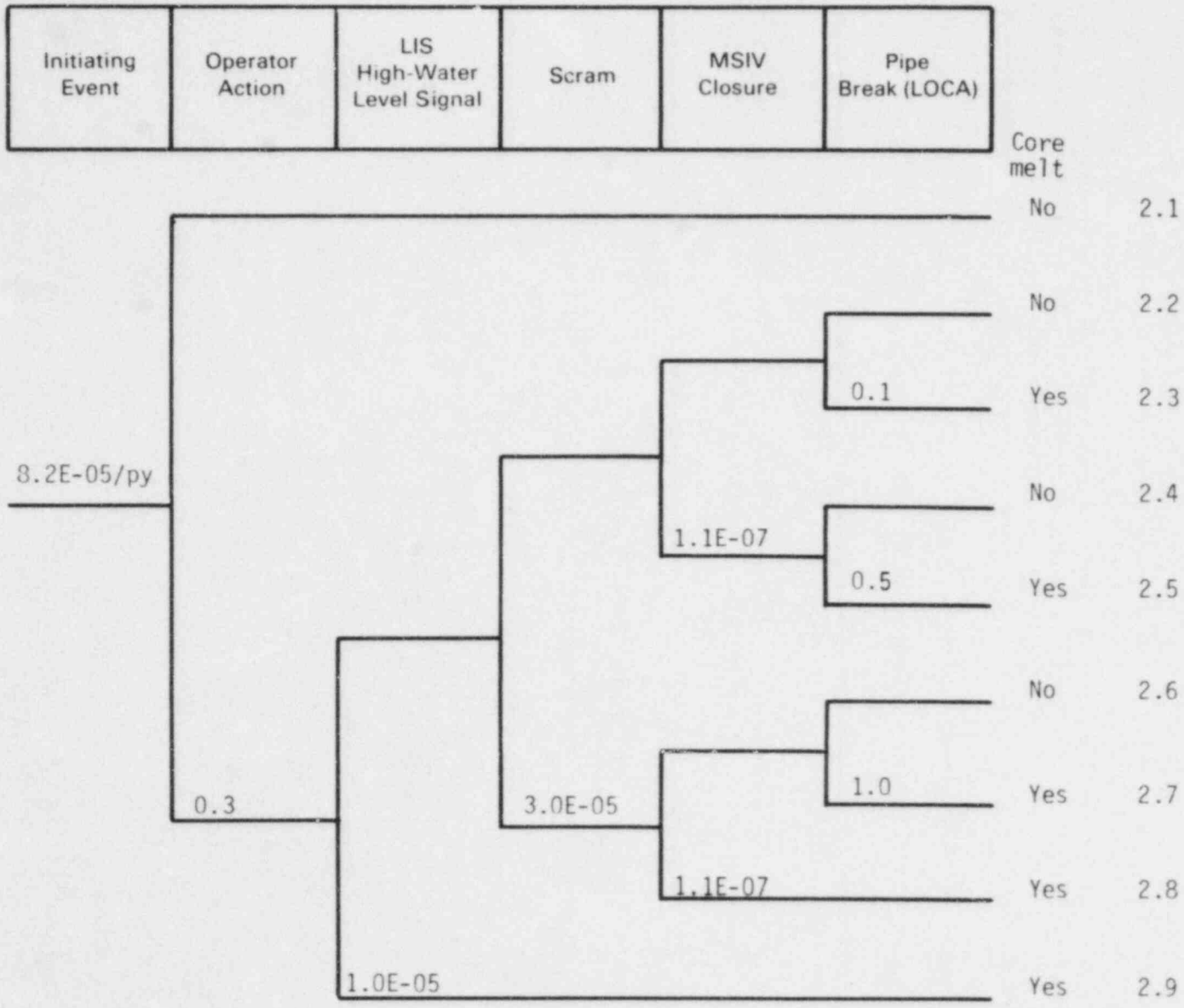


FIGURE 6.1. Sequence 2: LOCA Event Tree

The operator can terminate this transient by either tripping the condensate booster pump or shutting any of a number of isolation valves between the reactor and the reactor booster pump discharge depending on the lineup at the time. It is thus thought that the operator has a real potential for recognizing and terminating the overfill scenario before spillover occurs.

In Sequence 1, a 50 percent probability of operator failure to identify a feedwater level failure at 100 percent power was used. The error rate here is thought to be much less due to the lack of conflicting signals and duties of the operator at ascent to power. A probability of 30 percent that the operator will not be able to identify the real problem in time to end the transient will be used here. This is considered highly conservative, with values on the order of 1E-03 being more likely.

LIS High Water Level Signal

The reactor vessel level instrumentation was shown in Figure 3.1. Referring back to that figure, the LIS 3-203 A through D switches will generate a 1-out-of-2 twice signal on high water level for reactor SCRAM, HPCI, turbine trip, and MSIV closure.

Sequence 1 assumed that failures had occurred in the reactor water level indicating switches (LIS). The probability of LIS failure during an eight hour window between shifts would be on the order of 1E-05 (8 hours x 1.2E-06/hr).

It must, therefore, be assumed in this sequence that the high level LIS trip signals will be generated in this case as the vessel fills. The MSIVs will therefore be demanded, which at low power would be likely to end the sequence. In this case, however, the potential for a MSLB will still be assumed.

Reactor SCRAM

The Browns Ferry PRA estimates the SCRAM failure to be 3.0E-05. It is thought that this scenario would not affect the reactor SCRAM function.

MSIV Closure

The Browns Ferry PRA puts the probability of MSIV failure at close to 1.1E-07. This sequence should not change the valve performance, as the isolation signal occurs well before overfill occurs. This is in contrast to Sequence 1, in which spillover and subsequent MSLB were necessary to generate the isolation signal. Closure of the valves is again thought to significantly reduce mass flow in the system and thus reduce the probability for inducing pipe breaks.

MSLB-Pipe Break

The probability of inducing a pipe break is then assumed to be a function of the mass flow in the system at the time of overfill. If SCRAM fails, the probability is assumed to be 1.0. If SCRAM occurs but MSIV isolation fails, the probability is assumed to be 0.5 as with Sequence 1. If SCRAM and MSIV isolation occur, the probability of MSLB is assumed to be 0.1. This is considered conservative given the low system pressures at the time of overfill.

Resulting MSLB Sequence Frequencies

Referring back to Figure 6.1, the sequences that result in MSLB are summarized below. The MSLB sequences are identified to be Sequences 2.3, 2.5, 2.7, 2.8 and 2.9

Application of the assumed failure probabilities in the model event tree gives the probabilities shown in Table 6.2 for a MSLB with an initiation frequency of 8.2E-05/yr. This estimate is approximately 2 orders of magnitude smaller than the MSLB frequency estimate obtained in the previous analysis of Sequence 1 with feedwater overfill. The impact on core-melt and public risk is also considered to be 2 orders of magnitude smaller, making the contribution from this sequence insignificant to the overall contribution to plant core-melt and risk from transient overfill.

TABLE 6.2. Sequence 2 MSLB Frequencies

MSLB Sequence	Frequency, 1/py
	Best Estimate
Sequence 2.3	2.46E-06
Sequence 2.5	1.35E-12
Sequence 2.7	7.38E-10
Sequence 2.8	8.12E-17
Sequence 2.9	2.46E-10
Total MSLB Frequency	2.46E-06

7.0 SEQUENCE 3: LPCI FAILURE

The third reactor vessel overfill sequence identified by INEL dealt with false starts of the low pressure cooling injection (LPCI) system while at low reactor vessel pressure. This sequence also involves vessel overcool.

The LPCI system in Browns Ferry is a mode of operation of the Residual Heat Removal System pumps that floods water into the core. The core spray system starts from the same signal of low water level in the reactor or high pressure in the containment drywell and operates independently to achieve the same objective. The isolation valves for these two systems are opened when reactor pressure is less than 500 psig, but injection flow does not occur until the differential pressure across the check valves permits. This occurs when the RPV pressure is less than 300 psig.

The sequence initiators identified by INEL as the cause of false LPCI injection include the following:

Initiator A: Local LPCI pump switch shorts to power causing the pumps to start.

Initiator B: Remote LPCI pump switch shorts to power causing the pumps to start.

Initiator C: Shorts in pump control circuits (four pump control circuits) causing the LPCI pumps to start.

Initiator D: Short in 1 out of 2 taken twice logic circuit for reactor level occurs, resulting in LPCI initiation due to a false low-low level signals.

Initiator E: Short in 1 out of 2 taken twice logic circuit indicating a false high drywell pressure occurs, resulting in LPCI initiation.

Initiator F: Two drywell pressure switches fail closed due to common cause and initiate LPCI pump start.

Initiator G: Two reactor vessel low water vessel switches fail closed due to common cause and result in LPCI pump start.

Initiator H: Two independent (fail closed) failures of drywell pressure or reactor vessel water level sensors occur, causing LPCI initiation.

As with Sequence 2, the INEL analysis of initial plant response to these initiators assumed that the plant was in a startup mode, with the reactor power at 1 percent, reactor vessel pressure at approximately 270 psia, and the MSIVs

closed. These assumptions were made primarily due to computer modeling limitations. With the MSIVs closed, mass flow in the system is severely restricted and the potential for water hammer and pipe breaks is thus highly unlikely. Breaks due to overcooling at such reduced temperatures and pressures are also unlikely.

For the purposes of this analysis, it will again be assumed that the reactor power has increased to the point of opening the MSIVs, thus introducing a real potential for piping damage if overfill occurs. The sequence of events for reactor vessel overfill as postulated by the INEL is given below in Table 7.1.

TABLE 7.1. Sequence of Events for Reactor Vessel Overfill Sequence 3

Time, sec	Event Description
0.0	Startup operations. Reactor power is 1 percent, reactor vessel pressure is approximately 270 psia, and the main steam isolation valves (MSIVs) are closed.
0.05	Loss of condensate booster pumps occurs.
125.0	Steamlines begin to fill.
175.0	Steamlines are liquid full. Cooldown rate has exceeded 100°F/hr (cooldown limits).

Effects of Excessive Cooldown and Thermal Shock

As in the previous sequence, the failure of interest identified by INEL is not a steam line break, but that the cooldown rate of the primary system exceeds the technical specification limits.

It is again the current position of PNL that the potential for vessel damage and loss of coolant is negligible at the pressures, initial temperatures, and cooldown rates given. Probability of pressure vessel rupture is thus valued at zero. If more information were to become available, this conclusion could be updated. In any event, to be conservative the potential for inducing a steam line break given the overfill scenario will be considered below.

7.1 SEQUENCE 3: OVERFILL INITIATING FREQUENCY

As with Sequence 2 just examined, the initiating frequencies of this sequence and its subsequent progression to an MSLB are expected to be lower than those found for Sequence 1. As a result, it is felt that a less detailed

examination of the initiating frequency of this sequence is justified. For the purpose of this analysis, the original frequencies calculated by INEL will be used as a starting point. If the resulting core-melt frequencies are high enough, a more detailed examination of failure mechanisms can then be made.

The INEL estimate of initiation frequency for false start of the LPCI is put at 3.6E-03/py, with the upper bound of 7.7E-03/py. For this analysis, the best estimate value of 3.6E-03/py will be carried through to MSLB.

Note that as with the booster pump failure in Sequence 2, this frequency includes an estimate of the time per year that the reactor is at or under the output pressure of the residual heat removal (RHR) pumps used for LPCI. This occurs for only a relatively short period of time during startup. Once vessel pressure exceeds 350 psig, the pumps do not have sufficient pressure output to put water into the vessel, and the accident is no longer credible.

7.2 SEQUENCE 3: ACCIDENT PROGRESSION TO MSLB

The event tree used in modeling this scenario and the plant response to the overfill is given in Figure 6.1. It is again assumed that this accident must make a transition to a MSLB to be of safety concern. An overcool in itself is not a serious accident, requiring a pipe break, valve lift, or challenge of some safety system to represent an accident initiating event. Considering this as a transient initiator, no damage or impairment of RSS or ECCS systems is predicted. The potential for core damage would be very small given the transient initiating frequency of 3.6E-03/py. It is thus thought that the consideration of a MSLB as indicated in Figure 6.1 will bound the estimate of core damage from this sequence.

The specific steps in the event tree and the assumed failure probabilities are discussed further below.

Operator Action

This scenario is postulated to take place during a normal startup, at a time when vessel pressure is still low enough to allow input from the RHR pumps in LPCI mode.

The operator would be able to recognize this abnormal occurrence by indications that the RHR system has started in the LPCI mode. This includes valves repositioning, pump run indication, and pump discharge pressure and flow increasing.

During ascent to power, the operator attention will typically be focused on vessel water level and feedwater performance. The operator would be able to recognize an overfill condition by the reactor vessel high water level alarm, reactor vessel level indication (strip charts and meters) and increased reactor feedwater flow. All level indicators would also be in agreement on the overfill, as in Sequence 2.

INEL estimated the time available to the operator for diagnosis and action to be 2 minutes before spillover could occur. This is a minimum estimate, with time available for operator action increasing as vessel pressure approaches 350 psig and the pump output goes to zero.

The operator can terminate this transient by simply tripping the RHR pumps. It is thus thought that the operator has a real potential for recognizing and terminating the overfill scenario before spillover occurs.

In Sequence 1, a 50 percent probability of operator failure to identify a feedwater level failure at 100 percent power was used due to conflicting signals. For Sequence 2, this was reduced to a 30 percent failure rate due to likely operator awareness of vessel level during startup, and the time available to correct the problem. In this sequence the operator is still likely to be closely monitoring vessel water level during startup, but slightly less time is available. Operator termination is again thought to be very likely, but a highly conservative failure probability of 40 percent will be assumed here.

Initial System Response to Overfill

The initial response of the reactor systems to the overfill scenario are expected to be the same as developed previously for Sequence 2. This includes the LIS High Water Level Signal, the Reactor SCRAM, and the MSIV Closure functions. The progression of the accident is again not thought to impact the performance of these systems.

Main Steam Line Break (MSLB)

As in Sequence 2, the probability of inducing a pipe break is then assumed to be a function of the mass flow in the system at the time of overfill. If SCRAM fails, the probability is put at 1.0. If SCRAM occurs but MSIV isolation fails, the probability is put at 0.5 as in Sequence 1. If SCRAM and MSIV isolation occur, the probability of MSLB is put at 0.1. This is considered conservative given the low system pressures at the time of overfill.

Resulting MSLB Sequence Frequencies

Referring back to Figure 6.1 with the operator action probability at 0.4 instead of 0.3, the sequences that result in MSLB are summarized below.

The MSLB sequences are identified to be sequences 2.3, 2.5, 2.7, 2.8 and 2.9.

Application of the assumed failure probabilities in the model event tree gives the probabilities for an MSLB initiation shown in Table 7.2.

TABLE 7.2. Sequence 3 MSLB Frequencies

MSLB Sequence	Frequency
Sequence 2.3	1.44E-04
Sequence 2.5	7.92E-11
Sequence 2.7	4.32E-08
Sequence 2.8	4.75E-15
Sequence 2.9	1.44E-08 (less than)
Total MSLB Frequency	1.44E-04

This MSLB frequency estimate is thus approximately 10 times smaller than that estimated for Sequence 1 with feedwater overfill. As a result, the impact on core-melt and public risk is also considered to be 10 times smaller.

8.0 BROWNS FERRY MSLB EVENT TREES TO CORE-MELT

As discussed previously, the accident progression will generate an MSIV isolation signal (given an MSLB) from sensors in the main steam tunnel or dry well. In addition, sufficient condensation of steam in the main steam lines to below 825 psi will also produce an isolation signal. It is thus thought that the probability of an isolation signal is 1.0.

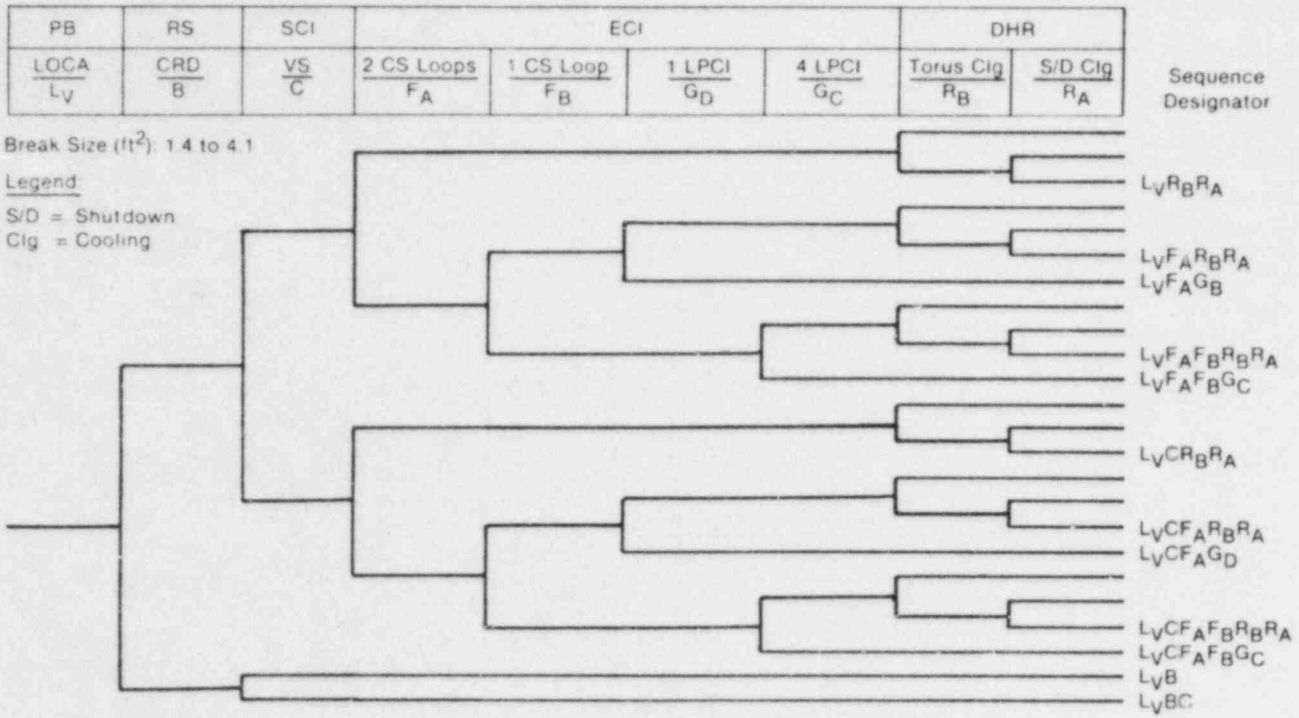
Pipe breaks downstream of the MSIVs would then require the MSIVs to close to successfully isolate the vessel. The Browns Ferry PRA considered the probability of failure of the two MSIVs to be 1.1E-07 (NRC 1982a), which would put the failure to isolate several orders of magnitude less than that for ruptures inside containment. A more conservative valve failure probability of 3.2E-03/demand or 1E-05/pair would still give a similar conclusion. The question remains, however, whether the performance of the MSIVs is affected in some fashion by the overfill transient.

The four main 26-in. pipe runs exit the vessel and drop down to a level where they exit the drywell. The MSIVs are then located on either side of the drywell penetration. Upstream of these are the safety relief valves, and the steam flow restrictors. This portion of the steam line then presents two 90 degree bends, but is otherwise relatively unrestricted. In the case of overfill, water hammer and vibrations of two phase flow could interfere with valve operation or cause outright damage[(a)]. The overall impression is that some chattering may occur during closing, but that the hydraulic forces would actually tend to force closure and seating of the valve. Increasing this failure probability is thus not thought to be justified at this time.

The event trees used in modeling the plant response to the overfill as developed in the Browns Ferry PRA are shown in Figures 8.1, 8.2 and 8.3. These represent large, medium, and small steam line breaks respectively above the MSIVs. Pipe breaks downstream of the MSIVs are possible: however, two MSIVs must fail to close in addition to the pipe break to be of concern. This is assumed to reduce the safety significance of such breaks to well below that of breaks upstream of the MSIVs, given their apparent ability to perform with water in the steam lines. As in the Browns Ferry analysis, it will therefore be assumed that the breaks occur upstream of the MSIVs. The appropriate system response for such breaks is shown in Figures 8.1 through 8.3.

The approach used by Browns Ferry to model pipe breaks above the MSIVs is therefore also thought to be the most conservative approach for the overfill analysis, and will be used here. However, the other systems on the event trees must also be examined to see if the overfill scenario impacts the associated failure probabilities.

(a) Personal communication with Elvis Hollins, Chairman, MSIV Task Force, Tennessee Valley Authority (TVA), June 19, 1984.

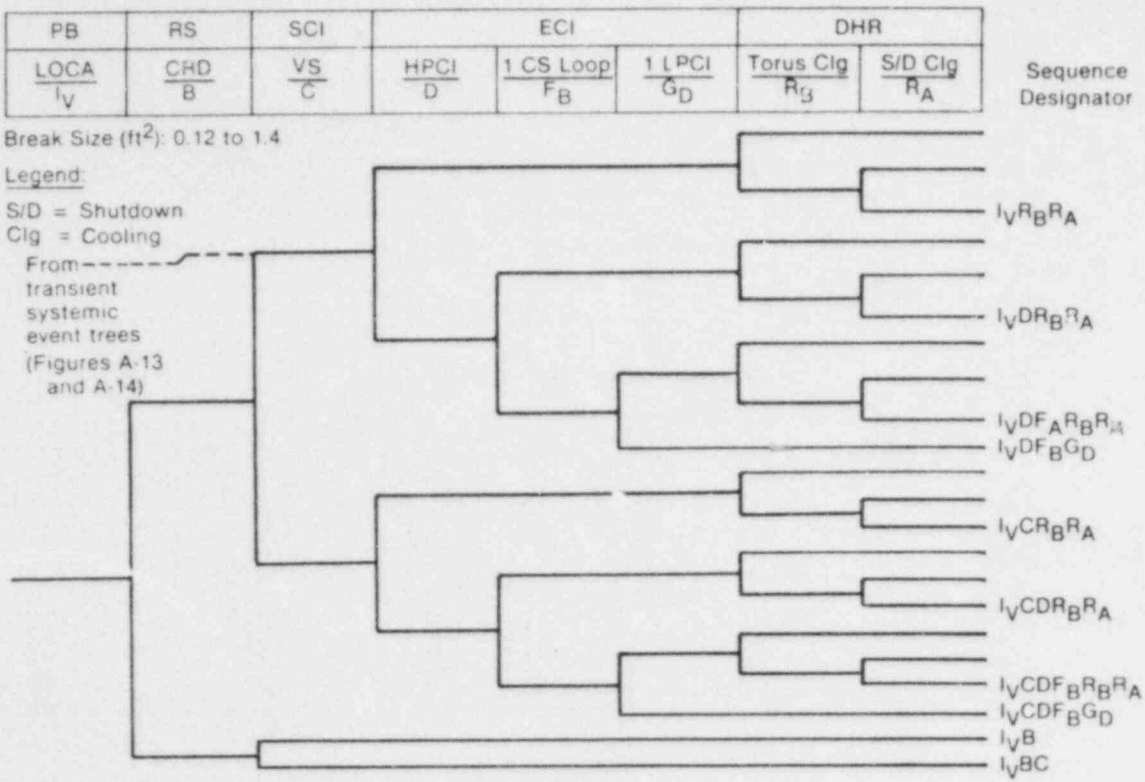


X = Function failure

RS	SCI	ECI	DHR	Remarks
				Core cooled
				Core cooled
			X	Slow melt
				Core cooled
				Core cooled
			X	Slow melt
		X	N/A	Melt
				Core cooled
				Core cooled
			X	Slow melt
		X	N/A	Melt
	X			Core cooled
	X			Core cooled
	X		X	Slow melt
	X			Core cooled
	X			Core cooled
	X		X	Slow melt
	X	X	N/A	Melt
	X			Core cooled
	X			Core cooled
	X		X	Slow melt
	X	X	N/A	Melt
X		N/A	N/A	Melt
X	X	N/A	N/A	Melt

INEL 2 1633

FIGURE 8.1. LOCA Systemic Event Tree for Large Steam Line Break (L_V).

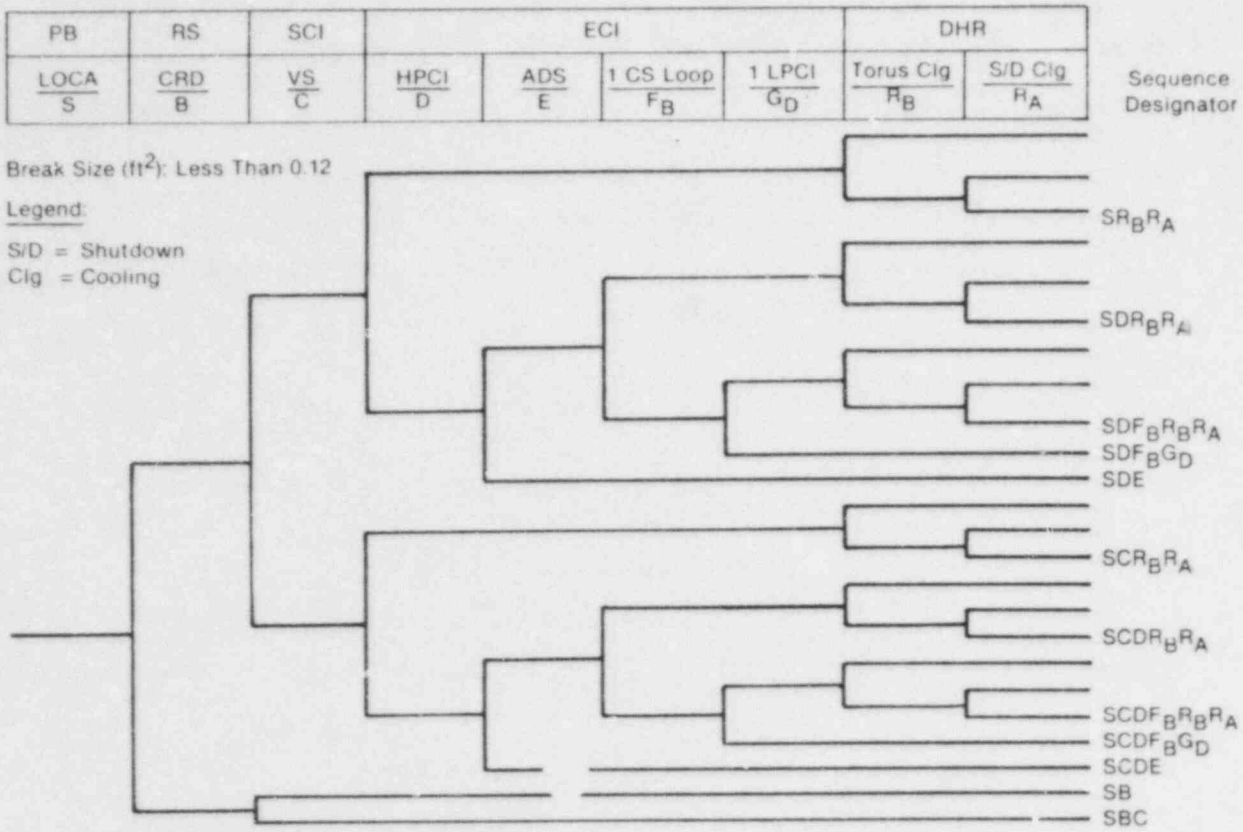


X = Function failure

RS	SCI	ECI	DHR	Remarks
				Core cooled
				Core cooled
			X	Slow melt
				Core cooled
				Core cooled
			X	Slow melt
				Core cooled
				Core cooled
			X	Slow melt
		X	N/A	Melt
	X			Core cooled
	X			Core cooled
	X		X	Slow melt
	X			Core cooled
	X			Core cooled
	X		X	Slow melt
	X			Core cooled
	X			Core cooled
	X		X	Slow melt
	X	X	N/A	Melt
X		N/A	N/A	Melt
X	X	N/A	N/A	Melt

INEL 2 1635

FIGURE 8.2. LOCA Systemic Event Tree for Intermediate Steam Line Break (I_V).



X = Function failure

RS	SCI	ECI	DHR	Remarks
				Core cooled
				Core cooled
			X	Slow melt
				Core cooled
				Core cooled
			X	Slow melt
				Core cooled
				Core cooled
			X	Slow melt
		X	N/A	Melt
		X	N/A	Melt
	X			Core cooled
	X			Core cooled
	X		X	Slow melt
	X			Core cooled
	X			Core cooled
	X		X	Slow melt
	X			Core cooled
	X			Core cooled
	X		X	Slow melt
	X	X	N/A	Melt
	X	X	N/A	Melt
X		N/A	N/A	Melt
X	X	N/A	N/A	Melt

INEL 2 1636

FIGURE 8.3. LOCA Systemic Event Tree for Small Liquid-Line or Steam-Line Break (S)

Reactor SCRAM

The feedwater overfill is not thought to impact the reactor SCRAM function in any fashion. The probability of SCRAM failure is 3E-05/demand.

Short-Term Containment Integrity (Vapor Suppression)

Performance of the vapor suppression function in the drywell and torus is not thought to be affected by the overfill scenario. The Browns Ferry failure probabilities are thus thought to be appropriate.

RCIC/HPCI Response

The HPCI system in Browns Ferry is a steam driven system, with the steam tap inboard of the MSIVs. The approach used here will model small, medium, and large breaks, so the possible scenarios and required response are covered.

However, the impact of the overfill on the HPCI system must also be considered. In this accident scenario the reactor vessel could blow down after MSLB, or isolate and remain relatively full. This is again highly unlikely given the loss of feedwater with MSIV closure, but will be considered here. If the vessel is still full, the steam delivery lines to the RCIC and HPCI may be solid with water or subject to steam collapse and water hammer. However, there would then be no initiation signal or flow in these lines while the vessel water level was still high. The four LISs used for safety actuation are not only distinct from those discussed earlier for feedwater failure, but they are also on a separate 2-in. instrument line. These again use a 1-out-of-2-twice signal logic for initiation. The vessel level must then actually drop to the low-low trip point as indicated by the independent set of the LISs. This can only occur through a period of system boil-off and lifting of the relief valves, starting from an extreme vessel overfill. The main steam line and RCIC turbine supply line would then continue to drain and boil off as the water level in the vessel dropped with actuation of the SRVs. If the vessel blew down before isolation, these lines would again be expected to drain accordingly.

The RCIC/HPCI steam driven turbines would thus still be isolated awaiting an initiation signal from the vessel water level indicating switches. As a result, the failures discussed earlier for the feedwater function have in no way impacted the performance of this function.

The other possibility is that the pipe break assumed actually occurs along the piping serving the HPCI system. This possibility has been considered in the Browns Ferry PRA, with the assumption that 23.2 percent of the piping susceptible to intermediate steam line breaks is HPCI piping. This assumption is also used here. The overall impact on assumed pipe break frequencies will be discussed further below.

As a result it is thought that at the point of RCIC/HPCI initiation, the steaming conditions in the vessel and supply line to the turbines will be as expected for their operation. The failure probabilities for this function as developed in the Browns Ferry PRA are thus thought to be appropriate.

ADS/LPCI CS Response

The ADS/LPCI is typically considered a backup to the high pressure systems. If the vessel remains pressurized but the HPCI fails, the ADS must depressurize the vessel before low pressure systems can be used. In this case, the dominant failure mechanism is the ADS function, where the valves fail to lift properly. However, if the system is already blown down as is the case with isolation failure, or breaks within containment, only the electrically driven LPCI must function.

The LPCI is thus not thought to be affected by the overfill transient. Water sources for this system are aligned initially with the condensate storage tank, then the suppression pool. Both are not thought to be affected. Thus, the Browns Ferry failure probabilities are again thought to apply here.

Long-Term Core Cooling

The long-term core cooling function is not thought to be impacted by the accident sequence in any fashion. Power and water supplies for residual heat removal are not associated with the systems that could be possibly subjected to water hammer damage during the course of the accident.

The net result of this consideration is that the Browns Ferry PRA approach is thought to be directly applicable here, with the only difference being the initiating frequency of the MSLBs assumed.

MSLB Frequencies Adjusted by Break Size

The Browns Ferry PRA assumed the distribution shown in Table 8.1 for pipe breaks inboard of the MSIVs.

TABLE 8.1. Browns Ferry Steam Line Break Frequencies

Break Size	Frequency (/py)	Percent
Large Steam Line Breaks (1.4 to 4.1 sq.ft.)	5.2E-05	4
Intermediate Steam Line Breaks (0.12 to 1.4 sq. ft.)	2.1E-04	17
Small Steam Line Breaks (up to 0.12 sq. ft.)	1.0E-03	79
Total	1.26E-03	100

It will be assumed that the same distribution applies to the pipe breaks under consideration here for the feedwater overfill transient. The total MSLB frequency is assumed to be (2.87E-03 + 2.46E-06 + 1.44E-04)/py = 3.01E-3/py. Dividing this up between large, medium, and small steam line breaks gives the results shown in Table 8.2.

TABLE 8.2. Assumed Distribution for Overfill Steam Line Break Frequencies

Break Size	Frequency/py	Percent
Large Steam Line Breaks	1.21E-04/py	4
Intermediate Steam Line Breaks	5.13E-04/py	17
Small Steam Line Breaks	2.38E-03/py	79
Total	3.01E-03/py	100

Core-Melt Frequency

The Browns Ferry results for core-melt are shown in Table 8.3 for large, medium, and small steam line breaks. These values have been adjusted by the differences in assumed MSLB frequencies. As discussed above for the HPCI system, pipe breaks that occur along the steam lines serving the HPCI steam driven turbine would effectively remove this system from service. The Browns Ferry PRA has taken this into account, assuming that 23 percent of the intermediate piping subject to MSLB would be associated with the HPCI system. The PRA thus already takes loss of HPCI due to pipe break into account. The assumed 23 percent probability is also assumed to apply to the overfill transient.

The variables given in the sequences in Table 8.3 match the system failures assumed on the events trees shown earlier.

TABLE 8.3. Core-Melt Sequence Frequencies

Large Steam Line Break

Sequence	BF PRA Frequency, py	Assumed A-47 Overfill Frequency, py
-	less than 1E-08	less than 2.33E-08

Medium Steam Line Break

Sequence	BF PRA Frequency/py	Overfill Frequency/py
IV RB RA	1.6E-08	-
IV C RB RA	1.3E-08	-
1V C D RB RA	1.3E-08	-
IV C D FB RB RA	1.3E-08	-
IV C D FB GD	1.3E-08	-
Total	6.8E-08	1.66E-07

TABLE 8.3. (Cont'd)

Small Steam Line Break

Sequence	BF PRA Frequency/py	Overfill Frequency/py
S RB RA	5.3E-07	-
S D RB RA	1.2E-07	-
S C RB RA	6.0E-08	-
S C D RB RA	6.0E-08	-
S C D FB RB RA	6.0E-08	-
S C D FB GD	6.0E-08	-
S C D E	6.0E-08	-
S B	3.0E-08	-
Total	9.8E-07	2.33E-06
Total Steam Line MSLB Core-Melt Frequency		
	1.1E-06	2.52E-06

As expected, given the slightly higher assumed MSLB initiating frequency, this issue has a slightly larger frequency for core-melt via steam line MSLB than calculated in the Browns Ferry PRA.

Public Risk

Public risk was likewise calculated assuming the same probabilities for containment failure modes as used in the Browns Ferry PRA for MSLBs, as shown in Table 8.4. The man-rem associated with the releases are those in the Value Impact Handbook (Heaberlin et al. 1983). The final results are given in Table 8.5.

TABLE 8.4. Assumed Containment Failure Probabilities and Man-Rem/Event

Release Category	Probability	Man-Rem/Event
BWR 1	0.01	5.4E+06
BWR 2	0.8	7.1E+06
BWR 3	0.2	5.1E+06

TABLE 8.5. Core-Melt and Risk due to Sequence 1
BWR Overfill Induced MSLBs

Core-Melt Cause	Frequency/py	Containment Failure Mode BWR 1	BWR 2	BWR 3
Large MSLB	less than 2.33E-08	2.3E-10	1.9E-08	4.7E-09
Intermediate MSLB	1.66E-07	1.7E-09	1.3E-07	3.3E-08
Small MSLB	2.33E-06	2.3E-08	1.9E-06	4.7E-07
TOTAL	2.52E-06	2.5E-08	2.0E-06	5.1E-07
Man-rem/py		1.4E-01	1.4E+01	2.6E+00
Total Man-rem/py	1.70E+01			

The total predicted public dose due to overfill-induced MSLBs is then 1.7E+01 man-rem/py. Note that if the core-melt frequency due to MSLB of 1.1E-06/py is simply ratioed with the new initiating frequency (1.79E-03/1.26E-03) and a worst-case release category 2 is assumed, this gives 1.11E+01 man-rem/py public risk with a core-melt frequency of 1.56E-06/py. A public risk of 17 man-rem/py will be assumed.

9.0. TRANSIENT SHUTDOWNS INDUCED BY CONTROL SYSTEM FAILURES

The transient shutdown represents the primary source for initiating a core-melt sequence in the Browns Ferry PRA. As a result, it will be necessary to examine the accident initiators identified by INEL for their contribution to the frequency of transient shutdowns.

The transients affecting Browns Ferry are divided in the PRA study (NRC 1982a) into the following:

T(LOFT) - transients due to loss of offsite power

T(U) - transients with the power conversion system (PCS) unavailable

T(A) - transients with the PCS available.

For the PCS to be available, the heat removal function must remain intact. This requires that the condenser remain available, along with a continued delivery of water.

The transient frequencies that have been observed for the Browns Ferry plant are cited below in Table 9.1, along with the transient frequency for BWRs in general (NRC 1982a).

TABLE 9.1. Browns Ferry Data on Transient Frequencies

	Event Frequency (events/yr)	
Transients that cause the PCS to be Unavailable	BF	BWRs
MSIV closure	0.58	0.24
Loss of normal condensor vacuum	0.56	0.41
Pressure regulator fails open	0.0	0.24
Loss of feedwater flow	0.51	0.17
Loss of offsite power	0.03	0.11
Loss of auxiliary power	0.0	0.03
Increased feedwater flow at power	0.05	0.18
Totals	1.73	1.39
Transients that do not cause PCS to be Unavailable		
Electric load rejection	1.02	0.74
Electric load rejection with bypass failure	0.0	0.0
Turbine trip	0.58	0.77
Turbine trip with bypass failure	0.0	0.0
Inadvertent closure of one MSIV	0.0	0.10
Pressure regulator fails closed	0.0	0.11
Bypass/control valve fails causing pressure increase	0.05	0.25
Recirculation control fails causing increased flow	0.03	0.10
Totals	1.68	2.07

9.1 CONTROL SYSTEM FAILURE CONTRIBUTION TO TRANSIENTS

INEL identified three sequences as a result of control system failures: one due to level control failure initiating a feedwater increase and defeating the high level trip, one involving condensate booster pump actuation at 1 percent power, and one involving false HPCI actuation at 1 percent power.

Note that the two overcool scenarios identified by INEL, and discussed in Chapters 6 and 7, are not considered to be of interest here for transient initiation due to the low power settings. These deal more with startup transients, or overfills during shutdown.

Of interest will be the feedwater control failures identifed by INEL leading to overfill as developed in Chapter 1 in this report. These failures initiate the overfeed and also cause loss of the high level trip leading to overfill. Referring back to the earlier chapters, PNL estimated the initiating frequency for these failures at 3.7E-03/py with an upper bound of 2.1E-02/py after a review of the INEL report. However, the INEL estimate of 6.5E-03/py will be used here.

Transients with the PCS Unavailable

Again, we must consider transients with the PCS available, T(A), and those with the PCS unavailable, T(U). A T(U) transient is assumed to be worse, since it involves the loss of the normal heat removal path. This could occur due to loss of the feedwater function, loss of the condenser, loss of the steam path, or any combination of these. These three modes of causing a transient without the PCS available are discussed further below.

In the previous analysis, the steam driven feedwater turbine was assumed to be very immune to damage as the overfill scenario progressed (probability of failure put at 0.1). This effectively weighted the analysis in favor of continued overfeed and potential steam line damage. Loss of feedwater function implies loss of the main and auxiliary feedwater sources. In the Browns Ferry Plant, the RCIC pumps serve this function. This could occur, given an overfill and a trip of the MFW (defeated in this scenario) or failure of the MFW steam-driven turbine, plus an independent loss of the AFW function.

The probability of failure of the MFW steam turbine was valued at 0.1. Rather than speculate on the survivability of the MFW turbine, it will simply be assumed here that the MFW turbine fails. The probability used in the ORNL Precursor Study (NRC 1982c) for failure of the AFW function and loss of decay heat removal of 1.1E-03 will then be used here. The accident scenarios identified by INEL have not specified any damage to the condenser, so it is assumed that an independent failure of the condenser would have to occur to cause loss of this function. With the assumed operator error probability of 0.517 for failure to terminate the overfill, the predicted frequency of this event would then be

$$(6.5E\text{-}03/py)(0.517)(1.1E\text{-}03) = 3.7E\text{-}06/py.$$

The progression of the overfill scenario to steam line break will also cause loss of the steam path to the condenser. This will occur via the break itself, or isolation with the MSIVs which close on MSLB. In the PNL analysis, it was again assumed that the MFW steam turbine and main turbine would continue operation (probability of 0.9) to the point of spillover to enhance the potential for water hammer and pipe break. As discussed in Chapter 5, this resulted in an assumed probability of pipe break given spill over of 0.95. When operator intervention is also added, this gave a net frequency of pipe break of

(6.5E-03/py)(0.517)(0.9)(0.95) = 2.87E-03/py.

As can be seen, the assumed high probability of steam line break results in this pathway also representing the dominant mode for inducing a T(U) transient. Referring back to Table 9.1, it can also be seen that any T(U) type of sequences postulated for control failures will be reduced by a factor of (2.87E-03/1.73) = 1.66E-03, or approximately a factor of 1E-03.

Transients with the PCS Available

The T(A) transient would essentially be the above case where main turbine trip occurs as the overfeed progresses. Again, the probability of turbine trip was put at 0.1 versus 0.9 for continued operation to the point of pipe break assumed above. The predicted frequency of T(A) transients then becomes

(6.5E-03/py)(0.517)(0.1) = 3.4E-04/py.

Again, referring back to Table 9.1 for the observed frequency of T(A) type sequences in Browns Ferry indicates that sequences initiated by such transients from control failures will be reduced by a factor of (3.4E-04/1.68) = 2.02E-04.

9.2 CORE-MELT AND RISK REPRESENTED BY CONTROL SYSTEM-INDUCED TRANSIENTS

The dominant transient sequence contributors to core-melt frequency for the Browns Ferry PRA are given in Table 9.2.

TABLE 9.2. Browns Ferry PRA Results for Transient Core-Melt

Sequence	Frequency	Release Category Probability BWR-1	BWR-2	BWR-3	Public Risk man-rem/py
T(U)R(B)R(A)	9.7E-05	0.0001	0.2	0.8	
T(U)B	5.1E-05	0.0001	0.2	0.8	
T(U)QR(B)R(A)	4.1E-06	0.0001	0.2	0.8	
Total T(U)	1.52E-04				6.20E+02
T(A)BM	3.7E-06	0.0001	0.2	0.8	2.04E+01
TOTAL	1.56E-04				6.40E+02

The risk associated with the release categories is based on 5.4E+06 man-rem for BWR-1, 7.1E+06 man-rem for BWR-2, and 5.1E+06 man-rem for BWR-3. Only the totals for T(U) and T(A) transient sequences are given. The overall core-melt frequency for Browns Ferry is put at 2.0E-04/py, so these transients represent 78 percent of the overall plant core-melt frequency.

The core-melt contribution to transients from the control system failures would then be expected to be reduced by a factor of 2.87E-03 for T(U) sequences, and a factor of 2.02E-04 for T(A) sequences, as shown in Table 9.3.

TABLE 9.3. Core-Melt Frequency and Risk for Control System Failure-Induced Transients

Core-Melt Transient Sequences	BF PRA Frequency, 1/py	PNL Estimated Frequency 1/py	Public Risk, man-rem/py
T(U) type	1.52E-04	4.36E-07	2.40E+00
T(A) type	3.7E-06	7.49E-10	3.16E-02
	1.56E-04	4.37E-07	2.43E+00

The overall public risk represented by transient shutdowns as a result of control failures is then on the order of 2.4 man-rem/py. The core-melt frequency is put at 4.37E-07/py. Again this is approximately three orders of magnitude smaller than the observed risk represented by transient shutdowns, being dominated by the T(U) transients where the PCS is not available for decay heat removal.

With the transients considered representing approximately 78 percent of the core-melt frequency for Browns Ferry, the control system transients here would then represent approximately (78%)(1E-03) = 0.078% of the plant risk.

10.0 VALUE/IMPACT ANALYSIS OF POTENTIAL CORRECTIVE FEATURES

In this chapter, various corrective features will be postulated to correct the control system failures identified by INEL. An estimate will be made of the effectiveness of such fixes in reducing or eliminating the failure frequencies, and this will be translated into effective reductions in core-melt frequency and public risk. The cost of implementing such corrective features will also be estimated, and the net value/impact ratio of man-rem saved per $1000 will be presented.

Again, the three sequences of interest are as follows:

Sequence 1. High Level Trip Failure
Sequence 2. Valve Failure Causing Feedwater Increase
Sequence 3. False Start of the LPCI.

These will be discussed further below.

10.1 SEQUENCE 1: HIGH LEVEL TRIP FAILURE

Referring back to Chapter 3, the initiators identified by INEL causing failure of the high level trip and feedwater increase are:

Initiator A: A leak or rupture of the variable leg of the water level sensing line that is common to two of the three reactor vessel water level sensors causing a false low signal and resulting in increased feedwater flowrate.

Initiator B: A common cause failure of two of the three level sensors or sensor circuitry causing a false low level signal and resulting in an increased feedwater flowrate.

Initiator C: Independent failure of two level sensors or sensor circuitry resulting in an increased feedwater flowrate.

Initiator D: A failure in the control circuit that regulates the feedwater pump speed and failure of two out of three high level trips resulting in an increased feedwater flowrate and overfill of the reactor vessel.

Postulated Fix 1: Improve Weld Integrity on Instrumentation Lines (Sequence 1A only)

The weld points on the 2-inch instrumentation lines were assumed by INEL to be subject to leakage or rupture. Better QA of welds (i.e., radiography or other non-destructive testing) could reduce the postulated failure rate. Due to stress corrosion cracking problems in BWRs, it is assumed that this would be required annually to be effective.

This fix will only impact the frequency of Sequence 1.A. The reduction in weld failure is likely to be small, given the QA to which the pipes are now subjected. A reduction in weld failures of 10 percent will be estimated here. Referring back to Table 3.2, the new predicted weld leakage frequency would then be (3.2E-04/py)(0.9) = 2.88E-04/py. The pipe failure frequency would remain the same at 1.1E-04/py, for a total frequency of 3.98E-04/py. The reduction in frequency is then (4.3E-04 - 3.98E-04)/py = (3.2E-04/py)(0.1) = 3.2E-05/py.

The reduction in core-melt frequency is ratioed from the total initiating frequency in Sequence 1 of 6.5E-03/py and the total core-melt frequency of 2.40E-06/py giving (3.2E-05/6.5E-03)(2.40E-06/py) = 1.18E-08/py. This is then a 0.0049 fraction of the base case. This also equates to a reduction in risk of 8.0E-02 man-rem/py or 2.4 man-rem over 30 years.

NRC study NUREG-1061 estimated the cost of NDE piping inspection to be approximately $3000/weld inspected (NRC 1985). For such a small line that is not safety grade, much of the cost associated with QA will not be applicable. This cost is reduced here to $500/weld, divided between labor and QA/records costs. The annual outage cost for 12 welds per instrument line, and 2 instrument lines is then $12,000/py. At a 10 percent assumed discount rate over 30 years, this represents cost of ($12,000)(9.43) = $1.13E+05.

The value/impact ratio is then

(2.4 man-rem)/($1.13E+05) = 2.1E-02 man-rem/$1000.

In-situ heating stress improvement is not considered viable for such a small pipe diameter. The pipe itself would probably be changed, as discussed below. The NRC (1985) study also predicts an occupational exposure of 0.8 man-rem per weld inspected for the large BWR pipes. These pipes also carry reactor coolant, but the radiation field would be expected to be significantly lower around the small pipe.

Postulated Fix 2: Hardened Instrumentation Lines (Sequence 1A only)

The pipe runs (probably 304 stainless steel) can be changed, using a material (e.g., 316 SS) that is more resistent to stress corrosion cracking. This fix will again only impact Sequence 1, Initiator A.

The 316 stainless steel piping would be expected to significantly reduce the frequency of weld failures due to the reduction in stress corrosion cracking. It is estimated that the frequency of pipe weld leakage could be reduced by a factor of 75 percent. It is uncertain that any reduction in pipe rupture frequency would be achieved. The new predicted weld leakage frequency would then be (3.2E-04/py)(0.25) = 8.0E-05/py. The pipe failure frequency would remain the same at 1.1E-04/py, for a total frequency of 1.90E-04/py. The reduction in frequency is then (4.3E-04/py - 1.90E-04/py)) = 2.40E-04/py.

Referring back to Table S.1, this equates to a reduction in core-melt frequency of 8.89E-08/py, and a reduction in risk of 6.0E-01 man-rem/py or 1.8E+01 man-rem over 30 years.

The cost for replacing the piping, replumbing and recalibrating of all instruments is estimated at 4 man-weeks per instrument line or 8 man-weeks of installation labor. The engineering and QA time is put at 4 man-weeks, for a total of 12 man-weeks at $2270/man-week or $27,240. The material costs are $5000 for approximately 200 feet of piping and fittings, for a total cost of $32,240.

- 4 man-weeks of engineering support at $2270/week, or $9080
- 8 man-week of craft services at $2270/week, or $18160
- $5000 in instrumentation and supplies.

The value/impact ratio is then

(18 man-rem)/($32.2E+03) = 0.56 man-rem/$1000.

Postulated Fix 3: Changes in Instrumentation or Trip Logic to Reduce Common Cause Failures Causing Feedwater Increase and Loss of Trip

To evaluate the effectiveness of changes in configuration and trip logic more thoroughly, seven configurations for hardware and logic were considered for both the level transmitters (LT) and level indicating switches (LIS). These are summarized in Tables 10.1 and 10.2. In addition, they indicate the instrument failures required to initiate the feedwater overfill and defeat the high level trips. The base case configuration of instruments as it exists in the Browns Ferry plant is given in Table 10.1, Case 4, for the level transmitters.

Again this does not reflect the fact that failures must be low-scale on the LT(A) control transmitter to initiate the feedwater overfill, as discussed in the earlier chapters. The other instrumentation must likewise be restricted to specific failure modes if the high level trips are to be avoided.

TABLE 10.1. Possible Configurations for Level Transmitters (LT)

Case No.	Sensors	Trip Logic	Failures that Initiate Feedwater and Defeat High Trip
0	1	no trip	A
1	1	1-out-of-1	A
2	2	2-out-of-2	A, AB
3	2	1-out-of-2	AB
4	3	2-out-of-3	AB, AC, ABC
5	4	2-out-of-3	AB, AC, ABC

The modifications of interest to Browns Ferry focus on Case 5 above, a modification to a 2-out-of-4 configuration. INEL has made some estimates of the expected frequency of the postulated overfill scenario for several of the scenarios above, as given in Table 10.2. The estimate for the 2-out-of-4 configuration is based on the INEL estimates of 1.2E-07/hr and 2.7E-07/hr for reduced capacity and inoperable failures in the controlling level transmitter and 2 others sufficient to drive the overfill and fail the high level trip. This gives a frequency of (1.2E-07+2.7E-07 = 3.9E-07/hr)(8760 hrs/py) = 3.4E-03/yr. No upper bound was given.

TABLE 10.2. INEL Estimate of Feedwater Overfill Frequencies For Different Level Transmitter Configurations

Case	Trip Logic	Estimated Frequency of Overfill and Defeat High Trip, 1/py		Fraction of Base Case
		Median	Upper	
0	no trip	1.0E-01	2.7E-01	15.4
1	1-out-of-1	9.0E-03	5.4E-02	1.4
2	1-out-of-1 separate feed and trip transmitters	4.2E-03	1.0E-02	0.6
3	1-out-of-2	-		
4	2-out-of-3	6.5E-03	3.0E-02	1.0
5	2-out-of-4	3.4E-03	-	0.5

The base case configuration for the Browns Ferry is again a 2-out-of-3 trip with three level transmitters, and a 1-out-of-2-twice trip with four level switches. As can be seen above, the modification to a 2-out-of-4 configuration could be expected to possibly reduce the frequency of feedwater overfills by a factor of 2.

A simpler 1-out-of-1 configuration with the controlling transmitter and high trip on separate transmitters actually is predicted to have less frequency overfills. However, spurious trips also introduce the potential for inadvertent feedwater fluctuations. Any spurious shutdown would require an estimated 24 hours to restore the plant to operation, with replacement power costs estimated to be about $300,000/day. One spurious trip could then negate any perceived benefits of reduced frequency for overfills.

As can be seen, the lowest failure rate relative to the base case configuration is predicted to be Case 5, with four transmitters using a

2-out-of-4 trip logic. This would require the addition of one level transmitter and changing the trip logic for the level switches. However, the current design is probably a compromise to provide the level of reliability deemed necessary without generating false trip signals. Going to the 2-out-of-4 logic may make the trip more reliable, but the price may be more frequent false trips.

The new failure frequency is seen to be approximately 0.5 of the base case of 3.3E-03/py from Table 3.8. The reduction is then (0.5)(3.3E-03/py) = 1.65E-03/py. Ratioing this to the total frequency and core-melt predicted for Sequence 1 gives a predicted reduction in core-melt frequency of (1.65E-03/6.5E-03)(2.40E-06/py) = 6.1E-07/py. The reduction in public risk predicted is then (1.65E-03/6.5E-03)(16.2 man-rem/py) = 4.1 man-rem/py, or 1.23E+02 man-rem per plant over 30 years.

Costs of Postulated Fix 3

The industry cost for adding one level transmitter on an existing 2-inch line is as follows:

engineering support - 4 man-weeks at $2,270/man-week or $9,080
pipe fitters - 2 man-weeks at $2,270/man-week, or $4540.
modifications to operating procedures - $0
level transmitter - $10,000
plumbing, supplies - $5,000
modifications to logic circuits - $5,000.

This totals $33,580. No license amendments are required for this modification. No annual costs are projected for this modification. Discussions with the NRC and GE concerning the addition of one level transmitter put costs at approximately $150,000 using existing penetrations through containment (electrical and pneumatic), as well as existing cable runs and cabinets. Qualification of this equipment to safety grade would cost an additional $100,000. The cost of the addition of the transmitter in a plant requiring a new penetrations was $1,000,000.

The predicted value/impact ratio can then range from 1.23E+02 man-rem/$33.58E+03 = 3.66 man-rem/$1000 for the minimal cost estimate, to 1.23E+02 man-rem/$150,000 = 0.82 man-rem/$1000 for the more likely realistic GE estimate, to 1.23E+02 man-rem/$1,000,000 = 0.123 man-rem/$1000 for the case in which new penetrations would be needed. The 0.82 man-rem/$1000 esimate based on the GE figures will be used here as the most likely estimate.

Limitations and Real-World Considerations for Postulated Fix 3

The indications are that real-world considerations could easily overshadow theoretical calculations, particularly for level control instrumentation where the ability to test often carries more weight than calculated reliabilty. Uncertainties in the failure data base for sensors could include hydraulic shocks which occur at different rates in separate instrument lines making some failure combinations of sensors more likely, or common mode failures of instruments due to faulty maintenance. The data currently available on

component failure rates are not specific enough as to failure cause (i.e., shocks, faulty maintenance, etc.) and failure mode (i.e., inoperable low-scale, drift low, etc.) to support specific recommendations for a 2-out-of-4 configuration based on theoretical calculations for level transmitters.

As a result, the value/impact ratio of 0.8 man-rem/$1000 for the 2-out-of-4 configuration is likely to be driven down by both possible higher costs and reduced effectiveness of any modifications to the level transmitter configuration.

No Trip

The estimate by INEL is that the no-trip plant would be subject to the overfill transient approximately 15 times more often than the reference plant, other factors being equal. It must be pointed out that any comparison between different level control and high level trips and other modifications is highly conditional on a number of factors, including basic hardware and reliability as well as operator response to system failures and the plant dynamics to failures. This can include plant-specific differences in and compensations for a number of factors, including:

- type of level control (three element, one element)
- power supplies
- backup or alternate level displays
- instrument line plumbing configuration
- controlling level display
- controlling level record
- annunciators and alarms
- operator training and procedures.
- maintenance, general age and state of equipment.

If the theoretical estimate by INEL is taken as an upper bound on the initiating frequency however, the potential risk reduction in implementing a 2-out-of-4 configuration is then on the order of (15.4 - 0.5)(123 man-rem/plant) = 1833 man-rem. Going to a simpler 2-out-of-3 configuration would give (15.4 - 1)(123 man-rem) = 1771 man-rem. In either case, the costs would likely approach or exceed the maximum GE esimates given above, or approxiately $1,000,000, due to the need to add instrument lines and penetrations. The value/impact ratio would then approach 1833 man-rem/$1,000,000 = 1.8 man-rem/$1000.

As such, the value/impact ratio given above is more favorable for requiring the additional level protection in the no-trip plants. However, the uncertainties are thought to be even larger than those associated with the reference plant actually analyzed by INEL, with the uncertainties in cost and risk reduction both again driving the resulting value/impact ratio down. The two plants in question (Oyster Creek and Big Rock Point) have apparently modified operating procedures to account for their specific designs. This is reflected in the operational history to date for Oyster Creek, which shows no record of increases in feedwater at power (EPRI 1982b). Given the lack of specific design studies for A-47 on these plants, any recommendations would have to consider the uncertainties in any recommendations for design changes.

10.2 VALVE FAILURE CAUSING FEEDWATER INCREASE

Sequence 2 is again initiated by a condensate booster pump failure, as discussed in Chapter 6. The three initiators are as follows:

Initiator A: Any one of three motor operated feedwater pump discharge valves fails open.

Initiator B: The air operated startup feedwater bypass valve fails open.

Initiator C: The condenser bypass air operated valve fails closed.

The frequency of the overall sequence was again put at 8.2E-05/py, with an upper bound of 5.6E-03/py. It is assumed that this value is primarily based on a simple valve failure rate of 3E-07/hr, times 192 hours per year for startup and shutdown, giving 5.76E-05 failures/yr.

However, as discussed in Chapter 6, it is thought that the system as currently configured already has safeguards to prevent excessive condenser flow to the vessel via a simple valve failure. These safeguards are discussed briefly below.

Proposed Fixes for Initiator A

As discussed briefly in Chapter 6, the feedwater pump isolation valves are normally closed during startup. The failure then requires the normally closed valve to fail open, implying a false control signal (1E-07/hr) or electrical short of the operator to power (1E-8/hr), or internal valve rupture that leaves the valve body intact (less than 1E-8/hr). If this failure provides excessive flow to the vessel, the control signal to the bypass valve will throttle flow via that pathway. If excessive feedwater flow continues via the failed valve, the train must be isolated manually using the additional motor-operated valve downstream of the feedwater pump.

The system already has high-level alarms and motor operated valves in series that will allow the operator to isolate the failed valve. Additional safeguards put on the control circuit or to the valve operator may be possible. However, this may also result in a decrease in the reliability of the valve to open on demand, thus impacting feedwater reliability. The most likely modification is to simply change the valve logic for the valve downstream of the feedwater pump to provide isolation when not in use.

For Initiator B, it was pointed out that the startup bypass valve already has a lock-up feature incorporated into the air supply system such that loss of air pressure will lock the valve in its existing position at the time of failure. The valve failing open would then require failure of the air supply, and failure of the lock-up feature. Modifications to the control circuit to prevent false full open signals may also make the control of the valve less reliable.

For Initiator C, it was pointed out that any failure of the condenser bypass valve would still result in flow to the vessel being regulated through the startup bypass valve, which can still be controlled to regulate vessel level. Multiple failures would again be required.

The core-melt frequency is put at 2.05E-09/yr, with a public risk of 0.01 man-rem/yr or 0.3 man-rem over 30 years. The contribution due to transients is very small, based on the ratio of its LOCA initiating frequency to the total of (2.4E-06/yr)/(1.67E-03/yr) which is approximately 0.1% or 7.9E-04 man-rem/yr.

The cost of any proposed modifications would have to be limited to several thousand dollars at most to represent cost-effective measures, which equates to approximately one man-week of effort. Any changes in the control circuitry for valve operators is likely to require a more substantial cost, plus the potential for reduced reliablity for feedwater delivery during operation.

At a minimum, the costs would be put at the following for changing the isolation logic of the motor operated valve downstream of the feedwater pump with no changes in the technical specifications or safety studies or license amendments:

- 2 man-weeks of engineering support at $2270/week, or $4540
- 1 man-week of craft services at $2270/week, or $2270
- $2000 in instrumentation and supplies.

This gives a cost of $8810, and a value/impact ratio of 0.3 man-rem/$8810 = 0.03 man-rem/$1000.

10.3 INADVERTENT LPCI ACTUATION

Finally, the third sequence identified by INEL involves the inadvertent actuation of the LPCI. The initiators identified included:

Initiator A: common cause failure of two drywell high pressure switches

Initiator B: common cause failure of two reactor vessel low water level switches

Initiator C: shorts in the pressure or level logic circuits causing pump start

Initiator D: pump switch shorts to power.

The median probability of failure for this sequence was 3.6E-03/yr, with an upper bound of 7.7E-03/yr.

Note that the pump switch short to power is not considered sufficient to cause LPCI. The discharge valve for each loop of the LPCI system is normally closed, requiring a control circuit signal and a low vessel pressure to enable opening of the valves. The pump short to power would not generate the control signal, thus no water delivery to the vessel could occur.

Postulated Fixes

For Initiators A and B, the system, as it is already designed, has fully independent initiation circuits for the LPCI function. Again these are the drywell pressure switches or a 1-out-of-2-twice signal from LIS -3-58 A through D shown in Figure 3.1.

In addition the nuclear system pressure must be below 450 psig, where the LPCI discharge valves open, allowing the pumps to actually inject water into the vessel.

Note that the system is currently designed in such a way that once an initiation signal is received by the LPCI control circuitry, the system will operate until manually reset. The operator is thus currently expected to observe and control the operation of the LPCI function.

The obvious design fixes are to reduce the spurious initiation signals, or add trips for the LPCI pumps or isolation circuits for the valves in the delivery piping. This would require a change in the design philosophy requiring operator action to terminate LPCI. However, this is not inconsistent with the use of high water level trips for the HPCI function.

The addition of a LPCI pump trip and valve isolation to the existing LIS-3-203 A through D high vessel water level trip for the HPCI and RCIC function would serve this purpose. This modification, then, would only involve a change in the control logic allowing a pump trip and valve isolation upon indication of high water level while in the LPCI mode. However, it is uncertain if this design modification would detrimentally impact some long-term function of the LPCI that originally specified the operator shutoff feature. As a result, it is thought that further accident analysis would be needed to determine the advisability of this trip. This is reflected in the costs below.

The reduction in core-melt frequency would then be bounded by the 1.2E-07/yr estimate for this issue. The reduction in public risk is put at 0.81 man-rem/py, or 24.3 man-rem over 30 years. With a LOCA initiation frequency of 3.04E-05/yr compared to the total for all three sequences of 1.67E-03/yr, this sequence contributes approximately 2 percent to the transient risk of 1.34 man-rem/yr which is small compared to the 24.3 man-rem/yr for this issue alone.

Development Costs

Because this modification changes the engineered safety system response to a design basis accident, this will also require accident analysis, modifications to the technical specifications, and a license amendment. The NRC may require generic studies as well as requiring individual plant analysis. For licensing amendments the current NRC policy is for full cost recovery; however, an estimate is made here based on the previous schedule in 10 CFR 172 (The Code of Federal Regulations, Title 10, Part 172).

These costs are:

- $150,000 NRC generic issue evaluation (spread over 24 completed BWRs), or $6250 per plant
- 6 man-months of utility time, or $50,000
- $4000 license amendment.

This gives a total of $60,250.

Implementation Cost

Assuming that this fix is implemented during normal outages, it is estimated that the actual work will require approximately the following:

- 2 man-weeks of engineering support at $2270/week, or $4540
- 1 man-week of craft services at $2270/week, or $2270
- $2000 in instrumentation and supplies.

This comes to $8810. Once implemented, no recurring costs for the utility or the NRC are foreseen. The total is then $60,250 + $8810 = $69,060.

Value/Impact Ratio

The best estimate of the value/impact ratio is then

19.6 man-rem/$69,060 = 0.29 man-rem/$1000.

10.4 VALUE/IMPACT SUMMARY

The fixes proposed for the accident initiators identified by INEL are summarized in Table 10.3 below.

TABLE 10.3. Proposed Modifications to GE BWRs and Estimated Value/Impact

Modification	Impact	Reductions in Core-Melt 1/py	Reductions in man-rem 30 yrs	Cost, $	Value/Impact man-rem/$1000
Instrument Line Weld Integriy	Reduce weld failures	1.18E-08	2.4	113,000	0.02
New 316 SS Instrument Lines	Reduce pipe failures	8.89E-08	18.0	32,220	0.56
Add new LT, 2-out-of-4 trip	Reduce high trip failures	6.10E-07	123	150,000	0.82
Modify Isolation Logic for Condensor Flow	Isolate flow from failed valve	2.05E-09	0.3	8,810	0.03
Add LPCI Trip on High Vessel Water Level	Isolate flow from LPCI pump short	1.20E-07	24.3	69,060	0.35

As can be seen, the addition of another level transmitter (LT) in a 2-out-of-4 trip logic is thought to be the most cost-effective measure to counteract the control system failures identified by INEL for feedwater overfill. However, uncertainties in cost and any real world benefit of a 2-out-of-4 versus 2-out-of-3 level transmitter configuration may force this ratio down.

Modifications to the instrument piping itself to reduce welding or piping ruptures and low-level indications are less effective, due to the lower initiation frequency assumed for such scenarios and the high cost of annual welding inspections.

The fixes to counter condenser and LPCI overfill are significantly less cost-effective, again primarily due to the engineered features already built into the plant to prevent false pump actuation signals or shorts. This is also reflected in the low initiation frequencies assumed for these failures. Modifications to these systems may also have negative impacts on the reliability of feedwater delivery during normal operation or LPCI during LOCAs.

Note that the development of these accident initiators to core-melt is thought to reflect a conservative approach to estimating the impact of these failures on-plant engineered safety systems. Cost estimates, likewise, tend to underestimate the true cost of nuclear plant modifications. These factors, when combined, tend to reduce the estimated value/impact ratios as given above. The best estimates as given above are thus thought to reflect the relative importance of each accident initiator and proposed fix, and its overall importance to plant safety.

11.0 CONCLUSIONS

This report presents the results of a probabilistic analysis of core-melt accidents that could potentially result from transient overfill scenarios in a BWR. This report uses the BWR/4 Browns Ferry class of General Electric BWR as a reference design. However, the dominant failure modes identified involve failures in the feedwater control system considered to be applicable to all GE BWRs.

This report relied on the previous identification and examination by INEL of failure mechanisms causing overfill in BWRs. An extensive effort was made to verify (to the extent possible) previous calculations for the frequency of initiating events. However, resources did not permit a re-examination of possible additional failure mechanisms causing overfill.

The sequences examined included feedwater control failure, condensate pump failure, and LPCI failure causing initiation of overfill. The latter two sequences result in cooldown rates which exceed the technical specification limits. However, no credible potential for vessel failure due to thermal shock was identified given the low pressures involved. Condensation of the large steam void present in the BWR makes it physically unlikely to create the concurrent high pressure and thermal cooling necessary for thermal shock to lead to vessel damage. As a result, the potential for steam line break given overfill was considered to be the dominant source of risk.

The PNL examination agrees with the INEL conclusion that the feedwater control failure is the dominant failure mechanism due to a higher initiation frequency. The PNL examination of Sequence 1 arrived at an initiating frequency of 3.7E-03/py for feedwater overfill. This was approximately 1/2 that predicted by INEL, but is based on a more detailed examination of the failure modes required in the level transmitters and switches to produce the desired feedwater increase. This was also well within their error bounds. The other sequences were several orders of magnitude less likely and not examined in detail by PNL.

The human reliability analysis performed resulted in an estimated probability of slightly less than 0.5 that the operator would interpret these signals correctly and terminate the sequence. Correct operator intervention during startup would likely be higher, but during operation the system would be on automatic control with operator attention not necessarily focused on the feedwater control. The inclusion of this factor in the analysis is justified given the presence of the operator and the extensive training received specifically for water level control.

Note that this human probability depends to some extent on the time available to the operator from the indication of level sensor failure or alarm to when overfill would occur. The INEL analysis of 125 percent feedwater overspeed at 68 percent rated power is estimated to result in overfill in approximately 1 minute. The initial reactor response to the overfill is a power increase to 90 percent, giving a net 35 percent excess in the fill rate. However, it is uncertain if a 125 percent feedwater overspeed could occur

at 100 percent rated power without causing an overpressure trip signal. The maximum overspeed possible without a trip is likely to decrease as the reactor nears 100 percent power and the net water excess would be reduced as well, giving more time available before spillover.

The potential for steam line break and MSLB was then examined. A consideration of main turbine failure and plant shutdown before spillover was thought to reduce the potential for pipe break somewhat, but the final assumption put the steam line MSLB probability at 0.95, given initiation of the overfill accident and failure of the operator to isolate feedwater. The net frequency of MSLB was then put at 2.87E-03/py due to overfill. Two other overfill scenarios increased this to a total frequency of (2.87E-03 + 2.40E-06 + 1.44E-04) = 3.01E-03/py.

The use of the Browns Ferry PRA event trees for large, medium, and small steam line breaks gives a conservative estimate of the potential for core-melt in this analysis. These event trees were developed for a steam line break upstream of the MSIVs, which is thought to represent a more severe accident to the plant than a downstream break. In the PRA, the break probability of up- or downstream breaks was assumed to be equal, with the downstream breaks also requiring a double failure of the MSIVs to isolate the line. Thus, the upstream break was the more conservative of the two in terms of failure frequency as well.

In this examination, consideration was given to possible reduced function of systems due to water hammer and entrained water in the flow. The MSIV and safety valves for the ADS system were thought to be particularly vulnerable. However, the indications to date are that the valves will function with the same reliability, although they may be subject to added chatter. The MSIV valves in particular were thought to actually seat better under the hydraulic forces of the flow. The same reasons then exist to model the upstream breaks for the overfill-induced MSLB as well.

The performance of other safety systems including the injection systems and depressurization system were also examined for the potential for degraded performance due to the overfill event. Any water in the steam lines for the HPCI system is thought likely to drain or flash to steam in the transition from overfill to MSLB before the system would be demanded. EPRI data indicate that the ADS valves would likely chatter in two phase flow, but reliability would not be affected. The SCRAM and RCIC functions would not be affected. The net result was that the system reliabilities predicted in the Browns Ferry PRA were directly applicable to this examination.

Using the Browns Ferry event trees for steam line MSLB induced core-melt, the result was a predicted core-melt frequency of 2.52E-06. This compares to the steam line break induced core-melt frequency of 1.1E-06/py in the Browns Ferry PRA, which has a total core-melt frequency of 2.0E-04/py. This represents only approximately 1 percent of overall plant core-melt frequency.

The risk associated with feedwater overfill was also estimated, assuming the same release categories as used for steam line induced MSLBs in the Browns Ferry PRA. The risk associated with core-melt was put at approximately 16 man-rem/py.

Finally, the overfill scenarios identified by INEL were considered as transient initiators for inducing reactor shutdown. An examination of the Browns Ferry PRA indicates that transients represent approximately 80 percent of the estimated overall plant core-melt frequency of 2E-04/py, and thus this contribution to core-melt could not be neglected.

The feedwater overfills leading to pipe break were assumed to represent transients where the power conversion system would no longer be available for the removal of decay heat. With a predicted frequency of 1.79E-03/py, this compared to the observed rate of such transients in Browns Ferry of 1.73/py, giving a ratio of 1.79E-03/1.73 or approximately 1E-03.

Likewise, simple overfills that did not result in pipe break but possibly tripped the feedwater turbine or main turbine were assumed to represent transients with the PCS available. With a predicted frequency of 3.40E-04/py versus the observed frequency of 1.68/py in Browns Ferry, this represented approximately 1E-04 of the risk associated with this type of sequence.

An examination of the Browns Ferry PRA then shows that the predominant risk is associated with sequences that involve loss of the PCS. Because control system failures were assumed to result most likely in this type of transient, the resulting prediction of core-melt frequency was approximately 1E-03 of that predicted for transients in the Browns Ferry PRA. The resulting core-melt frequency for control system induced transients was then 2.38E-07/py with 1.3 man-rem/py public risk.

The contribution to core-melt and risk from transients was found to be approximately an order of magnitude smaller than that predicted for overfill and steam line break.

Overall Core-melt and Public Risk

The overall predicted core-melt frequency and public risk are given in Table 11.1. The total core-melt frequency was put at a best estimate of 2.96E-06/py. The total public risk was then estimated to be 19.5 man-rem/py.

Value/Impact

Possible plant modifications to reduce the frequency of overfill can be bounded by comparison to the Safety Goal objective of 1 man-rem/$1000 of cost. Assuming a 30-year effective plant life, the total possible risk reduction is approximately 584 man-rem/reactor. Costs should then not exceed approximately $584,000 per reactor for corrective features to prevent overfill.

The specific fixes examined in Chapter 10.0 had estimated costs ranging from approximately $9,000 to $150,000, and man-rem reductions over 30 years ranging from 0.3 to 123. The resulting value/impact ratios then ranged from 0.02 to 0.82 man-rem/$1000. The most cost-effective measure at this time appears to be the addition of one level transmitter for 4 total with a 2-out-of-4 trip logic for feedwater on high vessel water level. Real-world considerations indicate, however, that the factor of 2 improvement in reliability assumed for a 2-out-of-4 versus 2-out-of-3 configuration in

preventing an overfill may be very optimistic. Costs could also easily exceed the $150,000 assumed, thus making any modifications questionable at this time. This also does not take into account possible improvements via operator training and procedures. Given the high failure probability assumed in this analysis for the operator and the fact that these are systems normally considered under operator control, improved operator training and procedures are likely to be a more fruitful area for correcting perceived control system deficiencies.

TABLE 11.1. Conclusions for Control System Failure Induced Core-Melt Frequency and Public Risk for the GE BWR

Sequence Initiator	Accident Initiating Frequency (/py) Median	Accident Initiating Frequency (/py) Upper	PNL Core-Melt Frequency Best Estimate (/py)	Public Risk Best Estimate (man-rem/py)
Reactor Vessel Overfill Sequence Number 1	6.5E-03	3.0E-02	2.4E-06	16.2
Reactor Vessel Overfill Sequence Number 2	8.2E-05	5.6E-03	2.05E-09	.01
Reactor Vessel Overfill Sequence Number 3	3.6E-03	7.7E-03	1.20E-07	0.81
Overfill Initiated Transient Shutdown				
With PCS Available	3.40E-04	1.57E-03	7.49E-10	3.16E-02
Without PCS	2.87E-03	1.26E-02	4.37E-07	2.40E+00
			4.38E-07	2.43E+00
TOTAL			2.96E-06	19.45

REFERENCES

Bruske, S. J., et al. 1985. Effects of Control System Failure on Transients and Accidents at a General Electric Boiling Water Reactor. NUREG/CR-4262, E.G.& G. Idaho, Idaho Falls, Idaho.

Bush, S. H., et al. 1982. A Review of Past Experiences in BWRs. EPRI NP-2590-LD, Electric Power Research Institute, Palo Alto, California.

EPRI. 1982a. Water Hammer in BWRs. EPRI NP-2590-LD, Electrical Power Research Institute, Palo Alto, California.

EPRI. 1982b. ATWS: A Reappraisal, Part 3: Frequency of Anticipated Transient. NP-2330, Electric Power Research Institute, Palo Alto, California.

Heaberlin, S.W., et al. 1983. A Handbook for Valve-Impact Assessment. NUREG/CR-3568, PNL-4646, Pacific Northwest Laboratory, Richland, Washington.

McClymont, A. S. and B. W. Poehlman. 1982. ATWS: A Reappraisal, Part 3: Frequency of Anticipated Transients. EPRI Report NP-2230, Science Applications, Inc., Palo Alto, California.

NRC. 1975. Reactor Safety Study - An Assessment of Accident Risks in U.S. Commercial Nuclear Power Plants. WASH-1400, NUREG-75/014, U.S. Nuclear Regulatory Commission, Washington, D.C.

NRC. 1982a. Browns Ferry Probabilistics Risk Assessment, Interim Reliability Evaluation Program. NUREG/CR-2802, U.S. Nuclear Regulatory Commission, Washington, D.C.

NRC. 1982b. Evaluation of Water Hammer Events in Light Water Reactor Plants. NUREG/CR-2781, U.S. Nuclear Regulatory Commission, Washington, D.C.

NRC. 1982c. Precursors to Potential Severe Core Damage Accidents: 1969-1979. A Status Report. NUREG/CR-2497, U.S. Nuclear Regulatory Commission, Washington, D.C.

NRC. 1983a. Common Cause Failure Rates for Instrumentation and Control Assemblies. NUREG/CR-3289, U.S. Nuclear Regulatory Commission, Washington, D.C.

NRC. 1983b. Regulatory Analysis for USI A-1, Water Hammer. NUREG-0993, U.S. Nuclear Regulatory Commission, Washington, D.C.

NRC. 1983c. VISA-A Computer Code for Predicting the Probability of Reactor Pressure Vessel Failure. NUREG/CR-3384, U.S. Nuclear Regulatory Commission, Washington, D.C.

NRC. 1983d. Regulatory Analysis Guidelines to the U.S. Nuclear Regulatory Commission. NUREG/BR-0050, U.S. Nuclear Regulatory Commission, Washington, D.C.

NRC. 1984. Evaluation of Water Hammer Occurrences in Nuclear Power Plants. NUREG/CR-0927, U.S. Nuclear Regulatory Commission, Washington, D.C.

NRC. 1985. Report of the U.S. Nuclear Regulatory Commission Piping Review Committee. NUREG-1061, U.S. Nuclear Regulatory Commission, Washington, D.C.

NUREG/CR-4387
PNL-5545
RG, R1, R4

DISTRIBUTION

No. of
Copies

OFFSITE

U.S. Nuclear Regulatory Commission
Division of Technical Information
and Document Control
Washington, D.C. 20555

Division of Risk Analysis and
Operations
Office of Nuclear Regulatory Research
U.S. Nuclear Regulatory Commission
Washington, D.C. 20555

A. J. DiPalo (20)
M. L. Ernst
F. P. Gillespie
J. A. Murphy
P. W. Baranowsky
J. C. Belote
J. C. Melaro
G. R. Burdick

Division of Safety Technology
Office of Nuclear Reactor Regulation
U.S. Nuclear Regulatory Commission
Washington, D.C. 20555

A. J. Szukiewicz (10)
N. Anderson
K. Kniel
W. Minners

Idaho National Engineering Laboratory
E. G. G. Idaho, Inc.
Idaho Falls, ID 83415

S. J. Bruske
C. B. Ransom

No. of
Copies

ONSITE

Pacific Northwest Laboratory
W. B. Andrews
W. E. Bickford (10)
A. S. Tabatabai (10)
M. F. Mullen
R. F. Rhoads
J. L. Braitman
Publishing Coordination (2)
Technical Information (5)

NRC FORM 335 (2-84) NRCM 1102, 3201, 3202

U.S. NUCLEAR REGULATORY COMMISSION

BIBLIOGRAPHIC DATA SHEET

SEE INSTRUCTIONS ON THE REVERSE

1. REPORT NUMBER (Assigned by TIDC, add Vol. No., if any)
NUREG/CR-4387
PNL-5545

2. TITLE AND SUBTITLE
Effects of Control System Failures on Transients, Accidents, and Core-Melt Frequencies at a General Electric Pressurized Water Reactor

3. LEAVE BLANK

4. DATE REPORT COMPLETED
MONTH: October YEAR: 1985

5. AUTHOR(S)
W.E. Bickford, A.S. Tabatabai

6. DATE REPORT ISSUED
MONTH: December YEAR: 1985

7. PERFORMING ORGANIZATION NAME AND MAILING ADDRESS (Include Zip Code)
Pacific Northwest Laboratory
Richland, WA 99352

8. PROJECT/TASK/WORK UNIT NUMBER

9. FIN OR GRANT NUMBER
B2386

10. SPONSORING ORGANIZATION NAME AND MAILING ADDRESS (Include Zip Code)
Division of Risk Analysis and Operations
Office of Nuclear Regulatory Research
U.S. Nuclear Regulatory Commission
Washington, D.C. 20555

11a. TYPE OF REPORT
Technical

b. PERIOD COVERED (Inclusive dates)

12. SUPPLEMENTARY NOTES

13. ABSTRACT (200 words or less)

Pacific Northwest Laboratory (PNL) performed probabilistic risk analyses to estimate core-melt frequency and public risk associated with control system failures in a General Electric boiling water reactor. PNL also conducted value/impact analyses of proposed modifications of these control systems to prevent these failures. These analyses were based on failure modes and effects analyses previously performed by the Idaho National Engineering Laboratory (INEL). The control system failure modes identified by INEL and analyzed by PNL fall into three main scenarios: 1) failures that initiate feedwater overfill and also defeat the high level feedwater trip, 2) a failure of the condensate booster pump that results in increased flow to the vessel (overfill), and 3) an inadvertent actuation of the low pressure coolant injection system (LPCI) that also produces an excessive cooldown (overcool). For each of these modes, two failure sequences were postulated. The results of PNL's probabilistic analysis of failure progression to core damage and value/impact analyses of possible resolutions to prevent the occurrence of these failures are presented in this report.

14. DOCUMENT ANALYSIS - a. KEYWORDS/DESCRIPTORS
probabilistic risk analyses
control system failure modes

b. IDENTIFIERS/OPEN ENDED TERMS

15. AVAILABILITY STATEMENT
Unlimited

16. SECURITY CLASSIFICATION
(This page) Unclassified
(This report) Unclassified

17. NUMBER OF PAGES

18. PRICE

NUREG/CR-4387

EFFECTS OF CONTROL SYSTEM FAILURES ON TRANSIENTS, ACCIDENTS, AND CORE-MELT FREQUENCIES AT A GENERAL ELECTRIC BOILING WATER REACTOR

DECEMBER 1985