Florida
Power
CORPORATION
Crystal River Unit 3
Docket No. 50-302

July 11, 1997
3F0797-05

U. S. Nuclear Regulatory Commission
Attn: Document Control Desk
Washington, D. C. 20555-0001

Subject: Individual Plant Examination - Internal Events

References: A. NRC to FPC letter, 3N0497-34, dated April 28, 1997

B. FPC to NRC letter, 3F0393-03, dated March 9, 1993

Dear Sir:

This letter provides Florida Power Corporation's (FPC) initial response to the NRC's request in Reference A for FPC planned actions to respond to weaknesses noted in the NRC's Safety Evaluation Report documenting its review of the Crystal River Unit 3 (CR-3) Individual Plant Examination (IPE) submittal. Consistent with NRC's request for a meeting, FPC suggests that a follow-up technical meeting be held in late August or early September, 1997 to discuss this submittal, the CR-3 IPE, and further activities that may be necessary to resolve Generic Letter 88-20 for CR-3.

A011

NRC's general comments, delineated in Reference A, are addressed individually in Attachment 1. FPC is deferring response to four of the NRC comments dealing with the IPE Back-End Analyses until the NRC suggested meeting takes place between the NRC and FPC. Attachment 2 is a discussion of the common cause failure and human reliability analysis for the current CR-3 Probabilistic Safety Assessment (PSA) model. This material is completely new. While the paragraph numbers are the same as those in the original CR-3 IPE report, this discussion is based on PSA model that exists today (July 1997) for CR-3. FPC has maintained the PSA model to be reflective of CR-3 in anticipation of its usefulness in areas such as Maintenance Rule compliance. Please insert this discussion in the back of the material submitted by Reference B.

Considering the responses to the specific areas of concern (especially the complete revisions to the human reliability and common cause failure analyses) and the insights and plant-wide incorporation of IPE-based knowledge described above, FPC has made a concerted effort to address the NRC's concerns regarding CR-3's approach to meeting the intent of Generic Letter 88-20.

FPC notified the NRR Project Manager verbally that this letter would be issued on July 11, 1997.

Sincerely,

JJHolden

J. J. Holden, Director
Nuclear Engineering and Projects

JJH/jwt/mwa

Attachments

xc: Regional Administrator, Region II
Senior Resident Inspector
NRR Project Manager

ATTACHMENT 1

FPC Response to NRC Review of Individual Plant Examination Submittal

GENERAL COMMENTS

The first general issue of concern addressed in Section 3.0 of the NRC's Safety Evaluation Report is the brevity of the section on plant improvements and insights from the performance of the IPE. The only design change prompted by the IPE process was the redesign of the Nuclear Service and Decay Heat Seawater (RW) System pump flush water in response to a vulnerability identified by the IPE. This vulnerability involved a single valve which, had it transferred closed, would have terminated the bearing flush water to all five RW System pumps, potentially failing the pumps. This vulnerability was discussed in the IPE submittal. Other improvements prompted by the IPE process were changes to the Emergency Operating Procedures, e.g., the addition of a step to the steam generator tube rupture procedure to refill the Borated Water Storage Tank (BWST) if High Pressure Injection (HPI) is active.

IPE guidance with respect to insights was to discuss unique plant safety features recognized during the IPE process. The unique safety feature mentioned in the IPE was CR-3's "feed and bleed" capability. CR-3's high-head makeup pumps make it possible to conduct successful "feed and bleed" cooling using one makeup pump and relieving (bleeding) through either the Pilot Operated Relief Valve (PORV) or one of the pressurizer safety relief valves (SRV). Other unique safety features include:

a. the diverse cooling sources available for two of the three makeup pumps. MUP-1A is normally cooled by the Nuclear Services Closed Cycle Cooling (SW) System; however, it has backup cooling provided by the "A" train of the Decay Heat Closed Cycle Cooling (DC) System. MUP-1C is normally cooled by the "B" train of the Decay Heat Closed Cycle Cooling (DC) System; however, it has backup cooling provided by the Nuclear Services Closed Cycle Cooling (SW) system. The operators are aware of this diversity, and procedural guidance is given regarding verification of cooling to the makeup pumps.

b. the leak-resistance of the CR-3 Byron-Jackson N9000 reactor coolant pump seals. Three events are necessary for an RCP seal LOCA at CR-3. These are: 1) failure of seal injection, 2) failure of seal cooling, and 3) failure of the operators to stop the RCPs after 1) and/or 2) occurs. Tests of the Byron-Jackson N9000 seals have shown that the seals will operate with little or no leakage without seal cooling, without seal injection, and even without either for a considerable period (hours) of time. The leak-resistance of the RCP seals significantly reduces the importance of RCP seal LOCAs in the CR-3 IPE results.

Another general issue of concern to the NRC is the question of whether the IPE-based knowledge has been incorporated into CR-3 plant operations. IPE/PSA-based knowledge is incorporated into many areas of plant operation. FPC developed the Probabilistic Safety Assessment Monitor (PSAM), which is an on-line risk monitor based on the IPE/PSA model. PSAM is used by CR-3's Operations and Scheduling organizations for on-line outage risk assessment. During outages, a Shutdown Risk Monitor (DIAL-CAFTA) is used to monitor the important shutdown issues during reduced Reactor Coolant System (RCS) inventory conditions. Most of the fault tree models for the Shutdown Risk Monitor were taken from the IPE/PSA model. The twelve-month schedule for on-line system outages at CR-3 is reviewed semi-annually using the IPE/PSA model to determine the instantaneous effect on risk during each outage as well as the cumulative risk of the scheduled on-line system outages for the upcoming year. When the Nuclear Operations Engineering Department processes a Request for Engineering Assistance (REA) on nuclear safety projects, FPC requires that a probabilistic safety assessment (PSA) be performed to determine whether or not improvements in the core damage frequency (CDF) are justified and what improvement is expected from the project.

Several training courses have been and are continuing to be given to the plant staff on PSA and its applications. A PRA summary document describing the CR-3 model and its applications was distributed to management at CR-3. Design and system engineers regularly contact the PSA staff for risk perspectives on proposed design changes. Licensing engineers also contact the PSA staff for risk perspectives on various licensing issues. Implementation of the Maintenance Rule has heightened the awareness and use of PSA in the System Engineering Department. The PSA staff also will provide support to CR-3's Nuclear Training Department in simulator training exercises by examining the dominant unrecovered core damage sequences (i.e., human error probability set to a value of 1).

A final NRC concern (also discussed in the attached response to NRC's specific comments) is the qualitative nature of FPC's definition of vulnerability. There is no precise definition of vulnerability for the CR-3 IPE; it is more of a process than a threshold. Review of the core damage cutsets looking for sequences with unusually high frequencies, sequences which reveal some heretofore unknown dependency, and risk-significant sequences which can easily be reduced to risk-insignificance via a procedure change or minor hardware change consisted of FPC's review of the IPE results for vulnerabilities. To state the definition of a vulnerability in purely quantitative terms would result in sequences which are normally expected to be dominant contributors, such as station blackout, being identified as vulnerabilities. Regardless of what procedure or design changes are implemented, there will always be dominant contributors. Just because they are dominant contributors does not mean they should be considered vulnerabilities. The PSA analyst is involved in the quantification of the risk of core damage and radioactive release. The core damage cutsets are examined in detail in order to understand them and to investigate possibilities for recovery. Risk importance measures are calculated, and the plant components are ranked by risk importance. This quantitative approach, coupled with the qualitative guidance above, will serve to enhance the identification of vulnerabilities.

FRONT-END ANALYSES

NRC Comment 1

Two initiating events: loss of dc power and loss of non-nuclear instrumentation, which have the potential to result in dominant accident sequences, were not included in the CR-3 IPE analysis and their omission requires justification. LOCAs are dominant contributors to core damage at CR-3, as reported by the licensee. However, the small and large break LOCA frequencies are about an order of magnitude lower, and the medium LOCA about half the frequencies described in NUREG/CR-4550. These frequency values require justification. The staff believes that these values may be sufficiently low as to erroneously impact the importance of these initiators.

FPC Response

Two loss of DC power initiators have been added to the model, one for the 'A' side and one for the 'B' side. The addition of these initiators had a negligible effect on the overall core damage frequency.

Review of system models indicated that no single failure of NNI would cause a reactor trip and significantly impact safety systems other than main feedwater. Therefore, loss of NNI is included in the loss of main feedwater initiating event frequency.

In comparing the small-break LOCA frequency used in the CR-3 IPE (2E-03 per year) to the frequencies used for small-break LOCA in other plant IPEs (see Table 1), it appears that the value used for CR-3 is reasonable. The small-break LOCA frequency in the CR-3 IPE is based on one actual event in approximately 500 reactor-years of operation of U. S. PWRs. Increasing the CR-3 small-break LOCA frequency by an order of magnitude would increase the CR-3 small-break LOCA frequency to 2.00E-02 per year. Such an increase in small-break LOCA frequency would place CR-3 in the top six of the IPEs in the IPE database. CR-3 shares many similarities to the other B&W type plants. As such, the small-break LOCA frequency used in the IPE is appropriate.

The average initiating event frequency for large-break LOCAs for the plants in the IPE database (see Table 2) is approximately 3.0E-04 per year, slightly less than one order of magnitude higher than the frequency used in the CR-3 IPE (5E-05 per year). However, a recent EPRI publication, "Pipe Failure Study Update," TR-102266, April 1993, based on historical industry data, recommends a frequency of 7.54E-06 per year for large-break LOCA for PWRs.

If the large-break LOCA frequency in the CR-3 IPE is increased to 3.0E-04 per year, the core damage frequency increases from 1.39E-5 per year to 1.45E-5 per year.

The average initiating event frequency for medium-break LOCAs for the plants in the IPE database (see Table 3) is approximately 7.4E-04 per year, slightly greater but comparable to the frequency used in the CR-3 IPE (5E-04 per year). A recent EPRI publication, "Pipe Failure Study Update," TR-102266, April 1993, based on historical industry data, recommends a frequency of 1.08E-05 per year for medium-break LOCA for PWRs.

Table 1
IPE Small-Break LOCA Frequencies
(IPE Database)

Plant Name	Initiating Event Frequency (/yr)
GINNA	3.70E-04
ST. LUCIE 2	4.06E-04
ST. LUCIE 1	4.06E-04
INDIAN POINT 3	9.14E-04
SAN ONOFRE 2&3	1.00E-03
FORT CALHOUN 1	1.00E-03
SALEM 1	1.00E-03
SALEM 2	1.00E-03
MAINE YANKEE	1.00E-03
CALLAWAY	1.00E-03
TURKEY POINT 3&4	1.00E-03
DIABLO CANYON 1&2	1.93E-03
CRYSTAL RIVER 3*	2.00E-03
SHEARON HARRIS 1	2.00E-03
HADDAM NECK	2.10E-03
MILLSTONE 2	2.25E-03
TMI 1*	2.32E-03
WOLF CREEK	2.50E-03
PRAIRIE ISLAND 1	3.00E-03
POINT BEACH 1&2	3.00E-03
PRAIRIE ISLAND 2	3.00E-03
DAVIS BESSE*	3.60E-03
OCONEE 1,2,&3*	4.00E-03
CATAWBA 1&2	4.00E-03
MCGUIRE 1&2	4.00E-03
WATERFORD 3	4.47E-03
FARLEY 1&2	4.70E-03
ARKANSAS NUCLEAR ONE 1*	5.00E-03
ARKANSAS NUCLEAR ONE 2	5.00E-03
CALVERT CLIFFS 1&2	5.04E-03
KEWAUNEE	5.12E-03
COMANCHE PEAK 1&2	5.83E-03
PALISADES	6.00E-03
BYRON 1&2	6.10E-03
BRAIDWOOD 1&2	6.30E-03
VOGTLE 1&2	6.60E-03
ZION 1&2	6.80E-03
D.C. COOK 1&2	6.80E-03
SUMMER	8.00E-03
PALO VERDE 1,2,&3	8.00E-03
MILLSTONE 3	9.07E-03
H.B. ROBINSON 2	1.50E-02
INDIAN POINT 2	1.68E-02
SEABROOK	1.79E-02
BEAVER VALLEY 1	1.85E-02
SEQUOYAH 1&2	1.99E-02
SURRY 1&2	2.10E-02
NORTH ANNA 1&2	2.10E-02
SOUTH TEXAS PROJECT 1&2	2.11E-02
BEAVER VALLEY 2	2.38E-02
WATTS BAR 1&2	2.88E-02

* Babcock and Wilcox 177FA Plants

Table 2
IPE Large-Break LOCA Frequencies
(IPE Database)

Plant Name	Initiating Event Frequency (/yr)
TURKEY POINT 3&4	1.00E-05
FORT CALHOUN 1	1.00E-05
CRYSTAL RIVER 3*	5.00E-05
WATERFORD 3	5.00E-05
ARKANSAS NUCLEAR ONE 2	1.00E-04
ARKANSAS NUCLEAR ONE 1*	1.00E-04
DAVIS BESSE*	1.00E-04
TMI 1*	1.43E-04
GINNA	1.80E-04
DIABLO CANYON 1&2	2.00E-04
PALISADES	2.00E-04
BEAVER VALLEY 1	2.02E-04
SOUTH TEXAS PROJECT 1&2	2.02E-04
INDIAN POINT 2	2.02E-04
CALVERT CLIFFS 1&2	2.02E-04
SEQUOYAH 1&2	2.02E-04
BEAVER VALLEY 2	2.03E-04
COMANCHE PEAK 1&2	2.03E-04
WATTS BAR 1&2	2.03E-04
SEABROOK	2.03E-04
PALO VERDE 1,2,&3	2.10E-04
ST. LUCIE 2	2.66E-04
ST. LUCIE 1	2.66E-04
MAINE YANKEE	2.70E-04
MCGUIRE 1&2	3.00E-04
FARLEY 1&2	3.00E-04
BYRON 1&2	3.00E-04
PRAIRIE ISLAND 2	3.00E-04
CATAWBA 1&2	3.00E-04
SUMMER	3.00E-04
BRAIDWOOD 1&2	3.00E-04
PRAIRIE ISLAND 1	3.00E-04
VOGTLE 1&2	3.00E-04
ZION 1&2	3.00E-04
D.C. COOK 1&2	3.00E-04
MILLSTONE 3	3.88E-04
HADDAM NECK	3.90E-04
INDIAN POINT 3	4.77E-04
KEWAUNEE	5.00E-04
NORTH ANNA 1&2	5.00E-04
POINT BEACH 1&2	5.00E-04
CALLAWAY	5.00E-04
WOLF CREEK	5.00E-04
SALEM 2	5.00E-04
SHEARON HARRIS 1	5.00E-04
H.B. ROBINSON 2	5.00E-04
SALEM 1	5.00E-04
SURRY 1&2	5.00E-04
SAN ONOFRE 2&3	5.00E-04
MILLSTONE 2	6.40E-04
OCONEE 1,2,&3*	7.00E-04

* Babcock and Wilcox 177FA Plants

Table 3
IPE Medium-Break LOCA Frequencies
(IPE Database)

Plant Name	Initiating Event Frequency (/yr)
FORT CALHOUN 1	1.00E-04
TURKEY POINT 3&4	1.00E-04
MCGUIRE 1&2	3.00E-04
CATAWBA 1&2	3.00E-04
DAVIS BESSE*	3.00E-04
TMI 1*	3.61E-04
PALISADES	4.00E-04
GINNA	4.00E-04
PALO VERDE 1,2,&3	4.50E-04
DIABLO CANYON 1&2	4.60E-04
INDIAN POINT 2	4.61E-04
BEAVER VALLEY 1	4.61E-04
CALVERT CLIFFS 1&2	4.62E-04
SEQUOYAH 1&2	4.62E-04
SOUTH TEXAS PROJECT 1&2	4.63E-04
BEAVER VALLEY 2	4.64E-04
SEABROOK	4.65E-04
WATTS BAR 1&2	4.65E-04
COMANCHE PEAK 1&2	4.65E-04
CRYSTAL RIVER 3*	5.00E-04
SHEARON HARRIS 1	6.00E-04
HADDAM NECK	6.10E-04
MILLSTONE 3	6.11E-04
OCONEE 1,2,&3*	7.00E-04
MILLSTONE 2	7.10E-04
FARLEY 1&2	7.70E-04
PRAIRIE ISLAND 1	8.00E-04
MAINE YANKEE	8.00E-04
SUMMER	8.00E-04
PRAIRIE ISLAND 2	8.00E-04
BRAIDWOOD 1&2	8.00E-04
BYRON 1&2	8.00E-04
VOGTLE 1&2	8.00E-04
INDIAN POINT 3	9.14E-04
D.C. COOK 1&2	9.17E-04
NORTH ANNA 1&2	1.00E-03
CALLAWAY	1.00E-03
SALEM 2	1.00E-03
POINT BEACH 1&2	1.00E-03
SALEM 1	1.00E-03
SAN ONOFRE 2&3	1.00E-03
WATERFORD 3	1.00E-03
ARKANSAS NUCLEAR ONE 2	1.00E-03
SURRY 1&2	1.00E-03
WOLF CREEK	1.10E-03
ZION 1&2	1.10E-03
KEWAUNEE	2.36E-03
H.B. ROBINSON 2	2.60E-03
ARKANSAS NUCLEAR ONE 1*	NA
ST. LUCIE 1	NA
ST. LUCIE 2	NA

* Babcock and Wilcox 177FA Plants

NRC Comment 2

ISLOCAs were not found to be significant contributors to CDF at CR-3. The ISLOCA analysis, although detailed, appears to have arbitrarily assumed that only 10 percent of valve ruptures occur in the critical parts of the valve, and the rest occurring in the valve bonnet. This assumption may have significantly influenced the ISLOCA result that they are not significant contributors to OF at CR-3. Since ISLOCAs themselves, can be a large component of the risk of offsite radionuclide release, the assumption regarding valve rupture locations requires justification.

FPC Response

Further research for generic data sources for "check valve internal rupture failure rates" resulted in the data shown in Table 4. The aggregated generic failure rate is 7.55E-08 per hour. This number is slightly less than what was used in the original IPE ISLOCA analysis (1.15E-06/hr * 0.1 = 1.15E-07/hr), even when making the assumption that 10% of the check valve ruptures occur through the disk versus the bonnet. Therefore, the ISLOCA analysis should not be non-conservative.

Table 4
Check Valve Internal Rupture Generic Failure Rates

Component Type Code:	CV	**Component Name:**	CHECK VALVE
Failure Mode Type Code:	R	**Failure Mode:**	INTERNAL RUPTURE

AGGREGATED GENERIC FAILURE RATE	MEAN	LOWER	MEDIAN	UPPER	P1	WEIGHT
Interim Aggregated	7.55E-8	2.76E-10	1.60E-8	2.57E-7		
Aggregated generic	7.55E-8	6.05E-9	3.94E-8	2.57E-7	6.52E+0	
Final	7.55E-8	6.05E-9	3.94E-8	2.57E-7	6.52E+0	

GENERIC DATA SOURCES	MEAN	LOWER	MEDIAN	UPPER	P1	WEIGHT
1						
NSAC-154	1.00E-7				10.00	0.250
LOG-NORMAL FIT	1.00E-7	3.75E-9	3.75E-8	3.75E-7	1.00E+1	
NOTE: TABLE A.2-1; RECOMMENDED VALUE; ERROR FACTOR ASSUMED						
2						
LER DATA	1.45E-8	4.94E-9		3.31E-8		0.250
LOG-NORMAL FIT	1.45E-8	4.31E-9	1.19E-8	3.31E-8	2.77E+0	
NOTE: NUREG/CR-5604, P. B-34; INTERNAL LEAKAGE (SEVERE); 4 FAILURES IN						
3						
NUREG/CR-5102	8.74E-8				10	0.250
LOG-NORMAL FIT	8.74E-8	3.28E-9	3.28E-8	3.28E-7	1.00E+1	
NOTE: TABLE A.2; LEAK RATE _ 200 GPM; ERROR FACTOR ASSUMED						
4						
NREP	1.00E-7	1.00E-10		7.00E-7		0.250
LOG-NORMAL FIT	1.00E-7	3.20E-11	2.68E-9	2.24E-7	8.37E+1	
NOTE: NUREG/CR-2815; CATASTROPHIC INTERNAL LEAKAGE						

NRC Comment 3

Certain aspects of the flooding analysis, for example, treatment of drains and maintenance induced floods, do not appear to have been included. Inclusion of these aspects may increase flood CDF. Their exclusion may mask potential procedure-based vulnerabilities.

FPC Response

During the plant walkdowns for the internal flooding analysis, the potential for water to drain into and out of the rooms was examined. It was found that the open design of CR-3 was such that there was little potential for the accumulation of water in the rooms due to drainage from another room or drain blockage.

Maintenance-induced floods were not considered in the CR-3 internal flooding analysis. To assess the impact of maintenance-induced floods on the CR-3 internal flooding analysis, generic industry internal flood data was obtained from the Oconee Nuclear Station Probabilistic Safety Assessment, Table 3.3-3 and Table C-1. It was determined that there have been three maintenance-induced internal floods in 1023.7 reactor-years, translating to a maintenance-induced flood frequency of 2.9E-3 per reactor year. This frequency is for auxiliary building maintenance-induced floods, but should be applicable to other rooms as well. For the screening analysis in the CR-3 internal flooding analysis, an internal flood frequency of 0.03 per year was used; therefore, the addition of maintenance-induced floods would not affect the screening analysis since the screening frequency is so much higher. The maintenance-induced flood frequency of 2.9E-3 per reactor-year (no credit for recovery) is comparable to the pipe rupture flood frequencies used in the CR-3 internal flood analysis, although in some cases adjustments were made to reflect the probability of pipe rupture versus leakage, resulting in CR-3 internal flood analysis pipe rupture frequencies in the 10^{-4} range, approximately an order of magnitude lower than the maintenance-induced flood frequency calculated above. Looking at Table 3.5-3 in the CR-3 IPE, it can be seen that the dominant scenarios are those associated with spray sources which are not affected by the omission of maintenance-induced flooding events. If the frequencies of the remaining scenarios were increased by one order of magnitude to reflect the addition of maintenance-induced floods, their contribution to the overall CR-3 core damage frequency would be minimal. In conclusion, maintenance-induced floods should have been included in the CR-3 internal flooding analysis, although it does not appear that their addition results in an appreciable increase in the overall core damage frequency.

NRC Comment 4

The staff frequently uses NUREG/CR-4550 as a basis for comparison with IPE submittal data. For CR-3, the plant-specific turbine driven emergency feedwater pump failure-to-run probability appears to be two orders of magnitude lower than NUREG-4550. This is an important plant feature for dealing with SBO situations and may contribute to an understated contribution to CDF from an SBO.

FPC Response

The NUREG/CR-4550 turbine-driven emergency feedwater pump fail-to-run probability is 5E-3 per hour and is taken from "an updated value from the Peach Bottom analysis." In the same table that this number appears, there is a column entitled "Range from Other Sources." This gives the range of failure rates from other sources. For turbine-driven emergency feedwater pump fail-to-run probability, this range is 8E-6 per hour to 1E-3 per hour. The NUREG/CR-4550 failure rate is therefore a factor of five greater than the high end of this range, suggesting that the NUREG/CR-4550 failure rate may be too high.

Researching generic data sources for "turbine-driven AFW pump fails to continue running" resulted in the data shown in Table 5. The range of failure rates given in the table is 1.00E-04 per hour to 3.98E-3 per hour. If the aggregated generic failure rate of 1.27E-3 per hour is used for the CR-3 turbine-driven EFW pump, the core damage frequency increases from 1.39E-05 per year to 1.45E-05 per year. This failure rate is now used for the turbine-driven EFW pump in the current CR-3 PSA.

Table 5
AFW Pump Generic Failure Rates

Component Type Code: TP **Component Name:** TURBINE-DRIVEN AFW PUMP
Failure Mode Type Code: F **Failure Mode:** FAILS TO CONTINUE RUNNING

AGGREGATED GENERIC FAILURE RATE	D	MEAN	LOWER	MEDIAN	UPPER	P1	WEIGHT
Interim aggregated		1.27E-3	3.22E-5	3.37E-4	5.37E-3		
Aggregated generic		1.27E-3	2.92E-5	3.78E-4	4.88E-3	1.29E+1	
Final		1.27E-3	2.92E-5	3.78E-4	4.88E-3	1.29E+1	

GENERIC DATA SOURCES	MEAN	LOWER	MEDIAN	UPPER	P1	WEIGHT
1						
NUREG/CR-1205	1.00E-4	9.09E-5		1.10E-4		0.200
LOG-NORMAL FIT	1.00E-4	9.06E-5	9.98E-5	1.10E-4	1.10E+0	
NOTE: P. 392						
2						
SEABROOK PSS	1.03E-3	6.35E-5	4.21E-4	3.00E-3		0.200
LOG-NORMAL FIT	1.03E-3	1.60E-4	6.92E-4	3.00E-3	4.33E+0	
NOTE: GENERIC						
3						
OCONEE	3.98E-3			1.25E-2		0.200
LOG-NORMAL FIT	3.98E-3	4.62E-4	2.41E-3	1.25E-2	5.21E+0	
NOTE: PLANT-SPECIFIC DATA FROM NSAC/60 & IPE; 2 FAILURES IN						
4						
ZION PSS			1.20E-4	1.58E-3		0.200
LOG-NORMAL FIT	4.09E-4	9.10E-6	1.20E-4	1.58E-3	1.32E+1	
NOTE: PLANT-SPECIFIC DATA; 0 FAILURES IN 1900						
5						
INDIAN POINT PSS	8.06E-4	4.15E-5		3.83E-3		0.200
LOG-NORMAL FIT	8.06E-4	3.27E-5	3.13E-4	3.01E-3	9.60E+0	
NOTE: PLANT-SPECIFIC DATA; 1 FAILURE IN 1240						

NRC Comment 5

As the licensee has indicated, common cause failures play a significant role in the CR3 IPE. While somewhat comparable to NUREG/CR-4550 values, the CR3 common cause beta factors are consistently lower, without adequate justification. In addition, common cause effects between the turbine driven and motor driven emergency feedwater pumps are not currently in the IPE model. Use of low values may skew the ranking of predominant accident sequences and mask potential vulnerabilities.

FPC Response

The common-cause failure analysis has been redone in a more rigorous fashion. A discussion of the revised common-cause failure analysis is included as Attachment 2. The impact of the revision of the common-cause failure analysis on the overall CR-3 core damage frequency and risk profile was minimal. Some of the new beta factors are higher; some are lower. No new vulnerabilities were found.

The common-cause failure analysis for the CR-3 PSA has been redone in a more rigorous fashion. A common-cause failure event for turbine-driven and motor-driven emergency feedwater pumps is now included in the model. A discussion of the new common-cause failure analysis is included in Attachment 2.

HUMAN RELIABILITY ANALYSES

NRC Comment 1

Post initiator human actions included recovery actions which typically are not covered by procedures. No justification was provided, however, for any of the modeled non-proceduralized actions and without such justification there does not appear to be an adequate basis for the human error probabilities (HEPs) assigned to the events.

FPC Response

The human reliability analysis for dynamic human error events has been completely redone. A discussion of the revised human reliability analysis is included as Attachment 2. The impact of the revision of the human reliability analysis on the overall CR-3 core damage frequency and risk profile was minimal. Very little credit is taken for non-proceduralized actions.

NRC Comment 2

Limited consideration of plant-specific performance shaping factors and dependencies and inadequate treatment of these factors can result in HEPs which are more generic in nature than plant-specific. Thus, an opportunity is lost to gain insights into operator performance. Also, the resulting HEPs may be either optimistic or pessimistic, especially when dependencies are involved which, if ignored, could lead to low HEPs.

FPC Response

The human reliability analysis for dynamic human error events has been completely redone. A discussion of the revised human reliability analysis is included in Attachment 2. The new method addresses specific opportunities for error in both the diagnostic and execution phases of the operator action. Dependencies between operator actions are also addressed.

NRC Comment 3

Documentation was inadequate on the process used to determine the time available for operators to diagnose needed actions and on the time needed to conduct the actions (particularly outside the control room). In general, because of the sparse documentation, it is not clear that time was appropriately considered in the quantification of operator actions.

FPC Response

The human reliability analysis for dynamic human error events has been completely redone. For each event, a time line was developed, including the estimated time for diagnosis and execution. These time lines were developed by examining procedures and interviewing operators. Descriptions of the event, procedure references, time lines, and breakdown of operator activities and opportunities for errors are documented in individual worksheets, one for each dynamic human error event. A discussion of the revised human reliability analysis is included as Attachment 2. This discussion is based on PSA model that exists today (July, 1997) for CR-3.

BACK-END ANALYSES

NRC Comment 1

Because a sensitivity study, as recommended in NUREG-1335, was not performed, the IPE did not provide any quantitative insights on how containment failure probabilities would change if uncertainties in containment phenomena were considered.

FPC Response

FPC will provide a response to this comment in accordance with a plan that will be developed following a technical meeting between the NRC and FPC on the CR-3 IPE.

NRC Comment 2

A relatively low source term (i.e., a release fraction less than 2E-06 for iodine and cesium), resulting from the late containment failure mode with no containment systems available, was reported by CR3, without adequate justification.

FPC Response

The source term for late containment failure mode with no containment systems available, referred to in the NRC comments, is the source term for station blackout (K7D), Table 4.67.6-3 in the CR-3 IPE. The iodine and cesium release fractions in this table are 1.77E-06 and 1.05E-06, respectively. In the "Evaluation of Severe Accident Risks: Zion, Unit 1," Vol. 7, Rev. 1, Part 2B, the release fractions reported on page B-129, Table B.3-2, "Zion Source Term Statistics for Release Fractions for Late Containment Failure," are 7.49E-05 for iodine and 5.43E-07 for cesium. The iodine release fraction for CR-3 is approximately one and a half orders of magnitude less than the Zion release fraction, and the cesium release fraction for CR-3 is approximately half an order of magnitude greater than the Zion release fraction. Both sets of release fractions are well within the uncertainty bounds for the calculations.

An explanation of the removal of cesium iodide (CsI) from the containment atmosphere for the "station blackout with late containment failure" scenario is given on page 304 of the CR-3 IPE and repeated here: "Since this KPDS sequence has no fan coolers in operation, the initial (before 500 minutes) removal of CsI from the containment atmosphere is due to the condensation of steam on heat structures while the later (after 500 minutes) removal is mainly due to the deposition of aerosol in an non-condensing atmosphere. This aerosol deposition behavior is typical not only of the volatile species, but also the non-volatiles. The fission product results show that, by about 700 minutes, essentially all the fission products are deposited and their release rates from the core-concrete interaction become small enough that no appreciable new airborne inventories are observed. The environmental source terms being carried by the containment leakage flatten out and increase at a negligible rate at approximately 700 minutes. The exceptions are the particulate inert aerosols, which are continuously produced by the core-concrete interaction as a result of the concrete decomposition. However, these aerosols are not radioactive, and therefore of no further interest in this discussion. As in the case of the K4K analysis, fission product deposition plays a primary role in removing the fission products generated by the core-concrete interaction."

The CR-3 key accident sequence analyses were performed employing three well-known computer codes. For the in-vessel thermal-hydraulic analyses, the MARCH3 code was run. TRAPMELT3 was used to examine the in-vessel behavior of fission products. MARCH3 and TRAPMELT3 are both part of the NRC's own Source Term Code Package (STCP). CONTAIN 1.1 was used to evaluate the thermal-hydraulic behavior of the containment along with the behavior of the fission products released to the containment from the primary system and the core-concrete interaction (CCI). At the time of the IPE submittal, CONTAIN was the U. S. Nuclear Regulatory Commission's principal best estimate mechanistic containment analysis code for severe accidents. Details of the modeling are included in Chapters 4.2 and 4.6 of the IPE. The fission product masses released to the environment for the "late containment failure mode with no containment systems available" case, and the other cases, were calculated by these code simulations and are based on the CR-3 plant-specific reactor and containment design which were input to the codes. Detailed explanations of the results of these calculations for each of the key plant damage states were given in Chapter 4.6 of the CR-3 IPE, including the explanation of the fission product deposition characteristics for the "late containment failure mode with no containment systems available" reiterated above. Such a detailed and plant-specific approach using NRC's own codes accompanied by the detailed narratives describing the severe accidents scenarios (with specific attention to source term behavior) is adequate justification for the calculated source terms.

<u>NRC Comment 3</u>

The discussion of plant-specific seal materials and their properties at elevated temperatures is not adequate. The licensee has stated that their gross containment failure pressure is slightly lower than many other similar large, dry containments. Since this failure pressure is approximately the same as the typical failure pressure for seal material failure under harsh conditions, they stated that it was not necessary to investigate seal behavior, since either the containment or the seals would fail at about the same time. The staff disagrees since it may be determined that the existing seal material itself, may have lower performance characteristics than the norm as did the containment structure; and consequently, may fail at a lower failure pressure than the containment.

FPC Response

FPC will provide a response to this comment in accordance with a plan that will be developed following a technical meeting between the NRC and FPC on the CR-3 IPE.

NRC Comment 4

Containment isolation failure was not discussed in enough detail for the staff to determine whether the analysis addressed the areas identified in GL 88-20.

FPC Response

FPC will provide a response to this comment in accordance with a plan that will be developed following a technical meeting between the NRC and FPC on the CR-3 IPE.

NRC Comment 5

There was virtually no discussion of the containment performance improvements program issue concerning the important phenomenology of hydrogen pocketing and detonation during accident progression following a core melt.

FPC Response

FPC will provide a response to this comment in accordance with a plan that will be developed following a technical meeting between the NRC and FPC on the CR-3 IPE.

VULNERABILITY DEFINITION

NRC Comment

The licensee reviewed core damage cutsets "for sequences with unusually high frequencies, sequences hinting of some heretofore unknown dependency, and risk significant sequences which can easily be reduced to risk insignificant via a procedure change or a minor hardware change." Based on this concept, the licensee did not identify any vulnerabilities. Similarly, no plant improvements were identified. As discussed below, the staff is concerned, however, that the CR3 IPE process, as described in the submittal, including the qualitative definition of a vulnerability, may not be adequate to uncover vulnerabilities or point to appropriate plant improvements.

FPC Response

There is no precise definition of vulnerability for the CR-3 IPE; it is more of a process than a threshold. Review of the core damage cutsets looking for sequences with unusually high frequencies, sequences which reveal some heretofore unknown dependency, and risk-significant sequences which can easily be reduced to risk-insignificance via a procedure change or minor hardware change consisted of FPC's review of the IPE results for vulnerabilities. To state the definition of a vulnerability in purely quantitative terms would result in sequences which are normally expected to be dominant contributors, such as station blackout, being identified as vulnerabilities. Regardless of what procedure or design changes are implemented, there will always be dominant contributors. Just because they are dominant contributors does not mean they should be considered vulnerabilities. The PSA analyst is intimately involved in the quantification of the risk of core damage and radioactive release. The core damage cutsets are examined in detail in order to understand them and to investigate possibilities for recovery. Risk importance measures are calculated, and the plant components are ranked by risk importance. This quantitative approach, coupled with the qualitative guidance above, will serve to enhance the identification of vulnerabilities. It is highly unlikely that a vulnerability will go undiscovered during this process.

ATTACHMENT 2

COMMON CAUSE FAILURE AND HUMAN RELIABILITY ASSESSMENT
FOR THE CURRENT CR-3 PROBABILISTIC SAFETY ASSESSMENT (PSA) MODEL
(36 pages)

3.3.4 Common Cause Failures

The assessment of common cause failures for the CR-3 PRA is consistent with the methods developed jointly by the USNRC and EPRI (References 3.3-6 and -7) and the data base of events collected by EPRI (Reference 3.3-8). This data base documents commercial U. S. light water reactor experience with redundant components that have experienced one or more common cause events. This generic data base was used because common cause failures are sufficiently rare that there was insufficient plant-specific experience to allow their probabilities to be quantified directly. The common cause analysis consisted of a review of the system fault trees comprising the core-damage model for CR-3 and quantification of the common cause failures using currently available methods and data. The quantification methodology consisted of the evaluation and application of parameters using the multiple Greek letter (MGL) approach.

The review of the system fault trees was primarily aimed at ensuring that groups of common cause failures had been incorporated in a systematic and comprehensive manner. This entailed examining the fault trees to identify groups of similar components serving redundant functions. The focus of this review was on components within the same system, although an attempt was made to identify candidate common cause groups that crossed system boundaries. For example, common cause failures were introduced that reflect the potential for failure of the pumps in both the nuclear services seawater (NSSW) and decay heat seawater (DHSW) systems. Although the pumps in these two systems are not identical, they were judged to be sufficiently similar with respect to both design and operating conditions that the possibility they could be subject to the same common cause of failure could not be ruled out.

In addition to ensuring that common cause failure groups were adequately identified, it was necessary to define new events to account for multiple combinations of failure in conjunction with the transformation to the MGL approach. This was done in selected cases for common cause failure groups of three or more components.

The process of quantifying the probabilities for the common cause events consisted of examining summaries of actual events that reflected common cause failures (or at least the potential for common cause failures). These events were compiled by EPRI (Reference 3.3-8). The events had previously been reviewed by

EPRI to assess, on a generic basis, the potential for each event to have been a common cause failure. The results of this generic review were reported in the form of an impact vector based on the effective number of independent or common cause failures represented by the event. EPRI also noted any particularly important conditions that would influence whether the event would constitute a common cause failure for a specific plant and system.

These events were then reviewed to develop an impact vector specific to the system configuration and operating characteristics at CR-3. This review entailed determining whether the failure mode corresponding to the event was relevant to the CR-3 system of interest. The impact vector was then adjusted to account for these plant-specific considerations. Next, the impact vector was adjusted to account for differences in the levels of redundancy between the system at the plant at which the event occurred and the comparable CR-3 system. This adjustment entailed "mapping up" or "mapping down", using a set of formulas defined for this purpose.

The results of the individual impact vectors for a particular component type and failure mode were then accumulated to determine the effective numbers of common cause failure events of a portion of a redundant set, or the entire set. These values were then used to quantify the MGL parameters through a Bayesian update process. The prior distribution for this Bayesian update was assembled by an expert panel, and is described in EPRI Report TR-100382 (Reference 3.3-8). The Bayesian update process was useful particularly for cases in which there was relatively weak evidence of common cause failures, especially for levels of redundancy greater than two. For other cases, in which there was somewhat more extensive evidence of common cause failures, the Bayesian update procedure had minimal impact on the results. The common cause parameters that were calculated using this process are summarized in Table 3.3-4. Quantification of these parameters was accomplished using Excel worksheets, an example of which is given in Figure 3.3-1.

For some components, the event data base did not provide information sufficient to permit common cause parameters to be quantified. For these cases, generic values suggested in NUREG/CR-5801 were applied. These factors are reiterated in Table 3.3-5 for reference purposes.

The probabilities for the specific common cause events defined during the review of the system fault trees were then quantified by multiplying the basic (independent) failure probability by the appropriate common cause factor from Table 3.3-4 or 3.3-5.

Table 3.3-4
Summary of Common-Cause Parameters

Component	Size of CCF Group	Failure Mode	CCF Parameter	Common-Cause Multiplier
Diesel generators	2 generators	Fail to start	b = 0.010	2 of 2; 0.010
		Fail to run	b = 0.016	2 of 2; 0.016
Circuit breakers	2 breakers	Fail to operate	b = 0.11	2 of 2; 0.11
Motor-operated valves	2 valves	Fail to operate	b = 0.031	2 of 2; 0.031
	4 valves	Fail to operate	b = 0.050	2 of 4; 0.0085
			g = 0.49	3 of 4; 0.0031
			d = 0.61	4 of 4; 0.015
Check valves	2 valves	Fail to open	b = 0.027	2 of 2; 0.027
	4 valves	Fail to open	b = 0.071	2 of 4; 0.022
			g = 0.097	3 of 4; 0.0013
			d = 0.42	4 of 4; 0.0029
Safety/relief valves[1]	2 valves	Fail to open	b = 0.055	2 of 4; 0.055
Makeup pumps	3 pumps	Fail to start	b = 0.12	2 of 3; 0.054
			g = 0.10	3 of 3; 0.012
		Fail to run	b = 0.0050	2 of 3; 0.0018
			g = 0.27	3 of 3; 0.0014
Decay heat pumps	2 pumps	Fail to start	b = 0.018	2 of 2; 0.018
		Fail to run	b = 0.012	2 of 2; 0.012
Building spray pumps	2 pumps	Fail to start	b = 0.22	2 of 2; 0.22
		Fail to run	b = 0.0085	2 of 2; 0.0085
Emergency feedwater pumps[2]	2 pumps	Fail to start	b = 0.027	2 of 2; 0.027
Closed cycle cooling pumps	2 pumps	Fail to start	b = 0.016	2 of 2; 0.016
		Fail to run	b = 0.017	2 of 2; 0.017
	3 pumps	Fail to start	b = 0.021	2 of 3; 0.0084
			g = 0.21	3 of 3; 0.0046
		Fail to run	b = 0.033	2 of 3; 0.013
			g = 0.22	3 of 3; 0.0073
Service water pumps	2 pumps	Fail to start	b = 0.045	2 of 2; 0.045
		Fail to run	b = 0.017	2 of 2; 0.017
	3 pumps	Fail to start	b = 0.037	2 of 3; 0.015
			g = 0.20	3 of 3; 0.0074
		Fail to run	b = 0.037	2 of 3; 0.015
			g = 0.18	3 of 3; 0.0067
	4 pumps	Fail to start	b = 0.030	2 of 4; 0.0079
			g = 0.22	3 of 4; 0.0013
			d = 0.39	4 of 4; 0.0025

Table 3.3-4 (continued)
Summary of Common-Cause Parameters

Component	Size of CCF Group	Failure Mode	CCF Parameter	Common-Cause Multiplier
Service water pumps (cont.)	4 pumps	Fail to run	β = 0.041	2 of 4; 0.0089
			γ = 0.35	3 of 4; 0.0036
			δ = 0.25	4 of 4; 0.0037
Chiller units	2 chillers	Fail to run	β = 0.048	2 of 2; 0.045
Fans	2 fans	Fail to start	β = 0.078	2 of 2; 0.078
		Fail to run	β = 0.086	2 of 2; 0.086
	4 fans	Fail to start	β = 0.019	2 of 4; 0.027
			γ = 0.57	3 of 4; 0.011
			δ = 0.71	4 of 4; 0.076
		Fail to run	β = 0.19	2 of 4; 0.038
			γ = 0.40	3 of 4; 0.0055
			δ = 0.78	4 of 4; 0.060

[1]Generic value used due to lack of reported events for this component type.
[2]Common-cause factors were evaluated for the emergency feedwater pump group, which includes one steam-driven and one motor-driven pump. There was no evidence of events involving common cause failure to run that would apply to EFW pumps with diverse drivers.

Table 3.3-5
Generic Common-Cause Parameters

System Size	Type of Failure	CCF Parameter	Common-Cause Multiplier
Two components	Fail on demand	β = 0.10	2 of 2; 0.10
	Fail during operation	β = 0.05	2 of 2; 0.050
Three components	Fail on demand	β = 0.10	2 of 3; 0.037
		γ = 0.27	3 of 3; 0.027
	Fail during operation	β = 0.050	2 of 3; 0.018
		γ = 0.27	3 of 3; 0.014
Four components	Fail on demand	β = 0.11	2 of 4; 0.021
		γ = 0.42	3 of 4; 0.0092
		δ = 0.40	4 of 4; 0.018
	Fail during operation	β = 0.055	2 of 4; 0.011
		γ = 0.42	3 of 4; 0.0046
		δ = 0.40	4 of 4; 0.0092

Figure 3.3-1
Assessment of Common-Cause Failure (MGL) Parameters

System:	Electric power (ac)	**Component:**	Diesel generators
System Size:	2	**Failure Mode:**	Fail to run

Impact Assessment

100382 Event	Shock [ρ]	Pop	Appl.	Impact Vectors 0	1	2	3	4	NA	Comment
1	NL	4	Original	0	1	0	0	0	0	
(p. 3-7)			CR-3 Ra	0	1	0	0	0	0	
			CR-3 ma	0.5	0.5	0	0	0	0	
2	NL	8	Original	0	0.93	0.07	0	0	0	
(p. 3-8)			CR-3 Ra	0	0.93	0.07	0	0	0	
			CR-3 ma	0.477	0.512	0.012	0	0	0	
3	NL	3	Original	0	1.97	0.017	0	0	0	
(p. 3-9)			CR-3 Ra	0	1.97	0.017	0	0	0	
			CR-3 ma	0.657	2.638	0.006	0	0	0	
4	NL	3	Original	0	0	0	1	0	0	
(p. 3-10)			CR-3 Ra	0	0	0	0	0	1	DGs not run in parallel.
			CR-3 ma	0	0	0	0	0	1	
5	NL	2	Original	0	0.01	0.07	0	0	0	
(p. 3-11)			CR-3 Ra	0	0.01	0.07	0	0	0	
			CR-3 ma	0	0.01	0.07	0	0	0	
6	NL	3	Original	0	0	0.9	0.1	0	0	
(p. 3-12)			CR-3 Ra	0	0	0.9	0.1	0	0	
			CR-3 ma	0	0.6	0.4	0	0	0	
7	NL	2	Original	0	0	1	0	0	0	
(p. 3-13)			CR-3 Ra	0	0	1	0	0	0	
			CR-3 ma	0	0	1	0	0	0	
Total		7		1.633	4.26	1.487	0	0	1	

Number of Independent Failures

Average system size	2.06	(EPRI TR-100382, Table 3-5)
Additional independent failures	174	(EPRI TR-100382, p. 3-24)
Effective independent failures	173.2	

Parameter Assessment

	Beta Distribution Parameters A	B	C	D	E	F
Prior distribution	0.246	21.2	NA	NA	NA	NA
Posterior distribution	3.221	194.4	NA	NA	NA	NA

Start or run? run

Results

	Independent	β	γ	δ
Raw assessment				
MGL parameters	–	1.7E-2	NA	NA
Multipliers (Qn/Qt)	0.983	1.7E-2	NA	NA
Bayesian update				
MGL parameters	–	1.6E-2	NA	NA
Multipliers (Qn/Qt)	0.984	1.6E-2	NA	NA

3.3.5 Human Reliability Assessment

The assessment of human reliability is one of the most important tasks in a comprehensive PRA. Operating experience has repeatedly demonstrated that human interactions can have a strong influence on the potential for an accident to occur or for one to be avoided. This influence has been reflected in the results of virtually every PRA that has been performed as well. The importance of this area in PRA is heightened because there are no universally accepted procedures for identifying risk-relevant human events or for quantifying their probabilities of occurrence.

The overall approach taken in the assessment of human interactions for the CR-3 PRA is consistent with the SHARP1 framework developed by EPRI (Reference 3.3-9). The SHARP1 framework emphasizes making the human reliability assessment an integral part of the process of developing and quantifying the models that define accident sequences and system failures. It suggests organizing the human reliability assessment into four stages:

1. Plant logic model development: including in the development of the event and fault trees the appropriate human actions and, in particular, reflecting explicitly dependencies of systems and equipment on human interactions.

2. Quantification: estimating the probabilities of the events included in the logic models.

3. Analysis of recovery actions: consideration of actions that could be taken to restore a lost safety function by making repairs or by implementing alternative system configurations during an upset event.

4. Internal review: ensuring that the way in which the human interactions are incorporated into the models and quantified is appropriate through review by a multi-disciplinary team.

Section 3.3.5.1 describes the approaches taken to incorporating the consideration of human interactions into the logic models that define the core-damage sequences. The methods used to quantify the probabilities of different types of human interactions, including the interactions that are part of recovery events, are then outlined.

3.3.5.1 Integration of Human Interactions Into Plant Models

The consideration of human interactions was an integral element in the process of developing the plant logic models (comprised of the event trees and their supporting logic and the system fault trees). These interactions fall into three general categories (again, consistent with the SHARP1 framework):

1. Type A interactions, which take place prior to an initiating event, and which usually leave a component or system in an undesired state that does not manifest itself until an initiating event occurs. These are referred to as pre-initiator events or latent human errors.

2. Type B interactions, which are human actions that contribute to the occurrence of an initiating event.

3. Type C interactions, which describe the response of the operating staff to an initiating event or other upset event. Interactions of type C are further categorized as type CP (procedure-driven actions) and type CR (recovery actions not generally governed by procedures).

Efforts during the modeling process were primarily directed at identifying interactions of types A and C. As is usually the case in PRAs, the initiating events for this study were identified and their frequencies estimated without attempting to pinpoint specific causes for the events. Type B interactions are therefore implicitly included in the initiating events, but they are not considered in detail.

One type of post-initiator interaction that requires special consideration is comprised of errors of commission. This refers to cases in which the operators have made a misdiagnosis of the situation, such that they take intentional (but erroneous) actions that exacerbate the accident. At the present time there are no well-developed methods for systematically identifying such actions or for quantifying their probabilities of occurrence. It is generally considered by human reliability analysts that the present use of symptom-based procedures significantly reduces the opportunities for these errors of commission. Throughout the modeling process, the analysts for this study maintained an awareness of the potential for such actions, but none that appeared to merit detailed consideration were identified. A different type of commission error was included in the assessment of both type A and type C interactions. These included execution errors (such as selecting the wrong valve for operation or closing the wrong breaker), rather than errors cognitive in nature.

Model Integration for Latent Human Errors

Because the nature of type A interactions is to leave equipment unavailable or in a degraded state, events corresponding to this type of interaction were incorporated directly into the system fault trees. These events reflect such faults as failure to restore a pump to operable status (e.g., by leaving the pump's breaker racked open); failure to reopen a manual isolation valve following maintenance or testing; and improperly calibrating instruments that could affect actuation of safety equipment. Events corresponding to latent human errors were included in the fault trees at the level of the affected components. The potential that a human action could leave more than one train of a standby system unavailable was also considered. These failures were modeled in the fault trees as well. The methods used to quantify the probabilities of type A events (latent human errors) are described in Section 3.3.5.2.

Model Integration for Post-Initiator (Type CP) Human Interactions

Consideration of those post-initiator human interactions that are directed by procedures, referred to here as type CP, was a more complex undertaking. Integration of type CP interactions into the modeling process was, however, potentially more important to accurate treatment of the core-damage sequences than was the case for pre-initiator actions.

To delineate system response to particular types of upset events, it can be as important to understand the intended response of the operating crew in using the system as it is to understand the design of the system itself. Thus, in defining the sequence delineation for particular initiating events, it was necessary to review carefully the operating procedures, including the emergency procedures and the various abnormal procedures. This review was aimed at identifying any operator-driven considerations that would affect the modeling process, such as the priorities that might come into play when multiple options were available for maintaining core cooling, or the cues that might indicate the need to change operating modes. These procedure reviews were augmented by obtaining input from operators. This was done by having a senior reactor operator review the core damage sequences for recovery possibilities, and through extensive discussions with operators regarding specific scenarios.

At the same time, operator actions, whose failures could lead to failures of the safety functions required to maintain core cooling, were identified in this process. Typically, these interactions were one of the following:

1. The failure to change the mode of a system under the appropriate conditions (such as accomplishing the switchover of the safety injection systems to draw suction from the containment sump when the BWST inventory is depleted); or

2. The failure to initiate the function of a system that normally requires manual actuation (such as starting the motor-driven feed pump) or to align a backup system.

Type CP interactions in the logic models were included at the highest level consistent with their effects. This treatment helps to highlight the events, and focuses consideration on cognitive aspects of the response to upset conditions. The methods used to quantify type CP events are described in Section 3.3.5.2.

Modeling for Non-Proceduralized (Type CR) Human Interactions

In contrast to type CP interactions, type CR interactions represent the failure to take action to compensate for one or more system failures by means that are not necessarily covered explicitly by procedures. The potential for type CR interactions arises when there is time to make a diagnosis and decide on a course of action, but the actions themselves are not guided explicitly by procedures. In these cases, it is the knowledge base of the operators and, often, of additional support staff such as those in the technical support center (TSC), that is important. Because of these fundamental differences, different approaches are taken in assessing type CP and type CR events. Interactions of type CR were not included directly in the logic models; instead, they were appended to the sequence cutsets as appropriate on a case-by-case basis during the sequence quantification process.

The process of identifying type CR events that should be considered involved a careful review of the minimal cutsets dominating each core-damage sequence. Each of these cutsets was examined first to ensure that the specific context of the scenario it implied to was well understood by the analysts. This was especially important for cutsets that included failures of support systems (such as electric power or cooling water). Support system faults could cause both the unavailability of the equipment modeled in the sequence and system logic and, potentially, other equipment that might not have been modeled explicitly, but might be needed to effect a particular recovery option. After developing the appropriate understanding of the context for a cutset, possible measures to use the equipment remaining were considered. This entailed first an examination of the operating procedures for any general guidance that might apply in such a circumstance, followed by discussions with plant operators to determine an expected course of action most likely to be pursued. Once these options were identified, they were examined more closely to determine whether or not they were feasible, given the time available for decision-making, execution and the impact of other failures in the cutset on the potential for the action to succeed. The potential that a successful recovery or unsuccessful attempt could introduce other sequences of events was also considered. Once these factors were identified, a probability for failure of the recovery action was estimated, as described in Section 3.3.5.2.

It should be emphasized that relatively few events of type CR were included in the quantification of the core-damage frequencies. Nearly all potentially important opportunities for recovery are well covered by the emergency or other operating procedures and are hence evaluated as type CP interactions. Only in cases with clear opportunities for success that include procedural guidance leading to the expected recovery action, and primarily for cases when the time available was relatively long, were type CR interactions considered in detail.

3.3.5.2 Quantification of Human Interactions

The approaches taken in quantifying the probabilities of the human interactions in this PRA reflect methods currently in wide use in nuclear plant PRAs. The methods for each of the types of human interactions discussed above are described in the following sections.

Quantification of Latent Human Errors

The techniques used in this assessment are based on the methods presented in the textbook Human Reliability Analysis by Dougherty & Fragola (Ref. 3.3-10). A latent human error (or "slip" in the taxonomy presented in Human Reliability Analysis or latent error) is an action not as intended, i.e., the person meant to do something and didn't, or did it wrong.

Latent events are usually the result of maintenance faults which have occurred long before the initiating event of the sequence being analyzed. Past HRA evaluations have generally set the probability of these type of events between 0.01 and 0.001. In the CR-3 PRA the basic probabilities used were 0.001 for electrical components and 0.003 for mechanical components. These base probabilities are then adjusted by using performance shaping factors (PSFs), which account for the use of surveillance procedures, functional testing, and multiples components. Additional factors can be added to account for special items such as a double signoff on surveillance procedures. The value used for the PSFs was 0.1.

The form of the probability calculation is:

$$Pr = base \times psf1 \times psf2\ \ldots$$

Table 3.3-6 lists the latent human errors used in this PRA. To simplify the data management, all of the specific latent events were related to one of four generic events as described below:

LGENSCRN A generic screening value for an electrical system component.

LGENELE1 An electrical system component, which is monitored by a surveillance procedure requiring a double verification signoff.

LGENMEC1 A mechanical system component, which is monitored by means of a procedural functional test.

LGENMEC2 A mechanical system component, which is monitored by a surveillance procedure. This event is also used for basic events which contain multiple components, although it is conservative for this condition.

Table 3.3-6
Latent Human Event Errors

BASIC EVENT	DESCRIPTION	PROBABILITY	SOURCE	SURVEILLANCE	FUNCTIONAL TEST	OPTIONAL PSF
ACB3103X	BREAKER LEFT UNAVAIL. FOLLOWING MAINT.	1.00E-03	LGENSCRN	N	N	1.00
ACB3104X	BREAKER LEFT UNAVAIL. FOLLOWING MAINT.	1.00E-03	LGENSCRN	N	N	1.00
EBIHPCHX	HI PRESS TRIP BISTABLES MISCALIBRATED HI	1.00E-05	LGENELE1	Y	N	0.10
EBILPCHX	LOW PRESS TRIP BIST. S MISCALIBRATED HI	1.00E-05	LGENELE1	Y	N	0.10
EPSRBCLX	RB ISO. PRESS SWITCHES MISCALIBRED LOW	1.00E-05	LGENELE1, SP-132	N	N	0.00
EPTCALHX	RC PRESS TRANSMITTERS MISCALIBRATED HIGH	1.00E-05	LGENELE1, SP-132	N	N	0.00
ESWRB10X	CHANNEL INADVERTENTLY BYPASSED	1.00E-03	LGENSCRN	N	N	1.00
ESWRB20X	CHANNEL INADVERTENTLY BYPASSED	1.00E-03	LGENSCRN	N	N	1.00
ESWRB30X	CHANNEL INADVERTENTLY BYPASSED	1.00E-03	LGENSCRN	N	N	1.00
ESWRC10X	CHANNEL INADVERTENTLY BYPASSED	1.00E-03	LGENSCRN	N	N	1.00
ESWRC20X	CHANNEL INADVERTENTLY BYPASSED	1.00E-03	LGENSCRN	N	N	1.00
ESWRC30X	CHANNEL INADVERTENTLY BYPASSED	1.00E-03	LGENSCRN	N	N	1.00
ESWRC40X	CHANNEL INADVERTENTLY BYPASSED	1.00E-03	LGENSCRN	N	N	1.00
ESWRC50X	CHANNEL INADVERTENTLY BYPASSED	1.00E-03	LGENSCRN	N	N	1.00
ESWRC60X	CHANNEL INADVERTENTLY BYPASSED	1.00E-03	LGENSCRN	N	N	1.00
LTEB10LX	TE-10 CALIBRATED LOW	1.00E-05	LGENELE1	Y	N	0.10
LTEBT8LX	TE-8 CALIBRATED LOW	1.00E-05	LGENELE1	Y	N	0.10
LTEBT9LX	TE-9 CALIBRATED LOW	1.00E-05	LGENELE1	Y	N	0.10
PHXCD--Z	CDHE TRAIN NOT RESTORED AFTER MAINT.	1.00E-03	LGENSCRN	N	N	1.00
PLL1109X	LOW LEVEL LIMITER 11.9 CALIBRATED LOW	1.00E-03	LGENSCRN	N	N	1.00
PSM1605X	LO LEVEL ON SIGNAL MONITOR MISCALIBRATED	1.00E-05	LGENELE1	Y	N	0.10
QBILLSLX	LOW LEVEL INITIATION SETPOINT SET LOW	1.00E-05	LGENELE1	Y	N	0.10
QLTCD59X	LEVEL TRANSMITTER CALIBRATED HIGH	1.00E-05	LGENELE1	Y	N	0.10
QLTEFT2X	EFT-2 LEVEL TRANSMITTERS CALIBRATED HIGH	1.00E-05	LGENELE1	Y	N	0.10
QLTLLCHX	LOW RANGE LEVEL TRANSMITTERS CAL. HIGH	1.00E-05	LGENELE1	Y	N	0.10
QXVEFP2X	PUMP COOLING LINES MISALIGNED CLOSED	3.00E-05	LGENMEC1	Y	Y	1.00
RPS8RC3X	PRESSURE SWITCH MISCALIBRATED	1.00E-03	LGENSCRN	N	N	1.00
SPSP151X	PRESSURE SWITCHES PS-151,206 CAL. HIGH	1.00E-05	LGENELE1	Y	N	0.10
SXV2AFLX	RWP-2A FLUSH WATER VALVES LEFT UNAVAIL.	3.00E-04	LGENMEC2	Y	N	1.00
SXV2BFLX	RWP-2B FLUSH WATER VALVES LEFT UNAVAIL.	3.00E-04	LGENMEC2	Y	N	1.00
SXV3AFLX	RWP-3A FLUSH WATER VALVES LEFT UNAVAIL.	3.00E-04	LGENMEC2	Y	N	1.00
SXV3BFLX	RWP-3B FLUSH WATER VALVES LEFT UNAVAIL.	3.00E-04	LGENMEC2	Y	N	1.00
SXVEFP1X	PUMP COOLING LINES MISALIGNED CLOSED	3.00E-05	LGENMEC1	Y	Y	1.00

Quantification of Type CP Interactions

The post-initiator interactions of type CP that were incorporated into the logic models were each initially assigned a probability of failure of 1.0. This was done, rather than assessing some (lower) screening value, because of the potential for combinations of events to occur in the sequence cutsets. Even a screening value of 0.1 could result in underestimating the combined probability for three or four events occurring together, considering the likelihood that some level of inter-dependence would exist for the events. Detailed estimation of failure probabilities for the post-initiator events was performed only after the sequence quantification was underway, and then only for those events that were found in the sequence cutsets above the cut-off frequencies used.

Quantification of the type CP events that survived this level of screening was performed using a methodology developed relatively recently by EPRI, and described in its report TR-100259 (Reference 3.3-11). The methodology entails considering both the failure to initiate correct response (due to failure in detection, diagnosis, or decision-making), and failure to execute the response correctly. The total probability for a particular human interaction is the sum of the probabilities for these two portions, which are denoted as p_c and p_e, respectively.

The report TR-100259 provides a process for evaluating individual human interactions by breaking down the detection, diagnosis, and decision-making aspects (the p_c portion) into different failure mechanisms, with causes of failure delineated for each. For this reason, EPRI refers to this as a cause-based approach. The failure mechanisms and corresponding causes allow a wide variety of performance shaping factors to be taken into account. Eight different potential failure mechanisms are identified in the methodology:

$p_c a$	Availability of information
$p_c b$	Failure of attention
$p_c c$	Misread/Miscommunicate data
$p_c d$	Information misleading
$p_c e$	Skip a step in procedure
$p_c f$	Misinterpret instruction
$p_c g$	Misinterpret decision logic
$p_c h$	Deliberate violation

A relatively simple decision tree is provided for each of these mechanisms in the EPRI report. Each of these decision trees identifies factors that could cause the relevant mechanism to lead to failure to initiate the proper action. It is the task of the human reliability analyst to select branch points in the decision trees that correspond to the aspects of the interaction being analyzed (e.g., the number and quality of cues for the operators, the ease of use of the procedures, etc.). For each outcome in the decision trees, a nominal probability of failure is suggested.

Depending on the failure cause, certain recovery mechanisms may come into play. Table 4-1 in TR-100259 outlines the nature of any recovery that may be credited for each of the eight failure mechanisms relating to the decision-based (p_c) part of the interaction. The potential for recovery is considered as follows:

1. Due to self-review by the operator initially responsible for the misdiagnosis or error in decision-making, as additional cues become available or additional procedural steps provide opportunity to reconsider;

2. As a result of review by other crew members who would be in a position to recognize the lack of proper response;

3. By the Shift Technical Advisor (STA), whose review might identify errors in response;

4. By the Technical Support Center (TSC) when it is staffed and actively involved in reviewing the situation; and

5. By oncoming crew members when there is a shift turnover.

For example, if the initial error results from a misinterpretation of the decision logic presented in the procedures (i.e., mechanism p_cg), it may be possible that other crew members and/or the shift manager would observe the error and provide input that would lead to taking the proper action.

Unlike some other approaches to the assessment of post-initiator human interactions, time is not a direct determinant of the probability of success or failure. Time is an important consideration, however, with respect to assessing the probabilities for these non-recovery measures.

Thus, after processing each of the decision trees to arrive at estimates for the basic failure mechanisms, the analyst must identify and characterize the appropriate recovery factors. The first element of the type CP interaction (i.e., p_c, the failure to initiate proper response) is then quantified by summing the decision-tree outcomes, as they have been modified by the appropriate recovery factors. This quantification process is relatively straightforward to implement, with the exception that the guidance provided in TR-100259 for characterizing the recovery factors is limited. Clearly, there are often interdependencies among the crew members who might have the opportunity to observe errors and contribute to correcting them. It is necessary, therefore, to characterize the crew members involved in the initial actions, and to identify additional personnel and the roles they might play. Table 3.3-7 identifies the staff at CR-3 that would be available to the control room and the time following an upset event at which their contributions might begin to be made (Reference 3.3-12). This tabulation is derived from a more general version provided in NUREG/CR-1278 (Reference 3.3-12). A comparison to the staffing levels assumed in NUREG/CR-1278 is also provided in the table.

The normal response to a plant upset is for one of the reactor operators to concentrate on the primary systems and for another to attend to the secondary systems. Typically, two such operators are present in the control room at all times. A third reactor operator may or may not be present to aid with specific tasks. A control room supervisor (who is a SRO) is always present in the control room, and it is typically his function to begin following the procedures that are relevant for the symptoms at hand and to direct the actions of the reactor operators. For most of the events in this study, this entails using first the emergency procedures, supplemented by abnormal or system operating procedures as the need arises. For the failure to initiate proper response (the p_c element of type CP interactions), the initial assessment is therefore assumed to apply to this control room supervisor.

Table 3.3-7
Availability of Staff to Respond to Abnormal Events

Time After Initiating Event	Staffing Available per NUREG/CR-1278	Minimum Staffing at CR-3 (AI-500)
0 - 1 min	• on-duty reactor operator	• a reactor operator or senior reactor operator (SRO) • the control room supervisor, a SRO
at 1 min	• on-duty reactor operator • shift supervisor or other SRO	• three reactor operators • the control room supervisor (SRO) • the nuclear shift supervisor (SRO)
at 5 min	• on-duty reactor operator • assigned SRO • shift supervisor • one or more auxiliary operators	• three reactor operators • the control room supervisor (SRO) • the nuclear shift supervisor (SRO) • the shift technical advisor, (STA, a SRO)
at 15 min	• on-duty reactor operator • assigned SRO • shift supervisor • shift technical advisor • one or more auxiliary operators	• three reactor operators • the control room supervisor (SRO) • the nuclear shift supervisor (SRO) • the shift technical advisor, (STA, a SRO) • four equipment operators stationed in plant as needed

The nuclear shift supervisor (also a SRO) has an office near the control room, and would be present in a very short time in the event of a plant transient. Additional chief nuclear operators and a nuclear operator would also be available to respond very quickly as well. The nuclear shift supervisor's role would generally be to make an overall appraisal of the situation, taking such actions as to begin considering the need to notify other personnel and to assess whether any action statements under technical specifications were applicable. The control room supervisor would assist in whatever role was required; this could include taking control for auxiliary panels, such as those dealing with the electrical distribution systems, or organizing and directing equipment operators who would need to accomplish tasks outside the control room.

The STA would be able to respond to the event quickly as well. During an upset event, the STA monitors the plant conditions and attempts to verify that plant conditions or responses have been recognized and attended to properly by the other members of the control room staff.

Opportunities for recovery are largely a function of the time available for response. Thus, for each type CP interaction a time line was constructed. This time line lays out the activities most immediately relevant for the interaction being assessed. This includes: the timing of any failures that lead to the need to take action, the time at which cues to take action (i.e., annunciators or control indications) would be present, and the time by which the interaction must be accomplished to be considered successful. For specific events, this timing was estimated based on available thermal-hydraulic calculations, simple hand calculations, or estimates from operators. The time required for actual implementation of the action was also estimated, usually based on operator interviews. The time window available for initiating response (T_W) is therefore the time between when the compelling cue to take action is received and when the action must be accomplished, less the time required to implement the action. The time after the initial upset and the time window for initiating action are used to determine the availability of additional personnel to review the response and to provide opportunity for recovery of errors.

In this study, where consideration of recovery via extra crew is considered appropriate, the extra crew members consist of the reactor operator to whom the assistant shift supervisor is giving instructions, and in some cases the other reactor operators (e.g., when failure to take appropriate actions relating to the secondary systems would have distinct effects on the response of the RCS). Where this recovery is credited, a constant value of 0.5 is applied, as suggested by Table 4-1 of EPRI TR-100259. Where Table 4-1 indicates credit for review by the STA, it is assumed that monitoring of the situation by the STA and nuclear shift supervisor may be considered. The TSC would be staffed within approximately one hour after an event had been classified as an alert or higher. This classification is made for a variety of accident types, but would not necessarily be made for a reactor trip. The nature of the event prior to the need for the human interaction must therefore be recognized to determine whether or not recovery, via review by the TSC, can be credited. For consideration of review during a shift change, it is assumed that the time window must be at least six hours long.

The levels of dependence assumed for the review functions in this study (aside from the constant non-recovery probability of 0.5 used for extra crew members) are summarized in Table 3.3-8. This table indicates the level of dependence assumed for review by the STA function, by the TSC, and by an oncoming shift, as a function of the relevant time. The qualitative descriptions of the levels of dependence have corresponding quantitative interpretations that are used to estimate the conditional probability of non-recovery. These dependence characterizations are those defined in the model presented in Table 20-17 of NUREG/CR-1278 (Reference 3.3-13). The total probability for a given decision tree is therefore the product of the probability for the basic outcome selected for that tree and whatever non-recovery factors apply. The non-recovery factors are calculated according to the following formulae:

Dependence Level	**Non-Recovery Factor**
Complete	1.0
High	$\frac{1 + \text{base probability}}{2}$
Moderate	$\frac{1 + 6 * \text{base probability}}{7}$
Low	$\frac{1 + 19 * \text{base probability}}{20}$
Zero	base probability

Table 3.3-8
Assumed Levels of Dependence for Recovery Factors Applied to Detection/Diagnosis/Decision-Making Portion of Human Interactions

Level of Dependence	Applied to Self-Review	Applied to Review by STA	Applied to Review at Shift Change	Applied to TSC Review
Complete (no credit for recovery)	Time window is very short (i.e., on the order of 10 minutes or less); OR Time window is relatively short (i.e., on the order of 10 to 30 minutes), and the procedure would not provide multiple opportunities for proper diagnosis and decision-making.	Time window is relatively short (i.e., on the order of 10 minutes or less), such that the STA would not be able to reach the control room and make a proper assessment.	Time window is less than about 6 hours.	Time window is less than about 1 hour.
High	Time window is relatively short (i.e., on the order of 10 to 30 minutes), and the procedure would not naturally guide the operator through multiple opportunities for proper diagnosis and decision-making.	Time window is relatively short (i.e., on the order of 10 to 30 minutes), and the critical cues would have been received within the first five minutes.	Time window is more than about six hours, and recovery based on low dependence assessed for others.	Time window is more than about one hour from alert status, and recovery based on low dependence assessed for others.
Moderate	Time window is relatively long (i.e., on the order of an hour or more), and there are multiple opportunities through the procedures and/or additional control indications or alarms to make a proper diagnosis and decision.	Time window is relatively short (i.e., on the order of 10 to 30 minutes), but significant additional cues would have been received after the first five minutes; OR Time window is relatively long (i.e., on the order of an hour or more), and limited additional cues would have been received since the first five minutes.	Not applicable for review at shift change.	Not applicable for TSC review.
Low	Not applicable for self-review.	Time window is relatively long (i.e., on the order of an hour or more), and significant new cues have been received since the first five minutes.	Time window is more than about 6 hours.	Time window is more than about 1 hour after alert is declared.

The second element of a type CP interaction represents failure to implement the action correctly, given that the action is properly initiated. This portion, referred to as p_e, is quantified using an abbreviated version of THERP, in which the specific acts that must be accomplished are identified, and failures to perform them properly (due to errors of omission or commission) are noted. These failures are then quantified using the data in NUREG/CR-1278 (Ref. 3.3-12).

In many cases, these execution errors are subject to review and recovery as well. This is particularly true for actions taken in the control room, where additional observers may be able to identify the need for corrective action. As in the case of the initiation errors, a set of guidelines for considering review and recovery by other crew members has been developed. These guidelines are summarized in Table 3.3-9. The levels of dependency are quantified as in the case of the recovery factors for the p_c portion of the type CP events (i.e., as indicated by the formulae summarized above).

Table 3.3-9
Assumed Levels of Dependence for Recovery Factors Applied to Execution Portion of Human Interactions

Level of Dependence	Applied to Self-Review	Applied to Review by Extra Crew*	Applied to Review by STA
Complete (no credit for recovery)	Time window is very short (i.e., on the order of 10 minutes or less); OR Time window is relatively short (i.e., on the order of 10 to 30 minutes), and subsequent steps would not provide opportunity for identifying and correcting previous errors.	No other crew observing (e.g., local manual actions whose effects would not be directly detectable in control room).	Activities would not be expected to be observed by STA or others; OR Time window is very short (i.e., on the order of 10 minutes or less).
High	Time window is relatively short (i.e., on the order of 10 to 30 minutes), and subsequent steps would provide opportunity for identifying and correcting previous errors.	Time window is very short (i.e., on the order of 10 minutes or less); OR Time window is relatively short (i.e., on the order of 10 to 30 minutes), with limited opportunity for feedback..	Time window is relatively short (i.e., on the order of 10 to 30 minutes), but the activities would be expected to be observed directly or the effects of the error would be clear through other plant response or non-response.
Moderate	Time window is relatively long (i.e., on the order of an hour or more), and there are multiple opportunities for identifying and correcting previous errors through subsequent activities.	Time window is relatively short (i.e., on the order of 10 to 30 minutes), but subsequent steps would provide opportunity for identifying and correcting previous errors.	Time window is relatively long (i.e., on the order of an hour or more), and the activities would be expected to be observed directly or the effects of the error would be clear through other plant response or non-response.
Low	Not applicable for self-review.	Time window is relatively long (i.e., on the order of an hour or more), and there are multiple opportunities for identifying and correcting previous errors through subsequent activities.	Not applicable for review by shift manager or others.

*Recovery credit given for review by extra crew or by shift manager, et al., but not for both.

Quantification of the probabilities of type CP interactions was performed using Excel worksheets. An example of one of these worksheets is given in Figure 3.3-2. The results of the assessments for each of the post-initiator human interactions that appeared in potentially important cutsets (and, therefore, for which detailed analyses were required) are summarized in Table 3.3-10. In addition to the probabilities estimated for each interaction, relevant aspects of the timing for the events are provided in the table. Included in this table are: an indication of the total time available from when a compelling signal to take action was received to when the action would need to be completed, as well as the time window for making the decision to implement the action. This time window is the difference between the total time and the actual time required to implement the action.

Quantification of Type CR Interactions

A limited number of recovery interactions that are not explicitly directed by procedures were assessed in this study. These recovery actions are knowledge-based, rather than procedure- (or rule-) based, and hence cannot be assessed in the same manner as for type CP interactions. Instead, a simplified methodology developed by EPRI was used to characterize these type CR interactions (Ref. 67). This methodology presents relative likelihoods of failure to accomplish recovery, based on the following attributes:

- The amount of time available for decision-making and action
  - Short (less than one hour),
  - Intermediate (one to four hours), and
  - Long (longer than about four hours);
- Whether or not training or some level of procedural guidance is available relative to the specific actions being considered;
- Whether the recovery action is simple (e.g., operating a manual valve) or complex (e.g., multiple steps required to cross-connect two systems); and
- Whether environmental factors, such as the heat, humidity, or radiation levels that might impede recovery efforts, are good or poor.

For various combinations of these factors, a qualitative assessment is made regarding the probability of failure. These qualitative assignments are then associated with a quantitative probability scale. The scale used in this study is the nominal scale from Reference 3.3-14. The non-recovery probabilities in this scale are as follows:

Low	0.01	High	0.1
Moderately low	0.03	Very high	0.3
Moderately high	0.05	Maximal	1.0

An example of the treatment of a type CR event is illustrated in Figure 3.3-3. As with the other worksheets, the first portion is devoted to a description of the event and its context in the sequence to which it applies. The assessment identifies each of the influencing factors identified above, producing an overall qualitative characterization of the likelihood of non-recovery. The corresponding probability is then assigned. Only one human interaction in the CR-3 PSA was classified as a CR event and quantified in this manner. This event was ZHUMU62R, failure of the operator to open MUV-62 to provide suction to MUP-1A, and is shown in the example in Figure 3.3-3.

As noted earlier in this section, each post-initiator interaction was initially assigned a value of 1.0. This was done to ensure that combinations of human interactions would not be inappropriately assessed as independent, possibly causing them to be lost. This could result if the combined probabilities would produce sequence cutsets below the truncation value used in the quantification process. The use of the screening value of 1.0 resulted in a large number of cutsets containing multiple human interactions. Each set of interactions was examined in the context of the cutsets in which they occurred to obtain a meaningful assessment of their combined probabilities. This was done in each case by laying out a time line for the sequence of events of interest, and by considering qualitatively the factors that implied dependence or independence for the combined events. For cases in which there were more than two events, this entailed considering the level of dependence between the first two events, and then the conditional level of dependence for successive events, given that the earlier failures had occurred. Once the qualitative levels of dependence were assessed, the corresponding quantitative characterizations summarized above were applied. The qualitative factors taken into account in assessing the level of inter-event dependence included the following:

- Events that refer to the same action were assessed to be completely dependent. For example, in a limited number of cases, separate human interactions could have been used to reflect the failure to initiate different trains of a particular system. This is actually a single event with respect to diagnosis and decision-making.

- Interactions related by time were assessed to have a decreasing level of dependence as the time between them increased:
  - Interactions occurring close in time (i.e., within about 15 minutes) were assessed to be at least moderately dependent (other factors could lead to an assessment of high or complete dependence).
  - Low dependence was assessed for interactions separated by up to one hour for which no other factors applied.
  - Interactions separated by more than one hour were assessed to be independent, unless factors other than time suggested dependence.

Figure 3.3-2

HUMAN INTERACTION WORKSHEET: TYPE CP

sh. 1
background information

EVENT INFORMATION

Name	***Definition***
LHULPRCY	Operators fail to switch from low pressure injection to low pressure recirculation following a large LOCA

DESCRIPTION

Context

This operator action is very similar to HHUHPRCY with the exception that there is significantly less time to accomplish the necessary actions. The rate at which the BWST is depleted will depend on the size of the break and on operator actions to control LPI flow and the reactor building spray system. If both DH pumps start and function properly and the spray system is actuated, the total flow rate could be as high as about 9000 gpm. At that rate, the level in the BWST would drop to the point at which the low-level alarm would be received (15 ft) within about 30 min. When the alarm is received, the operators are instructed to throttle LPI flow back to 2000 gpm for each train and to set spray flow to control at 1200 gpm in each train.

For breaks smaller than the maximum, the time would tend to be extended. The LPI flow would decrease, depending on the back pressure in the RCS, and actuation of the spray system would be delayed due to the slower pressurization of the reactor building.

Assuming that the effective flow rate from the BWST from the time the level diminishes to 15 ft is about 6500 gpm, it would take about another 12 minutes to reach a level at which the low-low level alarm would be received, and about another

To switch to recirculation, the operator must start the DH pumps, open DHV-11 and 12, open DHV- 42 and 43, close DHV-34 and 35, and close MUV-58 and 73.

Procedural Guidance

Procedural guidance for making the switch to high pressure recirculation is provided in EOP-07, steps 3.9 and 3.10. The alarm response procedure AR-303 for event points 234 and 235 (BWST low level and BWST low-low level, respectively) instruct the operator to switch to RB sump recirculation, given an ES actuation.

Figure 3.3-2

HUMAN INTERACTION WORKSHEET: TYPE CP

LHULPRCY sh. 2
assessment of pc

TIMELINE

T0 — 30 min. — T1 — 15 min. — T2 — 4 min. — T3

T0 Small/medium-break LOCA, HPI injection begun. Drain path from BWST to sump open upon ES actuation.

T1 BWST level reaches 15' level. Low-level alarm. Operators instructed to switch to recirculation.

T2 BWST level reaches 7' level. Low-low level alarm. Operators urgently instructed to switch to recirculation.

T3 BWST level reaches 5' level. Makeup pumps begin to cavitate.

Total time from compelling signal: 19 min
Time required to accomplish action: 10 min
Time window (Tw): 9 min

QUANTIFICATION

Detection, Diagnosis, & Decision-Making (pc)

Tree	Failure Mechanism	Selected Branch	Branch Probability	Non-Rec (Depend.)	Non-Rec. Probability	Probability w/ Recovery	Note
pca	Availability of information	a	neg	—	—	neg	
pcb	Failure of attention	h	neg			neg	
pcc	Misread/miscomm. data	a	neg	—	—	neg	
pcd	Information misleading	a	neg	—	—	neg	
pce	Skip a step in procedure	a	0.001	(H)*0.5	2.5E-1	2.5E-4	1,2,3
pcf	Misinterpret instruction	a	neg	—	—	neg	
pcg	Misinterpret decision logic	j	0.001	0.5*(C)	5.0E-1	5.0E-4	3,4
pch	Deliberate violation	a	neg	—	—	neg	
	Probability for pc					**7.5E-4**	

Notes

1. Action based on low-level and low-low level alarm. Procedure steps are highlighted with "caution" statement.
   H = recovery via self-review, with (H) high dependence assessed based on limited time available and multiple
2. alarms associated with low BWST level.
   No credit for STA review due to short time window.
3.
   0.5 = recovery via additional crew (constant probability of failure of 0.5 permitted).
4.

Figure 3.3-2

HUMAN INTERACTION WORKSHEET: TYPE CP

LHULPRCY sh. 3
assessment of pe

QUANTIFICATION (continued)
Execution (pe)

Error	1278 Tabl (Entry)	Basic Prob.	EF	Stress Mult.	Non-Rec. (Depend.)	Non-Rec. Prob	Final Value	Note
Omit step in procedure.	20-7 (2)	3.0E-3	3	2	(C)	1.0E+0	7.5E-3	1
Selecting wrong controls.	20-12 (4)	5.0E-4	3	2	(C)	1.0E+0	1.2E-3	1
Turning controls in wrong direction.	20-12(8)	1.0E-4	10	2	(C)	1.0E+0	5.3E-4	1
Failure to complete change of state.	20-12(10)	3.0E-3	3	2	(C)	1.0E+0	7.5E-3	1

Probability for pe **1.7E-2**

Notes

1. *Complete dependence due to short time window.*

Quantification Summary

Failure		Probability
Detection, diagnosis, & decision-making	pc	1.2E-3
Execution	pe	1.7E-2
Total event probability		**1.8E-2**
Assumed error factor		5

Table 3.3-10
Summary of Post-Initiator Human Interactions Quantified Using Cause-Based Approach

Event Name	Description	Time from Signal	Time Window	Probability
DHUSPBCY	Operators fail to switch in spare battery charger	8 hr	8 hr	1.5E-3
HHUHPIRY	Operators fail to initiate HPI given a SGTR and loss of all feedwater	50 min	40 min	1.8E-3
HHUHPRCY	Operators fail to switch from high pressure injection to high pressure recirculation	190 min	180 min	2.3E-4
HHUINJAY	Operators fail to switch MUV-23/24 to backup power	30 min	25 min	2.3E-3
HHUINJBY	Operators fail to switch MUV-25/26 to backup power	30 min	25 min	2.3E-3
HHULOCAY	Operators fail to throttle HPI flow through broken injection line during small LOCA	30 min	25 min	3.6E-3
HHUMANUY	Operators fail to initiate HPI for small-break LOCA or SGTR	30 min	25 min	1.5E-3
HHURCRCY	Operators fail to manually isolate HPI recirculation line	90 min	80 min	6.1E-4
HHUTHRTY	Operators fail to throttle HPI before SRVs lift	10 min	5 min	8.6E-2
LHUBWSTY	Operators fail to go to high pressure recirculation early	19 min	9 min	1.8E-2
LHULPRCY	Operators fail to transfer from low pressure injection to recirculation	19 min	9 min	1.8E-2
LHUXTYSY	Operators fail to accomplish DHR crosstie for small LOCA	5 min	3 min	1.9E-2
PHUAFSUY	Operators fail to switch AFW (FWP-7) suction	2 hr	105 min	1.9E-3
PHUFWP7Y	Operators fail to start AFW pump FWP-7 (following failure of emergency feedwater)	30 min	15 min	1.4E-2
PHUFP7LY	Operators fail to start AFW pump FWP-7 long term (after initiating HPI/PORV cooling)	20 hr	20 hr	1.0E-4 (default minimum)
PHUSGISY	Operators fail to isolate affected OTSG after SGTR	6 hr	6 hr	1.0E-4
QHUEFT2Y	Operators fail to switch emergency feedwater suction	2 hr	110 min	6.9E-4
QHUEFVTY	Operators fail to open EFIC cabinet doors for ventilation during station blackout	20 min	15 min	2.8E-2
RHUPRVNY	Operators fail to open PORV after SGTR with total loss of feedwater (long-term)	6 hr	6 hr	1.0E-4 (default minimum)
RHURCPSY	Operators fail to restart RCPs during SGTR	5 hr	5 hr	1.8E-4
RHURCPTY	Operators fail to trip RCPs given no seal injection or cooling	3 hr	3 hr	1.2E-3
RHUSTEAY	Operators fail to steam affected OTSG after SGTR	30 min	28 min	4.4E-3
SHUMADCY	Operators fail to align MUP-1A cooling to DHCCC-A	180 min	170 min	8.0E-4
SHUMCNSY	Operators fail to shift cooling of MUP-1 to NSCCC	180 min	165 min	8.8E-4
SHURW2AY	Operators fail to start RWP-2A	180 min	175 min	1.1E-3
SHUSWPAY	Operators fail to start SWP-1A following failure to auto-start	180 min	175 min	1.1E-3
WHUBWSTY	Operators fail to attempt BWST refill.	300 min	240 min	5.2E-4

Figure 3.3-3

HUMAN INTERACTION WORKSHEET: TYPE CR EVENT

EVENT INFORMATION

Name	*Definition*
ZHUMU62R	Failure to open MUV-62 to provide suction to MUP-1A.

DESCRIPTION

For a small-break LOCA where MUP-1C has failed to start and MUV-73 has failed to open, MUP-1B will eventually drain the MUT (since it has no suction from the BWST) and fail due to loss of suction, unless the operators stop it upon receiving the MUT low-low level alarm. No credit was given for this action. The standby makeup pump, MUP-1A, can be started and provide injection to mitigate the LOCA, but it will suffer the same fate as MUP-1B if suction from the BWST is not provided. This can be accomplished by either manually opening MUV-73, or opening MUV-62 to provide suction to the BWST via MUV-58. There is a possibility that the operator may misdiagnose the situation and start MUP-1A without providing suction from the BWST, but it would require ignoring some significant cues. The most obvious of these cues is the catastrophic failure of MUP-1B due to loss of suction. Another cue would be the low-low level annunciator alarm for the MUT prior the MUP-1B's failure. This alarm has as one of its procedural (AR-304) actions to ensure that MUV-58 and MUV-73 are open. Therefore the operator should verify the position of both of these valves. Upon finding MUV-73 closed, it is reasonable to expect that he will follow the procedure and attempt to open it. Failing this, opening MUV-62 to provide a suction flow path for MUP-1A is a logical next step. In either event, it is unlikely, given the cues and procedural guidance, that he would start MUP-1A without assuring suction from the BWST.

QUANTIFICATION

Probability Scale

State	Pr(Non-Rec)
Low	0.01
Mod. low	0.03
Mod. high	0.05
High	0.1
Very high	0.3
Maximal	1.0

Assessment

Influence Factor	Status
Time (short, intermediate, long)	intermediate
Training/practice (yes, no)	no
Complexity (simple, complex)	simple
Environment (good, poor)	good
Qualitative non-recovery factor	MHIGH
Non-Recovery Probability	0.05
Assumed error factor	5

- Interactions which imply actions based on nearly the same cues were assessed using one level of dependence higher than that implied by the nominal time-based delineation described above. For example, two events occurring close in time and based on the similar cues were assessed to be highly dependent.

- In some cases, a scenario might imply a successful action occurring between (in time) two events denoting failures. In these cases, the successful action may decouple the other two interactions (i.e., zero dependence would apply). This would be the case when the interceding event is directly relevant to at least one of the two failures. If the interceding event is completely unrelated, the level of dependence is assessed to be one step lower than that which would otherwise be used.

- For cases in which there are three or more human interactions, the third interaction is generally assessed to be at least moderately dependent on the first two, since each additional interaction may imply that it is more likely the operating crew has made a fundamental misdiagnosis. Subsequent interactions are likewise at least highly dependent on the preceding events. This is applied unless the multiple interactions are widely spaced in time, or later interactions are preceded by a successful action. For example, it is conceivable that two interactions could lead to a total loss of feedwater but that makeup/HPI cooling could be successfully initiated. The failure to establish high pressure recirculation several hours later could be construed to be decoupled from the earlier events.

Quantification of the probabilities of the combinations of human interactions were performed using Excel worksheets. An example of one of these worksheets is given in Figure 3.3-4. Clearly, a measure of analyst judgment enters into the selection of the appropriate level of dependence for a particular case. These guidelines help to assure a degree of consistency in the assessments. It should also be noted that lower-bound values were used in place of the calculations, when very low probabilities were assessed for some combinations. These lower bounds were as follows:

- A minimum value of 10^{-4} was used for any single interaction.

- A lower bound of 10^{-5} was used for interactions appearing in combination that were separated by less than about two hours.

As a practical matter, it should be noted that the event names used in the modeling process were retained in the cutsets as "flags" to aid in understanding the sequence of events, with their probabilities set to 1.0. For each cutset in which there were multiple human interactions, a new event representing the event combination was appended to the cutset. These added events all began with the letter "Z", and were numbered consecutively (i.e., ZHUC001E, ZHUC002E, etc.). For the cases in which there was only one human interaction in the cutset, the same event name was used, but with the first letter replaced with a "Z". Thus, type CP events beginning with this letter always represent the assessment of a human interaction specific to a particular sequence and cutset. The combination events are summarized in Table 3.3-11.

HUMAN INTERACTION: TYPE CP COMBINATION

sh. 1
background information

EVENT INFORMATION

Name

ZHUC001E	Operators fail to maintain suction supply for EFW pumps, and fail to establish AFW flow after EFW fails (QHUEFT2Y * PHUFWP7Y)

DESCRIPTION

Long-term operation of the EFW system will eventually deplete the inventory of tank EFT-2, requiring switchover to the condensate storage tank. Failure to accomplish this is assessed in event QHUEFT2Y. If this switchover is not performed, the EFW pumps will lose suction and fail. Following the loss of EFW, the operators could restore flow to the steam generators using the AFW pump (pump FWP-7). Failure to use this pump is considered in event PHUFWP7Y.

The inventory in tank EFT-2 would be expected to last at least 10 hr. When the alarm on low-low level in the tank is received, there should still be sufficient water left to support EFW flow for at least an additional 2 hr. It is nominally assumed that feedwater must be restored within 30 min after it is lost completely to ensure that core damage does not result. This time, however, is based on assuming complete loss of feedwater at the time of a reactor trip from full power. In this case, the reactor would have been shut down for a number of hours, and the decay heat load would be much lower. It is assumed that at least an hour is available to restore feedwater in this case, after EFW fails.

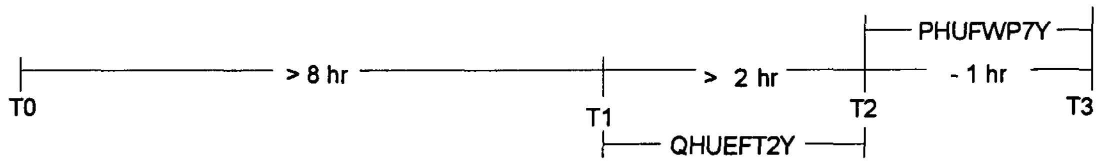
Although the nature of the two events is substantially different, both are concerned with maintaining feedwater flow to the steam generators. The need for the second action (starting AFW) would be necessitated, at least in part, by the failure to maintain a suction supply for EFW. On the other hand, there is a substantial amount of time available between the loss of EFW and when AFW would be needed to prevent core damage. Based on the common elements of the events and the relatively long time available, a low level of dependence is assumed to apply.

Figure 3.3-4

HUMAN INTERACTION: TYPE CP COMBINATION

sh. 2
quantification
ZHUC001E

TIMELINE



T0 Reactor trip
Loss of main feedwater
EFW provides core cooling

T1 Alarm on low-low level in EFT-2 received

T2 Inventory in EFT-2 depleted
EFW assumed to be lost without switchover to CST

T3 Initiation of flow to OTSGs from AFW pump FWP-7 required to prevent core damage

QUANTIFICATION

Event	Failure	HEP	Event HEP	Dep	Dep Prob
QHUEFT2Y	Detection, diagnosis, & decision-making	4.9E-4			
	Execution	2.0E-4			
			6.9E-4		6.9E-4
PHUFWP7Y	Detection, diagnosis, & decision-making	3.0E-3			
	Execution	1.1E-2			
			1.4E-2	low	6.3E-2

Composite value for event combination **4.3E-5**

Assumed error factor 10

Table 3.3-11
Summary of Combinations of Post-Initiator Human Interactions

Event Combination	Description	Constituent Probabilities	Assessed Dependence	Joint Probability
ZHUC001E = QHUEFT2Y * PHUFWP7Y	Operators fail to switch emergency feedwater suction AND operators fail to start AFW pump FWP-7 (following failure of emergency feedwater)	6.9E-4 * 1.4E-2	low	4.3E-5
ZHUC002E = SHUMADCY * RHURCPTY	Operators fail to align MUP-1A cooling to DHCCC-A AND operators fail to trip RCPs given no seal injection or cooling	8.0E-4 * 1.2E-3	low	6.1E-5
ZHUC003E = PHUFWP7Y * SHUMADCY	Operators fail to start AFW pump FWP-7 following failure of emergency feedwater) AND operators fail to align MUP-1A cooling to DHCCC-A	1.4E-2 * 8.0E-4	low	7.1E-4
ZHUC004E = QHUEFT2Y * PHUFP7LY	Operators fail to switch emergency feedwater suction AND operators fail to start AFW pump FWP-7 (long term during HPI/PORV cooling)	6.9E-4 1.0E-4	zero	negligible
ZHUC005E = QHUEFT2Y * HHUHPRCY	Operators fail to switch emergency feedwater suction AND operators fail to switch from high pressure injection to high pressure recirculation	6.9E-4 2.3E-4	zero	negligible
ZHUC006E = PHUFP7LY * HHUHPRCY	Operators fail to start AFW pump FWP-7 (long-term during HPI/PORV cooling) AND operators fail to switch from high pressure injection to high pressure recirculation	1.0E-4 * 2.3E-4	low	5.0E-6
ZHUC007E = PHUAFSUY * HHUHPRCY	Operators fail to switch AFW (FWP-7) suction AND operators fail to switch from high pressure injection to high pressure recirculation	1.9E-3 * 2.3E-4	zero	negligible
ZHUC008E = HHUTHRTY * HHUHPRCY	Operators fail to control HPI flow following ES actuation due to overcooling AND operators fail to switch from high pressure injection to high pressure recirculation	8.6E-2 * 2.3E-4	zero	2.0E-5
ZHUC009E = QHUEFT2Y * HHUINJAY	Operators fail to switch emergency feedwater suction AND operators fail to switch MUV-23/24 to backup power	6.9E-4 * 2.3E-3	low	3.5E-5
ZHUC010E = SHUR2WAY * HHUHPRCY	Operators fail to start RWP-2A AND operators fail to switch from high pressure injection to high pressure recirculation	1.1E-3 * 2.3E-4	zero	negligible
ZHUC011E = HHUHPIRY * PHUFWP7Y	Operators fail to initiate HPI given a SGTR and loss of all feedwater AND operators fail to start AFW pump FWP-7	1.8E-3 * 1.4E-2	moderate	2.5E-4
ZHUC012E = PHUFWP7Y * PHUSGISY	Operators fail to start AFW pump FWP-7 (given loss of all feedwater) AND operators fail to isolate affected OTSG after SGTR	1.4E-2 * 1.0E-4	zero	1.4E-6
ZHUC013E = RHUSTEAY * QHUEFT2Y	Operators fail to steam affected OTSG after SGTR AND operators fail to switch suction for emergency feedwater	4.4E-3 * 6.9E-4	low	2.4E-4
ZHUC014E = PHUSGISY * QHUEFT2Y	Operators fail to isolate affected OTSG after SGTR AND operators fail to switch suction for emergency feedwater	1.0E-4 * 6.9E-4	zero	negligible

References for Section 3.3.4

3.3-6 Mosleh, A., et al. Procedures for Treating Common Cause Failures in Safety and Reliability Studies. U.S. Nuclear Regulatory Commission Report NUREG/CR-4780 (EPRI NP-5613), January 1988.

3.3-7 Mosleh, A. Procedures for Treating Common Cause Failures in Safety and Reliability Studies. U.S. Nuclear Regulatory Commission Report NUREG/CR-5801, 1993.

3.3-8 Fleming, K.N., et al. A Database of Common-Cause Events for Risk and Reliability Applications. Electric Power Research Institute Report TR-100382, June 1992.

3.3-9 Wakefield, D.J., et al. SHARP1—A Revised Systematic Human Action Reliability Procedure. Electric Power Research Institute Report NP-7183-SL (Interim Report), December 1990.

3.3-10 Dougherty and Fragola, Human Reliability Analysis, John Wiley & Sons, Inc., 1988

3.3-11 Parry, G.W., et al. An Approach to the Analysis of Operator Actions in Probabilistic Risk Assessment. Electric Power Research Institute Report TR-100259, June 1992

3.3-12 Swain, A.D. and Guttman, H.E. Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Plant Applications, NUREG/CR-1278, Sandia National Laboratories, Albuquerque, NM, 1983.

3.3-13 "Conduct of Operations: Operations Department Organization and Administration", Crystal River Unit 3 Administrative Instruction AI-500, Florida Power Corporation, July 1, 1996

3.3-14 Moieni, P., et al., "Modeling of Recovery Actions in PRAs," Report APG#15 (NUS-5272) for Electric Power Research Institute (Draft), April 1991.