REVIEW OF RISK BASED EVALUATION OF INTEGRATED SAFETY ASSESSMENT (ISAP) ISSUES FOR MILLSTONE UNIT 1 - PHASE 2

Bahman Atefi
Daniel Gallagher
Phuoc T. Le
and
Paul J. Amico*

August 15, 1985

Prepared for:

U.S. Nuclear Regulatory Commission
Washington, D.C. 20555

Contract No. NRC-03-82-096

*Applied Risk Technology Corporation

Science Applications International Corporation
Post Office Box 1303, 1710 Goodridge Drive, McLean, Virginia 22102, (703) 821-4300

TABLE OF CONTENTS

TABLE OF CONTENTS (Continued)

LIST OF FIGURES

LIST OF TABLES

LIST OF TABLES
(continued)

1.0 INTRODUCTION

In Phase 1 of this study, a brief comparison between the ISAP and IREP studies was presented. This comparison was based on some preliminary and limited information about the ISAP study. Since the completion of the Phase 1 report, a more detailed report on Millstone Unit 1 Probabilistic Safety Study (PSS) (1) has been received.

The objective of the Phase 2 study is to perform a more detailed review of the Millstone Unit 1 PSS and to look more closely into major contributors to the core melt frequency in this study. It is important to note that due to limitations in time and level of effort, the review of the ISAP study is not performed in the traditional sense of a PRA review. Rather, it is done by comparing the results of each major section of this study with the results of the IREP study (2).

Using this comparison, significant differences between the two studies are identified, and the effect of these differences on the dominant accident sequences and overall core melt frequency are analyzed.

In addition to the above comparative review, the major contributors to the ISAP core melt frequency are identified, and a more detailed analysis of a few of these contributors are performed. Areas chosen for a closer look include those where changes in the existing system design or procedures could result in significant reduction in their contribution to the core melt frequency.

In the next section, a comparison between ISAP and IREP initiating events will be presented. This is followed by comments on the event tree analysis in Section 3.0. A brief review of the component and system reliability analysis used in the two studies is presented in Section 4.0. The subject of human reliability analysis is discussed in Section 5.0. The results and insights into major contributors to the core melt frequency is presented in Section 6.0. Finally, all the references are listed in Section 7.0.

2.0 INITIATING EVENTS

The initiating events in both ISAP and IREP studies were grouped in two broad categories of LOCA's (including interfacing system LOCA's) and transient due to anticipated initiators and support system initiators. Each of these broad groups was further broken into subgroups based on the systems required for mitigation of the initiators. A comparision between the initiator categories and frequencies used in the two studies follows.

2.1 LOCA Initiators

In the IREP study the LOCA initiators were grouped into two classes of steam line breaks and liquid line breaks. Each of these classes were further broken down by three break sizes. Table 2.1 shows the LOCA classes, approximate break diameters, systems required for mitigation of these initiators and frequencies assigned to each initiator. As can be seen in this table, the major reason for differentiating between the steam line and liquid line breaks is due to the difference in the systems required for mitigation of the same break sizes. For the small break LOCA, the mitigating systems are the same for the two classes. For the intermediate steam line break, the break would occur above the core level. This will result in an increase in the upward flow of steam, inhibiting the core spray system from providing sufficient downward coolant flow to cover the core. Thus, the core must be depressurized first before core spray system is effective. This is not true about the Low Pressure Coolant Injection (LPCI) system which injects into the core from a low vessel level. Thus, the LPCI system can, without depressurization, cover the core. The situation is reversed in the case of intermediate liquid break. In this case, because the break area is below the core level, the flow out of the core is downward and the core spray function is not inhibited. However, the LPCI system cannot provide the required mitigation function due to slower vessel pressure reduction and flow diversion from the liquid break area unless the primary system is depressurized.

In the case of large LOCA, for the large liquid break, there is too much diversion of the flow out of the break area to make the feedwater

Table 2.1 IREP LOCA Initiators

LOCA Class	Approximate Break Diameter (inches)	Systems Required for Mitigation	Frequency
1. Small Steam Break (SSB)	D<5.41	Feedwater OR ADS* & LPCI OR ADS & Core Spray	10^{-3}
2. Intermediate Steam Break (ISB)	5.41<D<5.90	Feedwater OR LPCI OR ADS & Core Spray	10^{-4}
3. Large Steam Break (LSB)	5.90<D<20.08	Feedwater OR LPCI OR Core Spray	10^{-4}
4. Small Liquid Break (SLB)	D<5.24	Feedwater OR LPCI OR ADS & Core Spray	10^{-3}
5. Intermediate Liquid Break (ILB)	5.24<D<6.05	Feedwater OR ADS & LPCI OR Core Spray	10^{-4}
6. Large Liquid Break (SLB)	6.05<D<32.60	LPCI OR Core Spray	10^{-4}

* Automatic Depressurization System

system an effective mitigating system, whereas in case of large steam break, feedwater system is assured to be an effective mitigating system.

In the ISAP study, the steam and liquid line breaks are not separated. The various break sizes in this study are categorized into four classes of LOCA's as shown in Table 2.2. The most noticeable difference between the two studies is inclusion of a small-small break LOCA with equivalent diameter of greater than 2.5 gallons per minute leak (Technical Specification shutdown limit) up to 1.35 inches in diameter. The initiating frequency of this class of LOCA is an order of magnitude larger than the small break LOCA. In the lower range of this new small-small break category, manual shutdown would be necessary whereas at the higher range automatic trip will occur. In addition, at the lower range of this break, automatic depressurization by the Automatic Depressurization System (ADS) might not occur due to lack of high pressure in the drywell necessary for the initiation of ADS. Thus, manual depressurization (MD) would be necessary in these situations.

Another difference between the two studies is that the inadvertent opening of safety/relief valves in the ISAP study is classified as a LOCA initiator whereas this event was classified as a transient initiator in the IREP. This classification should not have any effect on the actual sequence of events that are delineated for this initiator.

Overall, in classification of LOCA's, the most important difference between the two studies is creation of a small-small break LOCA in the ISAP study. This class of LOCA with a relatively large initiation frequency and some unique mitigation requirements has a significant contribution to the ISAP core melt frequency, as will be shown in Section 6.0 on the overall results. In the case of intermediate and large LOCA's, the major difference between the two studies is the differentiation of liquid and steam break lines. Without this differentiation, the assumptions for systems required for mitigation of a break size might be somewhat more conservative. Finally, in the case of inadvertent opening of S/R valves, the only difference between the two studies is the frequency of initiation of this event which is an order of magnitude smaller in the ISAP study due to replacement of the safety/relief valves with a new set of more reliable valves.

Table 2.2 ISAP LOCA Initiators

LOCA Class	Approximate Break Diameter (inches)	Systems Required for Mitigation	Frequency
1. Small-Small	2.5gpm<D<1.35	Main Feedwater (No Trip) OR Feedwater (Trip) OR ADS/MD & LPCI OR ADS/MD & Core Spray	10^{-2}
2. Small	1.35<D<6.05	Feedwater (Break flow < 3500 gpm) OR ADS & LPCI OR ADS & Core Spray	10^{-3}
3. Inadvertent Operation of Safety/Relief Valve	1.35< D<6.05	Main Feedwater	2.02×10^{-2}
4. Large LOCA	6.05<D	LPCI Core Spray	10^{-4}

2.2 Consideration of Interfacing System LOCA's

In the IREP study, the interfacing system LOCA's were not considered explicitly. The basic reason for this was that in WASH-1400 study, the interfacing system LOCA's were not found to be important to risk in BWR's. The Millstone Unit 1 interfacing systems were compared with Peach Bottom analyzed in WASH-1400, and since the systems were similar, no further analysis of these initiators was conducted.

In the ISAP study, five systems interfacing the primary system were considered in detail for the possibility of initiation of LOCA's. These are Isolation Condenser, Shutdown Cooling System, Reactor Water Cleanup System, Low Pressure Coolant Injection System, and Core Spray System. Of these systems, the Shutdown Cooling System was eliminated from further consideration because only multiple catastrophic failure could create an interfacing LOCA. For the other system, simple fault trees were used to determine the frequency of occurrence of unmitigated LOCA's due to interfacing system failure that would lead to a core meltdown. Table 2.3 shows the unmitigated interfacing system LOCA's, their frequencies, and their contribution to the total core melt frequency. As can be seen from these results, the contribution of interfacing system LOCA's to the overall core melt frequency is negligible.

2.3 Transient Initiators

Two major classes of transients were considered in the ISAP study. These are the anticipated transients and special initiators that result from support system failures. The anticipated transients in this study are grouped into the following five categories:

1. Reactor Transients with Power Conversion System Available
2. Reactor Transients with Power Conversion System Unavailable
3. Reactor Trip Events
4. Loss of Feedwater Events
5. Loss of Normal Power Events.

The first category of transients in the ISAP study is similar to Category T1 "Most Transients" in the IREP study. Table 2.4 shows the list and

Table 2.3 ISAP Interfacing System LOCA Event Frequency

Event	Frequency (per year)	Percentage of Total Core Melt Frequency
1. Unmitigated Isolation Condenser Tube Rupture	1.5E-7	0.02
2. Unisolated LOCA in the Core Spray System	1.1E-7	0.014
3. Interfacing System LOCA in the LPCI System	1.61E-8	0.002
4. Unisolated LOCA in the RWCU System	1.39E-8	0.001

Table 2.4 Comparison Between ISAP and IREP Initiator Frequencies Included in the "Reactor Transients With Power Conversion System Available" - Category 1

Initiator	Frequencies (per year) ISAP (Plant Specific)	IREP NP-801
1. Electrical Load Rejection	0.386	1.04
2. Turbine Trip	0.742	1.41
3. Pressure Regulator Fails Open	0.165	Included in Category 2; see Table 2.5
4. Pressure Regulator Fails Closed	0.009	0.14
5. Turbine Bypass Valve Fails Open	0.089	0.04
6. Recirculation Flow Control Fails (Increasing)	0.011	0.24
7. Recirculation Flow Control Fails (Decreasing)	0.006	0.06
8. Trip on One Recirculation Pump	0.345	0.02
9. Trip of All Recirculation Pumps	0.093	0.06
10. Recirculation Pump Seizure	0.000	ϵ
11. Feedwater Flow Control Failure (Increasing)	0.444	Included in Category 2; see Table 2.5
12. Feedwater Flow Control Failure (Decreasing)	0.630	0.43
13. Loss of a Feedwater Heater	0.004	
14. Loss of All Feedwater Heaters	0.096	0.02
15. Trip of One Feedwater/Condensate Pump	0.176	0.2
16. Inadvertent Control Rod Withdrawal	0.003	ϵ
17. Inadvertent Control Rod Insertion	0.008	0.1
18. Partial MSIV Closure	Included in Category 2; see Table 2.5	0.04
19. Control Valves Fail Closed		0.51
20. Abnormal Startup of Idle Recirc Pump		ϵ
21. Low Feedwater During Startup or Shutdown		0.35
22. High Feedwater During Startup or Shutdown		0.10
23. High Flux Due to Rod Withdrawal at Startup		0.04
24. Scram Due to Plant Occurrences	Included in Category 3; see Table 2.5	0.35
25. Spurious Trip Via Instrumentation, PPS Fault	Included in Category 3; see Table 2.5	1.16
26. Manual Scram is Out of Tolerance Condition	Included in Category 3; see Table 2.5	0.27
27. Detected Faults in RPS	Included in Category 3; see Table 1.6	0.02
28. Cause Unknown		0.02

frequency of transient initiators in this category used in these studies. The initiator frequencies in the ISAP study were calculated by performing Bayesian updating of the plant-specific data. For the prior distribution, the results of industry experience compiled in the EPRI report EPRI-NP-2230(3) was used. In developing the prior distributions from this source, the data on the first two years of each plant's operation was discarded so that the frequency of trips during the startup period was not included in the data base. The data was then fit into a Gamma distribution. Having these prior distributions, the posterior distributions for each initiator were developed by updating the plant-specific initiators.

Looking at Table 2.4, it can be seen that 16 out of 18 top initiators are the same in both categories. Initiators 3 and 11 this ISAP category were included in the "transient with power conversion system unavailable" category in the IREP study. Also, initiators 24 to 28 in the ISAP study were included in a new category of "reactor trip events." The mitigating systems required for this category are exactly the same as Category 1. The frequency of these initiators in the ISAP study is shown in Table 2.5. Initiators 19 through 23 and 28 included in the IREP study were not considered in the ISAP study.

To get an idea of the effect of the Bayesan updating on the initiator frequencies, we can compare the total frequency of the 19 common initiators in Categories 1 and 3. The total frequency of these initiators is 4.46 in the ISAP study and 5.56 in the IREP study. Thus, the ISAP initiators frequency for these categories is about 20 percent lower than IREP frequency in these categories. The total frequency of initiators in this category considered in the IREP and not considered in the ISAP is any category is 1.00 which is another 20 percent of the total ISAP frequency. Overall, the total frequency of the Categories 1 and 3 which have common mitigating systems requirements is 4.58 in the ISAP study and 6.6 in the IREP study. Thus, the total ISAP initiators frequency for these categories is about 30 percent lower than the IREP initiators frequency.

The ISAP Category 2 transients are reactor transients with power conversion system unavailable. The frequency of these intitiators are shown in Table 2.6. In this category, the IREP study included two initiators caused by support system failures. These initiators were treated separately

Table 2.5 Comparison Between ISAP and IREP Initiator Frequencies Included in the "Reactor Trip Events" - Category 3

Initiator	Frequencies (Per year) ISAP (Plant Specific)	IREP NP-801
Instrument Detected Fault in RPS	0.005	Included in T_1; see Table 2.4
Scram Due to Plant Occurrences	0.536	Included in T_1; see Table 2.4
Spurious Trip Due to RPS Instrumentation	1.298	Included in T_1; see Table 2.4
Manual Scram (No Out-of-Tolerance N.S.S.S. Condition)	0.119	Included in T_1; see Table 2.4
Total	1.958	

Table 2.6 Comparison Between ISAP and IREP Initiator Frequencies Included in the "Reactor Transient With Power Conversion System Unavailable" - Category 2

Initiator	Frequencies (Per year) ISAP (Plant Specific)	IREP NP-801
Load Rejection with Turbine Bypass Failure	0.002	
Turbine Trip with Turbine Bypass Failure	0.002	
Total Closure of One or More MSIVs	0.405	0.75
Loss of Normal Condenser Vacuum	0.026	0.67
Feedwater Increasing Flow	Included in Category 1; see Table 2.4	0.31
Pressure Regulator Fails Open	Included in Category 1; see Table 2.4	0.29
Loss of Circulating Water System*		0.06**
Loss of Plant Air Compressors*		0.06**

* Initiators based on support system failure
** Plant-specific data

by the ISAP study and will be discussed in Section 2.4. Excluding these events, the total frequency for this category is 0.435 for the ISAP study and 2.02 for the IREP study. Thus, the ISAP initiators frequency is about 80 percent lower in this case.

The ISAP Category 4 transients are the "loss of feedwater transients" which in the IREP study include two support system initiators and are shown in Table 2.7. Excluding these two events, the loss of feedwater system initiator in the ISAP study is about 60 percent higher than the value in the IREP study.

The fifth ISAP transient category is the "loss of normal power transient" shown in Table 2.8. In this category, the ISAP frequency is about 40 percent lower than IREP frequency.

Finally, as was mentioned earlier in the ISAP study, the inadvertent opening of safety/relief valves was treated as an LOCA initiator. This event was considered as a transient initiator in the IREP study. The frequency of this event is 2.02×10^{-2} in the ISAP study and 0.2 in the IREP study. The primary reason for this difference is replacement of the old safety/relief valves with a newer, more reliable set of valves.

In the next section, transient initiators due to support system failures will be discussed.

2.4 Support System Transients

To identify the plant-specific transient initiators due to support system failures, ISAP study performed a system level failure mode and effect analysis on the following classes of systems:

1. Cooling Water Systems

2. Electrical Systems

3. Power Conversion Systems

4. Auxiliary Systems.

Table 2.7 Comparison Between ISAP and IREP Initiator Frequencies Included in the "Loss of Feedwater Transients" - Category 4

Initiator	Frequencies (Per year) ISAP (Plant Specific)	IREP NP-801
Loss of Feedwater	0.096	0.06
Loss of Turbine Building Closed Cooling Water System*		0.06
Loss of Service Water System*		0.06
Total	0.096	0.18

*Initiators based on support system failure

Table 2.8 Comparison Between ISAP and IREP Initiator Frequencies Included in the "Loss of Normal AC Power Transient" - Category 5

Initiator	Frequencies (Per year) ISAP (Plant Specific)	IREP NP-801
Loss of Offsite Power	0.124	0.16
Loss of Auxiliary Power		0.04
Total	0.124	0.2

As a result of this analysis, four plant-specific initiators were identified. The frequencies of initiation of these events were calculated by a detailed analysis of the support system responsible for their initiation. These frequencies and the corresponding values used in the IREP study are shown in Table 2.9. The IREP initiator frequencies shown in this table are calculated using a zero failure approximation. Overall, for the support system initiators analyzed in both studies, the ISAP frequencies are from one to two orders of magnitdue smaller than IREP frequencies based on a more detailed support system analysis. The only exception is the service water system where change in its success criteria in the ISAP study has resulted in an increase in the short-term loss of service water system initiating frequency.

In the next section, a discusssion on the event-tree analysis used in the ISAP and IREP studies will be presented.

Table 2.9 Comparison Between ISAP and IREP Support System Initiator Frequencies

Initiator	Frequency (Per year) ISAP	IREP	Comments
Total Loss of Service Water (With Recovery)	7.83E-3	6.0E-4*	Included in T_3 in IREP, see Table 2.7
Loss of T.B.S.C.C.W.	8.05E-4	0.06	Included in T_3 in IREP, see Table 2.7
Loss of R.B.C.C.W.	4.73E-4	-	
Loss of 120 V Vital AC Power	1.65E-2	-	
Loss of Circulating Water System	-	0.06	Considered part of transients with PCS in ISAP
Loss of Plant Air Compressors	-	0.06	Considered bounded by other transients in ISAP

* This number consists of an initiating frequency of 0.06 and a recovery factor of 1.0×10^{-2}.

3.0 EVENT TREE ANALYSIS

The event tree analysis performed in the ISAP study has a number of differences from that performed in the IREP study. Some of the differences are conceptual and apply in general to all of the event trees, while others are more specific to a particular tree. The conceptual differences will be discussed here, and the specific differences will be discussed in subsequent sections.

The first difference is that the ISAP study included cognitive operator errors directly on the event trees. These are errors in the decision-making process during an accident. The IREP study did not individually assess these cognitive errors, but rather included them in the assessment of procedural errors. From the standpoint of event tree analysis, this difference in methodology is not significant to the final results. When these errors are properly evaluated, it makes no difference whether they are included independently on the tree or are incorporated at the system level. However, the method of analysis utilized for the human error rate determination in the ISAP study is significantly different from that used in the IREP study. This is discussed in more detail in Section 5.0 on human reliability analysis.

The ISAP study also included recovery actions (such as restoration of offsite power) as events on the event trees. In the IREP study, these actions were evaluated separately and incorporated into the analysis at the sequence cut set level. This difference is not significant to the analysis, since (as above) either method adequately incorporates the actions evaluated.

The ISAP study did not make a distinction between short-term core melts with and without containment cooling. That is, no credit was given for the operation of the containment cooling system to delay containment failure given that a core melt was occurring in the early or intermediate time frames. IREP did make this distinction. This does not affect the results of the ISAP study in terms of core melt frequency and timing, since the containment cooling system cannot prevent core melt in these scenarios. The only effect is in the area of plant damage states and consequences. This is an insignificant difference between the two studies, because the IREP study

determined that all of these sequences would have the same consequences whether or not containment cooling was successful (i.e., the release category split fractions were the same in both cases).

The following sections discuss specific differences in the event trees in the ISAP study and those representing the equivalent initiators in the IREP study. However, before beginning those discussions, it is useful to make a general observation regarding the ISAP study event trees versus the IREP study event trees. Despite the differences in appearance between the two sets of trees, the phenomenologies represented are virtually identical. That is, the functional and systemic failures leading to core melt are the same in both studies. This becomes obvious when one attempts to identify equivalent sequences from both studies. It is generally possible to select any sequence from the ISAP study and identify an equivalent sequence (or sequences) which were analyzed in the IREP study, although the details of the quantification may be different. This exercise is performed in Section 6.0 for the dominant ISAP sequences and is discussed in some detail in that section. The one major exception to this is the anticipated transients without SCRAM (ATWS), which are quantified significantly differently in the two studies. This is discussed in detail in Section 3.4.

3.1 Reactor Transients Event Tree

The ISAP study event tree includes a cognitive error of the operator failing to decide to restore RPV level when the feedwater system fails to continue to operate after the trip. This error encompasses the entire decision process of attempting to restore feedwater, initiating the isolation condenser, or depressurizing the RCS and using low pressure safety pumps, thus creating a linkage between the actions. The IREP study evaluated each of these alternatives to provide cooling; however, they were considered separate actions. This is a significant difference between the two studies which can result in substantial differences in human error and recovery actions, as will be discussed in Section 4. This difference in methodology is due in part to Millstone's change to a new type of symptom-oriented procedures and in part to advances in the methods available to analyze cognitive errors which have been developed since the IREP study. This is discussed in more detail in Section 4.

The ISAP study event tree also includes an event for restoration of AC power. This is included for the purpose of evaluating support states involving a consequential loss of power following a non-LNP event. As discussed in Section 3.4, this was not analyzed in the IREP and has a measurable effect on the results.

3.1.1 Loss of Feedwater Event Tree

The same comments as those made above apply also to this tree, except that the cognitive error applies to those sequences where either the isolation condenser fails or a safety/relief valve sticks open, thus requiring the operator to decide to restore RPV level.

3.1.2 Loss of Normal Power (LNP) Event Tree

The ISAP study event tree considers a cognitive error of failing to decide to restore reactor pressure vessel level as an error which is similar to the failure to manually depressurize the reactor coolant system (RCS), which is evaluated in the IREP study. The difference is that in the ISAP study, this error is considered to occur prior to reaching automatic safety actuation conditions, and it includes the decisions to manually start the isolation condenser and to attempt to restore offsite power, even though the Isolation Condenser (IC) will eventually start automatically and the operator has additional time to actually recover offsite power. This particular handling of this cognitive error, while different from the IREP, yields a logically identical model and thus does not affect the results.

The ISAP event tree includes an event for cross-connecting the 480v safety busses so that one of the emergency power supplies can pick up some loads from the opposite train. This action only affects the availability of shutdown cooling, and only in a minor way. It does not have any significant effect on the results.

The ISAP study event tree also includes an event for the recovery of offsite power, which was adequately considered in the IREP study at the sequence cut set level. However, a notable difference is that the IREP study assumed that recovery of offsite power terminated the sequence successfully. The ISAP study, however, models the other actions necessary

to initiate the systems required to actually terminate the sequence. This is a more detailed and accurate method than the IREP assumption, which was based on the belief that these scenarios were unlikely once power was restored. This difference does have an effect on the results.

The ISAP study event tree has an event which represents the actuation signal required for the plant to automatically respond to the loss of normal power event. This was handled in the fault tree models in IREP study, rather than at the event tree level. Both methods are adequate if properly applied, which is the case.

3.1.3 Station Blackout

This tree is just a specific version of the LNP tree to cover the case where all AC power is unavailable. Thus, the comments discussed above for the LNP apply similarly to this tree, with two minor modifications.

First, the cognitive decision process includes the additional decision to conserve DC battery power by stripping of nonessential DC loads. This was not considered in the IREP study, but did not effect the results.

Second, the tree considers sequences where the core is damaged but does not melt. This occurs in time frames where the power is not restored in time to prevent the core from briefly becoming uncovered but power is restored prior to significant uncovery. The IREP study did not make this distinction, but it is not important unless one is interested in the possibility of minor core damage. The time frames used for preventing core melt are similar to those used in the IREP study, whereas the time frames used for preventing damage are somewhat shorter. Thus, there is no effect on the core melt sequences.

3.2 Support System Initiator Event Trees

These event trees are subsets of the transient and loss of feedwater event trees. They are designed specifically to take into account the changes in system capabilities due to these initiators. The differences discussed for the transient and LOF event trees therefore generally apply to these trees. Otherwise, there is nothing notable about these trees and, in

fact, it would have been equally reasonable to utilize the transient and LOF trees to evaluate these initiators.

3.3 Loss of Coolant Accident (LOCA) Event Trees

The LOCA event trees in the ISAP and IREP studies are fairly similar except for the new ISAP event tree for the small-small break LOCA which is discussed in the next section.

3.3.1 Small-Small Break Event Tree

This ISAP event tree, which is used for the lower end of the IREP small break size, has a number of differences from the IREP small break event tree. The first difference is that automatic pressure relief does not appear on the tree. ISAP concluded that these breaks are too small to result in high drywell pressure, so only operator action to depressurize is considered. This seems to be a reasonable conclusion and was missed in IREP because IREP only considered break size ranges analyzed in the FSAR, which did not separately consider these break sizes. Intuitively, however, it is logical that there should exist breaks which are small enough that high drywell pressure would not occur. This difference had an effect on the results of the analysis.

Another difference is that ISAP concluded that feedwater could not continue to run indefinitely without some operator intervention. The operator is required to start a high-capacity condensate transfer pump to replenish the hotwell to provide sufficient suction water for feedwater. This is required to replace water lost through the break. IREP concluded that sufficient water would be supplied automatically by the condensate transfer system (CTS); however, only a small capacity CTS pump will start automatically to replenish the hotwell. Thus, an additional branch appears on the tree for the required action of manually starting a higher capacity pump (including the reliability of the CTS equipment). This difference had an effect on the results.

A third difference is the consideration of a cognitive error of failing to realize it is necessary to recover RPV level when FW is failed. This includes the same actions as the one discussed for the transient trees, and

links together all actions possible to recover level. As mentioned before, this has a significant effect on the results.

ISAP also considers a cognitive error of commission, that of the operator misdiagnosing plant conditions and prematurely terminating ECCS flow. This type of error was not considered in IREP, and it has an effect on the results. It is discussed in greater detail in Section 5.0 on human reliability analysis.

Finally, the ISAP tree has branches for successful long-term cooling using the main condenser or shutdown cooling (SDC) systems. IREP did not give credit for these cooling methods because they normally require that the vessel be isolated so that no coolant is lost. However, it is conceivable that these methods may work for the very small breaks which make up this break range. This is especially true when using the SDC system, where it is reasonable to assume that the SDC system can cool water taken from the vessel and return it to the vessel while the vessel level is maintained by circulating torus water through the core spray or LPCI systems to make up for continued coolant loss through the break. All that would be required is that adequate mixing take place in the vessel, which is a reasonable assumption. The use of the main condenser is somewhat more questionable. While it should be possible to remove some heat in this manner, it is not clear how steam flow to the condenser would be maintained. Once the decay heat level was below the heat removal rate of the break, it is logical to assume that all steam would be dumped to the torus, since this should be the path of least resistance. The question of how long this would take and whether a core melt would result must remain open until the basis for the ISAP assumption can be reviewed. However, the assumption does affect the results, and its elimination would increase the contribution of small-small breaks to core melt.

3.3.2 Small and Large Break Event Trees

There are two major differences between the ISAP trees for these initiators and the equivalent IREP trees. First, both trees contain the cognitive error of commission (premature termination of ECCS flow) mentioned in the previous section. For these initiators this difference does not have any significant effect on the results.

The second difference is that feedwater is not considered to be a sufficient mitigating system in ISAP for these breaks. This is based on the inability, even with manual action, of the condensate transfer system (CTS) to provide sufficient makeup flow to the condenser hotwell for breaks of these sizes. Thus, feedwater is assumed to be lost in a relatively short time. The IREP study assumed that CTS flow was sufficient, except for large liquid breaks, based on the Millstone FSAR. Regardless, this difference did not have a significant effect on the results, and further investigation is therefore not warranted.

3.4 ATWS Event Tree

There are significant differences in the way each of the two studies evaluates ATWS events. The IREP study assumed that an ATWS always resulted in a core melt, except for transients where the power conversion system (PCS) was available and continued to operate. Much study has been done on ATWS since that time, by both the NRC and the nuclear industry, and a much greater understanding of ATWS events has been attained. This understanding has allowed for the modification of plant design and development of new procedures to mitigate ATWS events. The present NRC position on ATWS is contained in the recently developed ATWS rule added to 10CFR50. It is more fruitful to compare the ISAP study evaluation with the analysis in the rule as opposed to that from the IREP study, since the former represents more advanced thinking on ATWS.

The ISAP study considers two general cases of ATWS: condenser (PCS) available and PCS unavailable. This is consistent with the ATWS rule. Each case will be considered separately.

For the PCS available case, the ISAP study deviates from the rule in that it assumes that operator actions are not as complex or imperative as the rule states. It takes substantial credit for the ability of the PCS to maintain automatically adequate heat removal for an extended period once the recirculation pumps are tripped. This is reasonable for the Millstone 1 plant. The need for complex operator actions in a short time frame in the ATWS rule is based on certain assumptions in the rule, as follows:

"It has been estimated that power will equilibriate at around 20 to 40 percent of full power...A BWR is typically designed to bypasss up to 25 percent of steam flow to the condenser. Thus, if the ATWS transient has not involved MSIV isolation or loss of condenser, a maximum of 15 percent of steam flow will be directed to the suppression pool."

It is this loss of steam to the suppression pool which is the limiting condition for the operator actions in the ATWS rule. However, Millstone 1 is not a typical BWR. Its bypass capability is 100% of steam flow; thus, there would be no loss of steam to the suppression pool. For this reason, we conclude that the ISAP event tree for ATWS with PCS available is acceptable despite its deviation from the ATWS rule.

For the PCS unavailable case, the ISAP study and the ATWS rule are in general agreement on the basis behind the mitigation of an ATWS. That is, they both consider the limiting condition for success to be the 200° F torus temperature limit. Also, the operator actions in the ISAP study are the same as those described in the rule. They deviate in the capability of the standby liquid control system (SLCS) to mitigate the ATWS. Specifically, the ATWS rule states the following:

"For these cases where all of the reactor power is dissipated in the suppression pool, the suppression pool temperature would exceed 200° F slightly even if the operator immediately followed the procedures and actuated the [43 gpm] SLCS. If SLCS capability is increased to 86 gpm, the operator must act within two minutes after the transient begins in order not to exceed the 200° F suppression pool limit. Therefore, it was conservatively assumed that all isolation transients will exceed the 200° F containment suppression pool limit with the current SLCS capacity of 43 gpm."

Thus, an event tree based on the ATWS rule would not have a success branch for SLCS because it is assumed to have insufficient capacity. However, it is important to note two things. First, the rule used the word "conservatively" to describe its assumption. Further, the analysis is apparently based on a "typical BWR." Once again, Millstone 1 is not typical. Its suppression pool is the same size as typical BWR-4s, but its core power is only about 60% of a typical BWR-4. Thus, Millstone 1 has a greater

heat rejection capability (in terms of equivalent full power seconds before exceeding 2000 F). Therefore, it may be possible that a 43 gpm SLCS is sufficient for Millstone 1. For the present, however, we must reserve judgment until we can review thermal/hydraulic calculations of this sequence to determine if this is so and how long the operator has to initiate SLCS. If a 43 gpm SLCS is not sufficient, ATWS will become a more significant contribution to core melt, assuming all other conditions remain the same (which they do not; see RPS analysis comments in Section 4.2, operator response comments in Section 5.2, and ATWS summary in Section 6.3).

3.5 Inclusion of Support Systems in Event Tree Quantifications

The ISAP study used an entirely different method from the IREP study to consider the effect of support systems on the sequences. In the IREP study the support system fault trees were merged with the front line system fault trees to create complete fault trees for the front line systems which include all potential support system faults. In the ISAP study, the support systems were evaluated separately and a support system event tree was used to define support states. These support states define the possible combinations of support system success and failures which can exist following an initiating event. Thus, each event tree is actually evaluated a number of times (once for each support state), and the system failure probabilities used are conditional on the support state being evaluated.

The review of the ISAP support states and the front line systems showed that the system interfaces modeled in the IREP study, as modified by actual plant changes, are adequately represented in the ISAP analysis.

The significant difference between the two support system interface models is that the ISAP study considered the subsequent loss of AC power after a non-LNP initiating event. The IREP study did not consider this possibility. The support states that result from this subsequent loss of power on either emergency bus do contribute to three of the ISAP study dominant accident sequences, all reactor transient initiated sequences. Two of these sequences would not have been dominant sequences if the subsequent loss of power support states had not been considered. The total contribution of these two sequences is approximately 5% of the total core melt frequency calculated in the ISAP study.

4.0 PLANT SYSTEMS RELIABILITY ANALYSIS

This section provides a brief review of both the component failure data used and the system reliability analysis performed in the Millstone 1 ISAP study. The review of the component unavailability data consists of a comparison of the data used in the ISAP study with that used in the Millstone 1 IREP study. No other attempt has been made to verify the accuracy of the plant-specific data used in the ISAP study. The review of the system reliability analysis was also primarily a comparison of the ISAP study system models to those used in the IREP study. This comparison was limited to a comparison of the success criteria, support system interfaces, and system descriptions in the two studies. A detailed review of the system fault trees used in the ISAP study was not peformed. However, the system unavilabilities used in the ISAP study were assessed for their reasonableness based on information that could be extracted from the Millstone 1 IREP study.

4.1 Component Failure Data

The Millstone 1 ISAP study applies Bayes Theorem to a combination of generic data and plant-specific data to develop the failure rate data used in the study. WASH-1400 was selected as the generic data source. The demand failure data in WASH-1400 was assigned a Beta distribution to generate prior means and variances; a Gamma distribution was assigned to the hourly failure data. The means and variances were then modified using the plant specific data by applying Bayes Theorem.

The Millstone 1 IREP study used WASH-1400 data almost exclusively. The only failure data not taken from WASH-1400 were for components not specifically identified in WASH-1400 or components where plant data justified using a plant-specific failure probability instead of the generic data. (All of the components found to be significant contributors to the IREP study dominant accident sequences were modeled using generic WASH-1400 data.)

Table 4.1 lists the failure data used in the two studies for significant components, i.e. those components whose failures are important contributors to the core melt sequences.

Table 4.1 COMPARISON OF IREP AND ISAP COMPONENT FAILURE DATA

COMPONENT	FAILURE ON DEMAND (MEAN)	
	ISAP	IREP*
MOV (Outside Drywell)		
Fail to open	4.45E-3	1E-3+
Fail to close	3.00E-3	1E-3+
MOV (Inside Drywell)		
Fail to open	3.79E-3	1E-3+
Fail to close	4.90E-3	1E-3+
ECCS check valves		
Fail to open	1.15E-4	1E-4
Fail to close	6.60E-4	--**
Feedpump check valves		
Fail to close	2.29E-3	--**
All electric motor-driven pumps		
Fails to start	-	1E-3
Fails to run	-	9E-5/hr
ECCS Pumps		
Fail to start	7.48E-4	
Fail to run	7.99E-5/hr	
Service Water Pumps		
Fail to start	7.89E-4	
Fail to run	3.81E-5/hr	
Emergency Service Water Pumps		
Fail to start	6.41E-3	
Fail to run	7.99E-5/hr	

* Ref. "IREP-Analysis of the Millstone Point Unit 1, NPP" Vol. 1; Table 7.1 a,b. Data given were based on monthly testing, except where noted IREP used median values, data has been converted to mean values.

** Not modeled in the IREP Study.

\+ A value of 1.6E-2 was used for components tested only during refueling outages, test interval was assumed to be 12,000 hrs.

Table 4.1 COMPARISON OF IREP AND ISAP COMPONENT FAILURE DATA
(Continued)

COMPONENT	FAILURE ON DEMAND (MEAN)	
	ISAP	IREP*
R.B.C.C.W. Pumps		
Fail to start	9.24E-4	
Fail to run	9.71E-6/hr	
Shutdown Cooling Pumps		
Fail to start	2.84E-3	
Fail to run	9.59E-6/hr	
T.B.S.C.C.W. Pumps		
Fail to start	9.67E-4	
Fail to run	1.02E-5/hr	
Feedwater Pumps		
Fail to start	9.48E-4	
Fail to run	1.46E-6/hr	
Condensate Booster Pumps		
Fail to start	1.66E-3	
Fail to run	5.05E-5/hr	
Condensate Pumps		
Fail to start	1.07E-3	
Fail to r	8.60E-7/hr	
Emergency Condensate Tranfer Pumps		
Fail to start	1.12E-3	
Fail to run	7.99E-5/hr	
C.R.D. Pumps		
Fail to start	1.57E-3	
Fail to run	1.58E-6/hr	

* Ref. "IREP - Analysis of the Millstone Point Unit 1, NPP" Vol. 1; Table 7.1 a,b. Data given were based on monthly testing, except where noted IREP used median values, data has been converted to mean values.

Table 4.1 COMPARISON OF IREP AND ISAP COMPONENT FAILURE DATA
(continued)

COMPONENT	FAILURE ON DEMAND (MEAN) ISAP	IREP*
Diesel-Driven Fire Pumps		
Fail to start	4.77E-2	
Fail to run	7.97E-4/hr	
Motor-Driven Fire Pumps		
Fail to start	1.13E-3	
Fail to run	7.99E-5/hr	
4.16KV Breakers		
Fail to operate	1.34E-4	1E-3+
480V Breakers		
Fail to operate	6.14E-4	1E-3+
Diesel Generator		
Fail to start	6.71E-3	3E-2
Fail to run	1.12E-3/hr	9E-3
Gas Turbine Generator		
Fail to start	4.80E-2	3E-2***
Fail to run	1.97E-3/hr	9E-3
Battery Charger		
Fails to operate	1.02E-5	--

+ A value of 1.6E-2 was used for components tested only during refueling outages, test interval was assumed to be 12,000 hrs.

*** Gas Turbine Generator failure probability was found to be similar to that of Diesel Generator - (Ref. "IREP - Millstone Point Unit 1"; Vol. 1, pg. 7-2.

For most components, the differences between the data used in the two studies are not significant. There are only three component failures where the differences in the data significantly impacted the quantification of the dominant accident sequences. The failure probability used for AC breakers is significantly lower in the ISAP study than in the IREP study, particularly for 4160V breakers. The ISAP study also used a significantly smaller failure probability for the diesel generator failure (both failure to start and failure to run) and for the gas turbine generator failure to run once started. All of these reduced failure probabilities would reduce the impact of loss of normal power (LNP) accident sequences. These failure probability reductions are a significant reason that the LNP sequences are not as dominant in the ISAP study as they are in the IREP study.

The differences in the remaining component failure probabilities are either insignificant or affect components that do contribute significantly to dominate accident sequences.

4.2 Plant Systems Reliability Analysis

The review of the plant systems reliability analysis performed in the Millstone 1 ISAP study was limited to a review of major differences found between that study and the Millstone 1 IREP study. The system descriptions in the two studies were compared with particular emphasis on system success criteria and the systems dependencies, i.e. support system interfaces.

A detailed analysis of the fault trees was not possible during the time available for the review. However, in some cases changes in the plant design which impacted this part of the analysis were identified. Differences in the identification of systems used in each study are also noted but not necessarily discussed in detail here.

There are two systems where differences in the success criteria used in the ISAP and IREP studies have resulted in significant changes to the calculated system reliabilities. The most important difference is in the success criteria for the Alternate Shutdown Cooling (SDC) System which is the Containment Cooling (CC) made of operation of the Low Pressure Coolant Injection (LPCI) system (referred to as LPCI/CC in the Millstone 1 IREP study). This system is one of the long-term cooling systems and uses the

Emergency Service Water (ESW) system to remove decay heat. The LPCI systems is a two-train system with each train consisting of two pumps and a single heat exchanger (used only in the containment cooling mode). The ESW system consists of two trains with each train consisting of two pumps. Each ESW system train supports only one LPCI train, i.e. two ESW pumps provide flow to one LPCI system heat exchanger; the other two provide flow to the second heat exchanger. The success criteria used in the IREP study for these systems were one LPCI pump operating with the corresponding heat exchanger and one of two corresponding ESW pumps operating. The ISAP study success criteria for these two systems are much more stringent. The ISAP study assumes that one LPCI pump in each train is required and both heat exchangers are needed. To remove the decay heat, the ISAP study uses a success criteria that requires all four ESW pumps to operate. This change in the success criteria results in a much higher alternate SDC system failure probability in the ISAP study than in the IREP study. The system failure probability used in the ISAP study is nearly two orders of magnitude larger than that used in the IREP study. (No system failure probabilities were provided in the IREP study. The change in system failure probabilities is based on estimated values for the systems on the IREP study. These estimates are derived from the IREP study sequence quantification.) The differences in the system success criteria account for nearly all of the two orders of magnitude difference in system failure probability.

The second system for which different success criteria were used in the two studies is the Service Water System (SWS). In the IREP study system reliability analysis, the success criteria for the SWS, under all conditions, requires one of the four SWS pumps to be operable. In the ISEP study, the SWS success criteria are sequence dependent. For most sequences, two of four SWS pumps are required, but for the Loss of Normal Power (LNP) sequences the SWS success criteria used were either two pumps operable or one pump operable and valve SW-9 must close. (The closure of this valve sheds loads from the SWS.) This change in system success criteria does not appear to have made a significant difference in the results of these two studies except for the frequency of initiation of a loss of service water transient. The impact on the initiator frequency is discussed in Section 2.5.

Some minor differences in the support system interfaces used in the two studies were also found. Neither of the differences would appear to make a significant difference in the results of the studies.

In the shutdown cooling (SDC) system, the ISAP study shows a support system interface where the loss of either DC bus (101A or 101B) would result in the loss of the SDC system. The IREP study model of the system indicated that failure of either DC bus would disable only half of the SDC system. Since the support states where one DC power train is lost do not contribute significantly to the ISAP study results, this difference in support system requirements does not appear to be significant.

The second difference in support system requirements affects the SWS. In the ISAP study, the valve that is required to close on an LNP, SW-9, is modeled as being powered from one of the two main AC power trains. In the IREP study, this valve is modeled as being powered from a bus that could be energized by either of the two AC power trains (a normal supply with an automatic transfer to a backup supply). This difference does not appear to significantly affect the results of either study.

Other than these two differences, the modeling of the support system interactions in the two studies is in agreement with each other. The differences in methodologies, support states versus merged fault trees, has not resulted in differences in the results of the studies. (The different methodologies did result in differences in the way some support systems were modeled). In the IREP study, there was only one AC power fault tree that included vital and instrument AC, and the actuation logic for the ECCS was included in each system fault tree. In the ISAP study, separate support system fault trees were produced for vital AC, instrument AC, and the actuation logic. These differences did not impact the study results.

At least two equipment changes have been made at Millstone 1 since the IREP study that were incorporated into the ISAP study. A change in the LNP reset logic was incorporated that would reduce significantly the impact of logic failures. These logic failures were a significant contributor to the IREP study dominant accident sequences. This modification reduces the importance of LNP initiated sequences in the ISAP study. The second modification was to the makeup valve (ICM-10) to the isolation condenser.

The power supply to this valve was changed from AC power to DC power greatly increasing the reliability of the isolation condenser makeup system, especially during an LNP event. This modification would also reduce the importance of several IREP study LNP sequences.

Finally, the reactor protection system (RPS) was modeled differently in the two studies. The ISAP study used a demand failure probability of approximately 5 E-5 based on a Bayesian analysis using historical data as of 1979. This is an old analysis and is probably quite conservative. The IREP study used a value of approximately 1E-5 based on detailed fault tree analysis of system. Common cause mechanical failure was dominant, and there was no contribution from electrical failures. The NRC's ATWS rule (10 CFR 50) agrees with the IREP study in that a 1E-5 RPS failure probability is a reasonable estimate for the mechanical failure contribution. (This excludes an additional 2E-5 contribution for electrical failure of the RPS for the RPS design existing at the time of the IREP study. If a plant has alternate rod insertion (ARI), the rules state that these electrical contributions are eliminated. Millstone Unit 1 now has ARI.) It would appear that the ISAP study used a conservative estimate for its RPS failure probability. The impact of this and other competing factors on the ATWS frequency is discussed further in Section 6.3.

5.0 HUMAN RELIABILITY ANALYSIS (HRA)

There are significant differences between the HRAs performed in the IREP study and the ISAP study. In particular, two areas are most significant. First, ISAP separately considered cognitive errors, which are errors in diagnosing and interpreting plant conditions and deciding (in a conceptual sense) what actions are appropriate. In IREP, these types of errors were not explicitly isolated. At the time of IREP, the only useful tool for quantifying human error was the Technique for Human Error Rate Prediction (THERP) (4), a technique which allowed for detailed modeling of procedural-type errors on a step-by-step basis. It considered the concept of decision making errors only as it applied to certain steps within a procedure. Since that time, new understanding of the cognitive errors has been gained, allowing for the quantification of the decision making process from an overall diagnosis of plant conditions outside of the step-by-step procedures. The consideration of cognitive errors in this manner is a major advance in HRA, and is generally recognized by experts as being a vast improvement over THERP. It should be noted that THERP is still recognized as the state of the art for evaluating strictly procedural errors. Two useful tools have been developed for the quantification of cognitive errors: the Time-Reliability Correlation (TRC) model (5), and the Systematic Human Action Reliability Procedure (SHARP) model (6). ISAP makes use of both of these modeling techniques. The use of cognitive modeling in ISAP has a significant effect on the results when compared with IREP. We believe the ISAP methodology is more reasonable.

The second significant difference between the two studies is also related to a change which has taken place since IREP. Millstone has converted its procedures to a new type called "symptom oriented procedures." These procedures are more concise, more understandable, and easier to follow than the procedures which existed at the time of IREP. Thus, procedural errors are less likely to occur during certain key operator actions. This has a significant effect on the ISAP results. In most cases, ISAP has considered procedural errors in addition to cognitive errors. That is, the probability of failing to properly perform the manipulations required (procedural error) was evaluated given that the operator has properly diagnosed the situation (cognitive success). Generally, these errors are incorporated directly into the system failure rate determinations. A significant

exception to this, which is discussed in more detail later, is the ATWS analysis. For some reason, procedural error was not considered despite the rapid and complex nature of the actions required.

5.1 Cognitive Error Modeling

The ISAP study explicitly models cognitive errors of decision-making. This was not done in IREP. These errors represent the incorrect decisions of the operator based on his misunderstanding of plant conditions. This results in the operator failing to enter the appropriate emergency operating procedure (EOP). In IREP, the only operator errors of this general type which were considered were whether the operator correctly read the instrumentation. That is, if he correctly read the meter/annunciators, it was assumed that he entered the correct procedure. Cognitive error modeling accounts for the addition of the possible error that the operator could fail to correctly interpret the instrumentation even if he reads it correctly. Additionally, the cognitive error concept tends to link together actions which were formerly thought to be relatively independent; i.e., the concept considers that if the operator fails to understand the plant conditions he may take no actions whatever. In the case of the ISAP study, this is particularly important because of the format of the new Millstone 1 procedures. The procedures in force at the time of IREP could be very complex and confusing; however, they had a certain amount of independence in that the operator might take an action to restore a system, even if he thought he didn't need to, just because it was unavailable. The new, symptom oriented procedures are much easier to comprehend and follow, but they are very proscriptive about what the operator should do for a particular plant symptomatic condition. Thus, if the operator fails to correctly interpret the plant condition, he would be set off on a series of tasks or a course of nonaction which would fail to aid his situation. In all, the addition of explicit cognitive error modeling and the switch to symptom oriented procedures has been a significant reason for differences between the IREP and ISAP PRA results.

As mentioned previously, the ISAP study utilized two cognitive modeling techniques for quantifying human reliability: SHARP (6) and TRC (5). The next two sections discuss these techniques and the cognitive errors modeled by each.

5.1.1 Time-Reliability Correlation (TRC) Model

A TRC model determines the probability of the operator failing to make a correct decision based on the amount of time the operator has available. The basic premise of the model is that the driving factor in the decision process is how long the operator has to think about it. Further, this factor is generally independent of other factors and constitutes a reasonable basis for selecting a screening human error probability (HEP). In order for an analyst to determine the HEP for a particular decision, he need only determine how long the operator has to take action and pull the corresponding probability off of a time vs. HEP curve. Such curves have been developed by human reliability experts and are published in a number of reports. The ISAP study used a curve from NUREG/CR-3010 (5, Figure 5-2) for quantification.

ISAP used the TRC for evaluating cognitive errors where the amount of time for making the decision exceeded about ten minutes. Five errors were evaluated in this way. These errors are shown in Table 5.1. For those actions which were related to scenarios considered in IREP, the times used in the ISAP study are generally reasonable. For the actions of initiating emergency condensate transfer and conserving batteries (not considered in IREP) the basis for the time frames appear reasonable. It is worth noting, however, that the HEP values used, although taken from an NRC report, do not correspond with the preferred screening values from NUREG/CR-2815, the PSA Procedures Guide (7). The right hand column of Table 5.1 gives the values which would be obtained if the TRC curve from that report is used. These values are significantly higher and could affect the results of the analysis.

After careful consideration, we have determined that the NUREG/CR-3010 curve used in ISAP is inappropriate for the type of analysis performed. The screening curve from NUREG/CR-2815 should have been used. There are two major reasons for this.

First, the NUREG/CR-3010 curve was developed by a single team of analysts from one organization. Although it is singled out in the report and used in the examples, it is actually only one of several curves discussed in the report. The NUREG/CR-2815 curve, on the other hand, is a

Table 5.1
Human Errors Evaluated Using the
Time Reliability Correlation

Error Description	Time Avail	ISAP HEP	NUREG/CR-2815 HEP
Operator fails to decide to restore IC makeup (IC operating)	50 min.	4.5 E-4	2E-3
Operator fails to recognize the need to initiate emergency condensate transfer during small-small LOCA w/FW available	40 min.	7.0 E-4	3E-3
Operator fails to recognize the need to manually depressurize during a small LOCA (manual backup to auto actuation)	10 min. (FW operating)	1.5E-2	0.5
Operator fails to recognize the need to conserve DC batteries by shedding non-essential loads during blackout	50 min.	4.5E-4	2E-3
Operator fails to recognize the need to restore RPV level during stuck-open S/RV event	20 min.	3.5E-3	0.1

consensus curve based on multiple information sources and represents the consensus of a multi-organizational group of experts.

Second, it is apparent from the discussion in NUREG/CR-3010 that the curve selected for use in the ISAP study is not intended for use in a screening analysis. Rather, the use of this curve assumes a detailed human reliability analysis, specifically, the development of an operator action tree (OAT) to represent overall operator response. Additionally, when using this curve it is necessary to specifically evaluate the "thinking time" interval based on the following equation:

$$t_T = t_0 - t_I - t_a$$

where

t_T = Thinking time

t_0 = Overall time from the initiation of an accident sequence to the point by which actions must be completed.

t_I = The time after initiation at which appropriate indications or other clues are given.

t_a = The time it takes to implement the actions decided upon.

This must be done because this curve represents the HEP as a function of thinking time alone. A further consideration when using this curve is the inclusion of modifications to the HEP due to other effects, such as reluctance factors. The ISAP study did not perform these detailed analyses, which should accompany the use of this curve.

On the other hand, the NUREG/CR-2815 curve was specifically intended as a screening curve. Thus, none of the above considerations are necessary when values are used from this curve. Therefore, this curve is much more appropriate for the simplified analysis performed in the ISAP study.

As mentioned above and shown in Table 5.1, the values obtained using NUREG/CR-2815 are significantly higher than used in ISAP. The use of these higher values may affect the ISAP results. Further investigation will be necessary to determine if this is significant.

5.1.2 Systematic Human Action Reliability Procedure (SHARP)

The SHARP method of cognitive error quantification differs from the TRC method in the selection of the driving factor behind human performance. Whereas the TRC method considers the time available as the driving factor, the SHARP method considers the type of action and the expected behavior. SHARP is therefore a time-independent model. The screening process used in ISAP calls for generating human error probabilities based on the type of action and the expected behavior.

In this model, three human behavior categories are defined. These are: skill-based, rule-based and knowledge-based behavior. The classification of each human action in the ISAP study into one of these categories is based on the following definitions:

- The behavior can be classed as skill-based if the operator is well trained, is motivated to perform the task, and has experience in performing the task.

- The behavior can be classed as rule-based if the operator has a clearly understood set of rules to follow in responding to a well-understood transient or situation.

- The behavior can be classed as knowledge-based if the above do not apply or the operator must understand the condition of the plant, interpret some of the instrument readings, or make a difficult diagnosis.

Figure 5.1 is a reproduction of Figure 4.2-3 of the Millstone Unit 1 PSS. This figure shows the logic that was used by each analyst in classification of different human action into one of the above categories. This guideline was used so that the classification done by different analysts is performed in a consistent manner. It should be noted, however, that a certain amount of "analyst creativity" is required in using this logic tree. For example, a nonroutine operation which is covered by a well written, understandable procedure might still be classified as knowledge-based if the amount of time available is short. In this case, the operator

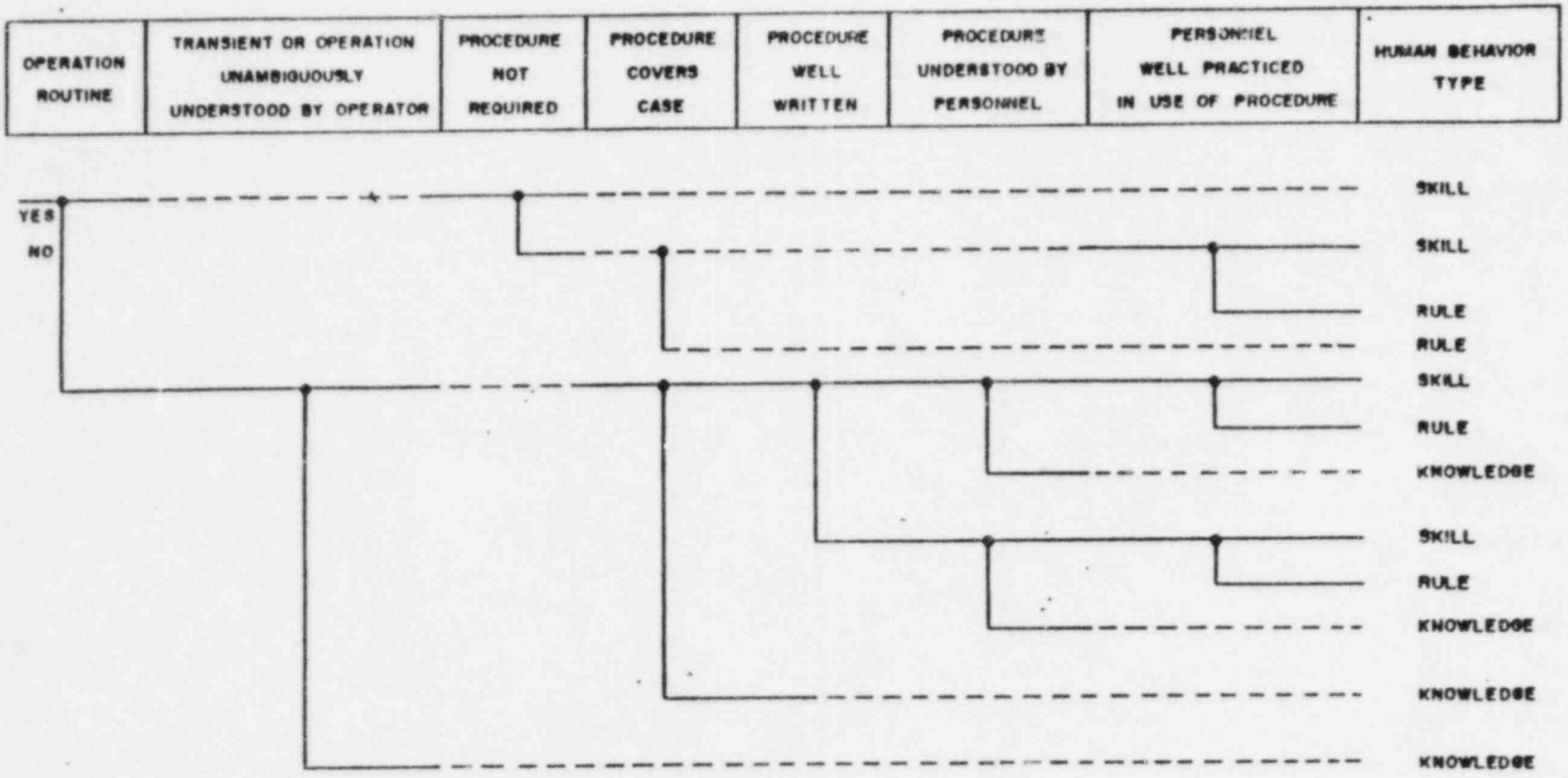

Figure 5.1. Logic Trees to Aid in Selection of Expected Behavior Type.

may not have time to access the procedure, which would make the operation equivalent to one which lacked a procedure.

Following the classification of each human action, the human error probabilities were found using the values reported in Appendix A of the SHARP report (6). To achieve a screening value for a behavior type from the range of values given in Reference 6, a log-normal distribution was assumed for each range of values. The mean and variance for the human error probabilities in each of these categories used in the ISAP study are shown below:

Behavior Type	Mean	Variance
Skill-based	1.3E-3	1.08E-5
Rule-based	1.3E-2	1.08E-3
Knowledge-based	1.3E-1	1.08E-1

The human errors evaluated by SHARP are shown on Table 5.2. Each of these errors was evaluated using SHARP because the operator decision time was assessed to be less than about ten minutes. The most important of these errors is the first one shown on the table. This is the error of the operator failing to recognize that the RPV level is decreasing and that he must respond to it. This error is important for two reasons. First, it appears on virtually all of the event trees because level is the key indicator that there is a problem at the plant (this is true of all BWR's). Second, because of the concept of cognitive errors and the new Millstone procedures, if the operator fails to recognize the need to respond and thus does not enter the level control procedure, it is assumed that he will not take any actions to actuate or recover any systems which could be used to prevent core melt. The ISAP study assumed that this decision had to be made within ten minutes (or in some cases even less) because part of the response includes manually initiating the isolation condenser. If the operator does not do this within ten minutes, it will actuate automatically. We believe that it would have been more reasonable to use time frames which reflect the actual times available. By way of comparison with this alternative approach, Table 5.2 shows estimated actual time frames available to the operator for the three sequence scenarios (Cases A-C) in which this error appears. The time frames shown are the times available for action to pre-

Table 5.2

Human Errors Evaluated Using the
Systematic Human Action Reliability Procedure

Error Description	Basis	ISAP HEP	Est. Actual Time Avail.	NUREG/CR-2815 HEP
Operator fails to recognize the need to restore RPV level (transient and small-small LOCA)	Rule	1.3E-2	Sequence Dependent	
			Case A: Stuck Open S/RV	
			Small-Small LOCA	
			Core uncovery-15 min	0.2
			Core melt-25 min	3E-2
			Case B: IC Fails	
			Core uncovery-25 min	3E-2
			Core melt-45 min	3E-3
			Case C: IC Makeup Fails	
			Core uncovery-70 min	1E-3
			Core melt-90 min	9E-4
Operator fails to recognize the need to disregard the indicated level and flood the RPV when drywell temperature reaches RPV saturation temperature (operator throttles or terminates injection based on erroneous high RPV level indication due to reference leg flashing)	small & small-small LOCA Skill	1.3E-3	Initial Error	
	large LOCA Rule	1.3E-2	+30 min recovery	<1E-3
Operator fails to recognize the need to reduce core power following ATWS (W/PCS available) before loss of condenser vacuum	Rule	1.3E-2	3 min	N/A
Operator fails to recognize the need to provide for long term decay heat removal (ATWS w/PCS available)	Rule	1.3E-2	>60 min	<1E-3

Table 5.2 (con't.)

Error Description	Basis	ISAP HEP	Est. Actual Time Avail.	NUREG/CR-2815 * HEP
Operator fails to recognize the need to reduce core power before torus heats up to 110o F (ATWS w/PCS failed)	Knowledge	1.3E-1	3 min	N/A (ATWS Rule = 0.5)
Operator fails to recognize the need to keep RPV pressure below heat capacity temperature limit of the torus (ATWS w/PCS failed)	Knowledge	1.3E-1	15 min	2E-1

vent core uncovery and core melt. They are taken directly from the ISAP study, where they were used in the station blackout analysis to evaluate offsite power recovery. The core melt time frames, which are what we are interested in, are in general agreement with the time frames used for the same scenarios in the IREP study. Using the TRC curve from NUREG/CR-2815, we get HEPs for the three cases for preventing core melt of 0.03, 0.003, and 0.0004. The HEP used for all cases in the ISAP study is the rule-based value 0.013. Obviously, the CR-2815 values are relatively close to the ISAP value in the overall sense. Further, the contribution from each of the three cases is approximately equal in the ISAP study, and thus the average of the three values (0.011) is a reasonable approximation of the composite HEP. Thus, using another approach yields the same number, and we can conclude from this that the value used for this extremely important cognitive error is reasonable.

The next error shown in Table 5.2 is significant in that it considers cognitive operator error of commission. That is, the operator takes an action which is detrimental to the mitigation of an accident due to his misinterpretation of plant conditions. This type of error is seldom considered in a risk assessment, although it has the potential to be significant. The values used in the ISAP study are reasonable for screening purposes given that we expect there to be around 30 minutes after the erroneous action for the operator to recover. From the NUREG/CR-2815 TRC curve, 30 minutes corresponds to an HEP of 0.01. This must be combined with the HEP for initially making the error. Even if this were as high as 0.1, which is doubtful, the total expected HEP would be 0.001. Thus, we expect that the values used in ISAP are probably conservative and even being so, they do not have a significant effect on the results. Therefore, further detailed analysis is not warranted.

The next two cognitive errors involve response to ATWS with PCS available. The first action is somewhat complex in total, i.e., many actions are required, but the only task which is essential in the immediate term is to trip the recirculation pumps. If the operator succeeds in doing that, the PCS will automatically maintain adequately safe conditions until the other actions are completed. No HEP is available from NUREG/CR-2815 for a time frame this short, however it is our opinion that the HEP used for ISAP is a reasonable screening number. In our opinion, this is because the action is

an automatic response to observing that rod bottom lights for the control rods are not present. It is an intuitive rather than diagnostic/interpretative action, and an HEP of about 1 in 100 trials seems reasonable. For the second error, the result appears conservative since the operator would have a long time to provide for decay heat removal. However, this error does not contribute to core melt, and so it is sufficient to note that we do not feel it is too low.

The final two errors in Table 5.2 pertain to operator diagnosis of the need to take certain actions during an ATWS with the PCS unavailable. While the actions are in some ways related, they are considered separately because the symptoms which direct the operator to enter a particular procedure are independent. That is, the procedure the operator enters to reduce core power does not specifically direct the operator to the containment temperature control procedure. The need to perform those actions must be realized separately. Again, for the actions required within three minutes, which are very complex and in this case cannot be delayed as in the PCS available case, no NUREG/CR-2815 values can be obtained. We do note, however, that the ATWS rule uses a value of 0.5 as the HEP for the operator failing to initiate the procedures in time. This value includes the probability of the operator failing actually to perform the initial action of starting the SLCS, whereas the ISAP cognitive error only considers the decision process. Thus, the ISAP number is generally reasonable. (Note: The procedural error is discussed in the next section.) For the other operator decision required (torus heat capacity), the ISAP value used is in general agreement with the value obtained from the NUREG/CR-2815 TRC curve.

5.2 Procedural Error Modeling

In addition to cognitive errors, the ISAP study also considered procedural errors. These are the errors which take place after the operator has diagnosed the situation, has selected the proper procedure, and is actually trying to perform the required actions. These errors were evaluated at the systems level (i.e. essentially considered in the system fault trees) as was done in the IREP study.

As far as we can ascertain from the limited information available, the ISAP study used two HEP values for procedural errors. A HEP of 0.0013 was

used for control room actions involving simple manipulations or systems with which the operators are very familiar. An HEP of 0.013 was used for actions outside the control room or for control room actions which were complex or unfamiliar. These values are essentially identical to the suggested screening values for procedural error given in NUREG/CR-2815 (0.001 for procedural error with recovery potential, common for control room actions, and 0.01 for procedural error without recovery potential, common for outside control room actions). Thus, these values appear reasonable, and our review indicates that these errors have very little effect on the results.

The one notable exception to this general conclusion is for ATWS with PCS unavailable. As noted in the previous section, the cognitive error modeling for this scenario is reasonable. However, despite the fact that the required actions are very complex, no consideration was given to procedural error. The ATWS rule gives a HEP value of 0.1 in this situation just for failing to reduce power properly while maintaining RPV water level above the top of active fuel. Additional questions regarding the probability of the operator failing to activate the SLCS properly, even given the proper diagnosis of the event, results in the ATWS rule using a value of 0.5 for the combined cognitive/procedural HEP for this task. Thus, we believe that procedural error could be a significant contribution to ATWS core melt, and its exclusion in the ATWS analysis is unacceptable. In the absence of a detailed analysis, it is our opinion that a screening value of 0.5 should have been used for this error. The significance of this conclusion is discussed in Section 6.3.

6.0 RESULTS AND INSIGHTS INTO MAJOR CONTRIBUTORS TO THE CORE MELT FREQUENCY

In this section, a comparison between the results of the ISAP and IREP studies will be presented. This is done by performing a detailed comparison between the ISAP and IREP dominant accident sequences to find out the major differences between similar sequences and the significance of these differences with respect to the overall core melt frequency associated with the operation of the plant. This comparison is presented in Section 6.1. The results of this analysis will be used in Section 6.2 to present the overall insights into the major contributors to the ISAP core melt frequency. Section 6.3 focuses on a few areas where changes to the current system configurations or procedures could conceivably result in major impacts on the plant's dominant accident sequences and overall core melt frequency.

6.1 Comparison Between ISAP and IREP Dominant Accident Sequences

To better understand the major contributors to core melt frequency at the system level, a detailed analysis of the most dominant ISAP core melt sequences was performed. This was done by closely looking at the ISAP dominant core melt sequences and comparing them with the corresponding IREP dominant core melt sequences. The comparison is done by looking at the sequence of events, the effect of methodologies on identifying the sequence of events, and the core melt frequency. With respect to core melt frequency, the ISAP calculations are done using mean component failure data whereas the IREP calculations are done using median values. To compare the sequence frequencies in the two studies, a simple conversion factor was used to convert the IREP results based on the following argument. Most of the generic component failure probabilities have been developed by assuming that the components have a log-normal distribution. These data in most cases have an error factor of either 3 or 10. For components with an error factor of 3, the mean value is 1.25 times the median value. For components with an error factor of 10, the mean value is 2.66 times the median value. Since the components contributing to failure of different systems are a combination of those with an error factor 3 and 10, a multiplier of 2 was used to convert the median IREP core melt frequencies to mean values. Note that the objective of comparing similar ISAP and IREP core melt frequencies is to identify those sequences that have large (order of magnitudes) differences and focus on the basic reasons for these kinds of differences. With the

level of uncertainty associated with most component failure data, much finer comparison does not provide any meaningful insights. With this fact in mind, Table 6.1 presents the dominant accident sequences found in the ISAP study along with the corresponding IREP dominant accident sequences. The sequences are grouped by their common initiator where the ISAP sequence numbers in the first column correspond to the sequence numbers identified in Table 5.3-5 of the Millstone Unit 1 Probabilistic Safety Study (1). A brief analysis of each sequence follows.

For sequence number 2, the ISAP and IREP sequences are fairly similar. The frequency of the ISAP sequences is lower than IREP principally due to reductions in the failure probabilities of several components, namely, the diesel generator, gas turbine, and AC breakers previously shown in Table 4.1. In addition, modification to LNP logic circuits to eliminate single relay failures, and to IC makeup to remove AC dependency from the makeup admission/control valve, also helped to reduce the contribution.

The same comments are applicable to sequence number 3 except that the LNP logic modifications have no effect here. Also, changes in the emergency operating procedures have reduced the chance of operator error in failing to depressurize the Reactor Pressure Vessel (RPV) and use the available low pressure pumps.

In sequence number 8, the contribution to core melt frequency is similar in both ISAP and IREP. Competing differences have opposite effects. Reduction in failure rates of the gas turbine and switchgear breakers, and modification to the IC makeup admission valve power supply tend to reduce the frequency of the ISAP sequences. However, a change in the alternate Shutdown Cooling (SDC) system success criteria, which requires both trains of Low Pressure Coolant Injection (LPCI) system and all four Emergency Service Water (ESW) pumps, increases the frequency of the ISAP sequence. The change in the success criteria of the alternate SDC system has substantially (by about two orders of magnitude) increased the probability of failure of this system and its contribution to the total core melt frequency. This is one of the areas that will be discussed in more detail in Section 6.3.

Table 6.1 Comparison Between ISAP and IREP Dominant Accident Sequences

ISAP Sequences					IREP Sequences	
Seq. #	Initiator	Failure of Support Systems	Sequence Description	Frequency (Mean)	Sequence	Frequency Median (Mean)
2	LNP	Station AC Blackout (Only DC buses are energized)	o Correct cognitive decision to initiate IC and restore normal power. o S/R valves reclose, IC is initiated, IC makeup fails and AC power not restored before CM initiates (i.e., within 90 minutes). OR S/R valves reclose, IC initiation and restoration fail, and AC power not restored before CM initiaes (i.e., within 45 minutes). OR S/R valve sticks open and AC power not restored before CM initiates (i.e., within 25 minutes).	(7.0E-5)	T_4LCEFG(9) T_4KCEFG(3) T_4JCEFG(2)	8.0E-5 (1.6E-4)
3	LNP	None OR AC Bus 14E	o Cognitive error in decision not to restore RPV level. o S/R valves reclose and auto IC initiation or IC makeup failed. OR S/R valve sticks open. o Auto FWCI initiation failed. Random failure for SS#1. Failure given (Q = 1) for SS#3. (No other auto system is available.)	(3.7E-5)	T_4KCD(4) T_4LCD(5) T_4JCD(1)	1.3E-4 (2.6E-4)
8	LNP	AC Bus 14E	o Correct cognitive decision to restore RPV level. o S/R valves reclose and initiation and restoration of IC or IC makeup fails. OR S/R valve sticks open. o FW fails (given). o Manual depressurization is successful.	(6.5E-5)	T_4KCMG(12) T_4LCMG(10) T_4CMG(8)	2.9E-5 (5.8E-5)

Table 6.1 Comparison Between ISAP and IREP Dominant Accident Sequences (continued)

ISAP Sequences					IREP Sequences	
Seq. #	Initiator	Failure of Support Systems	Sequence Description	Frequency (Mean)	Sequence	Frequency Median (Mean)
8 (cont'd)			o Low pressure pumps inject. o Off-site AC power recovery fails. o 14E bus energized by cross-connection to diesel generator. o SDC fails. (Note: FW and circulating water pumps cannot be loaded on the diesel generator. Therefore, the main condenser is not credited. Also, both trains of the alternate SDC cannot be powered by the diesel.)			
15	LNP	AC Bus 14E	o Correct cognitive decision to restore RPV level. o S/R valves reclose. Initiation and restoration of IC or IC makeup fails. OR S/R valve sticks open. o FW failed given (Q = 1.0) for SS#3. o Manual depressurization is successful. o Low pressure pumps inject. o Off-site AC recovery fails. o Energizing AC bus 14E by cross-connection fails. o SDC fails. (Note: The main condenser cannot be used unless FW is operating. Also, both trains of the alternate SDC cannot be powered by the diesel generator.)	(8.6E-6)	$T_4KCMG(12)$ $T_4LCMG(10)$ $T_4JCMG(8)$	2.9E-5 (5.8E-5)

Table 6.1 Comparison Between ISAP and IREP Dominant Accident Sequences (continued)

ISAP Sequences					IREP Sequences	
Seq. #	Initiator	Failure of Support Systems	Sequence Description	Frequency (Mean)	Sequence	Frequency Median (Mean)
9	LNP	AC Bus 14E	Same as in sequence #8, except: o Off-site AC power recovery succeeds. o Restoration of main condenser and IC makeup fails. (The latter is credited only in sequences where the S/R valves have reclosed.) o SDC and alternate SDC fail.	(4.0E-5)	None	
	LNP		Total	(2.20E-4)		2.39E-4 (4.78E-4)
7	Small Break LOCA	None	o Blowdown steam condensers in torus as vacuum breakers remain closed. o FW continues to run and maintains RPV level for short time until it trips on low hotwell level. o Correct cognitive decision to switch to low pressure pumps. o Core spray pumps inject and operator correctly maintains RPV level. o Containment cooling (i.e., torus cooling) fails. (No other system is adequate to provide long-term decay heat removal following a small break.)	(1.6E-4)	(ILB)CG (ISB)CEG	<E-6
1	Loss of Feedwater	None	o S/R valves reclose and auto IC initiation fails. OR S/R valve sticks open. o Cognitive error in decision not to restore RPV level. (No other auto system is available.)	(7.6E-5)	T_3KD T_3JD	<E-6

Table 6.1 Comparison Between ISAP and IREP Dominant Accident Sequences (continued)

ISAP Sequences					IREP Sequences	
Seq. #	Initiator	Failure of Support Systems	Sequence Description	Frequency (Mean)	Sequence	Frequency Median (Mean)
12	Loss of Feedwater	None	o S/R valves reclose, auto initiation of IC and IC makeup fails. OR S/R valve sticks open. o Correct cognitive decision to restore RPV level. o Restoration of IC or IC makeup fails (credited only in sequences where S/R valves reclose). o Restoration of FW fails. o Manual depressurization is successful. o Low pressure pumps inject. o SDC and alternate SDC fail.	(2.1E-5)	T_3KMG T_3LMG T_3JMG	<E-6
	Loss of Feedwater		Total	(9.7E-5)		<E-6
4	Reactor Transients	None OR AC Bus 14E	o FW fails to run post scram. Random failure for SS#1. Failure given (Q = 1) for SS#3. o Cognitive error in decision not to restore RPV level. o S/R valves reclose and auto IC initiation or IC makeup fails. OR S/R valve sticks open.	3.5E-5	$T_{1,2}$KCD $T_{1,2}$LCD $T_{1,2}$JCD	<E-6
11	Reactor Transients	None OR AC Bus 14E	o FW fails to run post scram. Random failure for SS#1. Failure given (Q = 1) for SS#3. o Correct cognitive decision to recover RPV level. o FW restoration fails.	(3.2E-5)	$T_{1,2}$KCMG $T_{1,2}$LCMG $T_{1,2}$JCMG	(<E-6)

Table 6.1 Comparison Between ISAP and IREP Dominant Accident Sequences (continued)

ISAP Sequences					IREP Sequences	
Seq. #	Initiator	Failure of Support Systems	Sequence Description	Frequency (Mean)	Sequence	Frequency Median (Mean)
#11 (cont'd)			Random failure for SS#1. Failure given (Q = 1) for SS#3. o S/R valves reclose. Initiation and restoration of IC and IC makeup fails. OR S/R valve sticks open. o Manual depressurization is successful. o Low pressure pumps inject. o AC bus 14E energized by cross-connection (credited only for SS#3 case). o SDC and alternate SDC fail.			
16	Reactor Transients	None	o FW continues to operate post scram. o The main condenser is isolated as a heat sink due to MSIV closure post scram. o S/R valves reclose, initiation and restoration of IC or IC makeup fails. OR S/R valve sticks open. o Restoration of the main condenser fails. o SDC and alternate SDC fail.	(4.5E-5)	T_2^{KMG} $T_2^{HLMG(21)}$ T_2^{JMG}	2.0E-6 (4.0E-6)
5	Reactor Transients	AC Bus 14E and 14F. Both fail to fast transfer post scram, i.e., station AC blackout - only DC buses (both) energized.	o FW fails (given). o Correct cognitive decision to restore and stabilize RPV. level. o S/R valves reclose and initiation and restoration of IC or IC makeup fails. OR S/R valve sticks open. (No other system is available.)	1.4E-5	$T_{1,2}^{KCEFG}$ $T_{1,2}^{LCEFG}$ $T_{1,2}^{JCEFG}$	< E-6
	Reactor Transients		Total	1.26E-4		2.0E-6 (4.0E-6)

Table 6.1 Comparison Between ISAP and IREP Dominant Accident Sequences (continued)

ISAP Sequences					IREP Sequences	
Seq. #	Initiator	Failure of Support Systems	Sequence Description	Frequency (Mean)	Sequence	Frequency Median (Mean)
6	Small-Small Break LOCA	None	o Blowdown steam condenses in torus as vacuum breakers remain closed. o FW continues to run post scram. o Cognitive error in decision not to start condensate transfer pump (to replenish the hotwell) or use low pressure pumps. o FW eventually trips on low hotwell level (given).	6.9E-6	(SB)CD	<E-6
14	Small-Small Break LOCA	None	o Blowdown steam condenses in torus as vacuum breakers remain closed. o FW continues to run post scram. o Correct cognitive decision to start emergency condensate pump. o Emergency condensate pump starts and transfers inventory from the CST to the hotwell. o Operator fails to disregard the indicated level when the drywell temperature reaches the RPV saturation temperature and therefore prematurely terminates or throttles injection.	1.35E-5	(SB)CD	<E-6
18	Small-Small Break LOCA	None	o Blowdown steam condenses in torus as vacuum breakers remain closed. o FW continues to operate post scram. o Correct cognitive decision to start emergency condensate transfer pump. o Emergency condensate transfer pump starts and transfers inventory from the CST to the hotwell.	8.3E-6	(SB)MG	<E-6

Table 6.1 Comparison Between ISAP and IREP Dominant Accident Sequences (continued)

ISAP Sequences					IREP Sequences	
Seq. #	Initiator	Failure of Support Systems	Sequence Description	Frequency (Mean)	Sequence	Frequency Median (Mean)
18 (cont'd)			o Correct cognitive decision to disregard the indicated RPV level when the drywell heats up to RPV saturation temperature. o Restoration of the main condenser fails. o SDC and alternate SDC fail.			
	Small-Small Break LOCA		Total	2.87E-5		< E-6
10	Loss of Service Water System	None except the SWS	o Correct cognitive decision to restore RPV level. o S/R valves reclose, initiation and restoration of IC or IC makeup fails. OR S/R valve sticks open. o Manual depressurization is successful. o Low pressure pumps inject. o Alternate SDC fails. (Note: both FW and SDC are unavailable due to loss of SW.)	3.4E-5	T_3KMG T_3LMG T_3MG	$\leq$ E-6
17	Inadvertent Opening of a Safety/Relief Valve	None	o FW continues to operate post scram. o MSIVs close post scram due to low pressure, isolating the main condenser as a heat sink. o Restoration of the main condenser fails. o SDC and alternate SDC fail.	1.9E-5	T_5HMG T_5MG	< E-6

Table 6.1 Comparison Between ISAP and IREP Dominant Accident Sequences (continued)

ISAP Sequences					IREP Sequences	
Seq. #	Initiator	Failure of Support Systems	Sequence Description	Frequency (Mean)	Sequence	Frequency Median (Mean)
13	Large Break LOCA	None	o Blowdown steam condenses in torus as vacuum breakers remain closed. o ECCS signal is generated. o Core spray pumps start and inject automatically. o Correct operator decision to disregard indicated high level when the drywell heats up to RPV saturation condition. o Containment cooling (i.e., torus cooling) fails. (No other system is adequate to provide long-term decay heat removal following a large break.)	1.6E-5	(LLB)G	<E-6

*Numbers in parentheses indicate IREP sequence core melt ranking from IREP study.

Sequence number 15 is very similar to sequence number 8, so the same comments apply.

For ISAP sequence number 9, there is no equivalent IREP sequence. This is due to the fact that IREP did not treat situations where LNP followed by recovery of offsite power could result in core melt. The assumption was made in IREP that recovery would successfully terminate the sequence. Consideration of this scenario along with increased failure rate of the alternate SDC system due to change in its success criteria mentioned before have made this sequence dominant.

Overall the LNP sequences in the ISAP and IREP studies are fairly similar. When there are differences in the frequency of similar core melt sequences, the difference is principally due to either lower plant-specific component failure probabilities for the diesel generator, gas turbine, and AC circuit breakers or higher unavailability for the alternate SDC system due to the revised success criteria for this system.

The next sequence in Table 6-1 is the Small Break LOCA, sequence number 7. This ISAP break size combines the IREP intermediate breaks with the upper end of the IREP small breaks. The contribution from this sequence is dominant in the ISAP study because of the change in the success criteria for containment cooling (alternate SDC system) which was mentioned previously.

The next two sequences are initiated by loss of the feedwater system. In sequence number 1, the IREP study treated recovery of feedwater and the use of manual depressurization with low pressure pumps as two distinct operator actions. The ISAP study considered the cognitive-based error of the operator failing to make the correct diagnosis of the need to restore RPV level. This linked the two actions to a single root cause, which resulted in a higher combined failure probability in the ISAP study. This was somewhat counteracted by a decrease in initiating event frequency, but the combined effect was to make this sequence dominant.

It is important to note that inclusion of cognitive human error on the event trees is one of the major differences between the ISAP and IREP accident sequence development methodology. As mentioned above, this change has resulted in a larger combined human error probability with significant

effect on the dominant accident sequences and overall core melt frequency. Another important point about this sequence is the need for manual depressurization of the RPV before any low pressure pumps can be used. The automatic depressurization at Millstone Unit 1 requires coincident indication of low-low RPV level, high drywell pressure, and a two minute persistance of the low-low water level. In addition, there must be an indication of at least one low pressure ECCS pump running. Thus, in all the non-LOCA sequences where there would be no high drywell pressure, the automatic depressurization will not be initiated. This implies that if there is an operator cognitive error in restoring the RPV level, the whole low pressure injection system consisting of LPCI and core spray pumps would be defeated. This brings up the possibility of addition of automatic depressurization for non-LOCA sequences, which is another area discussed in more detail in Section 6.3.

The progression of events in sequence number 12, which is the second loss of feedwater sequence, is very similar in the ISAP and IREP studies. The main difference in the sequence frequencies is due to the higher failure probability of the alternate SDC system, discussed earlier.

The next four sequences are Reactor Transient Sequences. In sequence number 4, the progression of events in the ISAP and IREP sequences are similar. The major reason for the ISAP sequence being more dominant is the cognitive human error in failing to restore the RPV level which combines several human error failures that are considered separately in the IREP sequences. This was discussed previously for sequence number 1. The higher probability of failure assigned to this cognitive error is the prime contributor to its higher frequency.

In sequence number 11, the ISAP and IREP accident sequences are similar. The main reason for higher ISAP core melt frequency is the higher unavailability associated with the alternate SDC system discussed before.

Sequence number 16 is affected by a number of competing differences. First, the initiating event frequency of the transient is lower in the ISAP study. Also, the IREP study did not give credit for recovering the main condenser due to limitations in the MSIV equalizing lines which prevented equalizing differential pressure on the valve disks within a reasonable

time. A modification to enlarge those lines has been accomplished, allowing the ISAP study to take this credit. These differences tend to reduce the contribution of these sequences. However, this is more than counteracted by the increase in alternate SDC system failure rate due to the change in the success criteria, which increases the overall contribution of the sequence.

The last transient sequence is sequence number 5. The main difference between the two studies is that the IREP study did not treat the possibility of station blackout for sequences not initiated by loss of normal power, assuming that the contribution was not significant. Consideration of this possibility in the ISAP study caused this sequence to become dominant.

The next three sequences are small-small break LOCAs. This initiator in the ISAP study represents an approximate break size resulting in at least 2.5 gpm leakage up to an approximate diameter of 1.35 inches. This break size represents the lower end of the IREP small break, which includes approximate break diameter up to 5.24 inches. The frequency of occurrence of the small-small break LOCA in the ISAP study is an order of magnitude larger than the small break frequency in the IREP study. Breaks in the lower end of this range require manual initiation of depressurization because high drywell pressure does not occur. In addition, the IREP assumption that condensate transfer pumps (CTP) would start automatically is not entirely correct. The high flow emergency CTP is required for these breaks, and must be started manually. In sequence number 6, both of these actions are coupled by a cognitive-based error (similar to sequence number 1). The high initiation frequency for this sequence along with the need for manual depressurization and start of condensate transfer pumps, which are coupled in one cognitive human error, have resulted in a high sequence frequency compared to IREP.

In sequence number 14, ISAP considered operator error of commission in misdiagnosing the plant conditions and taking an action to terminate a safety system prematurely. IREP did not adequately treat this type of error. Consideration of this type of human error along with a much higher initiator frequency resulted in a more dominant sequence compared to IREP.

In sequence number 18, ISAP has a failure to restore the main condenser. As previously mentioned, the IREP study concluded that restoration

of main condenser after isolation was not practical but credit was given for this action in the ISAP study due to a plant modification. This credit is compensated for by a higher initiating frequency and higher failure probability for the alternate SDC system, making this sequence more dominant than the IREP sequence.

Overall, the higher initiating frequency, combined cognitive error in performing depressurization and startup of condensate transfer pumps, consideration of operator error of commission in misdiagnosing the plant condition, and higher alternate SDC system failure probability result in higher frequency small-small break LOCAs in the ISAP study compared with the IREP small break LOCA sequences.

In sequence number 10 the ISAP study gave recovery credit to Service Water (SW) only in the short term, including it in the initiator frequency, resulting in the complete unavailability of the SDC system for all LOSW sequences. This greatly increased the contribution over IREP, which gave substantial credit for long term SW recovery, allowing for the SDC system to be used. Additionally, the ISAP success criteria for SW following a trip is more restrictive than IREP, resulting in an overall increase in the frequency of loss of service water in the short term. Combining this with increased alternate SDC failure rate due to a change in its success criteria made this sequence become dominant.

In sequence number 17, several competing effects result in the ISAP sequence being more dominant. The initiating event frequency in the ISAP study is significantly lower than the IREP study due to a plant modification and installation of more reliable safety/relief valves. This reduction in initiator frequency is opposed by two factors. First, in the ISAP study, it was assumed that the main condenser would be initially lost, whereas in the IREP study it was assumed it could continue to run post scram. Second, there is a higher failure probability of alternate SDC system in the ISAP study. The combined effect of these factors is to make the ISAP sequence more dominant than the IREP sequence.

The last dominant accident sequence in Table 6.1 is sequence number 13, initiated by a large break LOCA. The sequence of events in the ISAP and IREP studies is very similar in this case. The primary reason for a more

dominant ISAP sequence is the higher failure probability of the containment cooling (alternate SDC system).

In the next section a summary of the major contributors to the ISAP core melt frequency will be presented.

6.2 Insight into Major Contributors to the Core Melt Frequency.

In the last section, a detailed comparison between the ISAP and IREP dominant accident sequences was presented. This comparison provided some insights into changes, both systemic and procedural, that have taken place in Millstone Unit 1 since the original IREP study was performed, and the significance of these changes with respect to dominant accident sequences and the overall core melt frequency. Figure 6.1 shows the contribution of major classes of initiators to the total core melt frequency in both studies. The principle reasons for changes in the dominant contributors was explained in the last section during the discussion of individual dominant sequence. To put the results in a better perspective, a summary of these differences by the major classes of initiators identified in Figure 6.1 is presented here. More detail on these differences can be found in the appropriate sections in this report.

1. Loss of Normal Power (LNP); Overall decrease in ISAP vs IREP core melt contribution.

   Reasons for this decrease:

   a. Reductions in failure rate data of the diesel generator, gas turbine generator, and switchgear breakers.

   b. Modification to LNP logic to eliminate single relay failures.

   c. Modification to IC makeup to eliminate admission valve AC dependency.

   d. Change to symptom-oriented procedures eliminated confusing procedure for initiating manual depressurization when required, reducing human error probability.

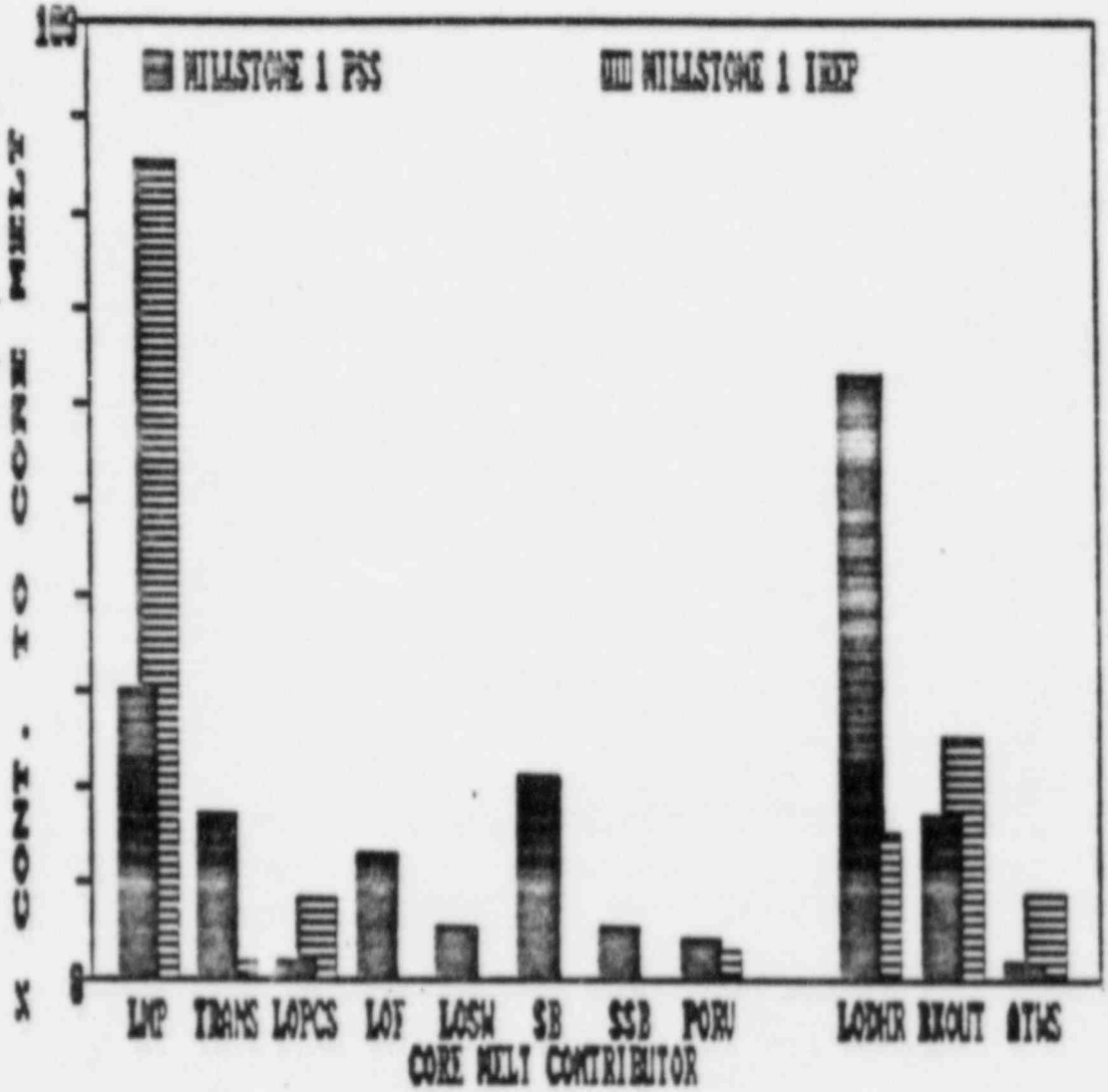

Figure 6.1. Comparison Between Dominant ISAP and IREP Contributors to the Core Melt Frequency.

The only mitigative factor that limited the amount of decrease in the ISAP core melt contribution was an increase in the failure probability of the alternate SDC system due to changes in its success criteria.

2. Transients (TRANS); Overall increase in the ISAP vs IREP core melt contribution.

   Reasons for this increase:

   a. Cognitive error modeling and symptom-oriented procedures linked failure to restore FW and failure to depressurize to a single decision process, increasing overall probability of human error and recovery failure.

   b. Consideration of the possibility of loss of normal power following a non-LNP initiating event.

   c. Increase in failure rate of alternate SDC system due to change in success criteria.

   Mitigative factors which limited amount of increase:

   a. Decrease in initiating event frequency.

   b. Modification to MSIV equalization lines allowing for recovery of main condenser for cooling.

3. Loss of Power Conversion System (LOPCS); Overall decrease in ISAP vs IREP core melt contribution.

   Reasons for this decrease:

   a. Reduction of initiating event frequency.

   b. Modification to MSIV equalization lines allows for recovery of main condenser for cooling.

The only mitigating factor that limited the amount of decrease in the ISAP core melt contribution was the increase in the failure probability of the alternate SDC system due to changes in its success criteria.

4. Loss of Feedwater (LOF); Overall increase in ISAP vs IREP core melt contribution.

   Reasons for this increase:

   a. Cognitive error linkage between recovery of FW and failure to depressurize.

   b. Increase in alternate SDC failure rate.

The only mitigative factor that limited the increase in the ISAP core melt contribution was the reduction in the initiator frequency.

5. Loss of Service Water System (LOSW); Overall increase in ISAP vs IREP core melt contribution.

   Reasons for this increase:

   a. No long term recovery credit for service water system.

   b. Increase in alternate SDC system failure rate.

   c. Increase in frequency of short-term LOSW due to change in success criteria.

6. Small Break LOCA (SB); Overall increase in ISAP vs IREP core melt contribution.

   The principle reason for the increase in the ISAP core melt contribution is the increase in failure probability of the alternate SDC system.

7. Small-Small Break LOCA (SSB); Overall increase in ISAP vs IREP core melt contribution.

Reasons for this increase:

a. Special consideration of breaks which do not actuate Automatic Pressure Relief (APR) because no high drywell pressure would be present, requiring operator action to depressurize.

b. Need for operator action to start high-capacity emergency condensate transfer pumps to supply sufficient flow to the hotwell.

c. Cognitive error modeling and symptom-oriented procedures link the above two actions to a single decision process.

d. Consideration of cognitive error of commission in prematurely terminating injection due to misinterpretation of instrumentation.

e. Increase in initiating event frequency.

The only mitigative factor that limits the amount of increase in the ISAP core melt contribution is the credit allowed for providing long-term cooling with the condenser or SDC system due to low break flow rate.

8. Inadvertent Opening of Power Operated Relief Valve (PORV); No major change between ISAP and IREP core melt contribution due to several compensating effects.

Factors Resulting in an Increase in ISAP core melt contribution:

a. Increase in alternate SDC system failure rate.

b. Automatic loss of condenser due to low pressure (pressure cannot be kept up after trip).

Factors Resulting in a Decrease in ISAP core melt contribution:

a. Credit allowed for recovery of condenser due to equalization line modification.

b. Initiating event frequency reduced due to modification to install more reliable valves.

In addition to the above classes of initiators, three groups of events are also compared in Figure 6.1. The first one is the group of events leading to core melt that include Loss of Decay Heat Removal (LODHR) function. In this case, the ISAP dominant sequence frequencies have increased substantially due to the increased failure probability of the alternate SDC system as a result of the change in its success criteria.

The second group is the Station Blackout (BKOUT) sequence. In this case the ISAP dominant sequence frequency has decreased due to:

1. Reductions in failure rate data of diesel and gas turbine generators and switchgear breakers.

2. Modifications to LNP logic to eliminate single relay failures.

3. Modifications to IC makeup to eliminate admission valve AC dependency.

The last group of events shown in Figure 6.1 is the Anticipated Transients Without Scram (ATWS) sequences. The overall ISAP core melt contribution in this case has decreased due to credit allowed for operator action to initiate the standby liquid control system (43 gpm) and take other actions to mitigate the event. This decrease was limited by a significant increase in the RPS failure probability, based on a simple statistical analysis. This event was assumed to lead to core melt in the IREP study. This assumption is one of the topics that will be discussed in more detail in the next section.

6.3 Discussion of Several Areas of Plant Vulnerability

In this section, three areas with significant contributions to the core melt frequency are discussed in detail. These areas were chosen for more

detailed discussion because they are areas where changes in the system configuration or procedures can result in substantial reductions in their contribution to the core melt frequency.

The first area is the reliability of the alternate SDC system. Referring to Figure 6.1, it can be seen that sequences involving loss of the decay heat removal system contribute to about 65% of the total core melt frequency. This contribution is substantially higher in the ISAP study compared with the IREP study. As has been mentioned previously, this increase is primarily due to the higher failure probability associated with the alternate SDC system. The increase in the failure probability of the alternate SDC system is due to the change in its success criteria.

In the IREP study, the success criteria for this system consisted of successful operation of one LPCI pump and the associated containment cooling heat exchanger with one Emergency Service Water (ESW) pump removing heat from the heat exchanger. Based on some new thermal hydraulic calculations, the success criteria for this system were changed in the ISAP study by requiring two LPCI containment cooling heat exchangers with one LPCI pump per heat exchanger and all four emergency service water pumps to remove the heat from the containment cooling heat exchangers. This change has dramatically increased the failure probability of this system.

To assess some alternatives in reducing the failure probability of this system, the detailed fault tree for this system, shown in Figure 3.2.24-2 of the Millstone Unit 1 PSS, was simplified and is shown in Figure 6.2. Based on the current configuration, the failure probability of this system with no support system failure is 0.148. Three scenarios for improvement in the reliability of this system were examined. In the first case, it was assumed that the LPCI/containment cooling loops are made redundant. In the second case, it was assumed that the emergency service water loops are made redundant. In the third case, it was assumed that both of the above improvements were incorporated. Table 6.2 shows the results of these evaluations. Incorporation of redundancy in the LPCI alone resulted in the reduction of the failure probability of the alternate SDC by a factor of about 1.7. The effect of making the ESW loop redundant is a reduction in the failure probability of the alternate SDC system by a factor of about 2.2. If both of these changes are incorporated, the failure probability of this system can

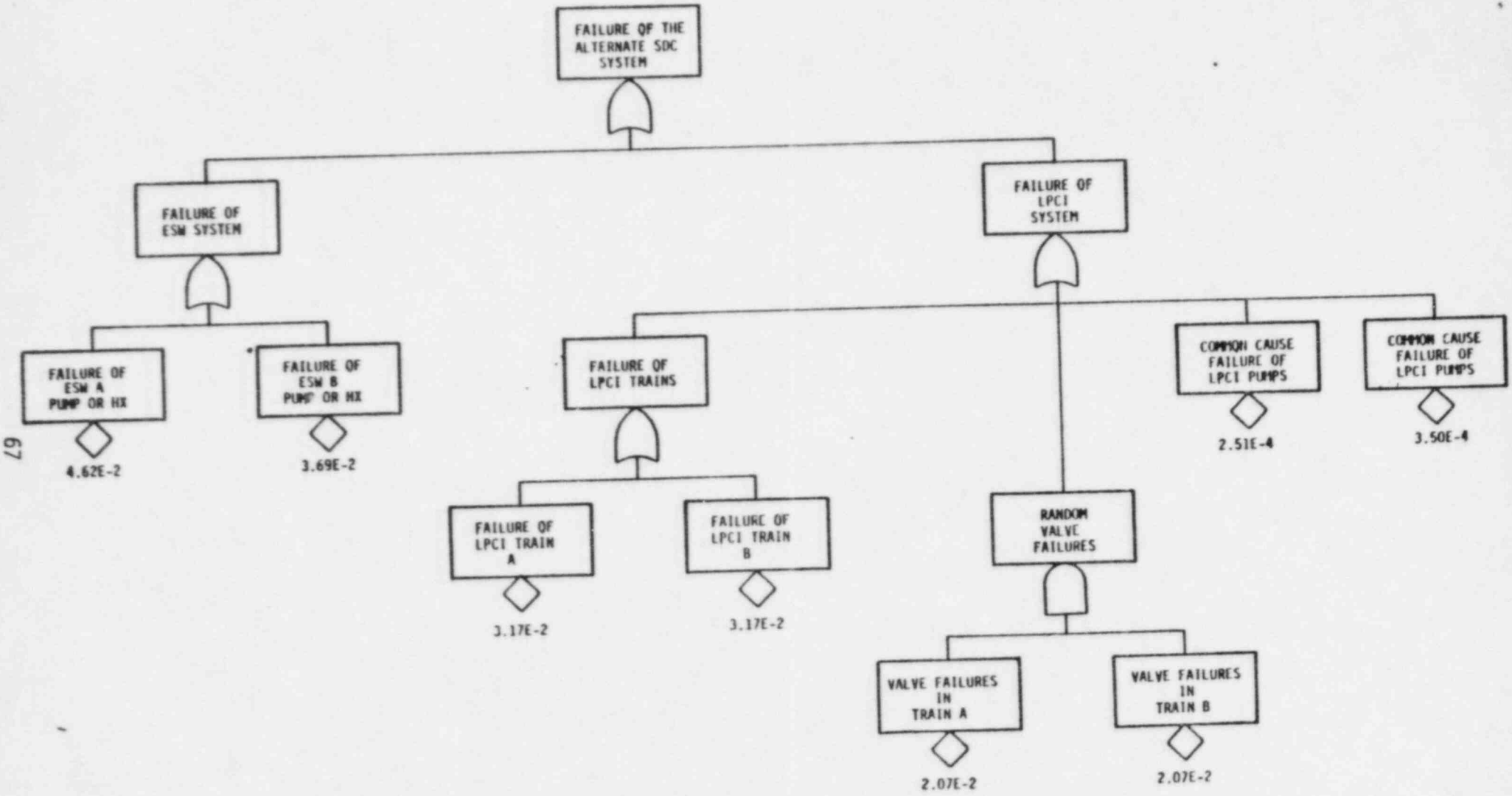

Figure 6.2. Simplified Fault Tree for the Failure of Alternate SDC System

Table 6.2 Alternate SDC System Unavailability Based on Different System Configurations

	System Configuration	Alternate SDC System Unavailability
1.	Present Configuration	0.148
2.	Redundant LPCI/ Containment Cooling Loops	8.51E-2
3.	Redundant ESW Loops	6.61E-2
4.	Redundant LPCI and ESW Loops	3.73E-3

be reduced by a factor of about 40. As was mentioned earlier, 65% of the ISAP core melt frequency was due to failure of long-term decay heat removal. Assuming that both the LPCI and ESW loops are made redundant, this results in a reduction in ISAP core melt frequency from 8.07×10^{-4} to 2.95×10^{-4}, a reduction of about a factor of 3.

The second area analyzed in more detail is the area involving those core melt sequences which require manual depressurization of the RPV. Depressurization is required in those events where the feedwater system is either unavailable or incapable of providing sufficient water to the core and low pressure systems are needed to keep the core covered.

Millstone Unit 1 has an Automatic Depressurization System (ADS) which is initiated when there is a coincident indication of reactor water low-low level for two minutes, high drywell pressure and indication that at least one low pressure pump is running. Because of the requirement of high drywell pressure, automatic depressurization occurs only when a LOCA has occurred. In other cases, such as loss of feedwater or other types of transients and the lower range of small-small break LOCAs, this system is not initiated automatically. In these sequences, if there is a cognitive operator error in not restoring the RPV level, the low pressure systems such as LPCI and core spray systems will be automatically defeated since the reactor pressure has to be below about 350 PSI before the pumps in these systems can inject into the core.

The ISAP dominant accident sequences that include this type of cognitive human error, i.e., failure to depressurize the reactor manually, contribute to about 21% of the total core melt sequences. The most dominant sequence among these is the loss of feedwater transient that contributes to about 9.5% of the total core melt frequency. If in these sequences there is the possibility of an automatic depressurization despite the cognitive operator error, the frequency of these core melt sequences will be reduced by the failure probability of the ADS.

The results of the analysis of the ADS in Millstone Unit 1 is given in Table 3.2.18-1 of the PSS. Based on this table, the failure probability of ADS with both DC buses available is 0.13. Currently the relay contacts in this system are never tested. If a more frequent (such as monthly) test of

these relay contacts is performed, the failure probability of this system can be reduced by about two orders of magnitude.

Based on the present system configuration and procedures, inclusion of an automatic depressurization system in the ISAP sequences which involve human error to depressurize the RPV will result in about an order of magnitude reduction in their contribution to the total core melt frequency. The net effect of this is a reduction of about 18% in the total ISAP core melt frequency.

The only negative aspect of addition of an automatic depressurization option to these sequences is the possibility of early depressurization before all efforts in restoration of the feedwater system are exhausted. Thus, it is crucial that initiation of this automatic depressurization is sufficiently delayed so that any possibility of recovery of feedwater system is not defeated.

The final subject considered is the Anticipated Transients Without Scram (ATWS). As was discussed previously in Section 3.4, the proper way to review the ATWS treatment is to compare it with the ATWS rule rather than the IREP treatment since the ATWS rule represents the more advanced understanding of the subject. The results of our comparison showed that for the transients with Power Conversion System (PCS) available, the ISAP analysis is acceptable despite its deviation from the ATWS rule.

For the case of transients with PCS unavailable, the ATWS rule indicates that if the Standby Liquid Control System (SLCS) has a flow rate of 43 gpm, as is the case in Millstone Unit 1, even immediate action by the operator would not prevent the increase in suppression pool temperature to the 200° F limit and subsequent failure of the containment system. If the flow rate is increased to 86 gpm, the operator has about two minutes to initiate the SLCS and restrict the suppression pool temperature increase to below the 200° F limit. The only reason that Millstone Unit 1 might be able to meet this limit with the existing 43 gpm SLCS is that it has a suppression pool that is the size of a typical BWR-4 but has about 60% of the typical BWR-4 power.

If this is not the case, the ATWS contribution to the core melt frequency would become much more dominant.

To put this in perspective, the ATWS core melt frequency based on transients with power conversion system unavailable can be estimated. This contribution consists of the frequency of all initiators that result in failure of PCS, which is 0.655, times the failure probability of the Reactor Protection System (RPS) in the ISAP study, which is 5.4×10^{-5}. The frequency of this sequence is 3.53×10^{-5}, which is 4.3% of the total ISAP core melt frequency. It is important to note that the failure probability of RPS used in the ISAP study is somewhat more conservative than the number suggested in the ATWS rule. If we use the RPS failure probability of 1.0×10^{-5} suggested in the ATWS rule, the ATWS core melt frequency will decrease to 6.53×10^{-6} which is about 0.8% of the total ISAP core melt frequency. If credit is given for the 43 gpm SLCS, the core melt frequency will be further reduced. The amount of that reduction depends on the human error probability used for failure to diagnose the condition and take all the proper action. However, it is unlikely for this reduction to be more than an additional factor of two.

7.0 REFERENCES

1. Millstone Unit 1 Probabilistic Safety Study, NUSCO 147, July, 1985.

2. Interim Reliability Evaluation Program: Analysis of the Millstone Unit 1 Nuclear Power Plant, NUREG/CR-3085, January 1983.

3. ATWS: A Reappraisal, Part 3: Frequency of Anticipated Transients, EPRI NP-2230, January 1982.

4. Handbook of Human Reliability Analysis With Emphasis on Nuclear Power Plant Applications, NUREG/CR-1278, October 1980.

5. Post Event Human Decision Errors: Operator Action Tree/Time Reliability Correlation, NUREG/CR-3010, November 1982.

6. Systematic Human Action Reliability Procedure (SHARP), EPRI NP-3583, June 1984.

7. Probabilistic Safety Analysis Procedures Guide, NUREG/CR-2815, January 1984.