ACCELERATED DOCUMENT DISTRIBUTION SYSTEM

REGULATORY INFORMATION DISTRIBUTION SYSTEM (RIDS)

ACCESSION NBR:9303010355 DOC.DATE: 93/02/24 NOTARIZED: NO DOCKET #
FACIL:50-315 Donald C. Cook Nuclear Power Plant, Unit 1, Indiana M 05000315
50-316 Donald C. Cook Nuclear Power Plant, Unit 2, Indiana M 05000316
AUTH.NAME AUTHOR AFFILIATION
FITZPATRICK,E. American Electric Power Service Corp.
RECIP.NAME RECIPIENT AFFILIATION
COOK,D.C. Document Control Branch (Document Control Desk)

SUBJECT: Provides individual plant exam responses to NRC questions.

DISTRIBUTION CODE: A011D COPIES RECEIVED:LTR 1 ENCL 1 SIZE: 103
TITLE: Generic Ltr 88-20 re Individual Plant Evaluations

NOTES: See Reports

	RECIPIENT ID CODE/NAME	COPIES LTTR	COPIES ENCL	RECIPIENT ID CODE/NAME	COPIES LTTR	COPIES ENCL
	PD3-1 PD	1	1	DEAN,W	1	1
INTERNAL:	ACRS HOUSTON,M	1	1	AEOD/DSP/TPAB	1	1
	NRR HERNAN,R	1	1	NRR/OGCB	1	1
	REG FILE 01	1	1	RES FLACK,J	3	3
	RES MITCHELL,J	1	1	RES/DSIR/SAIB/B	7	7
	RGN 1	1	1	RGN 2	1	1
	RGN 3	1	1	RGN 4	1	1
EXTERNAL:	NRC PDR	1	1	NSIC	1	1

NOTE TO ALL "RIDS" RECIPIENTS:

PLEASE HELP US TO REDUCE WASTE! CONTACT THE DOCUMENT CONTROL DESK, ROOM P1-37 (EXT. 504-2065) TO ELIMINATE YOUR NAME FROM DISTRIBUTION LISTS FOR DOCUMENTS YOU DON'T NEED!

TOTAL NUMBER OF COPIES REQUIRED: LTTR 24 ENCL 24

R I D S / A D D S

R I D S / A D D S

American Electric Power
Service Corporation
1 Riverside Plaza
Columbus, OH 43215
614 223 1000

AMERICAN ELECTRIC POWER

AEP:NRC:1082F

Donald C. Cook Nuclear Plant Units 1 and 2
Docket Nos. 50-315 and 50-316
License Nos. DPR-58 and DPR-74
INDIVIDUAL PLANT EXAMINATION
RESPONSE TO NRC QUESTIONS

U. S. Nuclear Regulatory Commission
Document Control Desk
Washington, D. C. 20555

Attn: T. E. Murley

February 24, 1993

Dear Dr. Murley:

In a letter dated December 23, 1992, the NRC raised a number of questions concerning the Donald C. Cook Nuclear Plant Individual Plant Examination. The attachment to this letter provides responses to these questions.

Sincerely,

E. E. Fitzpatrick
Vice President

RBB/gmd

Attachments

cc:
A. A. Blind - Bridgman
J. R. Padgett
G. Charnoff
NFEM Section Chief
A. B. Davis - Region III
NRC Resident Inspector - Bridgman

9303010355 930224
PDR ADOCK 05000315
P PDR

A011

bc: S. J. Brewer
W. M. Dean, NRC - Washington, D.C.
D. H. Malin/K. J. Toth
M. L. Horvath - Bridgman
J. B. Kingseed/R. B. Bennett
J. B. Shinnock
W. G. Smith, Jr.
AEP:NRC:1082F
DC-N-6015.1

ATTACHMENT TO AEP:NRC:1082F

INDIVIDUAL PLANT EXAMINATION

FOR THE

DONALD C. COOK NUCLEAR PLANT

RESPONSE TO NRC QUESTIONS

STEP 1 IPE REVIEW QUESTIONS OF D.C. COOK IPE SUBMITTAL

FRONT-END (CORE MELT ANALYSES) QUESTIONS

1. The discussion of initiator groups listed in the IPE for special initiators includes loss of essential service water, component cooling water and 250 VDC bus. Discussion in Section 2.3 indicates that loss of control air and loss of 120 VAC bus were considered as potential initiators; however, these potential initiators are not addressed in Section 3.1.1 of the submittal. In addition, there is no discussion whether loss of HVAC was examined as a potential initiator. Loss of these systems will typically result in a plant trip. Provide a discussion of the basis for why these support systems were not considered as initiators with subsequent event tree analysis.

Response:

Following a review of plant systems to determine which systems, if lost, would cause a reactor trip, the systems were then reviewed to determine if the loss of that system should be included as a separate special initiating event category. This review determined if the loss of the system would affect the accident mitigating capabilities of the plant or if reasonable operator action could be taken to prevent a reactor trip once the system was lost. The loss of control air, 120 VAC power and loss of HVAC were reviewed and it was determined that it was not appropriate to create separate initiating event categories for them.

Loss of Control Air - Loss of control air would cause the feedwater regulating valves to shut, which causes a reactor trip. The accident progression following the trip is the same as and was, therefore, included in the Transients without Steam Conversion Systems Available event.

Loss of 120 VAC - Loss of this system (specifically to the Control Room Instrumentation & Distribution panels -CRIDs) would lead to a plant trip. Accident progression would then be the same as the Transients with Steam Conversion Systems Available event and the loss of this power source would not impair the plant's ability to mitigate the transient. Also, the frequency of losing the right amount of CRID panel necessary to cause a trip was found to be very low (1.0E-06 range) especially when compared to the frequency of a Transient with Steam Conversion Systems Available (3.8 per year).

...9303010355

Loss of HVAC - Loss of Control Room HVAC would cause the Control Room to heat up, and after some time, the ambient temperature would exceed the maximum temperature rating of some vital instrumentation. At this point, equipment degradation and a resultant reactor trip would occur. However, it is expected that corrective measures would be in place long before this happens. Procedures exist for both Unit 1 and Unit 2 control rooms governing loss of control room ventilation. These procedures address HVAC failures such as air handling unit fan failures, chilled water circulation pump failures, and cooling system leaks.

Regarding HVAC support to vital equipment in the plant, AEPSC engineering analyses show that most of this equipment can survive without area cooling for anywhere from 32 to 72 hours. Equipment that cannot survive that long without area cooling had HVAC modeled within the associated system fault tree.

2. The method for determining the RPS failure probability is not provided in the IPE. If generic RPS value of 3E-5 (NUREG-0460) is used with the Cook transient frequencies (3.8 and 1.2E-1), the resulting ATWS initiator frequencies are 1.1E-4 (Tra) and 3.6E-6 (Trs), respectively, which differs from the ATWS frequency provided in the submittal. Provide discussion on how the ATWS frequency of 4.67E-5 was estimated and incorporated in the IPE analysis. In addition, it is not clear from the IPE if the ATWS success criteria analysis considered the effects of the moderator temperature coefficient (MTC). Provide a discussion of the rationale that core damage prevention is possible under ATWS conditions when an unfavorable MTC exists.

Response:

The ATWS initiating event frequency was estimated as the product of two parameters, q(RPS) and f(t), where q(RPS) is the probability of the reactor protection system failing to trip the reactor and f(t) is the frequency of initiating events challenging the reactor protection system. The f(t) value was determined from plant specific data and is the sum of the transient frequencies, i.e. 3.8 and 0.12, as noted in the question. The q(RPS) value, 1.2E-05, was derived from a Westinghouse calculation, which used reactor trip signal failure values from a study of the V. C. Summer plant. This calculation compared the components used in Cook Nuclear Plant's and V. C. Summer plant's pressurizer pressure and steam generator level analog channels and solid state protection system (SSPS) logic cabinets. These components were found to be identical. Thus, values from the V. C. Summer study were placed into RPS logic trees developed for the Cook Nuclear Plant IPE.

The impacts of moderator temperature coefficient were addressed within the ATWS accident event (Figure 3.1-12, page 3-18 of the IPE submittal), more specifically, within the Primary Pressure Relief (PPR) top event node. In the PPR node, two different success criteria were used in the ATWS model depending on the outcome of the manual rod insertion node (MRI - see Figure 3.1-12). Both success criteria required all 3 RCS safety valves to open, but fewer pressurizer PORVs were needed to relieve the ATWS pressure transient if MRI was successful. Since MTC early in a fuel cycle may not provide sufficient reactivity feedback to lower the ATWS pressure transient to within RCS pressure relief capacity, another factor known as Unfavorable Exposure Time (UET) was added to the PPR fault trees to represent this limited MTC. The UET to which the plant is exposed is lower if MRI is successful. The UET calculations drew data from Westinghouse WCAP-11992, "Joint Westinghouse Owners Group/Westinghouse Program: ATWS Rule Administration Process". Based on this calculation, the pressure relief efforts of PPR will not be successful for the first 5.6% of an 18 month fuel cycle even if the rods are inserted, or 17% of a fuel cycle if the rods are not successfully inserted.

3. NUREG-1335 requests that separate event trees, which may be needed to support special event analysis, be included in the IPE submittal. Although an ISLOCA event tree was provided in your IPE submittal, the documentation is insufficient to determine the process used to determine the initiating frequency and associated mitigating actions. Provide a discussion (with simplified diagrams) of specific systems and components and their associated failure modes modeled for the ISLOCA initiator. Include, for example, the configuration of residual heat removal system, check valves, motor operated valves, surveillance methods and frequency, independence of redundant systems, treatment of human errors associated with valve status, ability to isolate breaks and any administrative controls on MOVs. Also note the verification of design rating of low pressure piping and components, and the potential for loss of critical mitigating systems due to flooding.

Response:

Interfacing Systems LOCA (ISLOCA) Initiating Event Frequency Calculation and Event Progression:

A. Initiating Event Frequency:
This frequency evaluation involved the review of all piping which penetrates containment and is connected to the reactor coolant system (RCS). This listing was reduced by the following process:

- Determining which lines lead from RCS pressure to low pressure piping. Consistent with past PRA analyses, pipe ruptures of downstream systems designed for RCS pressure were eliminated.

- Lines which contained at least four pressure isolation boundaries between the RCS and the low pressure side were eliminated due to the line's extremely low frequency of failure to protect the low pressure system.

- Lines which are exposed to RCS pressure only after an RCP seal failure and are of low pressure design inside containment were eliminated.

- An evaluation was performed by AEPSC in response to NRC GL 87-06, "Periodic Verification of Leak Tight Integrity of Pressure Isolation Valves". This evaluation provided a list of valves which separate high pressure RCS piping from a low pressure system. Lines remaining from the above process were compared to this evaluation to determine if any valve

configuration communicated with a low pressure system outside containment.

Figure 3-1 (attached) shows the potential ISLOCA flow paths which remained from the above screening process. The flow paths are summarized as:

1. RHR injection to RCS cold legs
2. RHR injection to RCS hot legs
3. RHR cooldown connection to Loops 2 and 3 cold legs
4. SI (safety injection) to RCS cold legs
5. SI to RCS hot legs
6. RHR cooldown from Loop 2 hot leg

Further assumptions were then made to quantify the frequency of an ISLOCA through each of the above paths shown on Figure 3-1.

Technical Specification (T/S) 4.4.6.2.2 requires that check valves SI-170L2, SI-170L3, RH-133 and RH-134 be tested for leakage after each refueling outage, whenever the plant has been in cold shutdown for 72 hours or more if leakage testing has not been performed in the previous 9 months, and prior to returning the valve to service following maintenance and repair activities.

Valves SI-170L1, SI-170L4, SI-161L1 through -L4, SI-158L1 through -L4, SI-151-E, -W, SI-152-N, -S are leak tested during each refueling outage by procedure 12-THP-403-STP.226, which confirms proper seating of each valve disc and that each valve can independently sustain differential pressure across the disc. Thus, only failure to close was considered credible except when the plant leaves Mode 5 following outages other than refueling outages.

RHR cooldown suction isolation valves IMO-128 and ICM-129 are interlocked such that they will not open unless RCS pressure is less than 400 psig. Thus, only disc rupture was considered credible.

T/S 4.5.2 requires that valves IMO-315 and IMO-325 be verified closed at least once every 12 hours. Thus, only disc rupture and MOV spurious opening were considered credible.

Executing applicable surveillance testing procedures and adherence to applicable T/S sections accounted for operator actions regarding identification of potential ISLOCA pathways. Operator actions were also modeled during accident progression.

Using the above assumptions, the ISLOCA initiating frequencies from each potential flow path were summed together for the 6.7E-07 value shown in the IPE submittal. This was heavily dominated by the IMO-128 and ICM-129 (RHR cooldown from Loop 2 hotleg) flow path frequency and the ISLOCA event was modeled assuming that the leak occurs here. This pathway challenges both SV-103 and the RHR pumps. Safety valve SV-103 is in the lower containment annulus area and the RHR pumps are on a low level of the auxiliary building (573 foot elevation) beneath all other safety-related components in the auxiliary building. Thus, flooding from this pathway does not present a problem to accident mitigation.

Additionally, it was noted that the potential for an ISLOCA flow path past check valves SI-170L2 and SI-170L3 was found to be insignificant. These check valves are addressed within T/S 4.4.6.2.2 along with RH-133 and RH-134 (also shown on Figure 3-1). Adherence to this T/S requirement has been restrictive in the past and, in view of this evaluation, removal of this requirement appears warranted.

B. ISLOCA Event Progression: (refer to the ISLOCA Event Tree, Figure 3.1-5, page 3-11 of the IPE submittal)

RHR System Breach (BRH): This node identifies whether RHR system overpressurization results in piping failure. A vendor (Westinghouse) calculation analyzed pressurization of RHR piping from an ISLOCA event and concluded that RHR pump seal leakage was the most likely failure. Failure of the RHR piping due to creep rupture was found to have an insignificant failure probability over the 24 hour time frame of an IPE accident. BRH success meant that the piping stayed intact and that RHR pump seal leakage and subsequent loss of the RHR pumps is expected. The seal leakage rate is equivalent to that of a small or medium LOCA.

ECCS (high pressure) Injection (HP2): Consistent with the success criteria for small or medium LOCA, it is assumed that HP2 success requires 1 of 2 centrifugal charging pumps (CCPs - high head)) and 1 of 2 safety injection pumps (SI - high head) injecting into 1 of three intact cold legs. Since the break is assumed to be in the RHR cooldown piping, which is attached to the hot leg piping, all injected water, which goes through cold leg piping, is assumed to reach the core. Thus, this success criteria is conservative for an ISLOCA since ECCS injection is actually through four cold legs. ECCS injection would be required to maintain RCS inventory until pressure is reduced to less than 450 psig and the RHR relief valve (SV-103) closes (see Figure 3-1).

Operator Action to Isolate the RHR Seal LOCA (OIB): With RCS inventory loss through the RHR pump seals (in addition to relief valve SV-103), closure of IMO-310 and -320 stops this flow path.

Auxiliary Feedwater Actuation (AF4): AFW flow is necessary for maintaining steam generator inventory for decay heat removal and for cooling down the RCS using the steam generators. Success is 450 gpm to a minimum of two out of four steam generators. ECCS bleed and feed can also remove decay heat; but this would eventually fail during high pressure recirculation (no RHR system).

RCS Cooldown and RWST Conservation (RCE): RCS cooldown is necessary to reduce RCS pressure to less than 450 psig in order to shut the RHR relief valve through which RCS inventory is also being lost. Cooldown would be initiated at 100 degrees (F)/hr per Cook Nuclear Plant emergency operating procedures. This is accomplished by using condenser dump valves (if available) or steam generator atmospheric dump valves for two of the steam generators with AFW flow (see AF4).

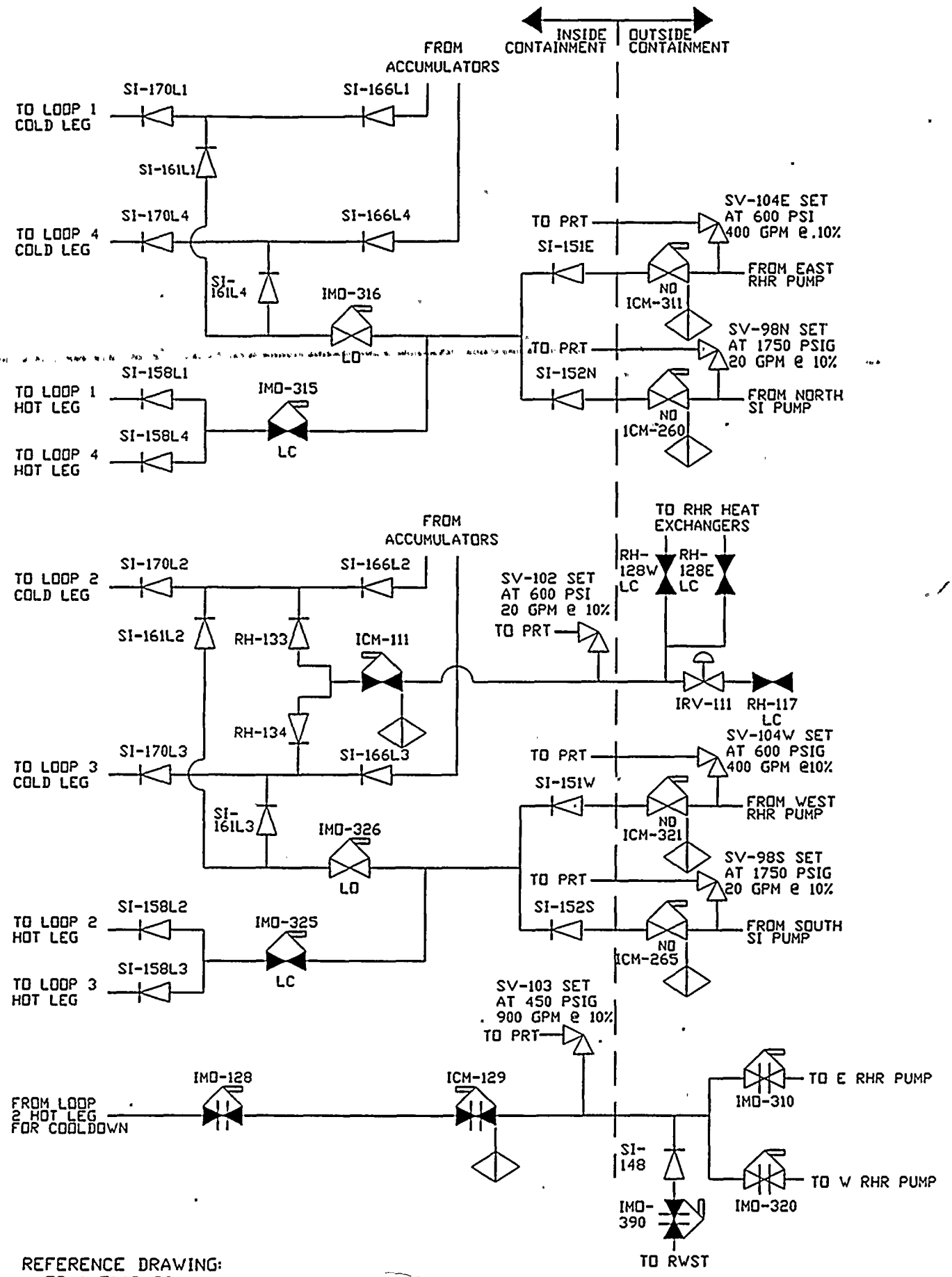
Also, RWST inventory depletion would be minimized to conserve water for accident mitigation by:

1. Securing containment spray pumps.

2. Reducing ECCS flow down to one train and then realigning to normal charging.

3. Depressurizing the RCS using one pressurizer PORV (normal spray and auxiliary spray are not assumed available).

RVC - Relief Valve Closure: This node modeled RHR relief valve closure following break isolation (IMO-310, -320) and RCS depressurization to below the relief valve setpoint.



REFERENCE DRAWING:
OP-1-5143-20

Figure 3-1

4. Tables 3.1-2 through 3.1-17 provide the equipment success criteria for successful accomplishment of each event tree top event. The combinations of systems (or events) that are required to function to prevent core damage is not discussed. Provide list of systemic success criteria for core damage prevention.

Response:

Figures 3.1-1 through 3.1-16 of the IPE submittal show the event trees for each analyzed accident. Sequences that were successful lead to "SUCCESS" on the right side of the event tree. Accident core damage states are also listed there. For the IPE project, preventing both core damage and containment failure defined "SUCCESS". In some cases, successful mitigation was listed as another end state. These are explained as follows:

Steam Generator Tube Rupture - Figure 3.1-4 in the submittal: Sequences 12, 22, 51 and 61 are shown as "LEAK", meaning that core damage was prevented (and no containment failure), but primary coolant leaked to the secondary and to the environment. This is terminated if the RCS can be cooled down and depressurized to atmospheric pressure.

Interfacing Systems LOCA - Figure 3.1-5 in the submittal: Sequence 1 is shown as "LEAK", meaning that, as above, core damage was prevented, no containment failure, but primary coolant was released in this case through the RHR cooldown suction pathway.

5. There is insufficient discussion in the submittal with regard to the development of the accident sequences in the Event Tree Analysis to determine if the success criteria was properly applied for delineating the accident sequences. Two examples: (1) The definition provided in Section 3.1.1.2.1 for the SCS available transient indicates that SCS is available for decay heat removal, that is, main feedwater is available for mitigation. It would seem, therefore, that failure of SCS would be required before AFW is needed. (2) The event tree of SCS available transient indicates that main feedwater can be successful after failure of OA5. The success criteria table for SCS available defines OA5 as supply to at least 2 steam generators from at least one condensate booster pump. The main feedwater pumps are typically high pressure pumps and in order to operate, generally require the condensate and condensate booster pumps to be functional. Provide clarification as to why failure of OA5 (which would include failure of condensate booster pumps as one failure mechanism) does not fail main feedwater.

Response:

As noted in Section 3.1.2 of the IPE submittal, success criteria as shown in the accident event trees were taken from UFSAR analyses or drawn from Cook Nuclear Plant emergency operating procedures or their background documents, in which case the success criteria was then verified using the MAAP computer code.

Within the Transients with Steam Conversion Systems (SCS) Available event tree, main feedwater is available for decay heat removal, but auxiliary feedwater is the normal source for this cooling following a reactor trip. The event tree, Figure 3.1-7 in the submittal, challenges the auxiliary feedwater top event node immediately after the transient (and trip) initiates. Please note, though, that the event trees did not necessarily model accident progression chronologically, but rather modeled actions (hardware & operator alike) necessary when mitigating accidents. The second through fifth nodes in the SCS available event tree model show all of the various methods available for removing decay heat. Also, it is true that both the OA5 (steam generator depressurization) and MF1 (main feedwater) nodes call upon the condensate system for support, but failure of the condensate system within OA5 is included within MF1 and affects the calculated failure rate of MF1 due to characteristics of the accident sequence quantification code (WLINK Code). Although different condensate models were developed to address both scenarios (OA5 and MF1), the same equipment basic event identifiers were used in both sets of logic trees (e.g., condensate pump failure was named by the

same identifier in all condensate models). Therefore, condensate failures within OA5 are identified in MF1 and not double counted. Thus, other failures within MF1 are allowed to be quantified. In short, OA5 condensate failures would also fail MF1, but our modeling approach and quantification code account for this. Additionally, our methodology accounts for failures other than condensate failures (OA5 may have failed from something else) within MF1.

6. The manner in which an accident progresses can affect the ability of systems to continue to function or systems not yet demanded to be able to operate. Insufficient discussion of the effects of the accident progression on the various accident sequences is provided in the IPE to determine if the Event Tree Analysis accounted for phenomenological effects on the success criteria. For example, environmental effects on equipment from the accident progression is not apparent. Provide discussion on the different phenomena and their effects on the success criteria, particularly in relation to system performance.

Response:

The various accident phenomena are not expected to impact the sequence modeling of the Cook Nuclear Plant Level 1 IPE. Instruments and equipment are already conservatively analyzed to survive design basis environmental conditions, which do not differ significantly from the typical severe accident conditions. The Emergency Operating Procedures take into account the impact of these environmental conditions on the instrument readings. Therefore, only environmental conditions more severe or prolonged than the design basis conditions should be questioned.

In the Cook Nuclear Plant IPE, recovery actions are not assumed after core damage has begun. Therefore, only a steam environment with enthalpies near or slightly exceeding the maximum enthalpy of pressurized water would be expected inside containment when operator actions would be taken to stop the accident progression. These conditions are approximately the level to which equipment and instruments are typically qualified for a 24 hour basis, or 340 degrees F. More severe conditions such as higher enthalpies or hydrogen burns would only be expected as core damage begins, when credit is no longer taken for operator actions. Therefore, instrumentation and equipment which are analyzed for design basis conditions would not be required to survive in environmental conditions which are more severe or prolonged than those for which they are qualified. In addition, from an engineering judgement viewpoint, the instruments and equipment would not be expected to fail precipitously if the qualification temperature is somewhat exceeded.

7. The IPE estimated the contribution of core damage from station blackout to be approximately an order of magnitude less than what the staff estimated for resolution of USI A-44. In order to facilitate our review, describe your blackout analysis, and the following aspects which we find important to understand your IPE effort:

- 0 reactor cooling pump (RCP) pump seal model employed, including timing of seal degradation and flow rates,
- 0 impact of severe weather conditions (e.g., snow/ice conditions) which could result in extended losses of offsite power conditions,
- 0 coping time, including estimates of battery and CST depletion times,
- 0 treatment of recovery of offsite power and EDGs,
- 0 treatment of EDG common cause failure, specifically the inclusion of higher order MGLs for a two diesel system,
- 0 ability to cross tie unit system during single unit blackout conditions,
- 0 treatment of mitigating actions or plant improvements that impact the analysis.

Response:

The Cook Nuclear Plant Station Blackout analysis was performed utilizing NUREG-1032 (Evaluation of Station Blackout Accidents at Nuclear Power Plants) and the Cook Nuclear Plant Emergency Operating Procedures for a Loss of All AC Power.

The SBO analysis gives no credit to cross-tie AC power with Unit 2. Unit 2 may or may not have AC power available.

The common cause failure probability for two EDGs failing to start and run was 1.66E-03. This value is achieved by multiplying the random failure, 6.64E-02 by a beta factor of .025. See response to question 13 for more information on common cause treatment.

The treatment of offsite power recovery was analyzed in accordance with NUREG-1032. A cluster group of 1 was selected to be the most representative group for the Cook Nuclear Plant based upon the following design and location characteristics: design classification of I2, composite grid reliability/recovery group of GR2, composite severe weather induced loss of offsite power frequency/recovery group of SR3, and an extremely severe weather induced loss of offsite power frequency group of SS2. Cluster 1 is generally described as follows:

"Sites with demonstrated high grid reliability and multiple sources of offsite power available through independent switch yard circuits and low severe weather hazards or design features to limit loss of offsite power or hasten recovery from severe weather events."

Upon the loss of all AC power, the turbine driven auxiliary feedwater pump would start on a reactor coolant pump bus undervoltage signal. A mission time of four hours is assumed, based upon the minimum availability of batteries for control and instrumentation. The emergency procedures instruct the operator to depressurize the intact steam generators by manually dumping steam at the maximum rate using the steam generator PORVs. If power has not been restored within 4 hours and this action has not been initiated, it is assumed that cooldown cannot be performed. This assumption is made because the station batteries are assumed to last for only four hours and the operator would have no indication of plant conditions and may not properly control the cooldown. Successful cooldown will minimize the reactor coolant pump leakage and delay core uncovery. After the batteries are depleted, control and instrumentation power are lost, but this does not directly result in a trip of the TDP since the trip throttle valve requires that a solenoid be energized to trip the pump. The condensate storage tank is expected to provide condensate to the TDP for a minimum of 6 hours, at which time the loss of AFW is postulated. Given the success and failures of AFW, RCS cooldown, and continued AFW after battery depletion, the times necessary for power recovery to prevent core damage due to the loss of RCS inventory and decay heat removal capability are determined based upon MAAP runs. The probability of not recovering power at each of these times is then calculated using the power recovery distributions for cluster group 1 in NUREG-1032.

The Westinghouse RCP seal LOCA methodology was used to model RCP seal LOCAs. This model is based upon Westinghouse Proprietary Class 2 WCAP-10541, Revision 2, November 1986 and the RCP Seal Integrity Generic Issue B-23 slides presented to the NRC in July 1987. The RCP model considers the probability of immediate catastrophic failure resulting in a 480 gpm leak rate per RCP. This is followed by a seal leak rate model probability distribution of increasing RCP O-ring leakage over time. The leak rates range from an initial value of 21 gpm up to 480 gpm per pump. This model determines the probability of core uncovery, which likewise increases over time. Thus every time AC power is recovered, the probability of core uncovery from RCP seal leakage is evaluated. If the core has uncovered, core damage is assumed. If the core is not uncovered, then core damage can be prevented if subsequent recovery actions such as restoring

RCS inventory, AFW, primary feed and bleed are successful.

The Cook Nuclear Plant Station Blackout event tree is modeled based upon existing plant procedures and performance. There are, however, several potential sources of margin that include:

0 No credit is taken for cross-ties to Unit 2, including the possibility for recovery of power, and RCP seal injection.

0 The RCP seal LOCA model assumes catastrophic leakage occurs at all RCPs at the same time.

0 Even though power to instrumentation is assumed lost after four hours, the operators may still be able to initiate and conduct successful cooldown.

0 No credit is taken for alternate methods of refilling the CST.

8. In addition to station blackout, consideration of reactor cooling pump (RCP) seal failure is important, because of its impact on the determination of dominant sequences (i.e., transients vs. LOCAs). Concisely describe your treatment of RCP seal degradation and failure during loss of key support systems which could lead to loss of seal cooling. Include in your discussion, the timing of RCP seal degradation and seal flow rates, and any recovery actions or improvements that would enhance mitigation of RCP seal cooling accidents, e.g., ability to cross tie cooling water systems between units, use of the fire water system or other water systems as an alternate source of cooling, specific RCP seal improvements.

Response:

The Cook Nuclear Plant IPE considers the essential service water (ESW) and component cooling water (CCW) systems as key support systems whose failures would lead to the loss of RCP seal cooling causing a small LOCA. Special event trees were developed to model Cook Nuclear Plant behavior following the loss of the ESW and CCW systems.

The loss of ESW event tree assumes that ESW flow is lost during normal plant operations; total loss of ESW would entail the loss of both Unit 1 ESW loops. The loss of CCW would entail the loss of both Unit 1 CCW loops. The ESW system is a shared system with Unit 2 and the CCW system also has a Unit 2 cross-tie.

The loss of ESW leads to the loss of CCW, which in turn leads to the loss of cooling to the SI pumps, charging pumps and the RCP thermal barriers. With the RCP seal support systems unavailable, leakage of RCS fluid through the RCP seals will occur without makeup capabilities. The Westinghouse RCP seal LOCA methodology was used to model RCP seal LOCAs. This model is based upon Westinghouse Proprietary Class 2 WCAP-10541, Revision 2, November 1986 and RCP Seal Integrity Generic Issue B-23 slides presented to the NRC in July 1987. The RCP model considers the probability of immediate catastrophic failure resulting in a 480 gpm leak rate per RCP. This is followed by a seal leak rate model probability distribution of increasing RCP O-ring leakage over time. The leak rates range from an initial value of 21 gpm up to 480 gpm per pump. This model determines the probability of core uncovery, which likewise increases over time. Thus every time ESW and CCW are recovered, the probability of core uncovery from RCP seal leakage is evaluated. If the core has uncovered, core damage is assumed. If the core is not uncovered, then core damage can be prevented if subsequent recovery actions are successful. If there are no RCP seal failures, the minimum seal leakage is expected to be 21 gpm.

The evaluation of seal degradation and leakage leading to core uncovery occurs at the times that ESW and CCW are recovered. The recovery of ESW and CCW systems is the primary means of stopping the loss of RCS inventory. If secondary decay heat removal is successful, via the AFW or MFW systems, and ESW and CCW are recovered within 1 hour, then the restoration of RCS inventory with continual recirculation can prevent core damage. If secondary decay heat removal fails, then initiation of an RCS cooldown via steam generator depressurization with steam dumping using the PORVs is required. If ESW and CCW are recovered within eight hours and if the core is not uncovered, then core damage can be prevented if subsequent recovery actions are successful.

Two improvements were recommended to enhance mitigation of RCP seal cooling accidents. First, since the contribution to core damage from both the ESW and CCW events were dominated by the failure of an operator action to trip the RCPs, the Emergency Operating Procedures were amended to add emphasis to this step. The second recommendation was to increase the priority of opening the centrifugal charging pump discharge CVCS cross tie to the opposite unit in the procedures. CVCS cross ties to the other unit were not modeled due to the late opening of the CVCS cross tie in the current procedures. This latter item is still under investigation.

9. The dependency table indicates which systems the front-line and support systems are dependent on for operation. The actual dependency or requirement that is needed for the system or component to be able to function on demand and to continue to function throughout the course of the accident is not provided. For example, room cooling could be required for the AFW TDP because the following dependency exists: (1) pump has a high room temperature trip and the room temperature in the accident is anticipated to exceed the trip temperature, or (2) pump will fail when room temperature exceeds design qualifications which is anticipated to be exceeded in the accident. In this example, cooling is supplied to the AFW TDP room by the HVAC system which is AC dependent. Therefore, although the AFW TDP is AC independent in the short term, it is AC dependent in the long term. Documentation provided in the IPE is inadequate to determine if method used for identification of dependencies is sufficient such that subtle dependent failures would be found. Provide a detailed discussion of the process that was used to identify dependencies with a list of systems and component dependencies.

Response:

Once the accident event tree logic was established, front line systems required for accident mitigation were identified. This marked the starting point for determining which mechanical and electrical systems were needed to support these front line systems in their required operational modes. AEPSC developed specific IPE procedures for each stage of the IPE, including the system fault tree analyses. These analyses drew upon a Westinghouse guidebook developed for this purpose, which outlined identifying mechanical, electrical, reactor protection (actuation signals) and cooling support systems. Most support systems (e.g. service water and electrical power systems) were modeled under separate system fault trees and linked in by quantification codes. HVAC requirements were reviewed for all systems modeled. Based upon AEPSC engineering calculations and existing plant procedures, most systems are able to survive a lack of area cooling for anywhere from 32 to 72 hours. Those systems not able to do this had HVAC modeled directly within the associated fault tree (HVAC was not linked in). Thus, the TDAFW pump required room cooling and HVAC fans were modeled accordingly.

Tables 3.1-2 through 3.1-17 in the IPE submittal listed a majority of the modeled support systems. The following elaborations are provided:

1. Electric Power, listed as a system dependency, entailed any or a combination of 4160 VAC, 600 VAC, 250 VDC and 120 VAC power systems, for which fault tree models exist.

2. Component Cooling Water (CCW) required cooling itself from the Essential Service Water (ESW) system. ESW is divided into two trains, each of which requires electric power and safety injection signals as system dependencies. Mission time was also 24 hours for ESW.

10. The level of detail to which a system is examined in the fault tree analysis will determine if any subtle failures exist and are found by the analyst. This is particularly true in regards to logic or maintenance dependencies. For example, some PWRs have steam generator isolation control systems that are designed to shut off feedwater given low secondary pressure. An inadvertent blowdown of the steam generators could possibly actuate the steam generator isolation control system, thereby isolating main feedwater and AFW. If sufficient detail is not analyzed, then both the mechanisms of the inadvertent blowdown and the subsequent isolation of feedwater and AFW may not be modeled. Another example, a room cooler is actuated from a thermostat. The cooler is tested monthly, but the thermostat is not tested. If the fault tree did not model to this level of detail, the above failure would be missed. Provide discussion of level of detail that was used in fault tree analysis to ensure any subtle failures were identified.

Response:

Using the guidance explained in the response to Question 9, the following steps, which were performed during the IPE, indicate the methodology used to assess and model plant systems;

Step 1: Using operational flow or electrical one-line diagrams, develop a simplified system diagram. Use established screening criteria for eliminating certain components (flow diversion percentage, valve interlocks, checks of manual valves, etc.).

Step 2: Using Boolean logic gates, construct a system fault tree that models system failure.

Step 3: Quantify the system fault tree using basic event, human error and test/maintenance probabilities.

Step 4: Based on the Step 3 quantification, determine common mode failures using Multiple Greek Letter methods.

Step 5: Requantify the system fault tree with common mode failures.

Data sources consulted when developing system fault trees included plant walkdowns, the UFSAR, system descriptions (authored by the Nuclear Engineering Department), Technical Specifications, test and maintenance procedures, elementary diagrams (circuitry diagrams) and discussions with plant operators and cognizant system engineers. Using these sources, the IPE analysts determined system configurations during both normal and accident conditions. Plant system responses to various reactor protection signals also were reviewed as part of this effort. Additionally, a single

system often had multiple fault trees developed that represented that system's responses to different accident scenarios: For example, the auxiliary feedwater fault tree for LOCAs was different than the fault tree for station blackout.

The data collection and analysis portion of the IPE established boundaries around system components when determining component failure. Pump failure, for example, included failure of the power breaker that directly feeds that pump. If it was determined that something such as pressure switch actuation was not within a component's boundaries, then the pressure switch was modeled.

11. Your submittal states that Unit 1 was found to be bounding for Unit 2. Briefly describe the Unit 1 features or operational attributes that cause this unit to be the bounding unit. Also describe any inter-unit dependencies found to have an impact on the internal initiating event analysis. List systems shared between the two units, and briefly describe how these shared systems were treated in the IPE.

Response:

Unit 1 was chosen as the analyzed Unit for the purpose of defining a starting point while differences between Unit 1 and Unit 2 were noted during the IPE. Both Units are Westinghouse 4 loop pressurized water reactors. Unit 1 operates at a thermal power of 3250MW, a nominal average temperature of 547 (deg F) and a nominal pressure of 2100 psig. Unit 2 operates at 3411MW, 573.8 deg F and 2250 psig. While the higher power may slightly affect the consequences of an accident once one has occurred, it is judged that this has no effect on the types of accidents analyzed or their frequency of occurrence. Though the different average temperatures could have an effect on the initial rate of coolant loss for a given break, the ECCS systems are identical in design. Also, UFSAR Large Break LOCA analyses indicates that the ECCS's ability to make up water to the vessel, which is based on break size, is important and not initial pressure. Therefore, Unit-to-Unit differences such as power level and operating pressure were judged to have no impact on accident initiating event frequencies and insignificant impact on the accident consequences. For conservatism, the number of tubes from Unit 2 steam generators were used for steam generator tube rupture frequency since these generators contain more tubes. Also, during the plant system fault tree development phase, Unit-to-Unit differences were noted and no major discrepancies were found.

Although systems such as ECCS, AFW and CCW can be cross-connected between Units 1 and 2, the only shared systems at Cook Nuclear Plant that normally run cross-connected are the ESW (safety-related service water), NESW (non-safety-related service water) and Plant Air systems. Plant Air feeds the individual Unit Control Air (instrument air) systems, which are not cross connected. Loss of NESW, which would ultimately lead to a loss of Control Air (Plant & Control Air compressor cooling) and thus a loss of the main feedwater regulating valves, progresses the same as a Transient Without Steam Conversion Systems Available. Loss of ESW was an analyzed accident event. Both ESW and NESW system fault trees accounted for flow from the Unit 2 side. The Loss of ESW initiating event frequency calculation employed a modified ESW fault tree and thus accounted for Unit 2 ESW flow. The ESW, NESW and Control Air systems were linked in where needed during the core damage frequency quantification process.

12. NUREG-1335 reporting guidelines requested the rationale if plant-specific experience was not utilized on a number of important items. Provide the rationale for your use of generic data for batteries, electrical buses, breakers, circulating water, feedwater, and condensate booster pumps and check valves.

Response:

The underlying philosophy of the IPE project regarding component failure rates was to use plant-specific data whenever possible and appropriate. Plant-specific data are defined as equipment reliability and availability information from operating and maintenance records for equipment installed at Cook Nuclear Plant. In cases where plant-specific data were insufficient, generic data was used or the plant-specific data was melded with generic data using Bayesian update techniques, which provided a statistical distribution for desired failure rates that were weighted toward the expected response. Referring to Table 3.3-1 of the IPE submittal, the far right column shows the data source from which that failure probability was derived. For the components listed in the NRC's original question, plant-specific data in sufficient quantity did not exist for failure of the listed components except as follows: Circulating water pump failure to run probabilities did use plant-specific data, and feedwater and condensate booster pump failure to run probabilities used Bayesian update techniques based on plant-specific and generic data.

13. NUREG-1335 reporting guidelines requested that the types of common-cause failures considered in the analysis (both in the event tree sequences and in the system analysis) be reported. Provide a list of the types of common failures (e.g., miscalibration of instrumentation, design deficiencies or manufacturing errors) that were considered in the IPE. In addition, our review notes that in comparison to other studies (NUREG-1150, NUREG-1032), some of the MGLs in table 3.3-6 appear low. Briefly describe how these values were generated specifically for the EDGs, MOVs, High Head and RHR pumps. Also discuss the apparent application of 4 component MGLs on two component systems (e.g., one out of two EDGs).

Response:

There are a few questions/comments posed within NRC question 13. To provide a more meaningful response, each sub-question is reiterated below along with the response.

13a Provide a list of the types of common cause failures (e.g., miscalibration of instrumentation, design deficiencies or manufacturing errors) that were considered in the IPE.

Response:

The generic common cause data base of common cause events from EPRI NP-3967, "Classification and Analysis of Reactor Operating Experience Involving Dependent Events" was used in the common cause failure analysis. Therefore the types of common cause failures identified in the report were considered in the Cook Nuclear Plant IPE. These include (per EPRI NP-3967):

- Design, manufacturing and construction errors,
- Erroneous procedures,
- Other plant staff error,
- Test and maintenance,
- Internal component,
- Environmental stress, and
- Other unknown causes.

The following components were evaluated for the common cause contribution:

- Diesel Generators,
- Motor Operated Valves,
- High Head Pumps,
- Residual Heat Removal Pumps,
- Containment Spray Pumps,
- Auxiliary Feedwater Pumps,
- Service Water/Component Cooling Water Pumps,
- Air Compressor,
- Air Operated, Hydraulic Operated, and Manually Operate Valves,

- 0 Electrical/Electronic Components such as: Battery Charger, Limit Switch, Invertor, Fuse Switch, Power Transformer),
- 0 Heat Exchanger,
- 0 Strainers and Filters, and
- 0 Motor Driven and Turbine Driven Pumps other than those specified above,
- 0 Check Valves

13b In addition, our review notes that in comparison to other studies (NUREG-1150, NUREG-1032), some of the MGLs in Table 3.3-6 appear low. Briefly describe how these values were generated specifically for the EDGs, MOVs, High Head and RHR pumps. Also discuss the apparent application of 4 component MGLs to two component systems (e.g., one out of two EDGs).

Response:

The Cook Nuclear Plant IPE used Multiple Grrek Letter (MGL) factors that were derived based on the data in EPRI NP-3967 and the calculation methods presented in NUREG/CR-4780. The data was reviewed and only those identified in the screening category, "C" (common cause events), were used in the calculations. No plant-specific evaluation of the common cause events was performed.

The equations provided in NUREG/CR-4780 were used to calculate the MGL factors for the EDGs, MOVs, high head and RHR pumps. Table 3-6 of NUREG/CR-4780 for the MLG method provides the equations for beta, gamma, and delta. The treatment of common cause data involves the use of impact vectors developed for each event as discussed in NUREG/CR-4780. The common cause group size for each common cause event is required to do a mathematically rigorous mapping of these events to a 4 component system prior to adding the vectors. Since the common cause group size is not given in EPRI NP-3967, the underlying assumption was that each common cause event had a common cause group size of 4 or greater. Thus, the number of linear single event failures was mapped up from a two component to a four component system (no_1 =4/2 * number reported). This in effect reduces the beta factor by approximately a factor of two for a component system that is dominated by independent failures. (Note that EPRI NP-3967 states that there is an unquantified bias because not all independent failures are reportable and are therefore not included in the data base. Hence the denominator of the parameters may be underestimated. This would result in a conservative bias.) The analysis also used a weighting factor of 0.1 for potential failures (consistent with EPRI NP-3967 and NUREG/CR-4780).

Based on the limited information contained in NUREG/CR-4550, Revision 1 (page 6-8), NUREG-1150 analyses also used the data in EPRI NP-3967. However, it does not state if any of the events were screened (i.e., only the C events were used) or

assumptions with respect to component group size. Based on this limited information, the Cook MGLs appear low due to the assumptions used in the derivation of the MGLs as stated above.

The assumption which justifies mapping of single failures from a 2-component to a 4-component system is a sound one. EPRI TR-100382, "A Database of Common Cause Events for Risk and Reliability Evaluations", June 1992, cites the average number of components per plant for each component type of interest. For the DG, RHR pump, high head pump, and MOV component groups the average number of components was 2.06, 2.8, 2.69, and 13.82, respectively. It should be noted that these values are average number of components per plant and not component group size. Similar components in the same application may not share the same common cause failure modes due to differences in the components relative to the common cause failures. This is applicable to RHR and high head pump component groups which contain both centrifugal and positive displacement pumps. All failure modes of similar components in different services cannot be considered as sharing like common cause. This consideration does not apply to the pump groups or DGs since there are multiple trains with the same service and the common cause grouping is done by system. However, since the data is not aggregated by system for MOVs, one must consider the group size of MOVs affected by the failure, not the total number of similar components. For any given MOV failure this number closely matches the number of system trains and approaches an average value of two for component group size. The mapping of single failures is also backed up by a statement already quoted above in this response and again stated in NUREG/CR-4780 with regard to the single failures as follows: "the LERs do not report all the independent events and that the under-reporting could be as high as a factor of 2 or 3". That is, if the system size for the single failures is greater than 2, there is a factor of 2-3 which could be applied to account for under-reporting of single failures to balance deviations from the assumed system size.

The calculation of the generic MGL factors was performed using data from EPRI NP-3967. This data has been re-evaluated by EPRI and re-issued in June 1992 (EPRI TR-100382). The group size for each common cause event is provided along with best estimate of the probability of 2,3, and 4 component failures. Plant specific analyses have been performed for numerous IPEs using this data which was provided in a June 1990 draft. These plant specific analyses support the generic values calculated only from EPRI NP-3967 data as being realistically conservative. Most of the plant specific arguments have been centered on circa 1990 procedures. Many of these procedures have been generated as a result of the common cause events cited in the database. Items included in these procedures for which credit was taken with respect to common cause failures include: post

maintenance testing, periodic test of components and inspection of purchased equipment, lubricant, and greases. In summary, the generic common cause factors for DG, RHR pump, high head pump and MOV component groups are realistically conservative when compared to common cause factors generated from EPRI TR-100382 when credit is taken for circa 1990 procedures.

14. It is unclear from the discussion in IPE submittal where the "average" CCF was applied and how it was applied. Provide complete list of CCF groups and identify where the average CCF was applied. In addition, the conclusion (p 7-1) that common cause failures are not a dominant contributor to core damage frequency, because individual component common cause contributors had not been modelled, may be misleading. Discuss the extent to which operational data at Cook Units 1&2 (data at the individual component level) supports this conclusion.

Response:

The impacts of common cause failures (CCFs) were applied at the plant system level for the Cook Nuclear Plant IPE. Thus, CCF logic gates were inserted into the system fault trees by the PRA analysts. Once an analyst constructed a system fault tree and performed an initial fault tree quantification using random, human error and test/maintenance probabilities, CCFs based on hardware failures were determined using the Multiple Greek Letter (MGL) method. For a given system, CCFs were calculated for each of the CCF groups in that system (such as pumps and MOVs) and then summed for an overall system CCF. For systems such as essential service water (ESW), multiple fault trees were developed for ESW responding to different accident scenarios (the ESW fault tree for LOCAs was different from the ESW fault tree for Loss of Offsite Power). Thus, an overall ESW CCF had to be calculated for each ESW fault tree.

Using the following guidance, CCF groups were established:

1. Same initial conditions (i.e. normally open, normally closed, energized, de-energized).

2. Same use or function such as system isolation, flow modulation, parameter sensing, etc..

3. Same failure mode such as failure to open or failure to start.

Once each CCF group was formed, the MGL parameters shown in Table 3.3-6 of the submittal were then applied for that group's CCF calculation. If a group did not fall specifically into one of the component groups of Table 3.3-6, then the ALL MGL factors of Table 3.3-6 were used for that group's CCF calculation. The ALL MGL factors represent the average of the MGL factors from Table 3.3-6. In general, the specific CCF groups in Table 3.3-6 are more complex, and thus more prone to CCFs, than the components which employed the ALL factors. Thus, use of the ALL MGL factors is viewed as conservative.

Since an overall CCF representing all of a system's CCF groups was calculated (for each operational mode), placing the CCF gate near the top of each fault tree was appropriate

for modeling purposes. This tended to give CCFs more weight in the system failure calculation, although it greatly simplified the fault tree model and was considered desirable. Had component specific CCFs been applied at lower tiers in the fault trees, CCFs would not be as dominant in system failure or ultimately in overall core damage frequency. As a result, the calculated CCFs are not viewed as dominant to core damage frequency, even though some of these failures appeared as such during the core damage assessment quantification. A review of the IPE data collection and analysis effort supports this conclusion.

15. The application of internal flood methodology, with respect to identification and selection of flood sources, frequency estimates, mitigation actions, flood propagation to redundant safety related equipment, qualification of equipment exposed to spray, etc., can have a significant impact on the perception of flood as a contributor to the core damage frequency. In order for the staff to fully understand and appreciate your treatment of internal flood, concisely describe the integration of this initiator into your PRA, i.e., discuss the structure of the internal flood event tree employed and integration of the impact of flood into the fault tree analysis. In addition, concisely discuss the rationale supporting the treatment, or assumptions (as appropriate), of the following aspects of the internal flood analysis reported in the Cook IPE submittal, including the perception of these aspects with respect to their overall significance to core damage/early containment failure:

- 0 estimation of the flood frequency (e.g., length of pipe, etc.), and the relationship of this frequency to the assumed 50% chance of one flood occurring over the lifetime of the plant. (Also define lifetime of plant [years]).
- 0 the term "bounded" in the section on turbine building operating floor (pg 3.4-6.5),
- 0 inter-zone flood propagation due to back flooding through drains, open flood doors, penetration seals, etc.
- 0 Spray or direct impingement of water on plant equipment,
- 0 treatment of circulating water system expansion joints, and potential for circulating water pump trip, back flow through the break, and isolation capability.

As per NUREG-1335, Section 2.3, also describe any strategies or potential improvements, and disposition of potential improvements, that stemmed from your treatment of internal flood in your IPE.

Response:

The Cook Internal Flooding PRA used a double guillotine break in an essential service water (ESW) pipe as the basis for the analysis. This break basically assumes that the contents of Lake Michigan are being pumped into the plant. This approach is consistent with internal calculations performed to determine maximum flood heights in areas of the plant containing Class 1E electrical equipment within 24 inches of the floor. These calculations determined that drainage capacity and operator actions are sufficient to mitigate the flood and maintain the equipment operable for this worst case flood.

The Internal Flooding PRA used screening criteria to focus

the analysis. The first criterion was established to determine the flood's ability to cause a reactor trip. If the flood in an area could not cause a reactor trip, the area was eliminated from further consideration, since no accident exists if the plant continues to operate. The second criterion evaluated the flood's ability to disable equipment in the area that would be needed to mitigate an accident. If the flood could not impact the operation of such equipment, the flooding event was considered to be covered under the transient event tree (TRA) and no further analysis was performed. The only areas receiving further analysis, therefore, were areas where a flood could cause a reactor trip AND disable equipment necessary for accident mitigation. After the zones were all tested using these criteria, eleven zones required further analysis.

Those remaining zones were further analyzed using plant walkdowns and by the use of existing internal flooding calculations that examined maximum flooding levels. This provided the basis for determining that important equipment would not be affected by water spray or flood in most of these areas. Inter-zone flood propagation due to such mechanisms as back flooding through drains, open flood doors, penetration seals, and spaces beneath doors was addressed in these evaluations. After this additional analysis; one area remained - the turbine building sub-basement.

The turbine building sub-basement houses the fire protection pumps, turbine sump pumps, and the non-essential service water pumps. Flood water from a postulated ESW break would eventually collect in this area, disabling the NESW pumps after some time. These pumps are used to cool the control and plant air compressors in the plant. Thus, the pressurizer PORVs, the S/G PORVs, and the feedwater regulating valves would be unavailable in this scenario due to loss of control air.

This scenario is a Transient Without Steam Conversion Systems (feedwater) Available (TRS), an event already evaluated in the Cook PRA. The TRS event tree was quantified assuming the above equipment failures. An initiating event frequency was calculated to represent the likelihood of an ESW pipe break. The initiating event frequency was conservatively calculated as being represented by the frequency of condenser expansion joint failure. This has historically been a source of flooding in nuclear plants, and has a much higher frequency than that typically used for low pressure pipe break. The flooding frequency used for Cook was 3.00E-03/year expansion joint flooding frequency. Since the ESW break was assumed only as a flooding source and it was not expected to break with this frequency, a loss of ESW transient is not modeled.

The core damage frequency resulting from this quantification was 2.00E-07/year. If a flooding frequency of 50% (0.5) over the lifetime of the plant (25 years for Unit 1 and 2

combined) is assumed, the initiating event frequency changes to 0.02/year. This would increase the core damage frequency due to internal flooding by a factor of 6.7 (0.02/0.003 = 6.7). This still yields a small core damage frequency, especially compared to the internal events CDF of 6.26E-05/year.

Spray and direct impingement of water on plant equipment was addressed through plant walkdowns of areas that survived the initial screening. No significant scenarios were identified from the walkdown.

Flooding concerns surrounding the condenser expansion joints and the general operation of the circulating water system did not survive the initial screening because of the lack of equipment in the area needed for accident mitigation.

Flooding concerns in the 4160 VAC safety bus rooms (both trains) were also screened out as a flood hazard area. Results of previously existing AEPSC flooding calculations and the IPE internal flooding walkdowns provided the basis for this conclusion.

Because the core damage frequency associated with internal flooding at Cook Nuclear Plant was very low, no plant changes to equipment or procedures were initiated.

16. Per NUREG-1335 reporting guidelines, provide a concise discussion of the criteria used to define "vulnerability," list any vulnerabilities so identified, and the fundamental causes of each. If explicit criteria had not been developed, discuss the process used to evaluate the need for plant improvements during and upon completion of the IPE, and the level at which plant improvements were implemented.

Response:

AEPSC does not have any formal criteria which define a "vulnerability". However, the following criteria are generally representative of AEPSC's concept of vulnerabilities:

1. Safety and non-safety related component failures that have a significant impact on core damage frequency. This came directly from the core damage frequency quantification or from the sensitivity analyses.

2. Operator actions whose failure has a significant impact on core damage frequency. This too came directly from quantification or from sensitivity analyses.

3. A mode of containment failure whose consequences or frequency of occurrence have a severe impact on offsite releases.

Identification of major vulnerabilities would mandate immediate action commensurate with the associated risk significance. Lesser vulnerabilities are addressed on a cost-benefit basis.

Based on the above criteria, no major vulnerabilities have been identified at Cook Nuclear Plant Units 1 and 2. Minor vulnerabilities are addressed in Sections 6 and 7 of the IPE submittal. The following is the most recent status of recommended plant improvements:

1. Add emphasis on RCP seal temperature in the Emergency Operating Procedures (EOPs) - The foldout page of the E-0 EOP (Reactor Trip/Safety Injection) has been amended with further guidance on tripping RCPs (including seal temperature).

2. Early initiation of opening CVCS cross-ties to opposite Unit - Still under evaluation.

3. Modifications to the compressed air system to increase its capacity - Design upgrades still under evaluation. EOPs being upgraded to include specific steps for restarting air compressors and/or cross-tieing to opposite Unit.

4. Training on the impact of primary and secondary system heat removal on containment pressure - Direction has been added to the EOPs for restarting containment cooling following reset of Phase A and B containment isolation signals. These procedural changes are then integrated into the normal training cycle.

5. Modifications to EOPs for maintaining feedwater flow to a faulted steam generator during a SGTR when secondary side integrity cannot be maintained (offsite release concern) - Still under evaluation.

6. Training on the importance of a wet reactor cavity on potential fission product releases - EOPs modifications have been made which require a second train of RHR (low head injection) to remain in service and aligned to the RWST until RWST low-low level alarm is reached. This ensures that the maximum available RWST inventory is pumped into containment prior to transfer to recirculation.

17. Your IPE identified a unique containment failure mode which could result from containment overpressurization. This failure mode leads to loss of all inventory available for ECCS recirculation and ultimately core damage. What is the estimated contribution to core damage from this failure mode? To what extent (positive and negative) has containment venting been considered as a strategy for preventing containment failure and associated core damage?

Response:

Please refer to the response to Back End (Containment Analyses) response 2.

18. Page 3-5 of IPE submittal states that the ice condenser was assumed to function as designed, and that the sequence involving ice condenser failure "would be below the cutoff frequency specified in NUREG-1335 as requiring further evaluation." Note that NUREG-1335 did not specify a "cutoff" frequency, but reporting criteria (see NUREG-1335, Appendix C, response to comments C.4.5 and C.4.6. Please provide the rationale for excluding failure of the ice condenser.

Response:

Failure probability of the Cook Nuclear Plant ice condenser system was found to be low since the ice condenser is completely passive with no on-line support system interrelationships with other systems. Since numerous technical specifications exist for this system, ice inventory is large and the chances of ice condenser lower inlet door blockage (random failures or failure to remove lower inlet door braces after refueling) are very low, the only credible failure mechanism is a number of the ice condenser lower inlet doors failing to open when challenged. This was basically a common cause failure calculation which led to a 1.0E-06/demand failure rate. Multiplying this value by any of the initiating event frequencies found in Table 3.1-1 of the submittal immediately leaves a value anywhere from the 1.0E-06 to the 1.0E-10 range. This is even before challenging the remaining accident mitigation systems, which set any sequence even lower in value. Thus, the ice condenser was not specifically included in the models for internal initiating events.

19. As an initiating event, SGTR is an important contributor to Cook's core damage frequency (11.3%). The IPE, however, does not appear to consider operator action to refill the RWST. Discuss the consideration and need for refilling the RWST during SGTR events.

Response:

With the main objectives of Steam Generator Tube Rupture (SGTR) mitigation being to isolate the faulted steam generator and to cooldown the primary side (decay heat removal and lower the leak rate to the faulted steam generator), explanations centering on Cook Nuclear Plant emergency operating procedures (EOPs) best address how a SGTR is approached with regard to RWST inventory. The following EOPs are referenced:

1. OHP 4023.E-3, "Steam Generator Tube Rupture"

2. OHP 4023.ECA-3.1, "SGTR w/Loss of Reactor Coolant - Subcooled Recovery Desired"

3. OHP 4023.ECA-3.2, "SGTR w/Loss of Reactor Coolant - Saturated Recovery Desired"

The actions of the E-3 procedure center on stabilizing RCS pressure at approximately the faulted steam generator (S/G) pressure (or the lowest S/G relief valve setpoint) before the faulted S/G fills due to the addition of AFW and break flow. This is normally accomplished by isolating the faulted S/G, initiating an RCS cooldown, depressurizing the RCS and terminating the SI (safety injection). Successful execution of the E-3 procedure would lead to reaching a stable condition in approximately 30 minutes. If recovery takes significantly longer or if multiple tubes fail, the faulted S/G may fill and challenge secondary integrity.

The ECA-3.1 and 3.2 procedures may be entered for different reasons:

1. S/G overfill occurs and a secondary side relief valve sticks open.

2. The faulted S/G cannot be isolated from the intact S/Gs used for cooldown.

3. There is no feedwater available to the intact S/Gs a thus forcing use of the faulted S/G for cooldown.

Per ECA-3.1, operators initiate a cooldown at a maximum rate of 100 deg F/hr. Once RHR entry conditions are established (less than 363 psig and 350 deg F), the RHR system can be placed in service to continue cooldown to cold shutdown. If the operators determine that the amount of water available for injection or recirculation is less than about half that

initially in the RWST, a transition is made to ECA-3.2. The first step in ECA-3.2 directs the operators to add makeup to the RWST as necessary. These actions within ECA-3.1 and 3.2 may appear complex, but the operators would have roughly 10 to 20 hours for them to be successful for a design basis SGTR provided high pressure SI (safety injection) is available. This is the approximate RWST depletion time for a break with an average injection flow requirement from 300 to 600 gpm (WCAP 12922 - WCGS PRA Event Tree Analysis Notebook; Wolf Creek and Cook Nuclear Plant are similar 4-loop plants). Thus, although refilling the RWST is not explicitly modeled in the event trees or system fault trees, RWST inventory and its impact on accident mitigation is addressed through modeling of the Cook Nuclear Plant EOPs.

20. During mitigation of certain initiators, (e.g. station blackout, loss of CCW) system success criteria require operators to open steam generator PORVs, and depressurize the secondary side to initiate RCS cooldown. Opening the S/G PORVs will place a differential pressure across the S/G tubes and in effect, increase the likelihood of tube failure. Discuss the consideration of subsequent tube rupture as part of these scenarios and potential impact on IPE results.

Response:

Please refer to the response to Back End (Containment Analyses) question 9.

21. The estimated conditional probability of failure of feed and bleed in the Cook IPE submittal was given as 2.19E-03. What is the estimated reduction in overall core damage frequency from having feed and bleed capability? Had the benefit of feed and bleed in conjunction with refilling the RWST been explored for SGTR and ISLOCA scenarios?

Response:

A further sensitivity run was recently made in response to this question allowing for primary bleed and feed (PBF) to have a very high failure probability. This resulted in core damage frequency increasing by 44%. However, this run entailed complete failure to follow procedures which direct initiating PBF. Given that the operator training program at Cook Nuclear Plant is extensive and INPO accredited, this is extremely unlikely.

Using PBF for removing decay heat is set forth in Cook Nuclear Plant emergency operating procedure (EOP) "Response to Loss of Secondary Heat Sink". Within this EOP, the RWST is addressed in that when level reaches 32%, a switch to high pressure recirculation (drawing from the containment recirculation sump) is made. In this case, high pressure recirculation is meant to be the long term cooling medium, which is shown in the SGTR event tree.

For the ISLOCA event, losing RCS coolant through the RHR cooldown suction valves is the most probable coolant loss pathway (see Figure 3-1, attached). Sealing this pathway, which is modeled, involves shutting the RHR pump suction valves, thus removing the RHR pumps from further service. This eliminates PBF, since PBF ultimately leads to high pressure recirculation, for which RHR pumps are required. Thus, PBF as a long term cooling medium (in this case) with refilling the RWST would be more difficult since containment pressure increases must now be addressed. First, the auxiliary feedwater system is the normal source of removing decay heat and is modeled as such in the ISLOCA event tree. Second, per the IPE submittal, not only was the ISLOCA initiating event frequency low (1.0E-07 range), but ISLOCA was the least contributing event to overall core damage frequency. Thus, further investigation of this event did not appear to be warranted.

BACK END (CONTAINMENT ANALYSES) QUESTIONS

1. It is stated in the IPE that the containment fails at the concrete basemat adjacent to the containment wall and results in a small rupture area. It is further stated that a time delay occurs while water in containment is being expelled out the "hole." It is assumed in the IPE that this time delay is 35 minutes for sequences without RWST and an hour for sequences with RWST. The IPE notes that while water is being expelled, the containment pressure continues to increase. Provide the containment pressurization rate before and after failure of the concrete basemat wall junction, and the sources of pressurization.

Response:

The MAAP code does not have the ability to model water releases from containment. Since preliminary evaluations indicated that the radiological releases were not sensitive to the water release timing, nominal times were chosen for water expulsion, and the containment break size was based on that assumption. During this time period of water expulsion, the pressure in the containment was allowed to rise at the same rate as before the break occurred. The rate of pressure increase was dependent on the accident scenario and was typically due to decay heat produced steaming, usually about 10 psi/hr. After the delay period, the water was "removed" from lower containment by manipulation of the code input, and the containment break area was added to the code input to allow containment depressurization. This simplification was necessary due to the code limitations, and little impact is expected on the calculation of the source terms from this simplification.

2. Given core melt, the Cook IPE estimated the conditional probability of containment failure on overpressurization to be 0.033. Provide the estimated conditional probability of containment failure on overpressurization prior to core melt, and contribution of this failure mode to core damage. Also discuss any consideration given to containment venting prior to core damage, i.e., potential benefit of venting.

Response:

The estimated conditional probability of containment failure before core melt is 0.5%, which is the same as its contribution to core melt. As noted, containment failure in the basemat region leads to a loss of water inventory available for ECCS recirculation. This core damage mode was only found in the large break LOCA sequence. Similar failures were found to be possible in smaller break sequences, but only after the 24 hour time frame required by NUREG-1335. Twenty four hours was considered to be a sufficient time to restore the containment spray system, so this conclusion is believed to be appropriate.

Due to the low core melt contribution of this failure mode, only limited consideration was given to containment venting. A cursory review of the existing vent system indicated that it would not provide an adequate vent path without significant modification. The existing vents are for low containment pressures, and have a filter in the line which would need to be bypassed for severe accident venting. In addition, actions which could be taken to restore the containment spray system or an investigation of the capability of the RHR sprays could further reduce this contribution to core melt. Therefore, containment venting was not considered further.

3. Documentation in IPE submittal was insufficient to understand what was analyzed for failure of containment isolation. The submittal only references that fluid lines were examined; the impact on containment isolation for failure of air and instrumentation lines were not reported. Identify and discuss the contributors to containment isolation failure, i.e., isolation signal failure, valve failures (including purge valves), degradation of valve seats, etc.

Response:

As part of the containment isolation analysis, both mechanical and electrical penetrations were reviewed. Mechanical penetrations were broken down into three categories:

1. Administratively controlled fluid system penetrations (such as those used during refueling operations)

2. Normal operation fluid system penetrations

3. Accident fluid system penetrations

It was assumed that for both types of penetrations (mechanical and electrical), there was no pre-existing leakage and that the mechanical and sealant materials of the penetrations are maintained throughout the course of an accident. This latter assumption is supported by the Level II analysis results. With this in mind, the electrical penetrations were actually addressed as part of the IPE Level II effort, which found that these penetrations would not be challenged by molten core debris since such debris would be contained within the crane wall of Cook Nuclear Plant's ice condenser containment. This removed a major threat to electrical penetration integrity and thus containment leakage past electrical penetrations was not considered a significant hazard. Therefore, the containment isolation analysis centered on fluid system penetrations.

In all, 98 fluid system penetrations and two access hatches penetrate the Cook Nuclear Plant containment shell. This listing was screened using the following:

1. All lines and isolation boundaries less than two inches in diameter were eliminated (slow containment depressurization and lower fission product release rates).

2. Lines that are part of a closed system and not subject directly to containment atmosphere were eliminated. Systems outside of containment whose design pressure is greater than 50 psig and not open to the environment were considered closed systems. The Level II used the ultimate strength of containment, 36

psig, as the initiating point for significant containment releases.

3. Lines whose failure probabilities were found to be low due to the necessity of multiple failures (valve and/or system components) having to occur were eliminated.

4. Lines whose isolation was part of the Level I effort were eliminated. For example, the steam generator secondary boundary provides isolation from the containment atmosphere to the environment. This path is not severely challenged unless a SGTR occurs. Isolation of the faulted steam generator during a SGTR is explicitly modeled in the SGTR event.

Lines remaining from this screening process were modeled in the containment isolation fault tree, which accounted not only for containment isolation valves mechanically failing to close, but also addressed common mode failures for both the valves and generation of the closing signals; closing signal failures; electrical power failures (4160 VAC, 600 VAC, 120 VAC, 250 VDC); containment spray, RHR, essential service water and component cooling water system failures; and human error failures for isolating containment and for the administratively controlled penetrations (leaving these penetrations open). Valve seat degradation was not assumed in this analysis (containment isolation failure) since containment response to a post-accident environment (pressure and temperature) was analyzed in the rest of the Level II analysis. However, as part of the Level II analysis, potential containment leakage past the purge and exhaust valves was reviewed since the purge and exhaust system has a low operating pressure (approximately 0.5 psig) and has blow out plugs to the auxiliary building. From this review, it was determined that the purge and exhaust valves have a low chance of leaking in a post-accident environment due to their construction and seating characteristics.

The largest contributor to containment isolation failure involved common mode failures (both valve and isolation signal generation). The next failure of significance was human error failure to maintain closed the administratively controlled penetrations.

4. In response to generic Letter 88-20 Supplement 3, licensees with ice condenser containments are expected to evaluate the vulnerability to interruption of power to the hydrogen igniters as part of the IPE. The Cook IPE submittal states that hydrogen combustion is not considered a failure mode of the Cook Nuclear Plant containment. With respect to your hydrogen ignitor analysis, describe the extent to which restoration of AC power and subsequent hydrogen combustion was considered. Identify initial conditions, e.g., blackout, loss of DC, etc,. walkdowns performed, important assumptions and rationale, codes exercised, potential for local pocketing and detonation, and any insights from other analyses as appropriate.

Response:

The Cook Nuclear Plant IPE evaluated hydrogen combustion relative to the availability and recovery of hydrogen igniters. The IPE Level I functional sequences which include failure of the igniter system were identified and tabulated based on a cut-off frequency of 10^{-7}. Excluded from the list were bypass and failure to isolate sequences. The systemic sequences that either analyzed or bounded these functional sequences included two station blackouts (SBO-50 and SBO-190) and a loss of offsite power (LSP-21). For the IPE analysis, igniters were assumed unavailable for the duration of the mission time of 24 hours in the loss of offsite power sequence. AC power was not recovered within the 24 hour mission time for the two station blackout cases.

Without power available to the igniters, the hydrogen inventory can readily accumulate up to combustible levels for any severe core damage scenario where a sufficient percent (i.e., > 30%) of the clad has been oxidized. Once hydrogen concentrations exceed 8%, very little energy (i.e., static charge) is required to ignite the mixture as long as the environment is not steam inerted.

In assessing the concern of hydrogen combustion at Cook Nuclear Plant, all three cases (LSP-21, SBO-50,SBO-190) were run using MAAP 3.0B Rev. 17.02 suppressing all hydrogen burns and analyzing the time dependent plot of hydrogen accumulation in the upper compartment. Following vessel failure, the mass of hydrogen in the upper compartment would increase rapidly then level off at a peak value (> 8%) and remain fairly constant throughout the sequence duration. Since these cases were all high pressure melt ejections, a negligible contribution to hydrogen accumulation due to concrete ablation was observed.

For each of the three cases, MAAP calculations were again performed allowing hydrogen combustion to occur at a time following vessel failure and prior to depletion of ice. It was assumed that recovery occurred within this time, thus establishing an ignition source. This provides a bounding

conservative analysis. The results for this analysis are tabulated below:

	Sequence		
	LSP-21	SBO-50	SBO-190
Time of Vessel Failure	4 hr	14 hr	4 hr
Time of Ice Depletion	8.5 hr	24.5 hr	10.2 hr
Time of Containment Failure due to Steam Overpressurization	11.8 hr	30.5 hr	14.3 hr
Time H_2 Burn was Initiated	5 hr	16 hr	5 hr
H_2 Concentration @ T_{burn}	12.4%	8%	11.7%
Steam Concentration @ T_{burn}	5.3%	45.1%	9.8%
Mass of H_2 Burned	260 Kg	175 Kg	265 Kg
Final ACOMPT Pressure after H_2 Burn	46 psia	58 psia	48 psia

The tabulated results indicate that the station blackout sequence (SBO-50) resulted in containment failure due to hydrogen combustion within the 48 hr mission time. Station blackout sequence (SBO-190) and loss of offsite power (LSP-21) did not result in exceeding the containment ultimate pressure of 50.7 psia due to hydrogen combustion. Note that these two sequences were successful in burning well over 8% H_2 without failing containment. Case SBO-50 had available auxiliary feedwater for a six hour period. This allowed for removal of decay heat over a six hour time period. Once auxiliary feedwater was lost, the time for melting of the core was extended compared to SBO-190 due to the earlier removal of decay heat. The result was a greater degree of oxidation and higher hydrogen production.

This sequence was not considered indicative of an early containment failure mode for the following reasons:

1. Under the IPE evaluation, no consideration was given to recovery of power after 8 hours. Nearly 8 additional hours would be available to initiate recovery actions in this sequence.

2. The hydrogen igniter system is a manual operation and would not automatically become operational upon recovery, due to limits on hydrogen concentrations.

3. The upper compartment is close to being steam inerted (i.e., 45% steam concentration).

4. The peak pressure exceeded the 95/95 containment failure pressure of 50.7 psia, but barely reached the mean containment failure pressure of 57.8 psia. In addition, significant containment pressure margin is known to be available by taking credit for actual material strengths.

5. The evaluation assumes conservative timing of hydrogen ignition. Ignition before or after this time would produce lower pressure spikes.

The insights gained from this analysis will serve as input to future accident management activities. These include:

1. Recovery from an SBO with feedwater operation should consider upper compartment sprays as a means to cool the gas space and lower the pre-burn pressure if recovery is prior to ice depletion.

2. Recovery actions following ice depletion should consider the potential for a steam inerted environment.

To further support the hydrogen analysis, two separate containment walkdowns were performed. The objectives of both were to ensure proper modeling of ignition sources.

The assessment provided in the phenomenological evaluation summary for the susceptibility of the Cook Nuclear Plant containment to detonations concluded that detonations induced by direct deposition of energy in a detonable mixture of containment gases was not possible due to the large energy source (i.e., explosive charge) required for this mechanism. Detonations due to a transition from a deflagration to detonation (DDT) were also considered. Two locations (ice condenser upper plenum and steam generator doghouses) were assessed to establish their susceptibility to the likelihood of a DDT interaction. Both of these locations were

analyzed using two separate approaches which resulted in very low probabilities for both methods. Due to the limited energy requirements of a deflagration with hydrogen concentrations greater than 8%, it is far more likely that combustible gas will be consumed within containment by deflagration rather than detonation.

5. In the modeling of severe accidents, there is uncertainty with regard to the phenomena and therefore, the manner in which an accident will progress and subsequently impact containment performance and source term. The assumptions associated with the various phenomena are varied among experts and the available modeling codes. It is important, therefore, to be aware of the differences and uncertainties, particularly in relation to their impact on containment performance and source terms. The staff notes that assumptions and conclusions in the Cook IPE are (1) primarily based on MAAP calculations and (2) differ from various "expert opinions" from other studies. NUREG-1150 analysis of Sequoyah, for example, found late containment failure dominated by basemat meltthrough, and also found early containment failure, through small, a contributor. It was not clear how these phenomenological differences (i.e., uncertainties) were accounted for in understanding the IPE results. Although a formal uncertainty analysis is not required, describe how your IPE findings and conclusions accounted for phenomenological uncertainties and differences between your results and those, for example, NUREG-1150.

Response:

Phenomenological uncertainties were addressed qualitatively in the Cook Nuclear Plant Level II IPE phenomenological position papers which were generated during the project by the Level II contractor, Fauske & Associates, and reviewed by AEPSC. For each physical phenomenon of interest, the relevant literature was reviewed and a relatively conservative technical basis developed. Based on this evaluation, the impact of each phenomenon on the containment event tree was determined. The MAAP code was not used extensively in all of these evaluations, and the code's use was typically limited to timing or sensitivity studies to better understand the phenomenon. After a relatively conservative evaluation of the phenomena was completed, no attempt was made to quantify and address the remaining uncertainty.

Some specific differences between the Cook Nuclear Plant IPE and the Sequoyah study described in NUREG 1150 can be assessed. The Sequoyah study expected 4% of early containment failures due to direct containment heating by a high pressure melt ejection. The Sequoyah containment was challenged when a large fraction of the molten core was ejected, and when all of the ejected molten core was assumed to participate in direct containment heating. This containment challenge was significantly more important when little or no ice was left in the ice condenser. For the Cook Nuclear Plant IPE, credit was taken for a less than complete coupling between the molten core and the atmosphere in the geometrically confined Cook Nuclear Plant reactor cavity. This was based on an experiment performed for Zion (Fauske & Associates, Inc. 1990, "FAI/CECo Direct Containment Heating Experiment for a

Zion Like Geometry", FAI/90-60, report submitted to Commonwealth Edison). Even combined with a direct containment heating initiated hydrogen burn, the containment ultimate pressure was not found to be exceeded.

The Sequoyah study also found both early and late containment failure due to hydrogen combustion. The hydrogen evaluation for the Cook Nuclear Plant IPE is discussed in response to question 4. The evaluation indicated that hydrogen combustion was not expected to be a significant contributor to Cook Nuclear Plant containment failure, although this failure mode could not be excluded. The MAAP computer was used extensively in this evaluation for the study of hydrogen generation rates and containment conditions as a function of time.

Considering containment failure by basemat concrete erosion, the difference between the Sequoyah study and the Cook Nuclear Plant IPE is due to the Cook Nuclear Plant IPE imposition of a 48 hour cutoff for containment evaluations. This time is felt to be sufficient for actions to be taken to cover the molten core in the cavity to stop further concrete erosion. The Sequoyah study assumed that concrete erosion would continue unimpeded. Both studies found that several days would be required for the core to erode through the containment basemat. Although it was not concluded that basemat failure due to concrete erosion could not occur under any circumstances in the Cook Nuclear Plant, it was concluded that either containment would fail by other, faster acting mechanisms or mitigation actions could take place before basemat failure.

6. The Cook IPE appears to assume that no concrete floor erosion occurs until there is a dry cavity; that is, the molten core is assumed to be completely quenched when there is any overlying water. However, Generic Letter 88-20, Appendix 1 states that both coolable and noncoolable outcomes should be considered. Provide the rationale for your assumptions with regard to core concrete interaction during wet cavity conditions.

Response:

The Cook Nuclear Plant basemat is 10 feet thick below the reactor cavity. Even in a dry sequence, basemat failure by concrete erosion is conservatively estimated to require at least 86 hours, using plant specific concrete composition data. As evaluated in our supporting analysis, even partial credit for overlying water in a wet cavity sequence would clearly increase the time to failure through the basemat to several hundred hours. Therefore, basemat failure was not considered to be an important issue for wet cavity sequences.

For MAAP analysis of wet cavity sequences, the core heat was assumed to be directed to the water layer. Otherwise, the core heat directed to the concrete could vary from sequence to sequence and at various times within a sequence. The steaming pressurization rate would be reduced, and some core concrete reaction products would be added to the containment atmosphere. Since basemat failure was not considered to be an issue as indicated above, little additional knowledge would be expected to be gained for a significant increase in the complexity in the analysis.

7. A containment failure pressure distribution is provided in the submittal. It is not clear, however, how the "uncertainty" of containment failure was considered in the study. For example, given a scenario that involves synergism between hydrogen combustion and other ongoing phenomena, was the 95/95 failure pressure utilized, or was the "mean" value utilized? In either case, discuss insights gleaned from the analysis.

Response:

The 95/95 failure pressure of 36 psig was consistently used in these analyses for MAAP code calculation of the source terms. When the containment is going to fail by steaming, pressure typically rises quickly, in the range of 10 psi per hour. If the mean pressure value of 47.8 psig had been used instead of the 36 psig value, only an hour delay would be expected with little change in the overall result.

The phenomenological evaluations also consistently used the 95/95 failure pressure of 36 psig as an acceptance criteria. The use of this conservative value was sufficient to eliminate direct containment heating and steam explosions from further consideration. In some isolated circumstances, some synergy is expected with hydrogen combustion and background steam pressure. The resultant pressure could potentially exceed the 95/95 containment failure pressure. In this case, some credit for pressure capacity beyond the 95/95 capacity helps to provide assurance that containment failure by hydrogen combustion is unlikely. The response to question 4 addresses this issue in more detail.

8. It is not clear in the documentation if the various phenomena, though concluded not to present a challenge to containment integrity, could nonetheless challenge system or human response. Provide discussion of how phenomenological effects were integrated into the CETs in regards to addressing the effects of environmental conditions on system performance. Identify any important human actions related to the backend analysis, and discuss how these actions were incorporated in the analysis.

Response:

The various accident phenomena are not expected to impact the sequence modelling in the Cook Nuclear Plant Level II IPE. Instrumentation and systems are already designed to survive conditions up to the point of vessel failure. Protection of the containment after vessel failure requires only containment spray recirculation and hydrogen igniters, and only equipment in the lower compartment would be directly impacted by the various phenomena. The igniters in the upper compartment are sufficient to protect the containment from hydrogen combustion failure, so failing igniters in the lower compartment is not important. The only mechanism identified which could potentially cause the failure of the containment spray system would be a mass of molten core sticking on the spray system piping, causing a failure of the piping. Since melt ejection would take place in the cavity and need to travel through the cavity to impact the sprays, this would be expected to be of low probability. The sprays are round piping, so a significant amount of molten core would not be expected to stick. In addition, the spray system is full of flowing water, which would cool the inside of the piping, preventing melt through. If the spray system was not full of water, the sprays would already be inoperable and failure is of no relevance. Therefore, a failure of the containment system due to the various phenomena was not considered.

Likewise, since recovery actions are not modeled after core damage has begun, the impact on human actions is of little relevance. The igniters would be turned on well before this point. The only other required action is switchover to containment sump recirculation, which is accomplished well before core melt and outside of containment. In addition, sump recirculation does not rely on any instrumentation inside of containment. Therefore, variable stress conditions depending on the containment environment were not modeled.

9. Induced steam generator tube rupture (ISGTR) during severe accidents is an important primary system failure mode because of the potential for containment bypass. In addition, the uncertainty with respect to SG tube integrity, evident in recent PWR operating experience, elevates the likelihood of ISGTR during severe accidents. Describe the extent to which SGTR had been considered in the IPE.

Response:

Consequential failure of steam generator (SG) tubes is not modeled in the Cook Nuclear Plant IPE. Although a plant specific review was not performed, the potential for a temperature induced steam generator tube rupture was considered low based on a review of NUREG-1150 and related documents for similar steam generator designs.

When this issue was reviewed by the expert panel as reported in NUREG/CR-4551, the 50th percentile rate of temperature induced failure before vessel breach based on the aggregate of the experts opinions was 0.0001. Given our core damage frequency of 6.26E-5, frequency of induced steam generator tube failures would be insignificant.

We understand that newly identified steam generator cracking characteristics and new steam generator plugging criteria are being reviewed for their failure risk. If appropriate, new information developed from these ongoing studies will be integrated into a future update of the Cook Nuclear Plant IPE.

10. The C-Matrix, or containment matrix which displays the plant damage states verses the fractional contribution of the various failure modes (bypass, early failure, late failure, basemat melt-through, vessel breach w/o containment failure, no vessel breach) provides useful level II insights. Has a C-Matrix been developed? If so, please provide.

Response:

A C-matrix has not been developed for the Cook Nuclear Plant IPE. Since the only consequential failure mode of significance was determined to be containment overpressure by steaming, the matrix was expected to provide little insight.

11 The Cook IPE study did not result in the identification of any containment, or containment system vulnerabilities. With respect to containment performance during accident conditions, and NUREG-1335 reporting guidelines which include a concise discussion of the criteria used to define vulnerabilities, provide a definition of vulnerability with respect to containment performance. If no explicit definition had been developed, discuss the utilization of the level II insights in enhancing safety at the Cook facility, i.e., the process used to identify and implement improvements.

Response:

Please refer to Front End (Core Melt Analysis) response 16.

HRA (HUMAN RELIABILITY ANALYSIS) QUESTIONS

1. What process was used to identify the various operator actions modeled in the IPE and for which HEPs were estimated?

Response:

Operator actions that needed to be modeled were identified by the individual analysts during the typical course of event tree and fault tree construction. For example, when a fault tree analyst identified an operator action necessary for successful system performance, the HRA analyst was given details surrounding the operator action (timing, complexity, indication, etc.) and a detailed human error probability (HEP) was calculated. Likewise, operator actions were included on the event tree level.

The basic philosophy used in identifying such operator actions was that, if the action was vital to successful functioning of the system, it was included as part of HRA. An exception to this philosophy was made if the exclusion of an action from the study was viewed as totally inconsistent with what the operators indicated they would do under the postulated scenario. It was felt that such an exclusion was required to maintain the "best estimate" approach for the analysis.

2. The estimated HEPs for the various human errors appear to be extremely low; the majority of the errors have probabilities less than 1E-3 (over 85 % of the human actions listed in Table 3.3-5). Human error probabilities of less than 1E-4 imply a 'precision' of human behavior that is not known. It is not clear how these values were estimated. Provide discussion of several examples illustrating the derivation of the HEPs and basis for such low values.

Response:

The estimated HEPs appear to be low because the generic probabilities (Table 3.3-2 of the IPE Submittal) are generally low and then typically reduced even further by the application of Performance Shaping Factors (PSFs) (Table 3.3-3). The PSFs (discussed in response HRA-8) listed in Table 3.3-3 are used consistently throughout the study.

In order to provide some examples of the methodology used, Appendix 1 contains sections from the Cook PRA Human Reliability Analysis. These sections include: 1) operator fails to restore control air through use of the plant air compressor during loss of offsite power, 2) primary bleed and feed, and 3) steam generator depressurization and condensate feed.

Item 1 is a simple hand calculation required in the compressed air system analysis. The PSFs used are taken from Table 3.3-3 and are used in a fashion that is consistent with the rest of the analysis. The 10 minute time frame reflects the amount of compressed air contained in the system after the compressors stop (it takes about 10 minutes for the air to leak from the system). This time was identified through discussions with plant personnel knowledgeable in this activity.

Items 2 and 3 utilize fault trees to calculate the required HEP. The fault tree is comprised of several individual HEPs including diagnosis, action, and verification activities. Each individual HEP uses the PSFs from Table 3.3-3 in a consistent manner. A degree of independence between the individual HEPs is assumed because the operators generally perform in something of an "automatic" mode while executing each step in the EOPs. The operator is not influenced greatly by stress or other factors that might affect one's performance normally because the operator is focused and well trained in the required actions. This is reflected in the fault trees.

3. It is unclear in the IPE submittal how dependencies were accounted for in the quantification process. This confusion appears for the human actions identified in the event trees and the faults trees. First, it is not clear if the dependencies associated with the human actions identified in the event trees are modeled. For example, for the small LOCA event tree, Operator Actions OA6 and PBF (which are top events) appear to be multiplied together in accident sequences #23 through 31. This multiplication would result in a combined HEP of 2E-8 (6.23E-4*3.37E-5). It is not clear how the dependency between these two human actions was considered. Second, in the various event trees, in several places the same operator action occurs and appears to be quantified in the core damage frequency estimation with the same probability of occurrence, that is, independent of the accident sequence. For example, for a SGTR, Operator Action OA3 occurs in several of the accident sequences. It appears that in the quantification the same probability value was used regardless of the sequence. This application implies that every sequence progression is identical in those factors that would affect human performance. Another example, for the PBF human action, the same probability appears to be used regardless of accident sequence for all the initiators. It is realized that with symptom based EOPs the operator should not have to "diagnose" the event; however, the initiator will effect the success criteria, and therefore, the timing, the manner in which the accident progresses. These differences should impact the human performance. It is not clear how the dependency of the action relative to the sequence was considered. Last, operator actions are identified in the fault trees as basic events. The assignment of the error probabilities appears to be independent of the accident sequence and independent of other operator actions. It is not clear how the dependency relative to the accident and with other operator actions was considered. When the fault trees are linked to form the accident sequences, the human action can appear in numerous places with a variety of different system or functional failures. Applying the same HEP implies that the human behavior is independent of these failures. In addition, when linking the fault trees, the potential exists for these operator actions to be multiplied. Although the text states that dependencies are treated, this statement is not apparent in the documentation provided. Provide a discussion on the details of how dependencies were treated addressing the examples described above.

Response:

Dependencies between human actions were considered in the analysis. A good example of this can be observed by examining top events MRI (manually insert rods) and PP1 (primary pressure relief). Top event MRI is challenged in the ATWS event tree. This event represents the operator action to diagnose an ATWS and manually insert rods. Following MRI (success or failure), PP1 is challenged. PP1

will only be challenged in an ATWS situation, and, therefore, the event must be first diagnosed. The diagnosis is the same as in MRI, however, so the same identifier is used. This tells the model that if the operator fails to correctly diagnose the ATWS, he will fail not only MRI, but also PP1. Thus, the dependency of both MRI and PP1 on the diagnosis of the event is correctly represented.

While one can argue that every human action is different due to changing conditions, it is not practical to attempt to calculate a different HEP for every postulated condition. After witnessing simulator activities and talking with operators, it is clear that once the diagnosis of the accident is complete and the operators know which EOP to enter, the actions that follow are simply performed step by step without many dependencies. This fact was carried throughout the analysis.

In the case of top events OA6 (operator action 6) and PBF (primary feed and bleed) in the small LOCA event tree, the events are indeed multiplied in certain sequences, thus they are treated independently. Both operator activities are dependent upon the initiator itself, but once the event diagnosis is complete, any dependencies are absent. The operator simply begins the activity because a step in the EOP instructs him to do so. These two top events represent two different methods of decay heat removal and are driven by two different procedures. The operators are not influenced by stress at this point, therefore, OA6 and PBF are treated independently.

In the case of OA3 (operator action 3) in the steam generator tube rupture (SGTR) event, OA3 represents the operator actions required to cool the RCS to atmospheric conditions by initiating cooling through the faulted steam generator. This would be used if RCS cooling cannot be performed using the intact S/Gs or if the faulted S/G cannot be isolated. Entry into top event OA3 is procedurally driven and would be initiated well into the accident mitigation. Since this action is simply another step that occurs in the EOP, unique failure rates for OA3 were not calculated for each accident sequence because it is felt that the OA3 entry conditions are very similar from the standpoint of possible human error. Since this action is unaffected by most outside influences such as stress, it was deemed appropriate to have only one failure rate for OA3.

In the case of PBF (Primary Bleed and Feed) which appears in many of the event trees, the entry conditions for PBF are very similar in all of the event trees, so the human errors were grouped and only one calculation performed. Initiation of primary bleed and feed is driven by a step in the EOP instructing the operator to evaluate plant conditions and follow the next step in the procedure. By this time the operator is well into the procedures, and is in the

"automatic" mode. This is consistent throughout the EOPs. While some differences might exist in response times or plant conditions, the entry conditions for PBF are always the same. It is felt that a single calculation adequately represents this top event in the Cook PRA.

In the development of fault trees, care was taken to ensure that an individual fault tree was unique to given accident conditions. If a fault tree clearly did not meet the needs of a given event tree model due to event-specific success criteria, failure modes, or human error requirements, a separate fault tree was developed. With regard to the same human action being modeled in several different places in the Cook PRA, the human error was assigned a unique identifier that prevented double-counting during the fault tree linking process. For example, the 250 V DC fault tree models the operator aligning the backup battery charger. This fault tree supports several other fault trees, therefore, the same battery charger operator action appears in many different fault trees. The fault tree linking process (the WLINK computer code was used in this capacity) uses Boolean logic, however, to eliminate the possibility of double-counting this action. This operator action will effectively appear only once in each event tree.

As addressed earlier, it is recognized that every action and the conditions surrounding it are different in some way. However, the human actions modeled in the fault trees are usually required due to a step in the EOPs. The step might not explicitly instruct the operator what to do, but it typically identifies a need and allows the operator to use his/her training to perform the function (e.g., the EOP might say initiate AFW flow, but allow the operator to determine which valve to open). Since each human action is typically demanded by the same conditions, only one HEP was developed and used repeatedly when needed. If the analyst felt that the action changed drastically from one event to the next event, the unique identifier was changed so that the WLINK code treated it as a different action.

4. NUREG-1335 states the "unless proper justification is provided .... all assumed or modeled recovery actions will have written procedures." In the D.C. Cook IPE, credit appears to be given for operator actions that are not proceduralized. Provide a list of these actions and justification for each on why credit should be given for these actions.

Response:

The Cook Nuclear Plant IPE submittal states that, for some operator actions, no detailed procedures are available, and only general direction is provided to the operator. Taking credit for such actions is considered acceptable for certain recovery evolutions when the recovery actions are "practiced" routinely as part of normal operations without the use of procedures. Where such credit has been taken in the Cook Nuclear Plant IPE, they are discussed in the next paragraphs.

The Cook PRA models very few recovery actions, and those modeled can be categorized as simple and complex. The simple tasks include actions such as manually opening a valve or manually aligning a battery charger. The two recovery actions that can be categorized as complex are recovery of failed CCW system and recovery of failed ESW system. In these cases, a combination of proceduralized actions and simple manual actions was evaluated to calculate the failure rates associated with recovery. The CCW system has a spare pump that is mechanically aligned, but not electrically aligned. A procedure exists for electrically aligning this pump. CCW recovery can also be accomplished by simple opening of a manual crosstie valve to the opposite unit. Another possible recovery action is the manual opening of a motor-operated valve that has failed. Recovery of ESW is based on simple actions such as manual opening of valves and manual initiation of backwash for the strainers, neither of which requires procedures.

Following is a list of recovery actions which either are not specifically proceduralized or assume some not specifically proceduralized actions, and a brief explanation of each:

Failure to align alternate battery charger - This is a simple action requiring an operator to simply walk to the battery charger location and energize the charger locally. An implementation procedure is not considered necessary as this activity is done periodically by operators who rotate the operational battery charger.

Failure to recover CCW within one hour - Procedures exist to instruct the operator in diagnosis of the cause of a loss of CCW. This operator action was evaluated to determine the failure rate of operator action intended to perform a simple recovery such as

manually opening a motor-operated valve, attempting to restart a CCW pump remotely, or opening a manual crosstie valve. Explicit steps in the recovery procedures do not exist for the simple actions because the operators are already knowledgeable in the performance of these actions.

Failure to recover CCW within eight hours - Procedures exist to instruct the operator in diagnosis of the cause of a loss of CCW. This operator action was evaluated to determine the failure rate of operator action intended to perform a complex recovery such as aligning the spare CCW pump for operation or replacing a valve operator. Procedures exist for the alignment of the spare CCW pump. Replacement of a valve operator is done routinely under normal maintenance procedures and does not require emergency procedures.

Failure to recover ESW within one hour - Procedures exist to instruct the operator in diagnosis of the cause of a loss of ESW. This operator action was evaluated to determine the failure rate of operator action intended to perform a simple recovery such as manually opening a motor-operated valve, attempting to restart a ESW pump remotely, or opening a manual crosstie valve. Procedural steps do not exist for these simple actions because the operators are already knowledgeable in the performance of these actions.

Failure to recover ESW within one hour - Procedures exist to instruct the operator in diagnosis of the cause of a loss of ESW. This operator action was evaluated to determine the failure rate of operator actions intended to perform a complex recovery such as repairing a failed strainer or replacing a valve operator. Replacement of valve operators and the repair of strainers are done routinely under normal maintenance procedures, and does not require emergency procedures.

To evaluate the impact of the treatment of simple, routine recovery actions that are not covered in detail in the recovery procedures, the human error probability for these steps was increased to the high error rate of item 18 on Table 3.3-2 of the IPE submittal. This item is described as "when written procedures are available and should be used but are not used." This assumption increased the probability of failing the recovery portion of the action by more than a factor of five. However, for the cases reviewed, the failure to diagnose the need for recovery action still dominated the failure probability of the entire recovery action. The impact on the core damage frequency of this modeling change would be negligible (less than 1%).

In summary, certain recovery actions were included in the Cook Nuclear Plant IPE even though they were not proceduralized in detail in the recovery procedures. Only a small increase in CDF would be expected if significantly less credit was taken for these recovery actions. Since these recovery actions are routine or simple, the existing credit that is taken for them is believed to be appropriate.

5. It is not clear if and how the impact of "faulty" instrumentation was considered in the HRA. It is stated in the IPE that "it was assumed that the EOPs .... were adequate to address the transient symptoms and ensure that the operator provides the correct functional response." This statement appears to also assume that the instrumentation and indications are functioning properly. Provide clarification of this issue - what was the impact of instrumentation and indication failures on the operator interaction model?

Response:

Instrumentation failures were addressed in the "diagnosis" sections of the HEP calculations by including instrumentation failure rates in the calculations. Those HEPs requiring complex calculations (i.e., those requiring individual fault tree analysis) often included the diagnosis of an accident. Diagnosis of an event is dependent on the availability of instrumentation, therefore, the instruments were modeled. Instrumentation failure does not appear as a gate in any fault tree; instead, it is included in the gate called "diagnosis." Even when multiple instruments existed during a particular sequence to aid the operator in the diagnosis, it was conservatively assumed that the failure of a single instrument would fail the diagnosis.

Looking at Table 2-5 of the appendix to this attachment, task A1a2b represents a case where the hardware failure rate for instrumentation is modeled. In this example, the operator can view two analog meters displaying different plant parameters (SG level, RCS temperature, and RCS pressure) to determine the need for primary bleed and feed. Failure of one of the instruments is conservatively modeled to result in the operator failing to read any of the available instruments. This is representative of how instrumentation failure is modeled throughout the entire analysis.

6. In Table 3.3-5, there are numerous places where the time available for the operator action is N/A. In regards to pre-initiator actions (e.g., failure to restore valve to proper position), it is clear why time would not be applicable. Several of these human actions do not, however, appear to be pre-initiator actions. Provide classification of human actions listed in Table 3.3-5 and provide rationale why time available is not applicable for the operator actions listed in Table 3.3-5.

Response:

For many of the entries in Table 3.3-5, thermal hydraulic analysis was performed to determine the amount of time available to perform the entry in question and the consequences should that action fail. The HEPs associated with these entries typically represent the calculated available time for diagnosis. Those entries which indicate that the time available is "N/A" typically represent actions where the time available had little bearing on any modeled activity associated with failure of the entry. Following is the list of those entries where the available time is "N/A" and justification for that categorization:

Containment isolation - This HEP was used in the Level II fault tree for containment isolation. If containment isolation failed (both automatic and manual), containment failure was assumed. No time limit associated with the action was calculated because no additional action depended on containment isolation.

Energize hydrogen igniters - This HEP was used in the Level II fault tree for hydrogen igniters. Failure of this action will result in the challenging of containment air recirculation fans to maintain acceptably low concentrations of free hydrogen in the containment. The action depends on the initial concentration of hydrogen, not on any calculated time, therefore, no entry for time available was included.

Align battery charger - This HEP was used in the 250 V DC fault trees. The battery has a four hour life, so the operator has four hours to perform this action. Since there exists so much time to perform this simple action, the HEP was not terribly dependent on the time available, thus, it was omitted from Table 3.3-5. The value could be listed as 4 hours.

Supply additional water to AFW - This action occurs as part of the EOPs. If the operator fails to perform this action, the S/Gs will eventually boil dry, and decay heat removal will be lost. There exists an audible alarm in the control room on low condensate storage tank (CST) level and the EOPs contain a

warning that CST level might be getting low. Operator interviews revealed that it takes about 45 minutes for the S/Gs to boil dry, so that is the appropriate entry. However, this value is felt to have little bearing due to the existence of multiple diagnostic tools and the operator's training in quickly responding to such an alarm.

Re-open AFW valves - This action occurs as part of the EOPs in the event of a steamline/feedline break. When the event occurs, the subject valves automatically throttle to a preset position to limit the amount of positive reactivity added due to overcooling. After the break is isolated, the operators are instructed to restore full AFW flow as part of cooldown. If AFW flow is not increased, S/G levels will become low, but decay heat removal will still be present; the cooldown rate will simply be small. Thus, there is no calculated time associated with this operator action.

Isolate MCM-221 - This action is performed to isolate the steam supply from the turbine driven AFW pump during a steamline/feedline break. Failure to isolate this valve will result in a failure to isolate the affected steam generator. This action is simply done as part of the EOPs, well after the accident has been diagnosed. Failure of the action will place the operators in a different part of the EOPs due to the affected S/G not being isolated. No calculated time limit is associated with this action; if the action is not performed, the operators will simply be instructed to do something else.

Isolate proper S/G - This action is defined as operator fails to diagnose a SGTR and isolate the proper S/G. Diagnosis is better discussed in the analysis of top event OA1. That analysis allows 30 minutes for the diagnosis of the event and initiation of action associated with the mitigation of the SGTR.

Close breakers for 69 kV line - This action is modeled as a recovery action in the loss of offsite power event. During a LOOP, the diesel generators are available, but the normal power supply and the automatic backup power supply are unavailable. If the diesel generators do not immediately start or randomly fail sometime during the incident, one of the operator's options is to attempt to restore offsite power using the 69 KV line. Timing is not considered of significant importance in this case since failure of the action puts the plant into a station blackout which is analyzed in detail elsewhere in the Cook Nuclear Plant PRA.

Close output breakers in switchyard - This action is modeled as a recovery action in the loss of offsite power event. Similar to closing the 69 KV line breakers, this action simply recovers the 69 KV line if the normal transformer fails. A manual switch in the switchyard must be closed to direct the power from another transformer to the plant. According to discussions with the operators, the action must be done locally by non-Cook Nuclear Plant personnel and will require at least an hour. Once again, failure of this action places Cook Nuclear Plant in a station blackout which is analyzed elsewhere in the Cook PRA.

Open breakers K and K1 - This action is an immediate action step in the first EOP entered by the operators on a loss of AC power. These breakers are the main generator output breakers tying Cook Nuclear Plant to the AEP grid. Failure to open these breakers will cause the offsite power needed for Cook Nuclear Plant to be placed on the grid instead of the Cook Nuclear Plant electric buses. The operators are in the "automatic" mode when they execute this step. It occurs within seconds after a reactor trip. If they fail to open the breakers, a step in the procedure soon after instructs them to verify that the buses are energized, thus, a verification step of sorts exists. The time needed was not considered critical since the procedural step dictating this action is memorized.

Strip emergency buses - This action requires the operators to manually strip the emergency buses given failure of the automatic load shedding for a diesel generator actuation. Failure to perform this task would impact diesel generator loading and could possibly place Cook Nuclear Plant in a station blackout. As stated earlier, station blackout is analyzed in detail elsewhere in the study. For this reason, the timing was not deemed critical.

Trip RCPs - This action requires the operators to trip the RCPs following a loss of CCW or loss of ESW. Failure to do so is conservatively assumed to result in a significant RCP seal LOCA. The action must occur immediately based on annunciators signaling high seal temperatures, so timing was not calculated.

Top events PPR and LTS - These top events are modeled in the ATWS event tree and are steps in the EOP associated with this action. The procedure dictates the conditions during which these events occur, so no time was calculated.

Top Event OIB - This top event models the operator closing the RHR isolation valves given an interfacing systems LOCA. A diagnosis time of 20 minutes is

modeled, and the only actions necessary are the remote closing of two motor operated valves. The time listed should be 20 minutes, not N/A.

7. Time available for various operator actions is provided; however, it is not clear if sufficient time is available to perform the required action. Provide the time that is needed to perform the operator actions listed in Table 3.3-5 and the basis or rationale for these times (i.e., how were the times derived).

Response:

After interviews with the operators, conversations with system engineers, and witnessing simulator activities, it was clear that proceduralized activities performed from the control room (e.g., starting pumps, verifying levels, actuating valves, etc.) typically took very little time when compared to the time it takes to diagnose the accident. For example, it takes the operator from 10-15 minutes to perform the switchover from ECCS injection to recirculation for a high pressure event. There exists about 45 minutes of water in the RWST when the low level alarm sounds. This is ample time to complete the diagnosis and the action. In the low pressure case, less time is available at the low RWST level (approximately 20 minutes), but less time is needed to perform the switchover since the high head pumps do not have to be enabled. Thus, ample time exists for the completion of the task.

In general, the time needed to perform the activities listed in Table 3.3-5 was not broken into diagnosis time and action time. Emphasis was placed on the existence of sufficient time for the entire procedure and on operator understanding of methods and procedures.

8. Performance shaping factors are provided in Table 3.3-3 of the submittal. The bases for those factors are not provided; therefore, it is not apparent what factors (such as difficulty of task, accessibility and location of "component," degree of burden, etc.) were considered in determining the performance shaping factors (e.g., stress level extremely high). In addition, it appears that it was assumed that the performance shaping factors are not impacted by the accident sequence. For example, since only one HEP was estimated for PBF, the stress level, for instance, was assumed to be the same for every accident sequence; that is, whether the accident involved a LOCA, SGTR, transient and which systems are available and not available does not impact operator performance. Provide the criteria that was used by the analyst in identifying and selecting the performance shaping factors listed in Table 3.3-3.

Response:

The PSFs used for Cook Nuclear Plant were developed using our best judgement and the assistance of the vendor (Westinghouse). The PSFs are generally consistent with those used by the vendor in other IPE studies. In addition, although only a limited amount of guidance was provided in NUREG-CR/2254, "A Procedure for Conducting a Human Reliability Analysis for Nuclear Power Plants," this document was also used extensively.

As discussed in response HRA-2, efforts were made to use the PSFs on a consistent basis throughout the study. These PSFs were formed using what guidance existed in the industry and using information obtained from operator interviews and the witnessing of simulator activities at Cook Nuclear Plant. It is considered unrealistic to attempt to calculate a unique HEP for each scenario or condition represented in the PRA. This would add an unnecessary amount of complexity to the study with little chance of gaining any unique insights. For this reason, HEPs were formed such that they could be used in multiple scenarios without jeopardizing the validity of the analysis. In the case of PBF (primary bleed and feed), a fault tree was constructed to model the operator response when PBF is challenged. Our operator interviews and simulator surveillance showed that differences in stress are mainly limited to the diagnosis of events. Primary bleed and feed is a mechanism that is challenged well into an event when the operators are in the "automatic" mode of executing steps in the emergency operating procedures. Stress is believed to play an insignificant role in the performance of this activity. In addition, PBF was felt to be similar enough in each scenario such that no other PBF model was needed.

The assignment of PSF values used mostly general reasoning. Some credit (PSF=0.1) was given for operators being trained

in certain actions. If the action was memorized (i.e., trained much more frequently), the PSF was reduced to 0.01. Also, since the simulator surveillance and the operator activities left us with the belief that entering the EOPs in the case of an accident is an automatic response of the operators, a PSF of 0.01 was assigned to failing to enter the EOPs. Stress PSFs follow the guidance found in industry guidelines (e.g., NUREG/CR-1278, "Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Plants").

9. The submittal provides little discussion of the significance of human error. Provide the estimated human error contribution (percent) to overall core damage frequency, and identify: (1) the most significant human errors with respect to that contribution, and (2) the most significant human actions with respect to the prevention of core damage.

Response:

Table 3.4-4 of the Cook Nuclear Plant IPE Submittal provides an importance listing of the most significant basic events (several hundred insignificant events were omitted from this list), including human actions, that were analyzed to calculate the core damage frequency. This list contains six human errors that affect core damage frequency. The most significant of these human errors, RCP, (line 8) contributes 18% of the overall core damage frequency. This event represents the operator's failure to trip the reactor coolant pumps when RCP seal temperatures rise beyond safe limits. This event is important in events such as station blackout, loss of CCW, and loss of ESW when the operators are attempting to avoid RCP seal LOCAs. The next human error in the list is the operator's failure to refill the condensate storage tank when the low level setpoint is reached (line 39). This event contributes 1.64% of the overall core damage frequency. The remaining human actions on the list, diagnosis of the need for secondary side cooling in top event OA6 (line 58), diagnosis of the need for restoration of RCS inventory in top event RRI (line 63), verification of the alignment of critical equipment following recovery from a station blackout (line 73), and alignment of critical equipment following recovery from a station blackout (line 78) contribute even less and are not considered to significantly affect core damage frequency.

Sensitivity analysis was performed on these human actions as part of the Cook Nuclear Plant PRA. When the probabilities of failing to trip the RCPs were increased and then decreased by an order of magnitude, CDF increased by a factor of 2.5 and decreased by 17%, respectively. When the probability of failing to refill the CST was raised and lowered by two orders of magnitude, CDF increased by a factor of 3 and fell by 4%, respectively. All of the other actions discussed were collectively raised an order of magnitude which resulted in CDF increasing by 23%.

APPENDIX TO

ATTACHMENT TO AEP:NRC:1082F

INDIVIDUAL PLANT EXAMINATION

FOR THE

DONALD C. COOK NUCLEAR PLANT

RESPONSE TO NRC QUESTIONS

R. Operator Fails to Restore Control Air Through Use of the Plant Air Compressor During Loss of Offsite Power (#672)

During a loss of offsite power (LOOP), the control air isolation valves will fail closed due to a loss of power to the valve circuitry (Reference 17). In order to restore control air to Unit 1, the plant air compressor will have to be started and manually loaded since the Unit 1 control air compressor alone does not have sufficient capacity to fulfill the air demands (Reference 17). The necessary operator errors are: 1) operator fails to respond to control air low pressure alarms in control room OR 2) operator fails to start plant air compressor OR 3) operator fails to manually load the plant compressor OR 4) operator fails to re-open control air isolation valves AND 5) operator fails to verify adequate control air flow/pressure AND 6) operator fails to notice lack of compressed air through subsequent mitigating actions.

Thus, failure of this action is quantified using the equation

$$HEP = [Q1 + \{(Q2 + Q3 + Q4) * Q5\}] * Q6$$

Q1) Operator fails to respond to a compelling signal within 10 minutes and diagnose the need to start plant air compressor and open isolation valves - Table A-2 #1 (2.7E-01)

Factor		Assigned Value
Stress:Moderate		X 5
Trained		0.1
	PSF	0.5

$Q1 = (2.7E\text{-}01) * (0.5)$

$= 1.35E\text{-}01$

Q2) Operator fails to start plant air compressor by selecting wrong controls from an array of functionally grouped set of controls - Table A-2 #21 (1.3E-03)

Factor		Assigned Value
Stress:Moderate		X 5
Trained		0.1
	PSF	0.5

$Q2 = (1.3E\text{-}03) * (0.5)$

$= 6.5E\text{-}04$

Q3) Operator fails to manually load the plant air compressor - Table A-2 #17 (1.3E-02)

Factor	Assigned Value
Stress:Moderate	X 5
Trained	0.1
PSF	0.5

Q3 = (1.3E-02) * (0.5)

= 6.5E-03

Q4) Operator fails to open necessary isolation valves by selecting wrong controls from an array of functionally grouped set of controls - Table A-2 #21 (1.3E-03)

Factor	Assigned Value
Stress:Moderate	X 5
Trained	0.1
PSF	0.5

Q4 = (1.3E-03) * (0.5)

= 6.5E-04

Q5) Operator fails to verify adequate air flow/pressure by viewing analog meter in control room - Table A-2 #51 (3.8E-03)

Factor	Assigned Value
Stress:Moderate	X 5
Trained	0.1
PSF	0.5

Q5 = (3.8E-03) * (0.5)

= 1.9E-03

Q6) Operator fails to notice lack of compressed air through subsequent mitigating actions (i.e. additional valves will not open) - Table A-2 # 34 (1.6E-02)

Factor	Assigned Value
Stress:Moderate	X 5
Trained	0.1
PSF	0.5

Q6 = (1.6E-02) * (0.5)

= 8.0E-03

Therefore,

HEP = [(1.35E-01) +[{(6.5E-04) + (6.5E-03) + (6.5E-04)} * (1.9E-03)]] * (8.0E-03)

= 1.08E-03

2.3 PBF - PRIMARY BLEED AND FEED

Application

Small LOCA (SLO)
Large Steam Line/Feedline Break (SLB)
Loss of Offsite Power (LSP)
Transients with Steam Conversion Systems (TRA)
Transients without Steam Conversion Systems (TRS)
Steam Generator Tube Rupture (SGR)
Station Blackout (SBO)

Description

If auxiliary feedwater fails to remove heat through the secondary side of the steam generators, the operator could remove decay heat through primary side bleed and feed cooling. By following the emergency operating procedures, the 01-OHP 4023 series, the operator would be advised to start this method of cooling. The cooling path is feeding from the high pressure ECCS system and bleeding from the pressurizer PORVs.

Success of this event requires the operator to open at least two of three pressurizer PORVs and their associated block valves, if necessary, after ensuring at least one centrifugal charging pump and safety injection pump is running and supplying water from the RWST. (Reference 1 Appendices C, D, G, H, I, J, and K)

Note that some references to PBF in the event trees follow the successful actuation of high head injection while others do not. Failure of the operator to start injection is conservatively included for all event tree nodes. The fault tree linking methods used for this project will accurately screen out any common dependencies.

For OLI, Steam Dump via the S/G PORVs was used to lower primary-side pressure to allow low pressure injection for the medium LOCA. Unlike OLI, PBF does not take credit for Steam Dump because it does not provide long-term primary-side cooling.

Procedure(s)

Reference 4b

Tasks

The following are the primary tasks which must be completed:

A1) Diagnose the failure of secondary-side cooling (AFW and MFW) and need for bleed and feed cooling

A2) Initiate feed action by manually starting 1 of 2 Charging Pumps and 1 of 2 Safety Injection Pumps

A3) Initiate primary-side bleed action by opening 2 of 3 Pressurizer PORVs

A4) Verify success of Bleed and Feed Cooling

Table 2-5 details the necessary subtasks for each of the above.

Analysis and Assumptions

Table 2-5 summarizes the derived HEPS.

For each of the Human Error Probability calculations, a stress factor of 5 (Table A-4) is assumed to apply for the diagnostic phase and a stress factor of 2 is assumed to apply for the implementation phase of operator actions. This generally represents the change in stress that the operator undergoes during accident conditions. A stress factor of 2 is applied to the response to the S/G low-low level annunciators which is considered more straightforward. An assigned value of 0.01 was used for the operators being trained in entering the EOPs. After discussions with operators and witnessing activities on the Cook control room simulator, it is felt that the operators would enter the EOPs without hesitation. An assigned value of 0.1 was used throughout this notebook for being trained in following the procedural steps once in the EOPs. The following provides a detailed list of the subtasks (see Table 2-1) and the descriptive scaling guides used in developing the PSFs for each item:

Subtask	Factor		Assigned Value
A1a	Trained in entering EOPs		0.01
		PSF	0.01
A1b	Trained		0.1
		PSF	0.1
A2a	Trained		0.1
		PSF	0.1
A2b	Trained		0.1
		PSF	0.1
A2c	Trained		0.1
		PSF	0.1
A3a	Trained		0.1
	Two steps in procedure		2.0
		PSF	0.2
A3b	Trained		0.1
		PSF	0.1

A3c	Trained		0.1
		PSF	0.1
A3d	Trained		0.1
		PSF	0.1
A4a	Trained		0.1
		PSF	0.1
A4b	Medium time frame for response		0.1
	Multiple support instruments		0.1
		PSF	0.01

It is conservatively assumed that accident diagnosis will only be performed by the operators for task A1b through response to the low SG level alarm. Credit is not taken for diagnosis by the STA's from looking at critical safety parameters or by subsequent EOP steps by the operators. In addition, it is conservatively assumed that up to 7-10 annunciators may be alarming at this stage of the transient.

Based on Reference 9 photographs, the Pressurizer PORV controls have no mimic lines, no violation of populational stereotypes, and are functionally grouped with other Pressurizer controls.

It is noted that head vents are available, but they are conservatively not modeled.

It is conservatively assumed that the time available for the diagnosis is 30 minutes instead of 50 minutes.

It is conservatively assumed that a failure to properly read any one of the multiple indicators which assist the operator in diagnosing the transient would lead to confusion and misdiagnosis.

To determine the conditional probability of human error in establishing primary bleed and feed cooling, a HEP fault tree was developed and is shown in Figure 2-2.

Table 2-6 describes the event identifiers, and Table 2-7 summarizes the input data for the fault tree.

Results

The conditional probability of the failure to establish feed and bleed cooling and the combinations of failures (cutsets) are identified in Table 2-8. PBF is dominated by diagnostic failures related to the operator identifying the need for feed and bleed cooling or responding to low SG level alarms.

TABLE 2-5
PBF HEP CALCULATIONS

Descriptions (error type)	Mean HEP (Table A-2 Reference)	Performance Shaping Factors			HEP	Fault Tree Identifier	Additional Notes (Equipment, Actions, Indications, Locations)
		Stress	Dependence	Others			
Task A1 - DIAGNOSIS							
a) Failure to diagnose within 30 minutes of a compelling signal							
1) given success in reading any of the multiple low SG level and high RCS temperature and pressure indicators (saturation meter also available)	2.7E-03 (3)	5	High (Success)	0.01	6.75E-05	PBF-DIAG-MN-HE	q(a1)=HEP(a1)*PSF/2
2) given failure in reading any of the multiple low SG level and high RCS temperature and pressure indicators	a) Diagnosis: 2.7E-03 (3)	5	High (Failure)	0.01	5.0E-01		q(a2a)=[HEP(a2a)*PSF+1]/2
	b) Reading (1 of 2 types of analog meter): 2*3.75E-03 (51)	5	--	0.01	3.8E-04 Combined: 2.58E-04		q(a2b)=HEP(a2b)*PSF Q=q(a1)+q(a2a)*q(a2b)

TABLE 2-5
PBF HEP CALCULATIONS

Descriptions (error type)	Mean HEP (Table A-2 Reference)	Performance Shaping Factors			HEP	Fault Tree Identifier	Additional Notes (Equipment, Actions, Indications, Locations)
		Stress	Dependence	Others			
b) Failure to respond to SG low-low level annunciator (under AND gate with A1a) (30 minutes into transient, it is assumed that 7-10 annunciators are alarming - conservative)	1.3E-01 (45)	2	--	0.1	2.6E-02	PBF-SGALARM-HE	
Task A2 - INITIATE FEED ACTION							
a) Error of Omission - Failure to follow procedures without checklist	1.3E-02 (17)	2	--	0.1	2.6E-03	PBF-I-FD-CK-HE	
b) Error of Commission - Selecting wrong control where controls are labeled and functionally grouped	1.3E-03 (21)	2	--	0.1	2.6E-04	PBF-I-FD-SL-HE	
c) Error in reading pump discharge pressure gauges or injection flow gauges	3.75E-03 (51)	2	--	0.1	7.5E-04	PBF-I-FD-RD-HE	

TABLE 2-5
PBF HEP CALCULATIONS

Descriptions (error type)	Mean HEP (Table A-2 Reference)	Performance Shaping Factors			HEP	Fault Tree Identifier	Additional Notes (Equipment, Actions, Indications, Locations)
		Stress	Dependence	Others			
Task A3 - INITIATE PRIMARY-SIDE BLEED ACTION							
a) Error of Omission - Failure to follow procedure w/o checklist	1.3E-02 (17)	2	--	0.2	5.2E-03	PBF-I-PR-CK-HE	PSF accommodates 2 steps (Control air restoration and bleed initiation)
b) Error of Commission - Selects wrong control for Control Air Restoration (labeled and functionally grouped)	1.3E-03 (22)	2	--	0.1	2.6E-04	PBF-I-PR-CA-HE	
c) Error of Commission - Selects wrong control for PZR PORV (labeled and functionally grouped)	1.3E-03 (22)	2	--	0.1	2.6E-04	PBF-I-PR-SL-HE	
d) Error in reading pressurizer pressure/temperature chart recorder	7.5E-03 (52)	2	--	0.1	1.5E-03	PBF-I-PR-RD-HE	

TABLE 2-5
PBF HEP CALCULATIONS

Descriptions (error type)	Mean HEP (Table A-2 Reference)	Performance Shaping Factors			HEP	Fault Tree Identifier	Additional Notes (Equipment, Actions, Indications, Locations)
		Stress	Dependence	Others			
Task A4 - VERIFY SUCCESS OF BLEED AND FEED COOLING							
a) Error of Omission - Fails to verify success when a long procedure is used w/o checkoff provision	1.3E-02 (17)	2	--	0.1	2.6E-03	PBF-V-BF-CK-HE	
b) Error in reading primary pressure and temperature trends in Strip Chart Recorder (conservatively taken as one failure)	7.5E-03 (52)	2	--	0.01	1.5E-04	PBF-V-BF-RD-HE	

TABLE 2-6

EVENT ID DESCRIPTIONS (PBF)

[redacted]ER Version 2.20 10/14/1991 16:24:22
PBF FAULT TREE
LIST OF BASIC EVENTS AND THEIR DESCRIPTIONS

1	PBF-DIAG-MN-HE	FAILURE TO DIAGNOSE DEPRESS. NEED WITHIN 30 MIN.
2	PBF-I-FD-CK-HE	FAILURE TO FOLLOW PROCEDURE W/O CHECKLIST
3	PBF-I-FD-RD-HE	OPERATOR ERROR IN READING ECCS PUMP DISCHARGE PRESS. OR FLOW
4	PBF-I-FD-SL-HE	OPERATOR SELECT WRONG CONTROL TO START ECCS PUMPS
5	PBF-I-PR-CA-HE	OPERATOR SELECTS WRONG CONTROL FOR CONTROL AIR RESTORATION
6	PBF-I-PR-CK-HE	FAILURE TO FOLLOW PROCEDURE W/O CHECKLIST
7	PBF-I-PR-RD-HE	OPERATOR MISREADS PZR PRESS. & TEMP ANALOG METERS
8	PBF-I-PR-SL-HE	OPERATOR SELECTS WRONG SWITCH TO DIRECTLY OPEN PZR PORVS
9	PBF-SGALARM-HE	OPERATOR FAILS TO RESPOND TO MULTIPLE ALARMS WITHIN 30 MIN.
10	PBF-V-BF-CK-HE	FAILURE TO FOLLOW PROCEDURE W/O CHECKLIST
11	PBF-V-BF-RD-HE	ANALOG METER READING ERROR (MULTIPLE)
12	SUB-HP2	FAILURE OF HIGH PRESSURE INJECTION (2/4 CHP OR SI PUMPS)
13	SUB-PORVP	2 OF 3 PRESSURIZER PORVS FAIL TO OPEN

TABLE 2-7

FAULT TREE HEP INPUT DATA (PBF)

SEE TABLE 2-3 FOR REQUIRED INFORMATION

PAGE 1 TREE NAME: \CODES\HRA\PBF
CUTDES VER.1.7, 11-17-89
INPUT FILE: \CODES\HRA\PBF.CDS

CUT SETS FOR GATE G0001 WITH CUTOFF PROBABILITY OF 1.00E-12
GATE G0001 IS: FAILURE OF THE OPERATOR BLEED & FEED COOLING ACTION (PBF)

NUMBER	CUTSET PROB.	BASIC EVENT NAME	EVENT PROB.	IDENTIFIER
1.	1.35E-05	FAILURE TO FOLLOW PROCEDURE W/O CHECKLIST	5.20E-03	PBF-I-PR-CK-HE
		FAILURE TO FOLLOW PROCEDURE W/O CHECKLIST	2.60E-03	PBF-V-BF-CK-HE
2.	6.76E-06	FAILURE TO FOLLOW PROCEDURE W/O CHECKLIST	2.60E-03	PBF-I-FD-CK-HE
		FAILURE TO FOLLOW PROCEDURE W/O CHECKLIST	2.60E-03	PBF-V-BF-CK-HE
3.	6.71E-06	FAILURE TO DIAGNOSE DEPRESS. NEED WITHIN 30 MIN.	2.58E-04	PBF-DIAG-MN-HE
		OPERATOR FAILS TO RESPOND TO MULTIPLE ALARMS WITHIN 30 MIN.	2.60E-02	PBF-SGALARM-HE
4.	3.90E-06	OPERATOR MISREADS PZR PRESS. & TEMP ANALOG METERS	1.50E-03	PBF-I-PR-RD-HE
		FAILURE TO FOLLOW PROCEDURE W/O CHECKLIST	2.60E-03	PBF-V-BF-CK-HE
5.	7.80E-07	FAILURE TO FOLLOW PROCEDURE W/O CHECKLIST	5.20E-03	PBF-I-PR-CK-HE
		ANALOG METER READING ERROR (MULTIPLE)	1.50E-04	PBF-V-BF-RD-HE
6.	6.76E-07	OPERATOR SELECTS WRONG CONTROL FOR CONTROL AIR RESTORATION	2.60E-04	PBF-I-PR-CA-HE
		FAILURE TO FOLLOW PROCEDURE W/O CHECKLIST	2.60E-03	PBF-V-BF-CK-HE
7.	6.76E-07	OPERATOR SELECTS WRONG SWITCH TO DIRECTLY OPEN PZR PORVS	2.60E-04	PBF-I-PR-SL-HE
		FAILURE TO FOLLOW PROCEDURE W/O CHECKLIST	2.60E-03	PBF-V-BF-CK-HE
8.	3.90E-07	FAILURE TO FOLLOW PROCEDURE W/O CHECKLIST	2.60E-03	PBF-I-FD-CK-HE
		ANALOG METER READING ERROR (MULTIPLE)	1.50E-04	PBF-V-BF-RD-HE
9.	2.25E-07	OPERATOR MISREADS PZR PRESS. & TEMP ANALOG METERS	1.50E-03	PBF-I-PR-RD-HE
		ANALOG METER READING ERROR (MULTIPLE)	1.50E-04	PBF-V-BF-RD-HE
10.	3.90E-08	OPERATOR SELECTS WRONG CONTROL FOR CONTROL AIR RESTORATION	2.60E-04	PBF-I-PR-CA-HE
		ANALOG METER READING ERROR (MULTIPLE)	1.50E-04	PBF-V-BF-RD-HE
11.	3.90E-08	OPERATOR SELECTS WRONG SWITCH TO DIRECTLY OPEN PZR PORVS	2.60E-04	PBF-I-PR-SL-HE
		ANALOG METER READING ERROR (MULTIPLE)	1.50E-04	PBF-V-BF-RD-HE
12.	5.07E-10	OPERATOR SELECT WRONG CONTROL TO START ECCS PUMPS	2.60E-04	PBF-I-FD-SL-HE
		OPERATOR ERROR IN READING ECCS PUMP DISCHARGE PRESS. OR FLOW	7.50E-04	PBF-I-FD-RD-HE
		FAILURE TO FOLLOW PROCEDURE W/O CHECKLIST	2.60E-03	PBF-V-BF-CK-HE
13.	2.93E-11	OPERATOR SELECT WRONG CONTROL TO START ECCS PUMPS	2.60E-04	PBF-I-FD-SL-HE
		OPERATOR ERROR IN READING ECCS PUMP DISCHARGE PRESS. OR FLOW	7.50E-04	PBF-I-FD-RD-HE
		ANALOG METER READING ERROR (MULTIPLE)	1.50E-04	PBF-V-BF-RD-HE

REDUCED SUM OF PROBABILITY OF FAILURE = 3.370E-05

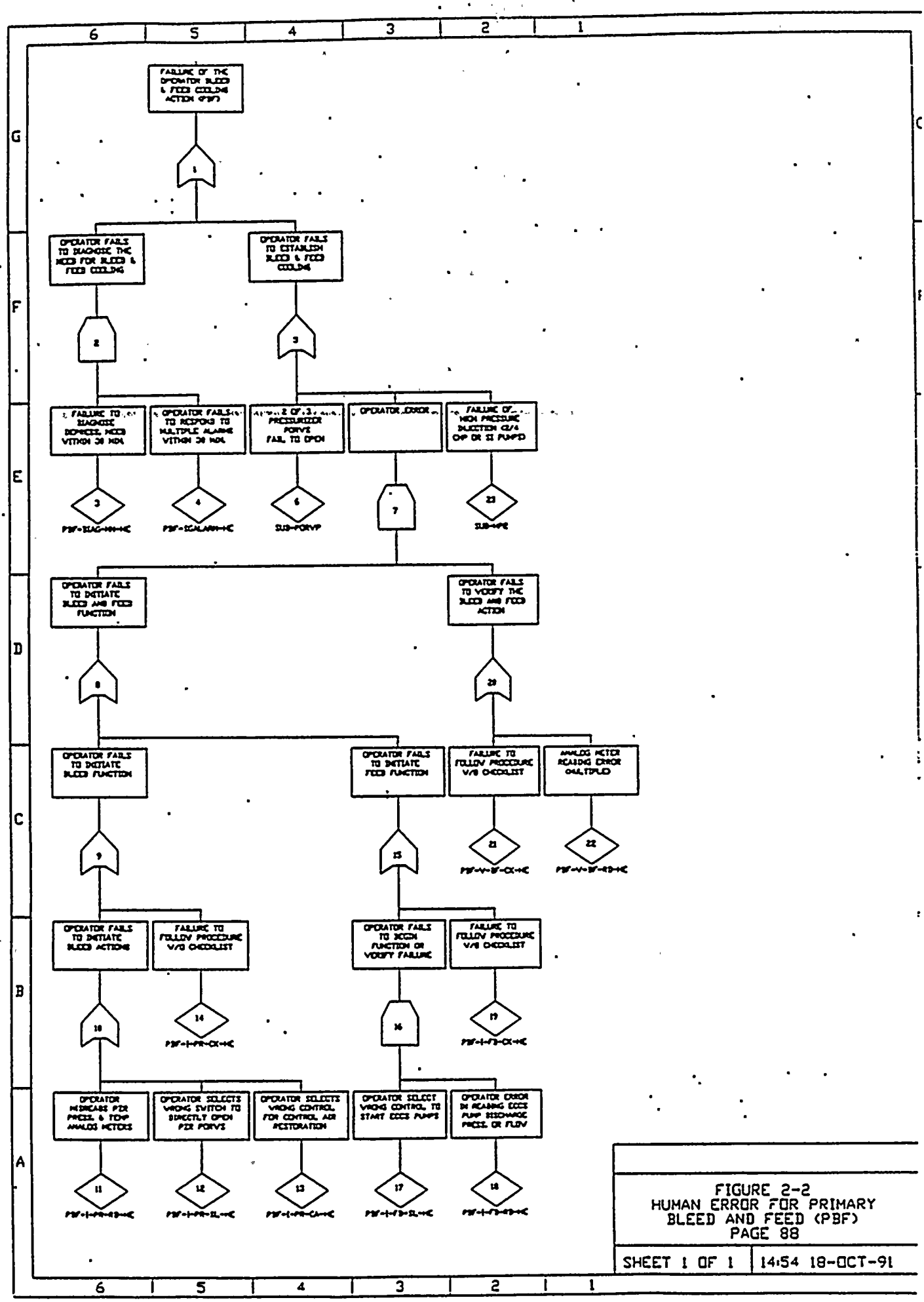


FIGURE 2-2
HUMAN ERROR FOR PRIMARY BLEED AND FEED (PBF)
PAGE 88

SHEET 1 OF 1 | 14:54 18-OCT-91

2.4 OA5 - STEAM GENERATOR DEPRESSURIZATION AND CONDENSATE FEED

Application

Transients with Steam Conversion Systems Available (TRA)

Description

If the main and auxiliary feedwater systems fail, it is possible to deliver feed flow to the steam generators using a condensate booster pump if the steam generators are depressurized. This event is modeled before the main feedwater top event, however, because of the main feedwater dependencies on the condensate system.

Success of this event is the operator depressurizing at least two of four steam generators and at least one of three condensate booster pumps operating (expected to remain operating unless a loss of power is experienced), which are each of greater capacity than any AFW pump, supplying feedwater to the depressurized steam generators (Reference 1; Appendix G). It will be assumed that this action must be initiated within 30 minutes of the accident initiation. If this top event fails, then core decay heat must be removed by primary bleed and feed cooling or the main feedwater system.

The operator actions modeled in the HRA Notebook are associated with the actuation of Steam Dump and are consistent with the emergency operating procedures. There are many means for the operator to achieve the necessary degree of heat removal (by releasing steam). The failure probability associated with the failure of ALL of these heat removal features considering both random mechanical and common cause failures is extremely low and greatly dominated by the associated human error probabilities. Therefore, the equipment failures associated with secondary-side heat removal for this mitigation feature need not be modeled.

Procedure(s)

Reference 4b.

Tasks

The following are the primary tasks which must be completed:

A1) Diagnose the need for secondary-side cooling

A2) Initiate steam dump

A3) Verify success of steam dump

A4) Initiate flow from Condensate Booster Pumps

A5) Verify success of condensate feed

Table 2-9 details the necessary subtasks for each of the above.

Analysis and Assumptions

Table 2-9 summarizes the derived HEPs.

For each of the Human Error Probability calculations, a stress factor of 5 is assumed to apply for the diagnostic phase of TRA and a stress factor of 2 is assumed to apply for the implementation phase of operator actions. This generally represents the change in stress that the operator undergoes during accident conditions. A stress factor of 2 is applied to the response to the S/G low-low level annunciators which is considered more straightforward. An assigned value of 0.01 was used for the operators being trained in entering the EOPs. After discussions with operators and witnessing activities on the Cook control room simulator, it is felt that the operators would enter the EOPs without hesitation. An assigned value of 0.1 was used throughout this notebook for being trained in following the procedural steps once in the EOPs. (The operator action OLI-I-SD-CK-HE was used in the Medium LOCA event tree also, and is multiplied by 2 to account for the lack of training in that event.) The following provides a detailed list of the subtasks (see Table 2-1) and the descriptive scaling guides used in developing the PSFs for each item:

Subtask	Factor		Assigned Value
A1a	Trained in entering EOPs		0.01
		PSF	0.01
A1b	Trained		0.1
		PSF	0.1
A2a	Trained		0.1
	MLO Factor		2.0
		PSF	0.2
A2b1	Trained		0.1
		PSF	0.1
A2b2	Trained		0.1
		PSF	0.1
A3a	Trained		0.1
		PSF	0.1
A3b	Medium time frame for response		0.1
	Multiple support instruments		0.1
		PSF	0.01

A4a	Trained		0.1
		PSF	0.1
A4b	Trained		0.1
		PSF	0.1
A4c	Trained		0.1
		PSF	0.1
A4d	Trained		0.1
		PBF	0.1
A5a	Trained		0.1
		PBF	0.1
A5b	Medium time frame for response		0.1
	Multiple support instruments		0.1
		PSF	0.01

It is conservatively assumed that accident diagnosis will only be performed by the operators for Task A1b through response to the low SG level alarm. Credit is not taken for diagnosis by the STA's from looking at critical safety parameters or by subsequent EOP steps by the operators, In addition, it is conservatively assumed that up to 7-10 annunciators may be alarming at this stage of the transient.

Based on Reference 9 photographs, the Steam Dump and steam pressure controllers have no mimic lines and no violation of populational stereotypes.

It is conservatively assumed that a failure to properly read any one of the multiple indicators which assist the operator in diagnosing the transient would lead to confusion and misdiagnosis.

It is recognized that the verification of Steam Dump success could be performed independently by individuals examining plant process parameters; however, credit is conservatively taken only for the procedural step requesting Steam Dump verification. Since one of the key functions of the Shift Technical Advisor is verification of the operator's activities, this may be very conservative.

To determine the conditional probability of human error in establishing RCS depressurization, a HEP fault tree was developed and is shown in Figure 2-3.

Table 2-10 describes the event identifiers, and Table 2-11 summarizes the input data for the fault tree.

Results

The conditional probability of the failure to establish Steam Generator depressurization and condensate feed and the combinations of failures (cutsets) are identified in Table 2-12.
OA5 is dominated by diagnostic failures related to the operator identifying the need for Steam Generator depressurization on responding to low SG level alarms.

TABLE 2-9
OA5 HEP CALCULATIONS

Descriptions (error type)	Mean HEP (Table A-2 Reference)	Performance Shaping Factors			HEP	Fault Tree Identifier	Additional Notes (Equipment, Actions, Indications, Locations)
		Stress	Dependence	Others			
Task A1 - DIAGNOSIS							
a) Failure to diagnose within 30 minutes of a compelling signal							
1) given success in reading any of the multiple low SG level and high RCS temperature and pressure indicators (saturation meter also available)	2.7E-03 (3)	5	High (Success)	0.01	6.75E-05	OA5-DIAG-MN-HE	q(a1)=HEP(a1)*PSF/2
2) given failure in reading any of the multiple low SG level and high RCS temperature and pressure indicators	a) Diagnosis: 2.7E-03 (3)	5	High (Failure)	0.01	5.0E-01		q(a2a)=[HEP(a2a)* PSF+1]/2
	b) Reading (1 of 2 types of analog meter): 2*3.75E-03 (51)	5	–	0.01	3.8E-04 Combined: 2.58E-04		q(a2b)=HEP(a2b)*PSF Q=q(a1)+q(a2a)* q(a2b)

TABLE 2-9
OA5 HEP CALCULATIONS

Descriptions (error type)	Mean HEP (Table A-2 Reference)	Performance Shaping Factors			HEP	Fault Tree Identifier	Additional Notes (Equipment, Actions, Indications, Locations)
		Stress	Dependence	Others			
b) Failure to respond to SG low-low level annunciator (under AND gate with A1a) (30 minutes into transient, it is assumed that 7-10 annunciators are alarming - conservative)	1.3E-01 (45)	2	--	0.1	2.6E-02	PBF-SGALARM-HE	
Task A2 - INITIATE STEAM DUMP							
a) Error of Omission - Failure to follow procedures without checklist	1.3E-02 (17)	2	--	0.2	5.2E-03	OLI-I-SD-CK-HE	
b) Operator selects wrong control or operates incorrectly when attempting to activate Steam Dump:							
1) Transfer Condenser steam dump to steam pressure mode - selecting wrong control (labels only) - Error of Commission	3.8E-03 (20)	2	--	0.1	7.6E-04	OA5-I-SD-SL-HE	

TABLE 2-9
OA5 HEP CALCULATIONS

Descriptions (error type)	Mean HEP (Table A-2 Reference)	Performance Shaping Factors			HEP	Fault Tree Identifier	Additional Notes (Equipment, Actions, Indications, Locations)
		Stress	Dependence	Others			
2) Error of Commission - Dump Steam to Condenser using steam pressure controller - turn control in wrong direction (when there is no violation of populational stereotypes)	1.3E-03 (23)	2	--	0.1	2.6E-04		

TABLE 2-9
OA5 HEP CALCULATIONS

Descriptions (error type)	Mean HEP (Table A-2 Reference)	Performance Shaping Factors			HEP	Fault Tree Identifier	Additional Notes (Equipment, Actions, Indications, Locations)
		Stress	Dependence	Others			
Task A3 - VERIFY SUCCESS OF STEAM DUMP							
a) Error of Omission - Fails to verify success when a long procedure is used w/o checkoff provision	1.3E-02 (17)	2	--	0.1	2.6E-03	OLI-V-SD-CK-HE	
b) Error in reading primary pressure and temperature trends in Strip Chart Recorder (conservatively taken as one failure)	7.5E-03 (52)	2	--	0.01	1.5E-04	OLI-V-SD-RD-HE	
Task A4 - INITIATE FLOW FROM CONDENSATE BOOSTER PUMPS							
a) Error of Omission - Failure to follow procedure w/o checklist	1.3E-02 (17)	2	--	0.1	2.6E-03	OA5-I-CP-CK-HE	

TABLE 2-9
OA5 HEP CALCULATIONS

Descriptions (error type)	Mean HEP (Table A-2 Reference)	Performance Shaping Factors			HEP	Fault Tree Identifier	Additional Notes (Equipment, Actions, Indications, Locations)
		Stress	Dependence	Others			
b) Error of Commission - Selects wrong control for FW isolation valves where controls are labeled and functionally grouped	1.3E-03 (22)	2	--	0.1	2.6E-04	OA5-I-CP-FW-HE	
c) Error of Commission - Selects wrong control where controls are labeled and functionally grouped	1.3E-03 (22)	2	--	0.1	2.6E-04	OA5-I-CP-SL-HE	
d) Error in reading pump discharge pressure gauges, injection flow gauges, or pump amperage meters	3.75E-03 (51)	2	--	0.1	7.5E-04	OA5-I-CP-RD-HE	
Task A5 - VERIFY SUCCESS OF CONDENSATE FEED							
a) Error of Omission - Fails to verify success when a long procedure is used w/o checkoff provision	1.3E-02 (17)	2	--	0.1	2.6E-03	OA5-V-CP-CK-HE	

TABLE 2-9
OA5 HEP CALCULATIONS

Descriptions (error type)	Mean HEP (Table A-2 Reference)	Performance Shaping Factors			HEP	Fault Tree Identifier	Additional Notes (Equipment, Actions, Indications, Locations)
		Stress	Dependence	Others			
b) Error in reading pressure and flow strip charts (conservatively taken as one failure)	3.75E-03 (51)	2	--	0.01	7.5E-05	OA5-V-CP-RD-HE	

TABLE 2-10

EVENT ID DESCRIPTIONS (OA5)

[redacted]ER Version 2.20 10/14/1991 16:27:53
OA5 FAULT TREE
LIST OF BASIC EVENTS AND THEIR DESCRIPTIONS

1	OA5-DIAG-MN-HE	FAILURE TO DIAGNOSE DEPRESS. NEED WITHIN 30 MIN.
2	OA5-I-CP-CK-HE	FAILURE TO FOLLOW PROCEDURE W/O CHECKLIST
3	OA5-I-CP-FW-HE	OPERATOR SELECTS WRONG CONTROL FOR FEEDWATER ISOLATION
4	OA5-I-CP-RD-HE	OPERATOR ERROR IN READING PUMP DISCHARGE PRESS. OR INJECT. FLOW
5	OA5-I-CP-SL-HE	OPERATOR SELECT WRONG CONTROL TO OPEN SG LEVEL CONTROL VALVES
6	OA5-I-SD-SL-HE	OPERATOR SELECTS WRONG CONTROL OR OPERATES INCORR. FOR STEAM DUMP
7	OA5-V-CP-CK-HE	FAILURE TO FOLLOW PROCEDURE W/O CHECKLIST
8	OA5-V-CP-RD-HE	ANALOG METER READING ERROR (MULTIPLE)
9	OLI-I-SD-CK-HE	FAILURE TO FOLLOW PROCEDURE W/O CHECKLIST
10	OLI-V-SD-CK-HE	FAILURE TO FOLLOW PROCEDURE W/O CHECKLIST
11	OLI-V-SD-RD-HE	ANALOG METER READING ERROR (MULTIPLE)
12	PBF-SGALARM-HE	OPERATOR FAILS TO RESPOND TO MULTIPLE ALARMS WITHIN 30 MIN.
13	SUB-13COND	FLOW FROM 1 OF 3 CONDENSATE BOOSTER PUMPS UNAVAILABLE

TABLE 2-11

FAULT TREE HEP INPUT DATA (OA5)

SEE TABLE 2-3 FOR REQUIRED INFORMATION

TABLE 2-12

HEP AND DOMINANT CUTSETS FOR OA5 FAULT TREE

1 TREE NAME: \COOES\HRA\OA5
CUTOES VER.1.7, 11-17-89
INPUT FILE: \COOES\HRA\OA5.COS

CUT SETS FOR GATE G0001 WITH CUTOFF PROBABILITY OF 1.00E-12
GATE G0001 IS: OPERATOR FAILS TO PROVIDE SECONDARY-SIDE COOLING (OA5)

NUMBER	CUTSET PROB.	BASIC EVENT NAME	EVENT PROB.	IDENTIFIER
1.	2.70E-05	FAILURE TO FOLLOW PROCEDURE W/O CHECKLIST	5.20E-03	OLI-I-SD-CK-HE
		FAILURE TO FOLLOW PROCEDURE W/O CHECKLIST	5.20E-03	OLI-V-SD-CK-HE
2.	1.35E-05	FAILURE TO FOLLOW PROCEDURE W/O CHECKLIST	2.60E-03	OA5-V-CP-CK-HE
		FAILURE TO FOLLOW PROCEDURE W/O CHECKLIST	5.20E-03	OA5-I-CP-CK-HE
3.	6.71E-06	FAILURE TO DIAGNOSE DEPRESS. NEED WITHIN 30 MIN.	2.58E-04	OA5-DIAG-MN-HE
		OPERATOR FAILS TO RESPOND TO MULTIPLE ALARMS WITHIN 30 MIN.	2.60E-02	PBF-SGALARM-HE
4.	5.30E-06	OPERATOR SELECTS WRONG CONTROL OR OPERATES INCORR. FOR STEAM DUMP	1.02E-03	OA5-I-SD-SL-HE
		FAILURE TO FOLLOW PROCEDURE W/O CHECKLIST	5.20E-03	OLI-V-SD-CK-HE
5.	7.80E-07	FAILURE TO FOLLOW PROCEDURE W/O CHECKLIST	5.20E-03	OLI-I-SD-CK-HE
		ANALOG METER READING ERROR (MULTIPLE)	1.50E-04	OLI-V-SD-RD-HE
6.	3.90E-07	ANALOG METER READING ERROR (MULTIPLE)	7.50E-05	OA5-V-CP-RD-HE
		FAILURE TO FOLLOW PROCEDURE W/O CHECKLIST	5.20E-03	OA5-I-CP-CK-HE
7.	1.53E-07	OPERATOR SELECTS WRONG CONTROL OR OPERATES INCORR. FOR STEAM DUMP	1.02E-03	OA5-I-SD-SL-HE
		ANALOG METER READING ERROR (MULTIPLE)	1.50E-04	OLI-V-SD-RD-HE
8.	5.07E-10	FAILURE TO FOLLOW PROCEDURE W/O CHECKLIST	2.60E-03	OA5-V-CP-CK-HE
		OPERATOR SELECTS WRONG CONTROL FOR FEEDWATER ISOLATION	2.60E-04	OA5-I-CP-FW-HE
		OPERATOR ERROR IN READING PUMP DISCHARGE PRESS. OR INJECT. FLOW	7.50E-04	OA5-I-CP-RD-HE
9.	5.07E-10	FAILURE TO FOLLOW PROCEDURE W/O CHECKLIST	2.60E-03	OA5-V-CP-CK-HE
		OPERATOR SELECT WRONG CONTROL TO OPEN SG LEVEL CONTROL VALVES	2.60E-04	OA5-I-CP-SL-HE
		OPERATOR ERROR IN READING PUMP DISCHARGE PRESS. OR INJECT. FLOW	7.50E-04	OA5-I-CP-RD-HE
10.	1.46E-11	ANALOG METER READING ERROR (MULTIPLE)	7.50E-05	OA5-V-CP-RD-HE
		OPERATOR SELECTS WRONG CONTROL FOR FEEDWATER ISOLATION	2.60E-04	OA5-I-CP-FW-HE
		OPERATOR ERROR IN READING PUMP DISCHARGE PRESS. OR INJECT. FLOW	7.50E-04	OA5-I-CP-RD-HE
11.	1.46E-11	ANALOG METER READING ERROR (MULTIPLE)	7.50E-05	OA5-V-CP-RD-HE
		OPERATOR SELECT WRONG CONTROL TO OPEN SG LEVEL CONTROL VALVES	2.60E-04	OA5-I-CP-SL-HE
		OPERATOR ERROR IN READING PUMP DISCHARGE PRESS. OR INJECT. FLOW	7.50E-04	OA5-I-CP-RD-HE

REDUCED SUM OF PROBABILITY OF FAILURE = 5.383E-05

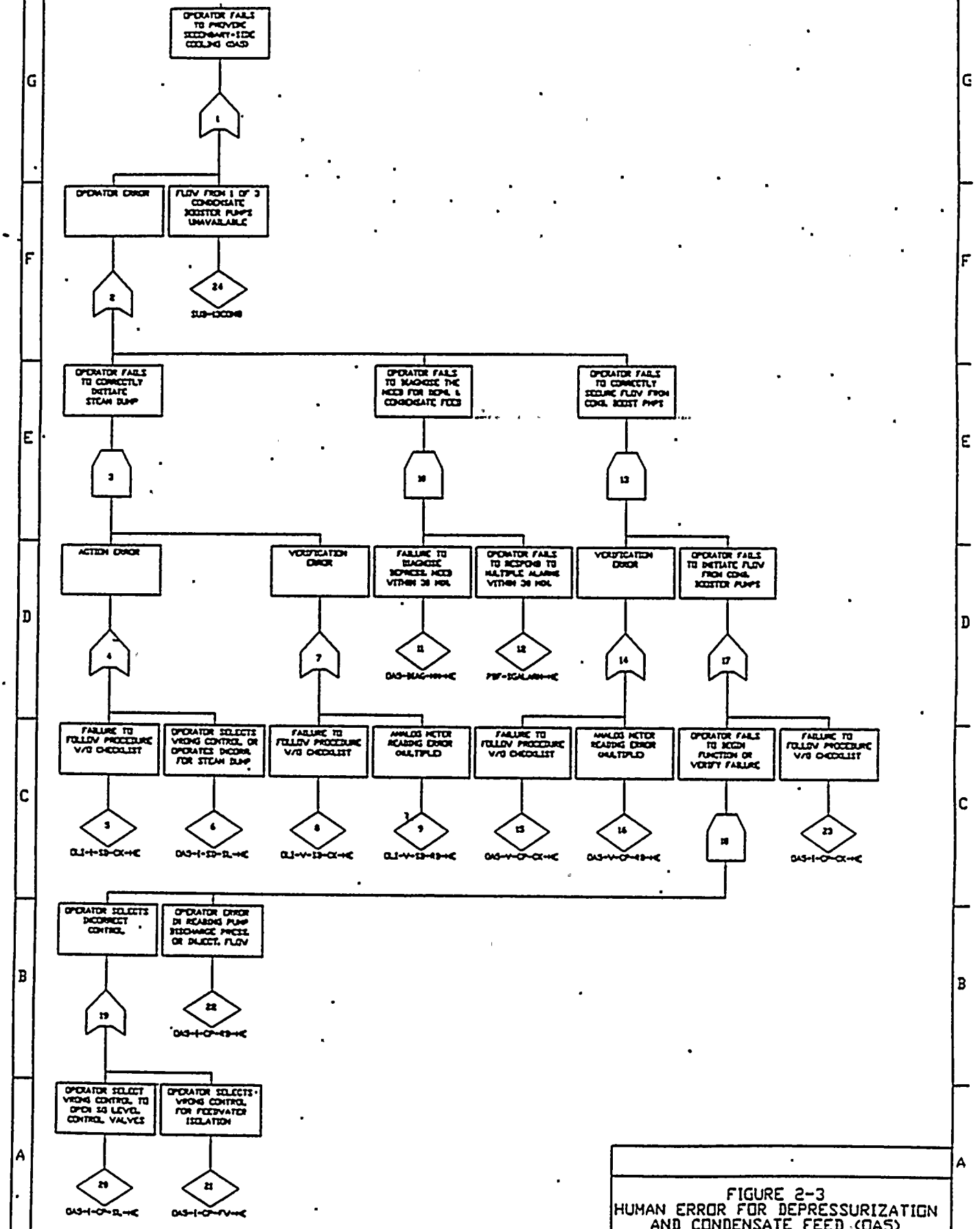


FIGURE 2-3
HUMAN ERROR FOR DEPRESSURIZATION AND CONDENSATE FEED (OAS)
PAGE 101

SHEET 1 OF 1 | 14:54 18-OCT-91