Northern States Power Company
Prairie Island Nuclear Generating Plant
1717 Wakonade Dr. East
Welch, Minnesota 55089

February 27, 1996

Generic Letter 88-20

U S Nuclear Regulatory Commission
Attn: Document Control Desk
Washington, DC 20555

PRAIRIE ISLAND NUCLEAR GENERATING PLANT
Docket Nos. 50-282 License Nos. DPR-42
50-306 DPR-60

Response to Request for Additional Information Related to the
Prairie Island Individual Plant Examination Report (TAC Nos. M74454 and M74455)

We submitted for NRC staff review the Prairie Island Individual Plant Examination Report (IPE) in response to Generic Letter 88-20. On December 21, 1996 the NRC issued a Request for Additional Information regarding our original submittal. Attachment 2 to this letter provides the information requested.

In this letter we have made no new Nuclear Regulatory Commission commitments. Please contact Jack Leveille (612-388-1121, Ext. 4662) if you have any questions related to this letter.

Michael D Wadley
Plant Manager
Prairie Island Nuclear Generating Plant

c: Regional Administrator - Region III, NRC
Senior Resident Inspector, NRC
NRR Project Manager, NRC
J E Silberg

Attachments:
1) Affidavit
2) Response to Request for Additional Information Related to the Prairie Island Individual Plant Examination Report

A011
1/1

UNITED STATES NUCLEAR REGULATORY COMMISSION

NORTHERN STATES POWER COMPANY

PRAIRIE ISLAND NUCLEAR GENERATING PLANT DOCKET NO. 50-282
50-306

GENERIC LETTER 88-20, INDIVIDUAL PLANT EXAMINATION
FOR SEVERE ACCIDENT VULNERABILITIES - 10 CFR 50.54(f)

Northern States Power Company, a Minnesota corporation, with this letter is submitting information requested by NRC Generic Letter 88-20.

This letter contains no restricted or other defense information.

NORTHERN STATES POWER COMPANY

BY Michael D Wadley
Michael D Wadley
Plant Manager
Prairie Island Nuclear Generating Plant

On this 27th day of February 1996 before me a notary public in and for said County, personally appeared Michael D Wadley, Plant Manager, Prairie Island Nuclear Generating Plant; and being first duly sworn acknowledged that he is authorized to execute this document on behalf of Northern States Power Company, that he knows the contents thereof, and that to the best of his knowledge, information, and belief the statements made in it are true and that it is not interposed for delay.

Marcia K. LaCore

MARCIA K. LaCORE
NOTARY PUBLIC-MINNESOTA
HENNEPIN COUNTY
My Commission Expires Jan. 31, 2000

ATTACHMENT 2

Response to Request for Additional Information Related to the
Prairie Island Individual Plant Examination Report

Level 1 Question 1: Treatment of Cross-Tied and Shared Systems

It is not clear from the transmittal how the cross-tied and shared systems are treated for the unit at power if the other unit is in cold shutdown and some of the shared (or potentially cross-tied) systems are experiencing extended downtime. How does the analysis account for the unavailability of the systems that are capable of being cross-tied or shared during the time the opposite unit is in shutdown? Please discuss how each shared/cross-tied system was treated in this regard. If this was not considered, please estimate the impact on your results.

A review of the modeling of maintenance unavailabilities identified several cases in which maintenance on opposite unit equipment was not correctly accounted for in the IPE. These are described below, and estimates of the correct unavailabilities are identified for each set of equipment that was incorrectly modeled. The total estimate of the impact on core damage frequency given all the changes is also given.

At Prairie Island there are several systems that are either shared by both units or that have the potential to be cross-tied from one unit to the other. These systems fall into two basic categories, each of which is operated differently by the plant and is modeled differently in the IPE.

The first category is systems that are shared by both units. Shared systems means that one set of equipment provides a given function for both units. For example, one chilled water pump with a second in standby provides safeguards chilled water for both units. The systems in this category are Cooling Water, Instrument Air, and Control Room Chilled Water. These are systems that are required to be fully operational when either unit is at power. The IPE is an at-power model, so these systems are modeled as being in operation. Maintenance on shared systems is normally done while both units are at power. This was included in the maintenance unavailability values calculated for the IPE. The status of either unit has no effect on the maintenance unavailability values used to model these systems. The only exception to this is that each outage the Circulating Water Intake Bay is drained for cleaning and other maintenance. This has the effect of making either 11 or 21 Cooling Water pump unavailable since these pumps draw their suction from the bay. This was not modeled in the IPE. The bay is drained each refueling outage for about 5 days. This maintenance is coordinated with work done on the non-safeguards 4KV bus that supplies electrical power to the affected cooling water pump which is performed every other outage. Therefore, the unavailability of the cooling water pumps caused by the circulating water bay draining only needs to be counted for every other outage since the maintenance on the 4KV bus will cover the other outage. Thus, there should have been 5 days of unavailability over 36 months (2 cycles) included on 21 Cooling Water pump. 11 Cooling Water pump is modeled as running without preventive maintenance since the IPE used a Unit 1 model. This amount of unavailability results in a maintenance frequency of 4.57E-03.

The second category of systems are those systems that can be cross-tied from one unit to the other. These are systems where each unit has a complete and independent set of equipment that performs the system's functions. However, these systems also have the ability to cross-tie trains across the units. For example, Train A of Unit 1 AC power and Diesel Generators has the ability to supply Train A of Unit 2. The systems which were modeled in the IPE that have this cross-tie capability are Component Cooling, 4160 Volt AC Power (including the Emergency Diesel Generators), and Auxiliary Feedwater. In addition, during outages, 480 V AC power for MCCs 1AB1, 1AB2, 1T1 and 1T2, DC Power to Panels 17 and 18 are transferred to the power supply on the opposite unit if they are not already on that power supply.

The Component Cooling Systems at Prairie Island can be manually cross-tied in many different ways. Any pump is capable of supplying flow to either train of either unit. To reduce the modeling effort required in the IPE a conservative model was used. The IPE model does not take credit for the capability of cross-tying across units. It only models the component cooling equipment of only one unit. Because of this conservative modeling a cold shutdown on one unit will have no effect on the Component Cooling System of the operating unit, since the shutdown unit's pumps are not modeled and no credit is taken for their backup function.

Safeguards AC Power and the Emergency Diesel Generators are both part of the same system. The safeguards electrical power system, which includes the diesel generators, can be cross-tied across units. If voltage to one of the 4160V buses is lost from its normal off-site power source an automatic voltage restoration sequence is started. This sequence will look for voltage on the normal supply, the second off-site supply and the associated diesel generator (which receives a start signal when no voltage is sensed on the second off-site power supply) in that order. When adequate voltage is found on one of these sources the bus supply breaker for that source is closed and the restoration sequence stops. If voltage is not found on any source the operators are instructed to manually restore power to the bus via cross-tying the bus to the same train bus on the other unit.

The IPE model included both the automatic and manual voltage restoration schemes. Therefore, the ability to cross-tie the system is modeled. Since the model is of an operating unit (Unit 1), safeguards 4160 V buses 15 and 16 are continuously energized and are not taken out of service for preventive maintenance. Therefore, Bus 15 and Bus 16 have only corrective maintenance performed at power modeled. The diesel generators associated with those buses, D1 and D2, do receive preventive maintenance at power and are modeled as such in the IPE. The models for Unit 2 4160 V buses 25 and 26, which can be cross-tied to Unit 1 buses if necessary, should have included both preventive and corrective maintenance. However, examination of the models shows that only on-line maintenance has been included. Data is available for maintenance during outages equal to 9 days unavailability performed every 3 years (9 days/1095 days or 8.22E-03).

The non-safeguards 4KV buses which power the non-safeguards cooling water pumps and the condensate pumps are also made unavailable for maintenance for maintenance during refueling outages. Each bus (23 and 24 for Unit 2) is unavailable for about 5 days every second outage. This was not modeled in the IPE model. The Unit 2 buses should have 5 days of maintenance every 36 months (2 cycles). This equates to a maintenance frequency of 4.57E-03.

Also, the power supplies for MCCs 1AB1 and 1AB2, which supply Cooling Water system motor operated header isolation valves, diesel cooling water pump auxiliaries, traveling screen and strainer control panels, and screenhouse ventilation, can be cross tied between Unit 1 and Unit 2. The MCCs are normally supplied from their Unit 1 power supply. When Unit 1 goes into a refueling outage these MCCs are transferred to their Unit 2 supply. The Unit 2 supply would also be used in the event of a failure of the Unit 1 supply. The operation of the power supplies for MCCs 1T1 and 1T2 are similar, as are the DC transfer switches to the diesel cooling water pumps. MCCs 1T1 and 1T2 supply the control room (safeguards) chilled water and air handling systems, and normally-open steam supply motor-operated valves for the turbine-driven auxiliary feedwater pumps. The power supply cross-tie capability for these MCCs and for the DC transfer switches was not modeled or credited in the IPE. However, the unavailability of the opposite unit power supply during outage maintenance (which would affect opposite unit shared equipment) is not significant to plant risk since the equipment is maintained available through transfer to the non-outage unit power supply. Failures of the transfer operation would be immediately known by the operations staff due to control room alarms and equipment failures.

Despite the above, an attempt was made to estimate the effects of modeling the MCC power supply cross-ties and the potential for that opposite unit's supply to be in maintenance during an outage on that unit. Five days unavailability over 3 years (2 cycles) was included for maintenance on their Unit 2 power supplies. This equals a maintenance frequency of 5.47E-03. DC transfer switch modeling was not included since complete unavailability of a train of DC power due to maintenance even during outages is not a normal or routine operation.

The motor driven auxiliary feedwater pumps can be cross-tied from one unit to the other. The pump on one unit is available for use on the other unit at any time except when it is in use on its own unit, in maintenance or when its power supply is unavailable. This cross-tie capability was modeled in the IPE.

The Auxiliary Feedwater fault tree model includes logic that makes 21 AFW Pump (the Unit 2 motor driven pump which can be cross-tied to Unit 1) unavailable for use on Unit 1 when there is a dual unit initiating event. This is done since the pump would be needed by Unit 2 during such an event. The model also included corrective and preventive maintenance which would make the pump unavailable. The value used for preventive maintenance unavailability only accounted for the monthly surveillance testing done on the pump, it did not include time the pump is unavailable due to an outage on its respective unit.

Preventive maintenance on the motor driven Auxiliary Feedwater Pump is normally done at the same time as preventive maintenance on the 4160V power supply to the pump. This unavailability is already accounted for by the preventive maintenance unavailability of the bus. However, since the bus is only worked on every other outage, some additional preventive maintenance will be done that would make the pump unavailable outside of the bus outage periods. Also, the opposite unit pump would be required during unit startup and cooldowns, whenever the steam pressure was insufficient for turbine-driven pump operation. It was conservatively assumed that the motor-driven pump would be unavailable to the unit experiencing a loss of heat sink during this time. The combination of maintenance unavailability and unavailability due to cooldowns and startups is approximately 14 days over 2 cycles (3 years), or 1.23E-02.

The combined impact of these omissions was estimated by incorporating them into the IPE model and quantifying the change in core damage frequency. Incorporating the changes is estimated to raise the core damage frequency by approximately 6% (to approximately 5.3E-5). Nearly all of this increase is due to the additional unavailability of Bus 25, which supplies power to the 21 AFW pump.

These preventive maintenance changes also have a slight impact on a few of the restoration errors modeled in the IPE (see Tables 2 and 3, and the response to HRA Question 1b).

Level 1 Question 2: Support System to Support System Dependency Matrix

No support system-on-support system matrix is given in the submittal. How did the analysis assure that no dependencies were missed? Please provide such a matrix.

The support system-on-support system matrix was inadvertently left out of the IPE report and is provided as a response to this question (see Table 1). The analysis used fault tree linking in which support systems were explicitly modeled using fault trees. The resulting support system fault trees were linked to each front-line or support system fault tree that they support. The resulting linked fault tree captured all of the dependencies between front-line and support systems. Plant procedures along with applicable system logic and P & ID drawings were also used to assure that all dependencies were captured.

The systems given in the columns in Table 1 support the systems shown in the rows on the table. An "X" indicates that the system or train in the column provides support to any component in the system or train in the row. For example, a power supply may only support a fuel oil transfer pump for a diesel generator. Failure or unavailability of the power supply would not necessarily mean that the system or train is unavailable, only that a component within that system or train is unavailable. A "B" indicates that the system or train provides a backup function in case the primary function (i.e., power supply) is unavailable. Support for signals that are used to

start pumps, open or close valves, etc. were considered in the fault trees but are not shown on the table in order to keep the table simple and understandable.

Table 1
SUPPORT SYSTEM TO SUPPORT SYSTEM DEPENDENCY MATRIX

	U1 Train A CC	U1 Train B CC	Cooling Water[3]	U1 Train A DC	U1 Train B DC	U2 Train A DC	U2 Train B DC
U1 Train A CC			X	X			
U1 Train B CC			X		X		
Cooling Water[3]				X	X	X	
U1 Train A DC							
U1 Train B DC							
U2 Train A DC							
U2 Train B DC							
U1 Train A 120V AC				B			
U1 Train B 120V AC					B		
U2 Train A 120V AC						B	
U2 Train B 120V AC							B
Instrument Air			X				
U1 Train A 4160V AC[2]			X	X		B	
U1 Train B 4160V AC[2]			X		X		B
U2 Train A 4160V AC[2]				B		X	
U2 Train B 4160V AC[2]					B		X
U1 Train A 480V AC				X			
U1 Train B 480V AC					X		
U2 Train A 480V AC						X	
U2 Train B 480V AC							X
U1 Train A 230V AC							
U1 Train B 230V AC							
U1 Train A Chilled Water (SG)			X	X			
U1 Train B Chilled Water (SG)			X		X		
HVAC			X				

LEGEND: X = System/train in column provides primary support for component(s) in system/train in row
B = System/train in column provides backup support for component(s) in system/train in row

Table 1, continued
SUPPORT SYSTEM TO SUPPORT SYSTEM DEPENDENCY MATRIX

	U1 Train A 120V AC	U1 Train B 120V AC	U2 Train A 120V AC	U2 Train B 120V AC	Instrument Air	U1 Train A 4160V AC[2]	U1 Train B 4160V AC[2]
U1 Train A CC						X	
U1 Train B CC							X
Cooling Water[3]							
U1 Train A DC							
U1 Train B DC							
U2 Train A DC							
U2 Train B DC							
U1 Train A 120V AC							
U1 Train B 120V AC							
U2 Train A 120V AC							
U2 Train B 120V AC							
Instrument Air							
U1 Train A 4160V AC[2]	X		B				
U1 Train B 4160V AC[2]		X		B			
U2 Train A 4160V AC[2]						B	
U2 Train B 4160V AC[2]							B
U1 Train A 480V AC						X	
U1 Train B 480V AC							X
U2 Train A 480V AC							
U2 Train B 480V AC							
U1 Train A 230V AC							
U1 Train B 230V AC							
U1 Train A Chilled Water (SG)					X		
U1 Train B Chilled Water (SG)					X		
HVAC							

LEGEND: X = System/train in column provides primary support for component(s) in system/train in row
B = System/train in column provides backup support for component(s) in system/train in row

Table 1, continued
SUPPORT SYSTEM TO SUPPORT SYSTEM DEPENDENCY MATRIX

	U2 Train A 4160V AC[2]	U2 Train B 4160V AC[2]	U1 Train A 480V AC	U1 Train B 480V AC	U2 Train A 480V AC	U2 Train B 480V AC
U1 Train A CC			X			
U1 Train B CC				X		
Cooling Water[3]	B[1]	X[1]	X	X	B	B
U1 Train A DC			X			
U1 Train B DC				X		
U2 Train A DC					X	
U2 Train B DC						X
U1 Train A 120V AC			X			
U1 Train B 120V AC				X		
U2 Train A 120V AC					X	
U2 Train B 120V AC						X
Instrument Air			X	X	X	
U1 Train A 4160V AC[2]	B		X			
U1 Train B 4160V AC[2]		B		X		
U2 Train A 4160V AC[2]					X	
U2 Train B 4160V AC[2]						X
U1 Train A 480V AC						
U1 Train B 480V AC						
U2 Train A 480V AC						
U2 Train B 480V AC						
U1 Train A 230V AC			X			
U1 Train B 230V AC				X		
U1 Train A Chilled Water (SG)					X	
U1 Train B Chilled Water (SG)					X	
HVAC			X	X	X	X

LEGEND: X = System/train in column provides primary support for component(s) in system/train in row
B = System/train in column provides backup support for component(s) in system/train in row

Table 1, continued
SUPPORT SYSTEM TO SUPPORT SYSTEM DEPENDENCY MATRIX

	U1 Train A 230V AC	U1 Train B 230V AC	U1 Train A Chilled Water (SG)	U1 Train B Chilled Water (SG)	HVAC
U1 Train A CC					
U1 Train B CC					
Cooling Water[3]	X	X			X
U1 Train A DC					
U1 Train B DC					
U2 Train A DC					
U2 Train B DC					
U1 Train A 120V AC					
U1 Train B 120V AC					
U2 Train A 120V AC					
U2 Train B 120V AC					
Instrument Air					
U1 Train A 4160V AC[2]	X		X		X
U1 Train B 4160V AC[2]		X		X	X
U2 Train A 4160V AC[2]					X
U2 Train B 4160V AC[2]					X
U1 Train A 480V AC	X		X		X
U1 Train B 480V AC		X		X	X
U2 Train A 480V AC					X
U2 Train B 480V AC					X
U1 Train A 230V AC					
U1 Train B 230V AC					
U1 Train A Chilled Water (SG)					
U1 Train B Chilled Water (SG)					
HVAC	X	X	X	X	

LEGEND: X = System/train in column provides primary support for component(s) in system/train in row
B = System/train in column provides backup support for component(s) in system/train in row

Table 1, continued
SUPPORT SYSTEM TO SUPPORT SYSTEM DEPENDENCY MATRIX

FOOTNOTES:

1) The 121 vertical motor-driven cooling water pump can be supplied from either Unit 2 Train A AC power or Unit 2 Train B AC power. It was assumed to be on Unit 2 Train B initially during any event.
2) Diesel generator fuel oil transfer pumps are assumed to be part of the 4160 V AC power system
3) Diesel CL pump fuel oil transfer pumps are assumed to be part of the Cooling Water system

Level 1 Question 3: Common Cause Failure Analysis

The following question pertains to analysis of common cause failures (CCF) in the IPE:

a) **A review of the CCF data used in the IPE, and presented in Table 3.3-7 of the submittal, indicates that the list of components may not be comprehensive. Provide the basis for the omission of the following types of components from the common cause analysis:**

Circuit breakers (particularly for voltage ≥ 480V AC)
Electrical switchgear
Relays (ESFAS)

Circuit Breakers and Electrical Switchgear

Common cause failures of circuit breakers and switchgear were not explicitly modeled, but common cause failures of loads supplied through the breakers, such as pumps, valves and other components that can be attributable to common cause mechanisms, were modeled. This implicitly captures circuit breaker common cause failures that are associated with these components. As with circuit breakers, common switchgear (in terms of function and the effects of failures) are implicitly analyzed with other failures, such as emergency diesel generator common cause failures.

Relays

Common cause failures of relays were not explicitly modeled but are covered under common cause of instrumentation and control trains. For each I&C train or loop, a transmitter or sensor was modeled to represent the entire train with respect to common cause failure. This covers all components within the instrumentation train (including relays).

b) **How was the common cause loss of AC buses or the common cause loss of DC buses as an initiating event treated?**

Loss of either train of DC power will cause a reactor trip and is modeled as an initiating event in the IPE (I-LODCA and I-LODCB). The failure of the second train of DC due to random failures during the 24 hours following the initiating event is explicitly modeled in the event tree analysis for Loss of a DC bus. In order to have a loss of both DC buses as an initiating event, both buses must fail simultaneously. This can only occur as a result of a single failure which affects both trains, or as a common cause failure of multiple components.

Prairie Island has two completely independent trains of DC power. Evaluation of the DC power distribution system showed that there are no single component failures that will result in a loss of both trains of power. Failure of a train of DC power can occur due to failure of the distribution buses or failure of the batteries. It was assumed that the battery chargers could not maintain voltage without the battery as a buffer to absorb load changes. The DC distribution buses did not have

common cause failure modes considered, but the batteries did include common cause failures. This failure mode did effectively, but not explicitly, model common cause failures of DC buses.

Random independent failure rates for batteries and chargers can be found in several published data sources. These rates are based on historical experience and are suitable for use in the IPE. There are no published data sources with defensible failure rates for common cause failure of distribution buses and chargers. We did not consider it worthwhile to approach this problem with generic failure rates and common cause factors.

The two trains of DC power are not susceptible to common-mode failures. Each train of components; battery, charger, and distribution bus, are located in a separate room with concrete walls and a fire door separating it from the other train. Maintenance also is not done on both trains at the same time. Maintenance on one train is completed, including post-maintenance testing, and that train is restored to service prior to commencing maintenance on the second train.

Due to the low frequency of this initiator, common cause failure of DC buses was not modeled as an initiating event in the Prairie Island IPE.

Loss of AC buses was treated differently. Loss of a single safeguards 4160V AC bus will not cause a trip and thus was not modeled as an initiating event. Loss of both safeguards 4160V AC buses also will not cause a trip. It would require that the plant be shutdown per tech. specs. due to the loss of emergency core cooling system components, but this would be a controlled manual shutdown.

There are no common mode failure mechanisms for the safeguards 4160V buses. Each bus is in a separate room with concrete walls and a fire door. Each room has an independent room cooling system. Maintenance on the buses is done on only one bus each outage. This means that maintenance is done every 18 months on one bus with each bus receiving maintenance every 3 years. The buses also have independent off-site power supplies and independent diesel generators. These factors combined make the common cause failure frequency for the 4160V safeguards buses low. The only remaining common mode failure for these buses is a loss of off-site power combined with a failure of the on-site emergency diesel generators. This failure mode is already modeled in the IPE as a Station Blackout (SBO).

Because of the low frequency of common cause failures of these buses, combined with the fact that their failure does not cause a plant trip, only a forced manual shutdown, this failure mode was not modeled as an initiating event.

Loss of individual non-safeguards 4160V buses can cause a plant transient to occur. These events are included in the transient initiating event frequency. Loss of entire non-safeguards systems, such as feedwater and instrument air, are modeled as separate initiating events.

The most likely common cause failure of non-safeguards buses is a loss of off-site power. This initiating event is already modeled in the IPE as I-LOOP.

Level 1 Question 4: Loss of 120 V AC Bus Initiating Event

The IPE does not consider the "loss of 120 VAC bus" as a potential initiating event (e.g. loss of panel 113 causes the direct loss of the chemical and volume control system component for the reactor coolant pump (RCP) cooling). Please provide the basis for omitting this initiating event.

The loss of a 120V AC bus was not considered as an initiating event because it did not meet our criteria of causing an automatic or imminent reactor trip. Manual shutdowns for refueling or administrative reasons were not evaluated for this study. With these criteria in mind, the first sentence under section 3.1.1.1 on page 3.1-1 of the IPE submittal describing our criteria for initiating events is unfortunately incorrect due to typographical error. Loss of 120V AC buses was not considered an initiating event as loss of a single 120V AC bus will not cause an automatic or imminent reactor trip. Loss of a 120V bus is also permitted by Technical Specifications to occur for a period of 6 hours before actions need to be taken to shutdown the affected unit.

Loss of two or more 120V AC buses will cause a reactor trip due to the protection bistables that they supply failing in the trip mode on loss of power. Loss of two or more instrument buses is not usually included in IPE studies because of the low potential for such an event. Loss of two or more busses must necessarily be caused by common cause failure. This type of failure has not occurred over the operating history of the plant and there are no published data sources with dependable failure rates for such an initiator.

It is true that loss of panel 113 does cause loss of RCP seal cooling from the charging system, but loss of this panel does not affect the operability of the Component Cooling (CC) water system which also provides RCP seal cooling thereby preventing a reactor trip.

Level 1 Question 5: Chilled Water System Initiating Event

The chilled water system is used for cooling the relay room which is common to both Unit 1 and 2. This would appear to be an important system which should be mentioned, the failure of which should be in the initiating event analysis. Please provide the basis for screening or not considering this initiating event. If it was not considered, please estimate the impact on the results.

Failure of the safeguards control room chilled water system (ZH) was not included in the IPE special initiating events analysis. "Special" initiating events, as defined for the IPE, generally include failures of support system or other equipment during normal plant operation which directly results in a reactor trip or shutdown with a concurrent loss of safeguards systems or functions.

Room ventilation concerns modeled in the IPE were based on the results of design basis room heatup analyses performed for various safeguards areas of the plant. These room heatup analyses were performed under the following conservative assumptions: 1) they assumed a concurrent steamline break had occurred in the adjoining rooms, a significant heat source; 2) they assumed that all available equipment in the room was running at full capacity, thus maximizing the room temperature and heat load; 3) the ventilation in the adjoining rooms was not functioning; and 4) the outside air temperature was assumed to be 96 °F.

The conservative room heatup analyses available at the time the IPE study was developed indicated that room ventilation in the Control Room and the safeguards 480 V bus rooms was critical to the operation of equipment contained in those rooms. Without ventilation, temperatures in those rooms were calculated to reach excessive levels within a short time (on the order of an hour or less). The assumed effect of excessive temperatures in the Control Room is habitability and excessive instrument error, while the effect of excessive temperatures in the 480 V bus rooms is failure of the buses. Also, although analysis was available to show that unavailability of one train of ventilation in the Relay and Computer Rooms and in the RHR pits (during recirculation) was acceptable, no analyses were available to show that loss of both trains of ventilation in those rooms was acceptable. The assumed effect of excessive temperatures in the Relay Room was introduction of excessive instrument error, and the assumed effect in the RHR pits was a gradual decrease in the qualified life of the RHR pumps (not instantaneous failure of the pumps) during sump recirculation. No critical safety functions modeled in the IPE are affected due to excessive temperatures in the Computer Room. Note that the RHR pit analysis did show that no ventilation is required as long as only one train of RHR is on recirculation. However, no guidance was available in the plant emergency procedures to prevent transfer of the second RHR train to recirculation should its ventilation be inoperable. Analyses available at the time also showed that safeguards equipment in the other rooms supported by the ZH system (i.e., 4160 V bus rooms) was found to be operable without credit taken for the availability of ventilation.

However, at the time that the IPE was developed, no Technical Specification or clear plant procedural requirements existed for the ZH system which would have required immediate plant shutdown for its inoperability. It is likely that the plant staff would shut the plant down based on inoperability of both trains of the various safeguards equipment supported by the ZH system unit coolers. However, by the time this occurred, room cooling in those rooms (other than the RHR pits) would likely have been restored due to operator response to the event required by procedures (C37.9 AOP1, C37.9 AOP2 and C37.11 AOP1). These procedures addressed restoration of room temperatures in the Control Room, the Relay Room and the 480 V bus rooms through electrical equipment load shedding and establishing air flow through the rooms by opening doors and installing fans. Also, a direct plant trip mechanism due to loss of the ZH system could not be determined which would occur before the operators had time to respond to the event. With respect to RHR availability, the conservative heatup analysis scenario that postulates excessive temperatures in the RHR pits assumes that the system is in post-DBA recirculation operation with hot sump water being pumped through the room. Since we are considering best-estimate

operability of the RHR system under a loss of safeguards chilled water initiator, these conditions will not exist in the RHR pits. Complete loss of the ZH system concurrent with a DBA LOCA is not probabilistically a credible event. Therefore, under this forced plant shutdown scenario, unavailability of the RHR function would not occur.

Based on the above, it was determined that no direct plant shutdown or trip coupled with the unavailability of safeguards equipment could be postulated for a loss of the ZH system initiating event without assuming additional equipment or operator action failures.

Very clear guidance now exists for plant shutdown should the entire ZH system be inoperable. The ZH system is now considered part of the control room air treatment system, and is therefore controlled by Technical Specification 3.13. Under a loss of all safeguards chilled water, at least one train of ZH must be restored within 1 hour to prevent initiation of steps to take the units to hot shutdown within the next 6 hours.

Per C18.1, plant shutdown could also be required should Control Room or Relay Room temperatures become excessive under Technical Specification 3.5.C. However, alarms and other indications are available (i.e., control room temperature) to notify the control room operators of the failure and procedures are available for operators to quickly respond to the problem (C37.9 AOP1 and C37.9 AOP2, and C37.11 AOP1). These procedures direct the operators to shed non-essential loads, lighting, etc. and to open doors and install fans to reestablish room cooling. With room temperatures under control, it is possible that minor repairs to the ZH system could be effected before shutdown would be required as described in the previous paragraph. This would allow complete recovery from the event without incurring a plant transient. Should these conditions be met, C37.9 AOP1 and C37.9 AOP2 now require that operators use backup instrumentation at the Hot Shutdown Panel to catch any instrument drift that could be occurring. Efforts to cool the affected rooms would continue until successful, making it highly likely that temperatures could eventually be reduced and controlled before equipment damage occurs.

Procedure C18.1 would lead the operators to perform plant shutdown under the same logic as that used for excessive Control Room or Relay Room temperature if both safeguards 480 V trains are declared inoperable, both 4160 V trains are declared inoperable, or both event monitoring trains are declared inoperable.

Since the previous special initiator determination depended on operator response, it was determined prudent to reconsider failure of the ZH system together with failure of the operator response, resulting in a manual shutdown of the unit, for possible analysis as an initiating event for future IPE updates. The equipment assumed unavailable during this transient was based on the latest room heatup analyses available. Since the IPE was submitted, room ventilation concerns involving ZH system considerations have changed as follows:

Unit 1 480 V Bus Room Ventilation: During the 1994 Unit 1 refueling outage, the Unit 1 480 V bus arrangement was changed, both in electrical configuration

operability of the RHR system under a loss of safeguards chilled water initiator, these conditions will not exist in the RHR pits. Complete loss of the ZH system concurrent with a DBA LOCA is not probabilistically a credible event. Therefore, under this forced plant shutdown scenario, unavailability of the RHR function would not occur.

Based on the above, it was determined that no direct plant shutdown or trip coupled with the unavailability of safeguards equipment could be postulated for a loss of the ZH system initiating event without assuming additional equipment or operator action failures.

Very clear guidance now exists for plant shutdown should the entire ZH system be inoperable. The ZH system is now considered part of the control room air treatment system, and is therefore controlled by Technical Specification 3.13. Under a loss of all safeguards chilled water, at least one train of ZH must be restored within 1 hour to prevent initiation of steps to take the units to hot shutdown within the next 6 hours.

Per C18.1, plant shutdown could also be required should Control Room or Relay Room temperatures become excessive under Technical Specification 3.5.C. However, alarms and other indications are available (i.e., control room temperature) to notify the control room operators of the failure and procedures are available for operators to quickly respond to the problem (C37.9 AOP1 and C37.9 AOP2, and C37.11 AOP1). These procedures direct the operators to shed non-essential loads, lighting, etc. and to open doors and install fans to reestablish room cooling. With room temperatures under control, it is possible that minor repairs to the ZH system could be effected before shutdown would be required as described in the previous paragraph. This would allow complete recovery from the event without incurring a plant transient. Should these conditions be met, C37.9 AOP1 and C37.9 AOP2 now require that operators use backup instrumentation at the Hot Shutdown Panel to catch any instrument drift that could be occurring. Efforts to cool the affected rooms would continue until successful, making it highly likely that temperatures could eventually be reduced and controlled before equipment damage occurs.

Procedure C18.1 would lead the operators to perform plant shutdown under the same logic as that used for excessive Control Room or Relay Room temperature if both safeguards 480 V trains are declared inoperable, both 4160 V trains are declared inoperable, or both event monitoring trains are declared inoperable.

Since the previous special initiator determination depended on operator response, it was determined prudent to reconsider failure of the ZH system together with failure of the operator response, resulting in a manual shutdown of the unit, for possible analysis as an initiating event for future IPE updates. The equipment assumed unavailable during this transient was based on the latest room heatup analyses available. Since the IPE was submitted, room ventilation concerns involving ZH system considerations have changed as follows:

Unit 1 480 V Bus Room Ventilation: During the 1994 Unit 1 refueling outage, the Unit 1 480 V bus arrangement was changed, both in electrical configuration

and physical location. Buses 110 (Train A) and 120 (Train B) were split into Buses 111, 112 (Train A) and Buses 121, 122 (Train B). Each of the new buses carries roughly half of the original 480 V bus loads, and only one of these buses now exists in a room. Although the ventilation provided for these new buses is still supported by the ZH system, each unit cooler now only has to provide cooling for approximately half the original load. Consequently, new conservative analyses (ENG-ME-186) shows that, without ventilation, these room temperatures do not reach debilitating levels within 12 hours assuming no operator action. With operator action (to open doors at 12 hours, which provides natural air circulation in the rooms), room temperatures decrease to a steady-state temperature well below operability limits for the duration of the analysis (144 hours).

Event Monitoring Room Ventilation: As a result of the Unit 1 and Unit 2 Electrical System Upgrade (ESU) project, two of the old 480 V bus rooms now only contain event monitoring equipment. Recent conservative analyses (ENG-ME-186) show that, assuming doors to the room are opened at 12 hours following loss of ventilation, the room reaches a steady state temperature above operability limits for the duration of the analysis (144 hours). However, the operability limits exceeded are only those for the hydrogen monitoring equipment. The only event monitoring room components modeled in the IPE are panels in those rooms which supply power to the Unit 1 safeguards 4160 V bus sequencers (see next paragraph). Operation at the calculated steady state temperatures in these rooms given loss of ventilation would not jeopardize this power supply over the short mission time required in the IPE. Also, procedures C37.11 AOP1 and C18.1 now cover operator actions to restore ventilation to these rooms.

Unit 1 4160 V Bus Room Ventilation: New conservative analyses (ENG-ME-185) show that unavailability of room ventilation in the Unit 1 safeguards 4160 V bus rooms is now expected to be of concern. This is due to the temperature sensitivity of the new bus sequencer units now located in those rooms. However, this is not significant to risk since the loss of safeguards chilled water initiating event itself does not require operation of the sequencers. Significant additional equipment must be lost (resulting in a reactor coolant pump seal failure, for example) or a coincident loss of offsite power must occur (not a probabilistically significant event given that it was not the initiator) before the sequencers would be called upon to operate. Even if this were to occur, equipment could still be operated without the sequencers (manually) in response to the event. Procedures C37.9 AOP2 and C37.11 AOP1 now cover operator actions to restore ventilation to these rooms.

RHR Pit Cooling: New conservative analyses (ENG-ME-177) shows that long term post-LOCA RHR pit temperatures reach only 140 °F with both trains of RHR in recirculation and no room ventilation available. This is well within the range needed for pump operability during the IPE mission time of concern (up to several days for containment purposes post-core damage). The unit coolers are required for Technical Specification operability of the pumps only to preserve the EQ margin for operation up to one year following a postulated accident. This justifies removal of RHR pit ventilation unavailability as a failure mode for the RHR pumps during recirculation operation for future IPE updates.

In total, these changes have reduced whatever risk there was associated with the proposed loss of ZH system initiating event. The additional time available for operator action to restore room temperatures in the new 480 V bus rooms (12 hours) greatly increases the probability of success of this action. Ventilation in the RHR pits has been shown to not be necessary at all for well beyond the IPE mission time. The additional concern regarding the potential loss of the safeguards 4160 V bus sequencers is not significant to risk since the event itself does not require operation of the sequencers. Even if other failures occurred such that the sequencers were called upon to operate, equipment could still be operated without the sequencers (manually) in response to the event.

Given the above, we believe that excluding the loss of the safeguards chilled water system as an initiating event was justified. Extensive changes have been made in the electrical and other systems served by the ZH system since the IPE was submitted. Also, new, conservative room heatup information justifies removal of the IPE RHR recirculation functional dependency on room ventilation. These changes would significantly reduce whatever risk there was associated with this initiating event, and with the overall risk significance of the ZH system as a support system. Therefore, we do not feel that estimation of the change in the original IPE core damage frequency had this initiator been modeled provides any meaningful information. The equipment support functions provided by the ZH system will remain modeled in future IPE updates to the extent supported by the most recent room heatup analyses. Best-estimate room heatup analyses will be used if available, which would further reduce the risk significance of the ZH system.

Level 1 Question 6: Excessive LOCA (Reactor Vessel Rupture) Initiating Event

The IPE does not consider the initiator "excessive loss of coolant accident (LOCA)," i.e. reactor vessel rupture. Please provide a discussion of your consideration of this initiator and the basis for screening it.

Previous PRA studies (WASH-1400, NSAC-60) have quantified reactor pressure vessel (RPV) rupture as an initiating event which is postulated to be of a size and location as to lead directly to core damage. The frequencies calculated were from 1E-7/yr to 1.1E-6/yr. These studies did not identify a specific failure mechanism for this event. The frequency calculation was based on statistical evaluation of historical data with no specific failure mechanisms other than pressurized thermal shock being identified to cause the event. The calculation of a frequency is therefore based on interpretation of existing data.

Pressurized thermal shock (PTS) has been identified as a credible mechanism for reactor vessel failure in PWRs with certain levels of copper in the vessel welds. The Prairie Island RPV is thought to not be as susceptible to PTS due to the low percentage of copper in the RPV weld joints. Inspection of irradiated RPV samples has also confirmed that the vessel is aging slower than expected from the effects of neutrons and radiation. Table 4.2-2 of the Prairie Island USAR lists a reference temperature for PTS (RT_{PTS}) of approximately 208° F at the most limiting reactor vessel weld (for either

unit) at 60 Effective Full Power Years (EFPY). This is well below the 10CFR50.61 screening criteria of 270 °F for plates, forgings, and axial weld materials and 300 °F for circumferential weld materials. Plants with higher calculated reference temperatures have been analyzed in NUREG-4550 and have an estimated CDF due to PTS of approximately 1E-8/yr (Surry and Robinson) which is a negligible contribution to CDF at Prairie Island. With the exception of PTS, no specific credible mechanism for reactor vessel failure has been identified and calculation of a frequency based on historical events is limiting due to lack of failures. RPV rupture was therefore not explicitly included as an initiator.

Level 1 Question 7: Small-Small LOCA Initiating Event

The IPE model neglects the small-small LOCA initiating events. Please provide a discussion of your consideration of this initiator (which includes potential random failures of the RCP seals) and the basis for screening it.

The IPE model includes small-small LOCAs in the sizing for the small LOCA initiating event. MAAP results have indicated that feedwater is only required in the range from 3/8" to 3/4" equivalent RCS pipe break size to prevent core damage. Breaks above 3/4" do not require decay heat removal via the steam generators as decay heat is removed from the break itself. The small LOCA success criteria covered reactor coolant system equivalent pipe break sizes from 3/8" to 5". Over this range, it was conservatively assumed that feedwater was required to enable decay heat removal from the RCS via the steam generators. Breaks below 3/8" in size were not considered LOCA initiating events but normal transient events as USAR analysis indicates that a single charging pump is adequate to maintain RCS makeup and pressure such that a reactor trip will not occur.

RCP seal cooling failures are included as a heading in all of the transient and LOOP event trees. In the event RCP seal cooling fails, the sequence conservatively transfers to the small LOCA event tree where the sequence is mitigated as a small LOCA.

Level 1 Question #8: Main Steam/Main Feedwater Line Break and Special Initiating Events

a) **Please explain why consideration of the steam line and feed line break initiators is limited to locations inside the containment.**

The steam line break and feedwater line break initiating events frequency calculation considered piping only within the containment for two reasons:

1) Only that portion of piping up to the first isolation valve which could be expected to automatically isolate the break was included in the initiating event frequency calculations. Addition of the frequency of any line breaks beyond this point which were not isolated would be insignificant with respect to plant risk. This

is due to the low probability of pipe rupture combined with the high probability of isolation valve closure.

2) A break outside containment, if not automatically isolated, would be contained by the auxiliary building or turbine building steam exclusion boundary. This boundary consists of walls, doors and other barriers to prevent the propagation of a steam environment to safeguards equipment necessary to mitigate the initiating event. For example, the auxiliary building boundary protects equipment in the relay and control rooms, the D5/D6 diesel generator building, the fuel building, the safeguards chiller rooms and equipment in the 695' elevation of the auxiliary building. The turbine building boundary protects the safeguards AC and DC electrical equipment and the auxiliary feedwater pump areas. Openings in these boundaries are under tight administrative control. Required safeguards equipment within the steam environment is qualified for harsh environments.

b) **Please discuss how the frequencies for loss of service water (SW) and loss of component cooling water (CCW) as initiators were calculated. Were pipe breaks considered in the analysis? If not, please provide the initiating event frequencies for single and dual loss of essential SW and single and dual loss of CCW when passive component failures are taken into account. Also, provide the impact of these new frequencies on the results (CDF and dominant sequences). If the pipe break events in the CCW or SW system have a potential for affecting the results of your flooding analysis, please update your flooding analysis and provide it for review (see also the question below).**

The frequencies for loss of CL (Cooling Water) and loss of CC (Component Cooling Water) were calculated through the use of fault trees with the following assumptions:

1. Support systems that themselves are initiators were removed from the fault tree. For a loss of CL, these systems include loss of 125V DC power, loss of instrument air or loss of offsite power while for a loss of CC event, the list includes loss of 125V DC power, loss of offsite power and loss of cooling water.

2. Non redundant components that are normally in operation were given a one year mission time. If there were two or more redundant components that must fail, one was given a 8760 hour mission time. It was assumed that the other components must fail within 24 hours of the first component, so they were given 24 hour mission times (the same as was used in the original fault tree).

3. The systems were quantified in the configuration that they are normally in when the plant is at 100% power. For the CC system, this is one CC pump and one CC heat exchanger in operation with the second CC pump and heat exchanger in standby with crosstie between units not credited. The CL system was modeled with two CL pumps in operation with the header crosstie valves open and the remaining three CL pumps in standby.

4. Pipe rupture probabilities were added to the quantified fault tree results by calculating the length of pipe in the system and multiplying by an appropriate pipe break frequency value.

5. After quantification of the fault trees, illogical cutsets that were not allowed by the plant Technical Specifications or administrative procedures were removed. The resulting frequencies were then input into the initiating events I-LOCC (Loss of Component Cooling Water) and I-LOCL (Loss of Cooling Water).

6. Pipe breaks were considered in the internal flooding analysis as described in the response to Level 1, Question 9.e.

Level 1 Question 9: Internal Flooding Analysis

The following questions concern the treatment of flooding in the IPE:

a) **Please describe your treatment of the spray effect resulting from the spurious actuation of the fire suppression equipment in your flood scenarios.**

Spurious actuation of fire suppression was not considered in the flooding analysis. The Prairie Island Plant has several wet pipe sprinkler systems in the plant. These systems have pressurized water inside the piping up to the spray nozzles. The nozzles have a fusible link in them that prevents flow through the nozzle until the nozzle is heated by a fire to some predetermined value. The value set for each nozzle is dependent on the ambient temperature of the area around the nozzle and is set by the type of alloy used in the fusible link.

A spurious actuation of this system would be caused by the failure of a fusible link in one of the spray nozzles. This would allow water flow through the affected nozzle and would cause an alarm to sound in the control room alerting the operators to the failure. This failure affects only a single spray nozzle and thus would be isolated to one small area of the plant. Any equipment located under that nozzle will be sprayed by the nozzle and that equipment may fail due to the spray.

The volume of water flowing into an area from a single spray nozzle is insufficient to cause flooding in any flood zone in the plant and therefore was not considered a flood initiator in the flooding analysis. The contribution to component failure rates from spurious actuation of fire suppression equipment is small and is considered subsumed by the random failures of the equipment. For any piece of equipment to fail from this mode, a fusible link must fail, it must be located near essential equipment, and spray from above must be able to fail the equipment. This combination of failures is considered a low probability event and thus is considered insignificant and was not modeled as a separate failure mechanism.

b) **Please elaborate on your statement that the spray effect was not considered if it could affect only one train of equipment. Please discuss how the effect of sprays was analyzed.**

Spray was only considered a failure mode if it would affect more than one component or train of equipment. As discussed in question 9a, failure of a single component caused by spray is considered insignificant as compared to random failures since the failure caused by spray first requires several other failures which cause the spray and then the spray must cause the component to fail. This combination of failures is considered to be subsumed by the random failure probability for the component.

Spray was considered a failure mechanism if it could fail multiple components that are not in the same train of equipment. Examples of this would be if the spray was in an area that had power distribution panels for both Train A and Train B, or if the spray could affect pumps from two different systems or from both trains of the same system. Spray was not considered if it could affect a pump and its motor operated discharge or suction valve since failure of either component affects only that train of equipment and failure of both at the same time has no greater affect than failure of only one.

c) **Did you consider backflooding through drains and drain failures (i.e., plugging) in developing your flooding scenarios? If not, please estimate the impact of this omission on the results.**

Floor drains were considered in the IPE internal flood analysis. After screening areas of the plant where either no flooding source was available or no equipment modeled in the IPE existed the next step in the screening process was to exclude areas where the potential flooding source could not provide enough flow into the area to flood it to a level great enough to fail equipment. The ability of floor drains to remove water from the area was included in this screening process.

Drawings of several different plant floor drains were reviewed to determine the typical configuration of plant floor drains. This review showed that all the drains for a given area combine into a single pipe which then carries flow to the final collection sump or tank. Therefore, the floor drain capacity for that area is limited to the capacity of the combined pipe to drain the area with gravity induced flow. A review of previous work done by NSP of floor drain flow capacity showed that the capacity of drains for several different areas with configurations similar to those at Prairie Island all had a flow rate within a narrow range. A value in the middle of that range of 75 gpm was assumed for floor drain capacity for all areas considered in this screening analysis.

Potential plugging of the drains was not considered a problem. The flowrate assumed for floor drains (75 gpm) was small when compared with other water removal mechanisms considered in the screening analysis, such as water flow under doors. The screening results would not have changed even if floor drains had not been considered.

Backflooding from one flood area to another through the floor drains was considered but deemed not a credible event. In each building where floor drains were analyzed, the area where the drains would backup to, should the sump or tank they drain to become full, is large enough to handle the excess water without flooding to a level where equipment could be damaged. Backflow from one flood area to another through the floor drains caused by a plugged drain pipe was not considered since there are no known instances where floor drains from more than one area combine into a single pipe.

Water flowing under a door or breaking a door allowing flow from one area to another was considered. Each area screened considered flow from adjoining areas as a possible flood source. Any area where it was likely that the flood would spread from one area into adjoining areas it was assumed that equipment in both areas would fail due to the flood.

d) **Please discuss how maintenance errors committed while in cold shutdown, which were left undiagnosed until the postulated flood event occurred while the unit was at power, were treated in the flooding analysis.**

Maintenance errors were included in the flooding analysis only when the maintenance task would be performed while the plant was at power. Also, the maintenance task would be a normal task performed on a periodic basis that opens the system pressure boundary. This would allow flooding from the system in the event that the system isolation was done incorrectly or an isolation valve was inadvertently opened. The areas that fit this criteria are mainly areas that contain equipment from both units. This allows maintenance on equipment from one unit which is in cold shutdown in an area where equipment is operating for the other unit which is at power.

It was assumed that flooding caused by maintenance activities could only occur while the maintenance activity is being performed. The systems that are considered potential flooding sources are all support systems that are operating prior to bringing the plant to power operations. It was assumed that any error in the maintenance task would be identified and corrected in the post-maintenance testing such as hydrostatic tests and operational testing. Any flooding during the testing is considered in the maintenance caused flooding events that were considered in the IPE. Any flooding from these systems that occurs after the testing is completed is considered random flooding events and was included in the random flooding that was analyzed in the IPE.

e) **How does your consideration of pipe breaks in the CCW and SW systems (see question above) impact the results of the flooding analysis?**

Pipe breaks were included in the Loss of Component Cooling Water (I-LOCC) and Loss of Cooling Water (I-LOCL) initiating event calculations as described in Level 1 Question 8b. These initiating events included the probability of pipe failure in any pipe in the system large enough to fail the system if it were to break. In the flood analysis breaks in the cooling water piping were considered, breaks in the component

cooling water system were not. The component cooling water system (CC) is a closed loop system with a limited amount of water in the system. The areas where CC piping exists are large areas such that there is not enough water available in the system to flood the areas. Therefore, the CC system was screened out as a potential flooding source.

The cooling water system (CL) was considered a flooding source. The CL system has an unlimited source of water; the Mississippi River. If a pipe breaks somewhere in the CL system the system will continue to dump water into the area until the break is isolated or until the CL pumps are turned off. Therefore, any area that contains CL piping could be flooded by that system given a high enough flowrate and adequate time.

The pipe break frequencies used in the flooding analysis and the pipe break frequency used in the initiating event I-LOCL are different. The pipe break frequency for the initiating event represents a break anywhere in the system. The frequencies calculated for the flooding analysis represent the pipe break frequency only for piping within a specific area of the plant which has been designated a flood area. Each value was calculated independently and the results of one calculation did not influence the results of the other.

Level 1 Question 10: Status of Recommended Plant Improvements

The status of the potential plant improvements to reduce the likelihood of core damage and/or improve containment performance discussed in the submittal is not clear. Please clarify the submittal information by providing the following:

a) **The specific improvements that have been implemented are being planned, or are under evaluation.**

b) **The status of each improvement, i.e., whether the improvement has actually been implemented, is planned (with scheduled implementation date), or is under evaluation.**

The IPE recommendations and their disposition (including current status) are described in Appendix 1. All of the items are listed as closed in Appendix 1 except Level 2, Recommendation 2, regarding the Sump C hatch doors. Currently, this improvement is being implemented by maintaining the Sump C hatch doors open during plant operation, with their mechanical hold-down devices ("dogs") turned inward and secured such that the doors cannot physically close without human action. The dogs are being administratively controlled in this position so that the doors are not unintentionally closed during plant operation. Other options for implementing this recommendation may be implemented in the future.

c) **The improvements that were credited (if any) in the reported CDF.**

There were no recommended improvements which were credited in the reported IPE CDF.

Referring to Attachment 2, Level 2, Recommendation 1 involved a change to emergency procedure FR-C.1, Rev 5, "Response to Inadequate Core Cooling" step 18 such that the operator checks for adequate steam generator level before attempting to start an RCP. The purpose of this change was to minimize the potential for induced steam generator tube rupture (termed "steam generator tube creep rupture" or "SGTCR" in the IPE report). The Level 2 analysis was quantified two ways: one quantification assumed that the recommended procedure change had been made (the results which exclude SGTCR, Figure 4.6-1) and one quantification which assumed that the change had not been made (the results which include SGTCR, Figure 4.6-2). Therefore, it could be said that the procedure change was "credited" in the results depicted in Figure 4.6-1.

Comparison of Figure 4.6-1 and 4.6-2 shows that inclusion of SGTCR in the results has a very large effect. Therefore, Table 4.6-1 listed the Level 2 end states involving SGTCR separately since 1) they would tend to mask the results of the other important end states and 2) implementation of an imminent procedure change would essentially eliminate the containment failure risk from this event.

Again referring to Attachment 2, Level 2, Recommendation 2 was credited in the Level 2 quantification. This recommendation was intended to initiate plant design or administrative control changes, if necessary, to ensure that the Sump C hatch doors remain open such that water injected from the RWST following an accident will flow through the doors and into the reactor cavity. The availability of this pathway to the reactor cavity allowed credit to be taken in the Level 2 quantification for ex-vessel cooling, a means by which molten core decay heat could be removed through heat transfer across the lower vessel wall and boiling of the water in the reactor cavity. This could then be terminated with the core remaining in the vessel.

d) **If available, the reduction to the CDF or the conditional containment failure probability that would be realized from each plant improvement if the improvement were to be credited in the reported CDF (or containment failure probability), or the increase in the CDF or the conditional containment failure probability if the credited improvement was to be removed from the reported CDF (or containment failure probability).**

The change in CDF or to the conditional containment failure probability for each plant improvement has not been generated. However, Section 6.17 of the report gives the change in CDF assuming that the procedure change to allow station air to be cross-tied to instrument air (Attachment 1, Level 1, Recommendation 1) and assuming the auxiliary feedwater pump room is segregated to prevent flooding propagation into both halves of the room (Level 1, Recommendation 3). Although not explicitly stated in Section 6.17, this value also accounts for the procedure change specified in Level 1 Recommendation 2. The other Level 1 recommendations involve operator training and their benefit is to focus on key operator actions that would assist in maintaining the current core damage frequency.

The Level 2 recommendations are each individually quantified and reported in the IPE report. Level 2, Recommendation 1 involved an EOP change to prevent steam generator tube creep rupture. The conditional containment failure probability reduction given this procedure change is identified in Table 4.6-1 as the conditional probability of the "Puff Release" and the L-SR-E end states following core damage. This is also shown graphically in the change between Figures 4.6-2 and 4.6-1. Since this procedure change was imminent, it was felt more beneficial to report both results, and to develop the other plant improvement recommendations based on the results shown in Figure 4.6-1.

Level 2, Recommendation 2 (plant modification to ensure that the Sump C hatch doors are maintained open) is addressed by the Level 2 sensitivity study on in-vessel recovery documented in Section 4.8.1 and Figure 4.8-2 of the IPE report. This sensitivity study showed that the increase in conditional containment failure probability if the hatch doors are assumed to be closed is very small. However, the plant improvement recommendation was made based on the opportunity to terminate a large fraction of the core damage at high pressure sequences in vessel through the implementation of a very simple plant design change.

e) **The basis for each improvement, i.e., whether it addressed a vulnerability, was otherwise identified from the IPE review, was developed as part of other NRC rulemaking, such as the Station Blackout Rule, etc.**

The plant improvements that were recommended through the IPE analysis, and the bases for each improvement, are identified in Section 1.4.6 of the IPE report. All were identified from the IPE review only.

Level 1 Question 11: Station Blackout Contribution to CDF

On page 1-9 of the Executive Summary of the submittal it is implied that station blackout (SBO) is a dominant contributor to the CDF, yet the SBO contribution to CDF is less than 10% of the total. Please explain the statement in the Executive Summary.

The statement in the Executive Summary is a true statement. Core damage frequency which is caused either directly or indirectly from a LOOP does account for 21% of the total CDF. In the IPE, an SBO was not considered a direct initiating event but rather an indirect initiating event. An SBO occurs as a result of a LOOP followed by failure of the safeguards diesel generators to supply power to the safeguards 4160V buses, so the LOOP initiating event is the actual event that started the sequence toward an SBO. The portion of the CDF from a LOOP that is a result of an SBO is approximately 6.5% as stated in section 3.4 of the IPE submittal.

Level 1 Question 12: Process Used to Ensure IPE Reflects "As-Built-As-Operated" Plant

Please explain the process used to ensure that the model in the IPE reflected the "as-built as-operated" plant.

A strong effort was made to ensure that the IPE model accurately reflected the plant "as-built as-operated". This began by using people knowledgeable in the plant to develop the model. Section 5.1 of the IPE submittal discusses the team which developed the model and shows the education, training, experience and other qualifications the team possesses. These people are all knowledgeable in the nuclear power industry and in the Prairie Island plant in particular. Outside consulting firms were used to help in the development of the IPE model. The consultants were used primarily to assist the utility PRA analysts with PRA modeling techniques and they provided much of the technology used to develop and quantify the IPE model.

This team of people was divided between the plant site and the corporate offices. Having people stationed at the plant site facilitated communication with the plant as well as allowing for inspection of plant systems when necessary to ensure accuracy in modeling the plant "as-built as-operated". The people at the corporate offices were able to ensure that management concerns were addressed and they were able to keep abreast of industry advances in PRA technologies due to their close contact with management and industry points of contact.

Plant specific component failure rates were used where possible to ensure "as-built as-operated" accuracy in the model. These failure rates were calculated using plant specific data and operating time for the plant components. This data was collected for a 10 year operating time to reduce the affect of statistical differences in year to year operating history. The use of plant specific failure rates ensured that the IPE model accurately reflects plant equipment. Any equipment at Prairie Island which fails either more or less often than industry failure experience will be modeled as such because of the plant specific data.

A wide range of plant documents were used when creating the system models. Section 2.4.3 of the IPE submittal provides a list of document types that were used. The most recent revision of the document available at the time the model was developed was used. These documents are maintained current by the plant staff and reflect the current plant equipment and operating practices. These documents were the basis for many aspects of the IPE model, including failure rates and operating times for equipment, operator actions credited in the model, assumed equipment response to accident conditions, and system initial conditions and success criteria.

Plant engineers with system responsibilities and operations staff were consulted throughout the development of the IPE model. Numerous discussions were held on an iterative basis with the plant staff to ensure the accuracy of the system models. The engineering staff was consulted to verify that assumptions made regarding system initial lineups and success criteria were correct, that maintenance frequencies and maintenance task durations were correct, and that assumed system response to initiating events was correct. The operations staff was asked to verify that assumptions about operator actions were valid. They were also asked to assist in identifying control room indications that would prevent system alignment errors and would alert

them to abnormal operating conditions. They also helped with the plant walkdowns for the detailed HRA analysis.

When developing the event trees used in the IPE the most current version of the plant operating procedures and emergency operating procedures were used. Prairie Island uses function based emergency operating procedure. The event trees in the IPE are also functional event trees. Each heading in the event trees represents a function that is needed to mitigate an accident. The plant functional restoration procedures were used to develop the heading equations. No credit was taken for a system performing a function if there was no procedure that told the plant operators to use that system for that function.

The Prairie Island IPE accurately reflects the "as-built as-operated" plant. This was ensured by the use of knowledgeable people to develop the model, the use of plant specific data where possible, the use of input from the plant staff in the development of the model, and the use of current plant documents including the plant emergency operating procedures.

Level 1 Question 13: Utility Involvement and Review

It is not clear from the submittal what the level of involvement of the utility was in constructing the probabilistic risk assessment (PRA) model. The level of depth of the in-house review is also unclear. Was only senior management involved in the review? Please describe the utility involvement in the PRA modeling as well as the in-house review in more detail.

Section 5.1 of the IPE submittal discuses the utility staff that developed the IPE model and wrote the IPE submittal report. This team of people were involved in all aspects of the development of the IPE. There are six individuals that comprise this team, and five of these worked on the IPE project from its beginning. In addition to these people many other utility personnel were involved in parts of the IPE development and in the final review of the IPE submittal report. Page iii of the report lists all the utility personnel who were involved in the in-house review of the IPE report.

System engineers were contacted as necessary to provide input for development of system success criteria, component failure modes, estimates of maintenance out-of-service times, and maintenance task frequencies. This input was sought by the PRA analysts during the development of the system models. The analysts asked the system engineers to provide input about how to properly model the systems. The input provided by the system engineers was then used to accurately model the systems and is documented in the calculation files created during the model development.

Licensed Control Room Operators were also used as a source of information on many aspects of the IPE model. Discussions were held with the operators to determine how systems were operated under normal full-power operations to ensure the proper system alignment was modeled. They also provided information on system maintenance line-ups for systems where maintenance is performed on-line. Discussions were also held to determine the expected plant response and operator response to specific events. Operators were involved in some plant walkdowns, particularly the control room walkdown used to verify

the basis for assumptions in the detailed human reliability analysis for control room operators.

The draft submittal was distributed widely to the plant staff for review and comment. The reviewers were asked to pay particular attention to portions of the report that fell within their area of expertise. Many comments and questions were raised during the review process. These were studied and changes were made to the model and/or the report as necessary to answer the reviewer's questions and comments.

Level 1 Question 14: Failure and Maintenance Data

This question concerns the failure and maintenance data used in the IPE:

a) **Spot checks of your plant-specific failure data revealed it to be generally lower or much lower than generic data from NUREG/CR-4550 "Analysis of Core Damage Frequency from Internal Events." For example, failure of check valves to open and to close are 1 to 2 orders of magnitude below what was reported in NUREG/CR-4550. Please provide the basis for the calculation of your plant-specific data and verify that the low values are indeed appropriate.**

The Prairie Island PRA has a combination of plant specific data values and generic data values. Plant specific data was preferred to ensure that the model was as specific to Prairie Island as possible. Therefore, whenever possible, plant specific values were used. For many types of components it is very difficult to estimate a failure rate because it is not possible to estimate the operating time or demands on the component. These components are things such as level or pressure transmitters, relays, room cooling fans, and fuel oil transfer pumps. In these cases generic data was used. The sources of generic data used in the Prairie Island IPE are listed in the submittal in Section 3.3.2. They are:

1) NUREG/CR-2815
2) NUREG/CR-4550
3) IEEE Standard 500 data
4) EPRI TR-100320, Vol. 2, Reliability Centered Maintenance (RCM) Technical Manual
5) WASH-1400, Reactor Safety Study (NUREG 75/014)

For most major components it was possible to calculate failure rates and maintenance unavailability rates. Section 3.3.3 of the IPE submittal describes the process used to calculate the plant specific values. A variety of plant records were used to collect the data used to calculate the plant specific failure rates. All of this data was entered into an electronic database which was then used to sort the data and calculate failure rates and maintenance unavailabilities.

Each plant specific value calculated was compared with generic values to check the reasonableness of the calculated value. When a discrepancy occurred the calculation was checked to determine the reason for the

discrepancy. If there was sufficient plant data to make a good estimate of the failure rate the plant value was used. The example stated in the question of check valves is an example of this.

Plant specific values were used for valves. Plant procedures, surveillance procedures, and maintenance procedures were used to collect component demand data. Any valves that were opened or closed due to the procedures were entered into the database. To calculate failure rates for valves all valves of a specific type, such as motor valves, air operated valves or check valves, were pooled together to create a large data pool of demands and failures. For check valves this created a pool with over 25,000 open demands and an equal number of close demands. There were no failures of check valves found in the plant records. However, since no equipment can be assumed to have a zero failure probability, a value of 0.5 was used for the number of failures. This value, while conservatively exceeding the observed number of failures, allows some credit to be given for the high observed reliability of the equipment (as opposed to simply assuming 1 failure had occurred). The resulting failure rate is lower than generic industry values, however, the large pool of demands coupled with the lack of failures justifies using the plant specific value.

There are other components that had few or no failures and also had failure rates lower than generic data values. They also were compared with the generic data and the plant specific value was considered reasonable. The lack of failures, even with a large number of demands or high operating hours, is a compelling reason to use the plant specific values.

b) **Your failure data does not include the failure mode "check valve rupture." Was this failure mode considered in your ISLOCA [interfacing-systems LOCA] analysis, and if not, what is your estimate of the impact on your results?**

The analysis for ISLOCA reviewed all piping systems that are exposed to RCS pressure and penetrate the containment. The review found three containment penetrations that met the criteria for ISLOCA consideration. One of these penetrations had one check valve that would need to fail for an IS LOCA and one had two check valves in series that would have to fail. The other penetration had no check valves.

A fault tree was developed to assess the probability of an ISLOCA at any one of these three penetrations. Included in the fault tree is the failure mechanism of "check valve catastrophic leakage". This failure mode models valve disc rupture or excessive internal leakage.

The value used for this failure mode was taken from NUREG/CR-2815 "Probabilistic Safety Analysis Procedures Guide". The value listed is 1.00E-07/hr. The check valves are given a mission time of one cycle (about 18 months). The resulting failure probability for the check valves is 1.31E-03.

Level 1 Question 15: Level 1 Success Criteria

The submittal states that success criteria for front-line systems are built upon Modular Accident Analysis Program (MAAP) runs given certain core damage criteria. These core damage criteria allow substantial time to elapse (30 min) while certain areas of the core are at elevated temperatures (1200°F). For shorter durations temperatures range up to 2000°F. Some of the success criteria calculated (and presumably used) significantly relax criteria used in other PRA work (e.g. NUREG-1150, "Reactor Risk Reference Document"). Examples are:

a) For large LOCA, one residual heat removal (RHR) pump is sufficient to prevent core damage, i.e. no accumulators need to inject. In previous analysis, the accumulator in the intact leg would need to inject.

b) For a medium LOCA of 5-inch break size, one RHR pump is sufficient to prevent core damage. Typically (e.g., NUREG/CR-4550 analysis for Surry) it is assumed that a high head injection pump (HPI) is needed as well.

c) For a medium LOCA of 12-inch break size, one safety injection (i.e., HP) pump is sufficient. This would be a large LOCA size in the NUREG/CR-4550 analysis for Surry, and an LPI (low pressure injection) pump in conjunction with accumulator injection is needed.

1) What is the basis for these novel success paths? Are they included in operator guidance (e.g. emergency operating procedures (EOPs)) and are the operators trained in them? If not, how were the human error probabilities (HEPs) quantified?

2) Please estimate the impact of these novel success paths on your results (CDF and important core damage sequences).

3) For small LOCAs, no credit seems to be given (short term) for power operated relief valve (PORV) manipulation to help with decay heat rejection. Is feed and bleed not an option used in the EOPs to deal with small LOCAs?

(1) These success paths are the result of using the MAAP program and the definition of core damage at Prairie Island. The following is a discussion of the basis for our definition of core damage.

Previous PRA studies (NUREG-1150 and 4550) conservatively assumed core uncovery signified core damage. This would assure that there would be no release of fission products from the fuel to the RCS. Therefore the maximum release of fission products from the RCS would be limited to the initial inventory in the RCS prior to the initiating event. Subsequent studies have shown that steam cooling on the upper portion of the core (after core uncovery) can be effective in delaying or preventing core damage.

The Westinghouse Emergency Operating Procedures (EOPs) define inadequate core cooling as a core exit thermocouple reading of 700°F and Reactor

Vessel Level Instrumentation System (RVLIS) readings less than 41% or core exit temperatures of 1200°F. If either of these two condition are reached, the EOPs transfer to Functional Restoration Procedures (FRP) dealing with the restoration of core cooling (FR-C.1 and FR-C.2).

Based on studies documented in NUREG-1228 (Source Term Estimation During Incident Response to Severe Nuclear Power Plant Accidents, 1988), there are four temperature ranges for fuel rods that may be defined when looking at core coolability and integrity. The four ranges are described briefly below:

1. At a core temperature up to 1400°F, analyses and evaluations of the behavior of the core indicate that there are no changes in the structural integrity of the fuel rods in the core.

2. At core temperatures between 1400 and 2000°F, the zirconium cladding begins to lose some of its structural integrity. At these temperatures, ballooning of the cladding and bowing of the fuel rods could occur. The experiments and analytical models indicate that some local breeches (bursting) of the cladding may be due to pressure differences across the cladding, although the capability to cool the core under these conditions is not compromised. The breech of the cladding would permit the release of any fission product gasses which have accumulated in the fuel rod gas space. This release would only represent 1% of the total fission product inventory.

3. At core temperatures between 2000 and 4000°F, zirconium undergoes an exothermic reaction with steam in the primary system. These zirc-water reactions cause the zirconium to oxidize, forming zirconium dioxide. Experimental evidence has shown that zirconium dioxide loses its structural capability via cracking, which will result in wide spread breeches in the cladding boundary. The initiation of zirc-water reactions will begin to compromise the capability of the Emergency Core Cooling System (ECCS) to cool the core, primarily due to the additional heat from the zirc-water reactions. Analyses and evaluation indicate that core cooling may still be possible during this time frame. In this temperature range, significant gaseous and volatile fission products will be released to the primary system as a result of temperature enhanced diffusion and additional loss of cladding integrity. A reasonable approximation indicates that up to 50% of the core inventory of noble gasses and volatile fission products may exist outside the boundary of the fuel in the primary system.

4. At core temperatures greater than 4000°F, the zirconium cladding and the uranium dioxide form a eutectic, melt and begin to relocate. As relocation occurs, cooling channels are blocked and cooling the core becomes more difficult. At these core temperatures, all of the gaseous and volatile fission products would be released from the fuel to the primary system as a result of the core melt. Analyses and experience indicate that core

cooling may still be possible in this time period, as shown by the TMI-2 experience. The primary reason for this is that the dominant heat transfer mechanism will no longer be convection, but rather conduction.

Based on the characteristics of the fuel as the temperature increases during accident conditions, it is reasonable to select a value below 1400°F to represent the peak core exit thermocouple reading for the definition of core damage. A choice of 1200°F as the lowest temperature for which core damage could not occur is justified based on the following considerations:

1. If the fuel rod temperatures are below 1200°F, there is no additional fission product release to the primary system. Therefore, the maximum release from the plant during an accident scenario would be limited to the initial fission product inventory prior to the initiating event.

2. At temperatures below 1200°F, the core will always be in a coolable configuration. There is no point just beyond 1200°F where the accident conditions change drastically. Thus, the core can always be recovered by simply providing sufficient water to remove decay heat.

3. The 1200°F value used for defining core damage refers to the peak fuel rod temperatures predicted by realistic, best estimate analyses; the 1200°F value used in the EOPs for defining inadequate core cooling refers to steam temperatures as measured by core exit thermocouples. There can be a 200 to 300°F difference in these temperatures for a given accident initiator.

MAAP 3.0B analyses indicate that if the hottest core temperature remains less than 2000°F and does not exceed 1600°F for longer than 30 minutes, less than 1% of the total core fuel rods will experience a temperature in excess of 1200°F. Assuming that fission product release to the primary system occurs around 1400°F, the release from the fuel using MAAP 3.0B can be determined. Experience with MAAP indicates that the potential fission product release from the fuel in which the fuel rod temperatures exceed 1400°F are approximately two orders of magnitude less than an accident scenario where the entire core was severely damaged (temperatures >4000°F). Consequently, a core temperature greater than 1400°F for a short period of time, but not exceeding 2000°F would result in a negligible impact on plant risk profile. However, if core temperatures were sustained above 2000°F for a substantial period of time, the cladding failures and subsequent fission product releases would increase.

Therefore, the success criteria for determination of core cooling can be stated as: "core fuel rod temperatures which are not in excess of 1200°F for a prolonged period of time, where a prolonged period of time is

defined as greater than 30 minutes, and not in excess of 2000°F for any period of time whatsoever".

Using this definition for core damage, the various success criteria for different initiating events were arrived at. Control room operators are trained in the use of the Westinghouse EOPs which instruct the operator to use whatever equipment is available at the time of the accident. If high head injection (SI) pumps are not available, the operator is instructed to depressurize the steam generators to allow use of the low head (RHR) pumps and accumulators. There is not a specified list of equipment in the EOPs that is required to deal with a specific accident. If equipment is not available, the EOPs instruct the operator down different paths to use other equipment or different injection pathways. HEPs were derived from the use of the current revisions of the Westinghouse EOPs that all control room operators have been trained on.

(2) By assuming accumulators were necessary for LOCA sequences, the resulting accident sequence probabilities will not be impacted as accumulators are passive components at Prairie Island. The accumulator outlet motor valves are already open, and the accumulators are pressurized with nitrogen gas. The probability for the failure of both accumulators is approximately 1E-6, which when multiplied by the LOCA frequencies becomes an insignificant contributor to CDF.

In the case of a medium LOCA, using more conservative success criteria of a high head injection pump together with an RHR pump will cause accident class SEL (medium or large LOCA with failure of short term RCS inventory) to increase from 7.6E-8 to approximately 8.4E-7/yr, which increases the contribution of this accident class from 0.2% to 1.6% of total CDF.

(3) Bleed and feed is credited for a small LOCA as indicated on Figure 3.1-4 (Small LOCA Event Tree) of the IPE report. The branch labeled as SI + Pzr PORV + Operator Action is the bleed and feed option as the Safety Injection (SI) system together with the pressurizer PORVs and an operator action are the requirements for bleed and feed. Bleed and feed is used in the EOPs in the event that the secondary portion of the heat sink critical safety function is lost. Since secondary heat sink is part of the requirements for successful small LOCA accident mitigation, bleed and feed has been credited. It must be added that recirculation is also a requirement after use of bleed and feed in order to recirculate the coolant spilled into containment through the pressurizer relief tank rupture disk.

Level 1 Question 16: Plant Changes Made Due to the Station Blackout Rule

It is not clear in the submittal if plant changes due to the Station Blackout Rule were credited in the analysis. Please provide the following: (1) identify whether plant changes (e.g., procedures for load shedding, alternate AC power) made in response to the blackout rule were credited in the IPE and what are the specific plant changes that were credited; (2) if available, identify the

total impact of these plant changes to the total plant CDF and to the SBO CDF (i.e., reduction in total plant CDF and SBO CDF); (3) if available, identify the impact of each individual plant change to the total plant CDF and to the SBO CDF (i.e.; reduction in total plant CDF and SBO CDF); (4) identify any other changes to the plant that have been implemented or are planned to be implemented, that are separate from those in response to the Station Blackout Rule, that reduces the SBO CDF; (5) identify whether the changes in # (4) are implemented or planned; (6) identify whether credit was taken for the changes in # (4) in the IPE; and (7) if available, identify the impact of the changes in # (4) to the SBO CDF.

(1) NSP evaluated the requirements of the SBO rule using guidance in NUMARC 87-00 except where Regulatory guide 1.155 takes precedence. In its original configuration, with two emergency diesel generators (EDG) shared between units, Prairie Island was classified as an eight hour coping plant. In order to reduce the coping category to four hours or less in accordance with NUMARC 87-00 Initiative 1A, Prairie Island chose to modify the 4.16 KV Auxiliary System to provide two dedicated EDGs per unit. Each EDG is capable of supplying the required SBO shutdown loads for both units for the required coping duration. The alternate AC power source consisting of an EDG of the non-blacked out unit is available to the blacked out unit within ten minutes of the onset of station blackout. Plant procedures addressing SBO were reviewed and modified, if necessary, to meet the guidelines of NUMARC 87-00, Section 4.

The IPE submittal included the two additional EDGs that were added along with the applicable procedures that operators would use to crosstie the EDGs between the two units. Load shedding procedures for the DC batteries were also credited in the IPE analysis.

(2) In order to evaluate the change in CDF credited to these SBO modifications, the IPE model would need to be requantified again with the plant modeled as it was without the modifications installed. Suffice it to say that the SBO modifications did provide a significant reduction in CDF over the plant as it existed before the two EDGs were added, as the new EDGs are not dependent on cooling water for diesel cooling. The importance measures for the two diesels added (D5 and D6) are similar, with the Risk Achievement Worth (RAW) being approximately 2 and the Fussel-Vesely value being approximately 7E-02.

(3) See (2) above.

(4) As part of the modifications that were performed to add the two new EDGs, the safeguards 480V system was also modified such that there are now four safeguards 480V buses per unit where there were only two before. This change enabled the safety related MCCs to be directly fed from a safeguards 480V bus rather than sub fed from another MCC. The bus ties between units for the 480V safeguards buses were also eliminated. As part of the SBO modification process, #121 cooling water pump was repowered from a safeguards 4.16 KV source backed by the new EDGs instead of its normal non safeguards power supply. With this change, there are now three cooling water pumps available following a LOOP, with

one being motor driven and two being diesel driven instead of two as was the case before the modification.

(5) The plant changes delineated in (4) above have all been implemented.

(6) The IPE took credit for the 480V changes listed in (4) above for Unit 2 only as the modifications for Unit 1 were not complete before the IPE freeze date. The repowering of #121 cooling water pump was also credited.

(7) The 480 V changes did not have a large impact on the overall CDF but the repowering of #121 cooling water pump was estimated to have a significant effect on the overall CDF by providing an extra cooling water pump with a driver diverse from the other two safeguards pumps that can be made available following a LOOP. The RAW importance measure for #121 cooling water pump is approximately 10 while the Fussel-Vesely value is approximately 1E-02.

Level 1 Question 17: PORV Block Valve Position

There is no discussion in the submittal about the PORV block valve position and how it affects various scenarios (feed and bleed, anticipated transient without scram). What is the fraction of time that either or both block valves are closed? How is the possibility of the PORV block valve being closed accounted for in the model? If the block valves are not modeled, what is the effect on your results?

The Pressurizer PORVs are included in the model for feed and bleed and for ATWS. However, in neither case are they modeled such that the block valves are required to open. In the ATWS modeling, the fraction of time that either block valve was assumed to be closed due to leaking PORVs was estimated as one month per year based on a discussion with operators in the control room. That estimate results in an unavailability value of 8.3E-2 for each block valve.

In the feed and bleed model, the block valves are only modeled as failing to remain open. The fault tree success criteria assumes that one PORV is required for successful feed and bleed. If one block valve is closed it was assumed that the operator would use the other PORV for feed and bleed. If both block valves were closed it was assumed that the operator would simply open one block valve and perform the feed and bleed operation. However, the possible failure of the block valve to open was not modeled. This omission has a negligible effect on the core damage frequency. The failure probability for a motor valve combined with the probability that the block valve is closed is 3.93E-4. Since the success criteria for the fault tree assumes that only one PORV must open, the failure of the block valve is ANDed with the failure of the other PORV or block valve making this failure on the order of 1E-6 or less. This is significantly lower than the human error probability for bleed and feed of 4.50E-2.

Block valve closure to isolate a leaking PORV was included in the ATWS model. The pressure relief portion of the ATWS event tree was modeled with a fault tree. This tree models failure of the PORVs and pressurizer safety valves to

protect the RCS from overpressure during an ATWS event. The success criteria for this tree changes depending on where in the fuel cycle the plant is at. It is assumed that both pressurizer safety valves are always needed for successful overpressure protection and that the required number of PORVs changes depending on the moderator temperature coefficient. Four different plant conditions of control rod insertion and Auxiliary Feedwater availability are modeled in the IPE, each of which require a different number of PORVs (with both pressurizer safety valves) to protect the RCS from overpressure. The four plant conditions are modeled in the event tree as four branches that enter the PR (Pressure Relief) heading. The event tree model is documented and explained in Section 3.1.2.2 of the IPE submittal and is included as Figure 3.1-9 of the submittal. The fault tree which inputs to the PR heading models the four PORV combinations. The fault tree has four top events, one for each plant condition. The block valves were included in this fault tree as a failure mechanism for the PORVs. Failure modes modeled for the block valves included failure to remain open (for cases in which the block valve was assumed to initially be open) and block valve closed due to excessive leakage of the PORV. Occurrence of either of these events is modeled as a failure of the associated PORV for the pressure relief function.

Level 1 Question 18: USI A-45 (Decay Heat Removal) Evaluation

In consideration of Unresolved Safety Issue A-45, decay heat removal (DHR) evaluation, please provide the contribution of DHR and its constituent systems (e.g., auxiliary feedwater, feed and bleed) to CDF. There is a substantial discussion in the submittal on the various front-line systems performing DHR functions and the relative impact of loss of support systems performing the DHR function. There is also a system importance ranking output, but it doesn't include certain DHR functions such as feed and bleed, etc., nor a summary of your insights and any vulnerabilities found regarding this issue. Please provide this information.

As stated in section 3.4.4.3 of the IPE submittal, loss of DHR is synonymous with CDF as there are no credible core damage sequences that do not involve loss of DHR. The substantial write-up in section 3.4.4 of the IPE submittal describes in detail every system that was credited as being able to provide a DHR function. Each means of DHR is also analyzed as to how initiating events may affect their reliability and the top failure modes for each system are also given. Insights are also provided for each DHR system. Since loss of DHR is synonymous with CDF and no vulnerabilities were found for the Prairie Island Plant then it must be assumed that there are also no vulnerabilities for DHR.

Figures 3.4-1 and 3.4-2 of the IPE submittal are importance rankings of the systems credited in the IPE. The systems that provide DHR are also included in these tables. Bleed and feed is not included as bleed and feed is a function that consists of the SI system , the pressurizer power operated relief valves (PORV) and an operator action. The bleed and feed function is described in section 3.4.4.2.2 of the IPE submittal, together with a description of the various failure modes. The results of this section are that the operator error to lineup for bleed and feed is 95% of the cause of failure of bleed and feed.

The Fussel-Vesely of this operator action is 9E-2 so the approximate Fussel-Vesely of bleed and feed is 9E-2.

Level 1 Question 19: RCP Seal LOCA Model Used

In many PRAs, RCP seal LOCA is a significant contributor to the CDF either as an initiating event or as a system failure consequential to another initiator. While the submittal discusses RCP seal LOCA consideration, please provide the additional information requested:

a) **Please provide a discussion of the RCP seal LOCA model used. Include the probability vs. leakage rate vs. time data and any specific test results.**

The RCP seal LOCA model used for the Prairie Island IPE is the Westinghouse RCP seal LOCA model as described in WCAP-10541, Rev 2 which models core uncovery due to seal failure as a function of time from loss of seal cooling and includes the effects of restoration of offsite power. Two cases are used: one with RCS cooldown and one without. The model used represented the unqualified Westinghouse RCP seal O-ring material as this is what is installed in the RCP seals at Prairie Island.

b) **Provide a discussion of operator actions which are proceduralized and their timing in the event of a loss of one or the other method of RCP seal cooling.**

Component Cooling Water (CC) provides RCP thermal barrier and motor cooling to the RCPs at Prairie Island. Loss of CC will cause bearing temperatures to increase and generate numerous alarms in the control room. In the event of loss of component cooling water, the control room operators are directed to C14 AOP1, "Loss of Component Cooling" which provides guidance to the operators to trip any RCP that is without CC and whose bearing temperatures approach 200° F. The tripping of the RCPs by an operator is not explicitly modeled in the IPE but the loss of CC is. The contribution of loss of CC to the overall CDF is approximately 1%.

RCP seal injection provides the primary means of RCP seal cooling by providing a source of cool water to the RCP seals. In the event of loss of seal injection, various annunciators such as low RCP labyrinth seal ΔP, seal water injection low flow and RCP seal inlet or outlet high temperature alarms would alert the operators to the situation. Procedure C12.1 AOP1, "Loss of RCP Seal Injection", delineates the steps to follow. Loss of seal injection is not a serious condition as CC provides the necessary seal cooling by way of the RCP thermal barrier heat exchanger. Because of this, operator actions for this event were not modeled in the IPE.

In the unlikely event that all seal cooling is lost to the RCPs, operators are directed to procedure C3 AOP2, "Loss of RCP Seal Cooling",

where they are instructed to trip the reactor and trip the affected RCP if any RCP bearing temperatures reach 200° F. The operator tripping the RCPs following loss of seal cooling is not explicitly modeled in the IPE, although other functionally equivalent sequences are. If the operator did not trip the RCPs as directed, a small LOCA concurrent with a loss of RCP seal cooling would be the result. Safety Injection (SI) would not be available as the pumps require CC for lube oil cooling. This is the scenario of small LOCA sequence 5 which has a core damage probability of 6.5E-6/yr.

In the event of an SBO, the operator is directed by emergency procedure ECA-0.0, "Loss of All Safeguards AC Power", to attempt to restore power to the safeguards buses. In the event this fails, the operator is directed to depressurize the steam generators to 270 psig using the steam generator Power Operated Relief Valves (PORV) to cooldown and depressurize the Reactor Coolant System (RCS) and cause injection of the accumulators. This action is an attempt to makeup for inventory lost through RCP seal leakage and to reduce the temperature and pressure across the RCP seals to slow down the RCP O-ring degradation. MAAP runs have shown that the operator must perform this action within 4 1/2 hours of the SBO to prevent core damage if the turbine driven auxiliary feedwater pump is successful in running for 2 hours. The MAAP code used the most probable RCP seal leakage from the Westinghouse RCP seal LOCA model in WCAP 10541, Rev 2.

c) **Please provide an estimate of the impact of your assumptions regarding the RCP seal LOCA model on your results (CDF, significant sequences, system importance measures, and important operator actions).**

RCP seal LOCAs account for 79% of accident SEH class (see IPE submittal for a description of the listed accident classes) and are essentially 100% of accident classes BEH-NOPWR and BEH. This means that RCP seal LOCA contributes 9.5E-6/yr to the total CDF of 5E-5/yr or approximately 19%.

HRA Question 1: Treatment of Pre-Initiator Human Actions

In Section 3.3.5 the submittal mentions that human errors such as incorrect calibration of sensors or instruments were included as explicit events in system fault trees as was failure to restore components to service after their isolation for maintenance.

a) **Please provide a list of the types of pre-initiator human events in order of importance considered in the analysis.**

Pre-initiator human errors were modeled in the Prairie Island IPE fault trees as basic events and are referred to as Restoration Errors. They represent errors made in the restoration of systems that were out of service for maintenance. These basic events represent failure that could occur due to errors committed during maintenance or during the restoration of the system following maintenance (i.e., improper valve or switch positioning, etc.)

Table 2 below is a list of all events of this type that occur in the final cutsets for the IPE. They are shown with their probability, Fussell-Vesely value, and Risk Achievement Worth values. They are listed in descending order of their Fussell-Vesely value. Table 3 below is a complete list of all restoration errors that were included in the system fault trees. Of the restoration errors listed, only the 14 shown in Table 2 appear in the results. All others were truncated from the results.

The events in Table 3 that have 0 listed for their probability are events that were included in the model, but for which later it was determined that the operators would have indication that the system was not properly aligned and would correct the error. The probability of the error was therefore set to 0. A decision was made to keep the event in the model for use in possible sensitivity studies at a future date.

Table 2 - Pre-Initiator Restoration Errors Included in Final IPE Cutsets

Name	Description	Probability	Fus Ves	RAW
EFTBXXXXXZ	Train B AF Not Correctly Restored Following Test Or Maintenance	3.00E-03	3.89E-02	1.39E+01
EFT21XXXXZ	AF Train 21 Not Restored After Test Or Maintenance	3.00E-03*	2.87E-03*	1.96E+00*
EFTAXXXXXZ	Train A AF Not Correctly Restored Following Test Or Maintenance	3.00E-03	2.86E-03	1.95E+00
EFTB2XXXXZ	U2 Train B AF Not Restored Following Test Or Maintenance	3.00E-03	1.24E-03	1.41E+00
RTRAINBXXZ	Failure To Restore RHR Train B After Maintenance	5.43E-04	7.76E-04	2.43E+00
RTRAINAXXZ	Failure To Restore RHR Train A After Maintenance	5.43E-04	6.91E-04	2.27E+00
SPM121XXXZ	121 CL Pump Not Correctly Restored Following Test/Maintenance	5.60E-05	3.70E-04	7.60E+00
HTRAINBXXZ	SI Train B Failure To Restore After Maintenance	9.87E-05	7.05E-05	1.71E+00
Z12RHUNITZ	12 RHR Unit Cooler Not Correctly Restored Following Maintenance	9.96E-05	5.20E-05	1.52E+00
Z122CRMCHZ	122 Control Room Chiller Not Correctly Restored Following Maintenance	9.96E-05	4.51E-05	1.45E+00
HTRAINAXXZ	SI Train A Failure To Restore After Maintenance	9.87E-05	3.68E-05	1.37E+00
ABS27XXXXZ	Bus 27 Misaligned After Maintenance	1.10E-06	1.95E-05	1.87E+01
ABS25XXXXZ	Bus 25 Not Restored Correctly After Test Or Maintenance	1.10E-06*	1.89E-05*	1.82E+01*
Z11RHUNITZ	11 RHR Unit Cooler Not Correctly Restored Following Maintenance	9.96E-05	1.80E-05	1.18E+00

*See slight corrections to these values described in the response to part b) of this question.

Table 3 - All Restoration Errors Modeled in the IPE

Name	Probability	Description
ABS11XXXXZ	1.10E-06	Bus 11 Fast Transfer Knife Switches Left Open After T&M
ABS12XXXXZ	1.10E-06	Bus 12 Fast Transfer Knife Switches Left Open After T&M
ABS13XXXXZ	1.10E-06	Bus 13 Fast Transfer Knife Switches Left Open After T&M
ABS14XXXXZ	1.10E-06	Bus 14 Fast Transfer Knife Switches Left Open After T&M
ABS15XXXXZ	1.10E-06	Bus 15 Not Restored Correctly After Test Or Maintenance
ABS16XXXXZ	1.10E-06	Bus 16 Not Restored Correctly After Test Or Maintenance
ABS23XXXXZ	1.10E-06	Bus 23 Fast Transfer Knife Switches Left Open After T&M
ABS25XXXXZ	1.10E-06*	Bus 25 Not Restored Correctly After Test Or Maintenance
ABS26XXXXZ	1.10E-06*	Bus 26 Not Restored Correctly After Test Or Maintenance
ABS27XXXXZ	1.10E-06	Bus 27 Misaligned After Maintenance
ACB11231XZ	1.85E-06	Circuit Breaker 112-31 Left Open After Maintenance
ACB11236XZ	1.85E-06	Circuit Breaker 112-36 Left Open After Maintenance
ACB12231XZ	1.85E-06	Circuit Breaker 122-31 Left Open After Maintenance
ACB12234XZ	1.85E-06	Circuit Breaker 122-34 Left Open After Maintenance
ACB12236XZ	1.85E-06	MCC 1AC2 Circuit Breaker 122-36 Left Open After Maintenance
ACB12401XZ	0	12 Inverter CB-401 Misaligned After Maintenance
ACB12CB4XZ	0	12 Inverter CB-4 Misaligned After Maintenance
ACB13CB4XZ	0	13 Inverter CB-4 Misaligned After Maintenance
ACB14401XZ	0	14 Inverter CB-401 Misaligned After Maintenance
ACB14CB4XZ	0	14 Inverter CB-4 Misaligned After Maintenance
ACB21136XZ	1.85E-06	MCC 2AC1 Circuit Breaker 211-36 Left Open After Maintenance
ACB22136XZ	1.85E-06	MCC 2AC2 Circuit Breaker 221-36 Left Open After Maintenance
ACB28401XZ	0	28 Inverter CB-401 Misaligned After Maintenance
ACB28CB4XZ	0	28 Inverter CB-4 Misaligned After Maintenance
ACBCB4013Z	0	13 Inverter CB-401 Misaligned After Maintenance
ACBCB4017Z	0	17 Inverter CB-401 Misaligned After Maintenance
ACBCB4018Z	0	18 Inverter CB-401 Misaligned After Maintenance
ACBCB401XZ	0	11 Inverter CB-401 Misaligned After Maintenance
ACBCB4027Z	0	27 Inverter CB-401 Misaligned After Maintenance
ACBCB417XZ	0	17 Inverter CB-4 Misaligned After Maintenance
ACBCB418XZ	0	18 Inverter CB-4 Misaligned After Maintenance
ACBCB427XZ	0	27 Inverter CB-4 Misaligned After Maintenance
ACBCB4XXXZ	0	11 Inverter CB-4 Misaligned After Maintenance
ACBCKT14XZ	0	Panel 117 Circuit 14 Left Open After Maintenance
ACBCKT15XZ	0	Panel 117 Circuit 15 Left Open After Maintenance
ACBCKT16XZ	0	Panel 117 Circuit 16 Left Open After Maintenance

ACBCKT17XZ	0	Panel 117 Circuit 17 Left Open After Maintenance
ACBCKT20XZ	0	Panel 117 Circuit 20 Left Open After Maintenance
ACBCT1921Z	0	Panel 217 Circuit 19 Left Open After Maintenance
AGED1XXXXZ	4.73E-06	D1 Not Restored Correctly After Maintenance Or Testing
AGED2XXXXZ	4.73E-06	D2 Not Restored Correctly After Test Or Maintenance
AGED5XXXXZ	4.73E-06	D5 Not Restored Correctly After Test Or Maintenance
AGED6XXXXZ	4.73E-06	D6 Not Restored Correctly After Test Or Maintenance
ASM134BTXZ	0	Circuit Breaker 134BT Auto/Man Switch Misaligned In Manual
ASM13MXXXZ	1.10E-06	Circuit Breaker 13M Auto/Manual Switch Misaligned In Manual
ASM14MXXXZ	1.10E-06	Circuit Breaker 14M Auto/Manual Switch Misaligned In Manual
ASM156BTXZ	0	Circuit Breaker 156BT Control Switch Misaligned In Manual
ASM15MXXXZ	1.10E-06	Circuit Breaker 15M Auto/Manual Switch Misaligned In Manual
ASM16MXXXZ	1.10E-06	Circuit Breaker 16M Auto/Manual Switch Misaligned In Manual
ASW11INVXZ	0	11 Inverter Manual Bypass Switch Left In Alternate Position After Maintenance
ASW12INVXZ	0	12 Inverter Manual Bypass Switch Left In Alternate Position After Maintenance
ASW13INVXZ	0	13 Inverter Manual Bypass Switch Left In Alternate Position After Maintenance
ASW14INVXZ	0	14 Inverter Manual Bypass Switch Left In Alternate Position After Maintenance
ASW17INVXZ	0	17 Inverter Manual Bypass Switch Left In Alternate Position After Maintenance
ASW18INVXZ	0	18 Inverter Manual Bypass Switch Left In Alternate Position After Maintenance
ASW27INVXZ	0	27 Inverter Manual Bypass Switch Left In Alternate Position After Maintenance
ASW28INVXZ	0	28 Inverter Manual Bypass Switch Left In Alternate Position After Maintenance
BU1TRNAXXZ	5.31E-06	Unit 1 Train A CC Not Restored After Test Or Maintenance
BU1TRNBXXZ	5.31E-06	Unit 1 Train B CC Not Restored After Test Or Maintenance
CTRAINAXXZ	9.89E-05	Failure To Restore Train A CS After Corrective Maintenance
CTRAINBXXZ	9.89E-05	Failure To Restore Train B CS After Corrective Maintenance
CVHCS11XXZ	9.89E-05	Flow Diversion Through Valve CS-11 Back To 11 RWST
CVHCS12XXZ	9.89E-05	Flow Diversion Through Valve CS-12 Back To 11 RWST
DBC11XXXXZ	1.85E-06	11 Battery Charger Restoration Error After Maintenance
DBC12XXXXZ	1.85E-06	12 Battery Charger Restoration Error After Maintenance
DBC21XXXXZ	5E-06	21 Battery Charger Restoration Error After Maintenance

DBC22XXXXZ	1.85E-06	22 Battery Charger Restoration Error After Maintenance
EFT21XXXXZ	3.00E-03*	AF Train 21 Not Restored After Test Or Maintenance
EFTAXXXXXZ	3.00E-03	Train A AF Not Correctly Restored Following Test Or Maintenance
EFTB2XXXXZ	3.00E-03	U2 Train B AF Not Restored Following Test Or Maintenance
EFTBXXXXXZ	3.00E-03	Train B AF Not Correctly Restored Following Test Or Maintenance
F13CDPMPXZ	2.00E-04	13 Condensate Pump Not Correctly Restored Following Maintenance Or Test
HTRAINAXXZ	9.87E-05	SI Train A Failure To Restore After Maintenance
HTRAINBXXZ	9.87E-05	SI Train B Failure To Restore After Maintenance
QSM46259XZ	0	Operator Leaves CS-46259 In Close Position
QSM46260XZ	0	Operator Leaves CS-46260 In Close Position
QSMHC431KZ	0	Operator Leaves 1HC-431k In Manual
RTRAINAXXZ	5.43E-04	Failure To Restore RHR Train A After Maintenance
RTRAINBXXZ	5.43E-04	Failure To Restore RHR Train B After Maintenance
SPD12XXXXZ	2.45E-05	12 CL Pump Not Correctly Restored Following Test/Maintenance
SPD22XXXXZ	2.45E-05	22 CL Pump Not Correctly Restored Following Test/Maintenance
SPM121XXXZ	5.60E-05	121 CL Pump Not Correctly Restored Following Test/Maintenance
Z11RHUNITZ	9.96E-05	11 RHR Unit Cooler Not Correctly Restored Following Maintenance
Z122CRMCHZ	9.96E-05	122 Control Room Chiller Not Correctly Restored Following Maintenance
Z12RHUNITZ	9.96E-05	12 RHR Unit Cooler Not Correctly Restored Following Maintenance

*See slight corrections to these values described in the response to part b) of this question.

b) Since the submittal does include pre-initiator human actions, it is important to describe the process used to identify and select the pre-initiators involving miscalibration of instrumentation and the failure to properly restore equipment to service after test or maintenance. The process used to identify and select instrumentation calibration related human action events may include the review of calibration procedures and discussions with appropriate plant personnel on interpretation and implementation of the plant's calibration procedures. For assessing the failure to restore equipment to service after test or maintenance, the process may include the review of maintenance and test procedures and discussions with appropriate plant personnel on the interpretation and implementation of the plant's test and maintenance procedures. Please provide a description of the process that was used to identify pre-initiator human actions involving miscalibration of instrumentation and failure to restore equipment to service after test or maintenance. In addition, please provide examples illustrating the processes using several relatively important pre-initiator human actions.

Section 3.3.5 of the IPE submittal deals with the treatment of common cause failures. The statement in the report that "incorrect calibration of sensors or instruments were included as explicit events in system fault trees" requires further explanation. Some human errors, such as miscalibration of sensors, were treated through the inclusion of common cause failure modeling for the sensors themselves. Common cause failures of all sensors that can be affected by the miscalibration error(s) were analyzed. Calibration errors can affect groups of instruments that perform identical functions, since calibration is usually done on a group of instrumentation at a time with guidance from a calibration procedure. Since common cause failure of a group of instruments is explicitly modeled, it is used to represent failures due to miscalibration, which are similar in their effect on a group of instruments. Common cause failure of sensors were determined to be insignificant contributors to plant risk. This is due to the fact that safety systems which provide for reactor trip, emergency makeup and containment heat removal functions are initiated by a variety of signals from different groups of instruments. Therefore, loss of multiple instrumentation groups would be required to result in the loss of all signals for automatic initiation of these safety functions. This is also the case for miscalibration errors, since multiple failures of other instrumentation are required coincident with the instrument group that was miscalibrated in order to fail the safety functions.

The following process was used to incorporate restoration from maintenance and testing into the fault trees. A review of the testing and maintenance procedures was performed to determine if the component is effectively disabled and cannot automatically be restored or realigned on an appropriate initiating signal. If this was the case then a basic event was added to the fault tree to reflect the potential for failing to restore the component to its appropriate configuration. (The response to HRA Question #3 describes other criteria that were used in determining whether pre-initiator human events were modeled in the fault trees.) If the maintenance procedure included a verification of

component status then a relatively low failure to restore probability was assigned (0.003). Without such a verification, a higher failure probability would have been used (0.01). Other factors, such as maintenance frequency and duration, test frequency and interval, refueling outage frequency, time from completion of the corrective maintenance to the retest of the component were also included in the development of the probabilities reported in Tables 2 and 3.

Table 2 shows the most important pre-initiator events calculated in the IPE analysis. The event with the highest Fussel-Vesely ranking was EFTBXXXXXZ, Train B AF Not Correctly Restored Following Test Or Maintenance. The following describes the calculation of the restoration error probability for this event:

Unavailability = (CM*E*MT) + [(PM+T+RF)*E*TI/2] from ASME paper 91-JPGC-NE-11 (McClymont/Rohrer)

where CM = Corrective maintenance frequency (per hour)

E = Human error probability

MT = Time from completion of corrective maintenance to the retest of the component (hours)

PM+T = Frequencies of preventive maintenance and testing which remove component from service (per hour)

RF = Refueling outage frequency (per hour)

TI/2 = One-half of the system test interval (regularly performed test which would verify the equipment functions properly)

For this case,

CM = 7.79E-5/hr from IPE data collection

E = 0.003 for procedures that include component status verification

MT = 4 hours

PM+T = 2.69E-3/hr from IPE data collection

RF = 9.13E-5/hr

TI/2 = 30 days/2 = 360 hours for Surveillance Procedure SP-1100

Unavailability = (7.79E-5 * 0.003 * 4) + [(2.69E-3 + 9.13E-5)* 0.003 * 360]

= 3.00E-3

Another example is RTRAINBXXZ, Failure to Restore RHR Train B after Maintenance. The following describes the calculation of the restoration error probability for this event:

For this case,

CM = 2.27E-5/hr from IPE data collection

E = 0.003 for procedures that include component status verification

MT = 4 hours

PM+T = 4.11E-4/hr from IPE data collection

RF = 9.13E-5/hr

TI/2 = 30 days/2 = 360 hours for Surveillance Procedure SP-1089

Unavailability = (2.27E-5 * 0.003 * 4) + [(4.11E-4 + 9.13E-5)* 0.003 * 360]

= 5.43E-4

Since preventive maintenance frequency is included in the restoration error calculation, the errors described in the response to Level 1, Question 1 would affect these calculations as well. The probabilities of two values in Table 2, EFT21XXXXZ and ABS25XXXXZ, were recalculated. The corrected probabilities and importance measures for these events are tabulated below:

Name	Description	Probability	Fus Ves	RAW
EFT21XXXXZ	AF Train 21 Not Restored After Test Or Maintenance	3.11E-03	2.98E-03	1.96E+00
ABS25XXXXZ	Bus 25 Not Restored Correctly After Test Or Maintenance	1.64E-06	2.82E-05	1.82E+01

These changes do not have any effect on the core damage frequency. Note that event ABS26XXXXZ (Bus 26 Not Restored Correctly After Test or Maintenance) on Table 3 would also be impacted by these changes. Its probability should also have been 1.64E-6. However, this slight increase in its probability would not have significantly increased its importance to the results (would have remained truncated), since it does not power the risk-significant loads that Bus 25 does (Bus 25 powers the 21 motor-driven AFW pump).

HRA Question 2: Screening Values for Pre-Initiator Human Events

The submittal does not provide all the screening values used for pre-initiator human events or the basis for the values provided. Screening values for some of the typical operator actions are given in Table 3.3-10.

a) **Please provide all of the screening value(s) used and the basis for the value(s); i.e., provide the rationale of how the selected screening value(s) did not eliminate (or truncate) important pre-initiator human events.**

Table 3 for question 1a above provides a complete list of pre-initiator human error that were included in the IPE fault tree models. This list also includes the values calculated for each event. The events in the list that have 0 listed for their probability are events that were included in the model, but later it was determined that the operators would have indication that the system was not properly aligned and would correct the error. The probability of the error was therefore set to 0. A decision was made to keep the event in the model for use in possible sensitivity studies at a future date.

The values listed on the table are the final values used. No screening values were used when modeling pre-initiator human errors. Pre-initiator human errors were identified in the process of developing the system fault trees and then values were calculated for them based on actual plant corrective and preventive maintenance frequencies where possible, or based on generic maintenance frequencies and these values were then used in the quantification of the IPE.

b) **In addition, please provide the list of all pre-initiator human actions initially considered and all those screened.**

Tables 2 and 3 of HRA Question #1 a) above provides a complete list of all pre-initiator human actions that were included in the IPE model. Those events that have a 0 listed for their probability were determined to be inappropriate due to indications the operators would have that an error occurred. Their probability was set to 0 but they were retained in the model for possible use in sensitivity studies. Of these 14 appear in the results, the others appear in cutsets below the truncation limit.

HRA Question 3: Recovery Factors Applied to Pre-Initiator Human Events

The submittal does not clearly identify actual recovery factors applied in quantifying the pre-initiator events. Factors that are used to modify the generic basic human error probabilities (BHEP) can include, for example, post-maintenance or post-calibration tests, daily written checks, independent verification checks, administrative controls, etc. If they were used, please provide a list of pre-initiator recovery factors considered, their associated values, and provide specific examples illustrating their use. Also, if used, please provide a concise discussion of the justification and process that was used to determine the appropriateness of the recovery factors utilized.

Pre-initiator human errors were included in the IPE model as basic events in the system fault trees. As the analyst developed the fault tree one potential

failure mode for components considered was pre-initiator human errors. When the analyst considered pre-initiator human errors to be a valid failure mode for the equipment being modeled, then that failure mode was included in the event tree. If, based on his review (described below), the analyst did not consider pre-initiator human errors to be a valid failure mode, it was not included in the fault tree.

Several criteria were used to determine the applicability of pre-initiator human errors. The most important consideration was the operating status of the system. If a system is normally running when the plant is at power it was modeled as such. In that case a pre-initiator human error is not a credible failure mode since the system is already operating properly. If a system must start operation or change operating mode in response to the initiating event then a pre-initiator human error may be a credible failure mode and would be modeled.

Another important criteria used was the indications that the operations staff would have that an error had been made. If there would be indication in the control room, such as valve position indication, that would alert the operators to the error the pre-initiator human error was not included. Also, if there would be indication in some other area of the plant that is normally toured by an operator in the performance of rounds, the error was only considered for the interval of time between rounds (usually 4 hours). It was assumed that the operator would identify and correct the problem during the rounds.

Other criteria, such as those listed in the question, were used by the analyst to determine the applicability of pre-initiator human errors. The analyst reviewed operating procedures, maintenance procedures, administrative control documents, and emergency operating procedures in the process of developing the system fault tree. If these documents showed that the system was susceptible to pre-initiator human error induced failures then that failure mode was modeled.

After the system fault trees were developed and all pre-initiator human errors were identified and in the model values were calculated for them. The calculation included errors committed during corrective and preventive maintenance and testing, errors committed while restoring a system to service after maintenance and errors committed while restoring the system following a refueling outage. Plant specific maintenance frequencies were used for systems where plant specific values were available.

HRA Question 4: Dependencies Associated With Pre-Initiator Human Errors

It is not clear from the submittal how dependencies associated with pre-initiator human errors were addressed and treated. There are several ways dependencies can be treated. In the first example, the probability of the subsequent human events is influenced b the probability of the first event. For example, in the restoration of several valves, a bolt is required to be "tightened." It is judged that if the operator fails to "tighten" the bolt on the first valve, he will subsequently fail on the remaining valves. In this example, subsequent HEPs in the model (i.e., representing the second valve) will be adjusted to reflect this dependence. In the second example, poor

lighting can result in increasing the likelihood of unrelated events; that is, the poor lighting condition can affect different operators' abilities to properly calibrate or to properly restore a component to service, although these events are governed by different procedures and performed by different personnel. This type of dependency is typically incorporated in the HRA model by "grouping" the components so they fail simultaneously. In the third example, pressure sensor "x" and "y" may be calibrated using different procedures. However, if the procedures are poorly written such that miscalibration is likely on both sensor "x" and "y", then each individual HEP in the model representing calibration of the pressure sensors can be adjusted to reflect the quality of the procedures. Section 3.3.4 of the submittal states the following human dependency related information, "the cutsets were reviewed after sequence quantification and when more than one human error appeared in the same cutset, either independence of the human actions was confirmed, or a change was made to correctly model dependence between the human errors." Please provide a concise discussion of how dependencies were addressed and treated in the pre-initiator HRA such that important accident sequences were not eliminated. If dependencies were not address, please justify.

The quote from section 3.3.4 of the IPE submittal is discussing post-initiator human errors. Adjustments were made for dependencies in individual cutsets when more than one post-initiator human error occurred in a single cutset. This was not however done for pre-initiator human errors.

Pre-initiator human errors were considered independent events. Work on these systems is done independently of other work. The systems are tested and proven operable before they are placed back into service and most of these systems are tested monthly or quarterly to prove that they are operable and capable of performing their safeguards function. Also, work is done on only one train of a system at a time. There may be several instruments that are worked on for a procedure, but they are all on the same train. If any one of them were to fail, the whole train would fail. Therefore, any common mistake the maintenance person made would affect only that train and would have no greater affect than a mistake that affected only one instrument.

The procedures that are used by the maintenance personnel are reviewed for errors prior to each use. The procedures are kept current to reflect all changes to systems and operating practices and to include lessons learned from previous mistakes. Any weakness identified in one procedure is corrected in that procedure and is looked for in other procedures as well.

The values used for pre-initiator human errors were calculated for entire trains of equipment. The calculation includes both corrective and preventive maintenance and is based on actual plant historic maintenance frequencies and planned maintenance intervals.

<u>HRA Question 5: Post-Initiator Human Error Types</u>

The Submittal does not clearly describe the type of human errors considered for each post-initiator human event identified. For example, a human event identified may be the failure to feed and bleed, while the types of human errors considered may involve failure to open the correct valve (error of

omission), or opening an incorrect valve (error of commission). No mention of types of human errors was found in the submittal's section 3.3.4. Please identify what types of human errors were considered for each post-initiator human event identified.

In general, error of commission was not explicitly modeled in the IPE. All post-initiator human error events included in the IPE represent errors of omission. The five most important human actions in the IPE were analyzed using the THERP methodology as described in NUREG/CR-1278, "The Handbook for Human Reliability Analysis with Emphasis on Nuclear Power Plant Applications". Error of commission was considered in the THERP analysis performed for the five human actions, but the overall human action was actually an error of omission type of human error. Error of commission was not explicitly modeled anywhere else in the IPE.

HRA Question 6: Response-Type Versus Recovery-Type Human Actions

The submittal does not clearly describe the method used to identify and select response type actions and recovery type actions for analysis. The method utilized should confirm the plant emergency procedures, design, operations and maintenance procedures were examined and understood to identify potential severe accident sequences. The submittal is not clear on the identity of the response type actions and recovery actions used (see request below). Also, the method used was not addressed. Please provide a description of the process that was used for identifying and selecting the response and recovery actions evaluated.

Response type actions were modeled only for those systems which were not automatic, but required operator action for system or component initiation. Response type actions were chosen where clear procedural guidance existed for the operator, including information contained in normal, abnormal and emergency procedures. Recovery actions on the other hand, were those actions in which procedural guidance may not be available, but the operators training or knowledge are assumed to lead him to perform the required action. Recovery actions include repair activities or local operation of systems and components when remote operation is not possible.

HRA Question 7: Screening of Post-Initiator Human Actions

It is not clear from the submittal what screening values were used for post-initiator human actions and the bases for the values.

a) **Please provide the screening value(s) used and the basis for the value(s), i.e., provide the rationale of how the selected screening value did not eliminate (or truncate) important post-initiator human events.**

All modeled post-initiator operator actions and their values used in the quantification are listed in Tables 3.3-3 and 3.3-10 of the IPE submittal. All operator recovery actions and their values used in the quantification are listed in Table 3.3-4.

A number of methods were employed to provide assurance that screening values did not eliminate or truncate important human events. First, credit given for operator action was limited in the model to only those actions which are not backed up by an automatic signal. Limiting the number of operator events modeled inherently limits the potential for loss of important operator actions through truncation. Next, the IPE was quantified using low truncation values throughout the analysis, including support and frontline systems fault trees, functional event tree headings and accident sequences (minimum of four orders of magnitude below the core damage frequency - 1E-9).

b) **Also please provide the list of all post-initiator human actions initially considered and all those screened.**

All initially considered post-initiator human actions are listed in Tables 3.3-3, 3.3-4, and 3.3-10 of the submittal (none were screened).

HRA Question 8: Available and Required Time Estimates and Bases for Several Human Events

In applying performance shaping factors (PSFs), the consideration of time is important. The submittal is not clear on how available time and "required" time were calculated for the various post-initiator human events. "Required" time is the time needed for the operator to detect, diagnose, and perform the necessary actions. Section 3.3 ' of the submittal and Tables 3.3-5 and 3.4-6 provide a "diagnosis time" but no available time or "required" time. For several of the important post-initiator human events examined, provide the available and "required" times estimated for the operator action and the bases (e.g., calculated from simulator exercises, estimated from walkdowns) for the time chosen. Also provide illustrations of how different times were calculated for the same task but in different sequences.

All post-initiator human errors were initially calculated using screening values as described in the IPE submittal (Section 3.3.4.4). All the important post-initiator human errors were then recalculated using the method described in NUREG/CR-4772 for deriving nominal human error probability estimates (referred to hereinafter as the "ASEP" method). A more refined estimate was then calculated for the five most important human errors using THERP (NUREG/CR-1278), but the timing for the refined estimates were still based on the analysis performed as a part of the previous ASEP calculation. The ASEP approach to deriving post-initiator human error probabilities is to divide each human action into diagnosis and post-diagnosis tasks, derive the HEP estimates for each, and derive a total HEP by summing the separate contributions. The diagnosis HEP is derived by considering the time available for the operator to diagnose the situation in order to carry out the necessary tasks. The HEP for post-diagnosis tasks is derived by evaluating the probability of mistakes in performing each task necessary to operate the system or components covered by the human action.

The equation used for the timing portion of the ASEP analysis is given below.

$$T_d = T_m - T_o - T_a$$

where,

T_d = Time available for diagnosis
T_m = Latest time event can be completed
T_o = Time compelling signal is received
T_a = Time required to complete action

The determination of the time required to complete an action was generally performed using the guidance in Table 8-1 of NUREG/CR-4772. Time estimates outside the control room were based on estimates from an engineer that recently held an SRO license at Prairie Island. Confirmatory walkdowns were performed on selected local operator actions and control room panels to verify assumptions made during the human reliability analysis.

The Modular Accident Analysis Program (MAAP) was used to determine the latest time an operator action could be completed, and when the compelling signal would have been received, if the information could not be found in existing plant documents. MAAP 3.0B, PWR Revision 19.0 was used with best-estimate, Prairie Island specific parameters.

The table below provides information on four specific post-initiator human events. Failure to restore main feedwater or initiate bleed and feed are typical of calculations based on the ASEP method. To illustrate how different times were calculated for the same task but in different sequences, event timing is provided for a classic task in 2 different situations. The two situations are large and medium LOCAs. The task is to recognize that a LOCA is in progress prior to receiving a low RWST level alarm. This diagnosis HEP is a part of the transfer to recirculation calculation using THERP.

In general, relatively conservative times were calculated and used in all accident sequences. Bleed and Feed could have used different diagnosis times for different accident sequences. For example, the need for bleed and feed in some accident sequences occurs relatively early in the accident sequence (about 40 minutes after the initiating event). In other accident sequences, the need for bleed and feed does not occur until decay heat levels are lower (station blackout with restoration of AC power). Rather than distinguish between these types of accident sequences, a relatively conservative time for bleed and feed was applied to them all. This was done by assuming secondary cooling was lost at time zero for all accident sequences in which bleed and feed were credited. There are a few cases in the IPE where different times were calculated for the same task. The two tasks associated with LOCAs in the table below are examples of that.

Task	T_o		T_m		Ta		T_d	
	Value	Basis	Value	Basis	Value	Basis	Value	Basis
Medium LOCA			41	A			30	B
Large LOCA			21	A			15	B
Restore Main Feedwater	10	C	58	D	9	F	39	G
Bleed and Feed	10	C	43	E	11	F	22	G

Notes for Value column:

1. All times in minutes.
2. No values were given in the T_o and T_a columns for the two LOCA examples due to slight differences in how diagnosis time is estimated between the THERP analysis and the ASEP analysis. However, the concept for determining time for diagnosis is similar.

Notes for Basis Column:

A. This is the amount of time after the initiating event that the low RWST level annunciator alarms. The value is based on a MAAP run.
B. This value represents a conservative estimate of the amount of time the operator has to diagnose that a LOCA is taking place prior to the low RWST level annunciator alarming.
C. Estimate based on ASEP Table 8-1 (NUREG/CR-4772) and MAAP run.
D. Estimate based on MAAP run that shows core damage does not occur if feedwater is restored 15 minutes after steam generator dryout.
E. Estimate based on when steam generator dryout occurs in a MAAP run.
F. Estimate based on ASEP Table 8-1 and consultation with previously SRO licensed engineer.
G. Value calculated from other three values in row as described above.

HRA Question 9: List and Discuss Performance Shaping Factors (PSFs)

It is not clear from the submittal what plant-specific PSFs were used to modify the BHEP and what the bases were for reducing the HEPs through their application. The plant-specific information could include the size of the crew, availability of procedures, time available and time required, etc. The process could include an examination of procedures, training, human engineering, staffing, communication, and administrative controls. No mention of plant-specific PSFs were found in the submittal. Please provide a list of the types of plant-specific PSFs considered and their values, and discuss by way of example how these PSFs were used to modify the BHEPs of important post-initiator human events.

A review of section 3.3.4.4 of the submittal revealed that the performance shaping factors were discussed for the HRA screening process and THERP analysis, but were not included in the discussion of ASEP. Since ASEP was used for most of the important human error calculations, the discussion that

follows will concentrate on the ASEP calculations. Unless stated otherwise, all tables and figures referred to below are from NUREG/CR-4772.

The diagnosis portion of the HEPs are based on Figure 8-1, "Nominal Diagnosis Model", except when Table 8-4, "The Annunciator Response Model", is more appropriate. The value is determined by calculating the diagnosis time and then choosing the appropriate curve on Figure 8-1 (upper bound, median or lower bound). The diagnosis time calculation is described in the response to HRA Question #8 and #15. Table 8-1, "Procedure for Nominal HRA of Post-Accident Tasks" and Table 8-3, "Guidelines for Adjusting Nominal Diagnosis HEPs", were used to determine which curve on Figure 8-1 to use. The factors that are considered when selecting which curve to use can be considered plant-specific performance factors. The factors are:

1. Is the event covered in training?
2. How often is the event practiced during simulator training?
3. Is the event covered in symptom-orientated EOPs?

A value can not be assigned to the above factors because they only affect which of the three curves in Figure 8-1 are used.

The post-diagnosis portion of the HEPs are based on table 8-5, "Assessment of Nominal HEPs for Post-Accident Post-Diagnosis Actions". The performance shaping factors included in this table, and therefore our calculations, are whether:

1. There are written procedures
2. The procedural actions are dynamic or step by step
3. Stress is moderately high or extremely high
4. Size of crew and time allow credit for recovery (items 6, 7 & 8 of Table 8-5)

The values associated with these factors are given in Table 8-5 of the NUREG. For example, the value associated with performing a critical action as part of a step-by-step task done under moderately high stress is 0.02, where the value associated with performing a critical action as part of a dynamic task done under extremely high stress is 0.25.

Example calculations for two of the important HEPs are given below.

<u>Restore Main Feedwater</u>

1. Diagnosis HEP: For the case described in the response to HEP Question #8 the diagnosis time is 39 minutes. Using the median curve in ASEP Figure 8-1, the diagnosis error is 0.0005.

2. Post Diagnosis HEP: The post diagnosis HEP calculation is based on ASEP Table 8-5. The actual calculation is 0.02 x 0.2 x 1.0 x .5 = 0.002, where,

   0.02 is operator failure to perform single task of step by step procedure under moderate stress
   0.2 is Shift Supervisor failure to recover step by step action

1.0 is failure of other control room operator to recover missed action
0.5 is failure of shift manager to call for action (dynamic action under moderate stress).

3. Total median HEP = 0.002 + 0.0005 = 0.0025. The total mean HEP is 0.004.

Bleed and Feed

1. Diagnosis HEP: For the case described in the response to HEP Question #8 the diagnosis time is 22 minutes. ASEP Figure 8-1 lower bound is used per Table 8-1, item 9d because bleed and feed is in the symptom orientated portion of the Prairie Island EOPs (heat sink red path) and is well covered in training. This results in a diagnosis error of 0.0005.

2. Post Diagnosis HEP: The post diagnosis HEP calculation is based on ASEP Table 8-5. The actual calculation is (0.02 x 6) x 0.2 x 1.0 x 1.0 = 0.024, where,

   0.02 is operator failure to perform single task of step by step procedure under moderate stress
   6 is the number of task the operator must perform to complete the action
   0.2 is Shift Supervisor failure to recover step by step action
   1.0 is failure of other control room operator to recover missed action
   1.0 is failure of shift manager to call for action (no time available for second recovery).

3. Total median HEP = 0.024 + 0.0005 = 0.024. The total mean HEP is 0.039.

HRA Question 10: Response-Type Versus Recovery-Type Human Actions

The submittal is not clear whether response type actions and recovery type actions were considered. Response type actions include human actions performed in response to the first level directive of the EOPs. For example, suppose the EOP directive instructs the operator to determine reactor water level status, and another directive instructs actions - reading instrumentation to determine level and actuating system X to maintain level - are response type actions. Recovery type actions include those performed to recover a specific failure or fault and may not be "proceduralized". For example, suppose the EOP directive instructs the operator to maintain level using system X, but the system fails to function and the operator then attempts to recover it. This action - diagnosing the failure and then deciding on a course of action to "recover" the failed system - is a recovery type action. The submittal is not clear on the identity of the response and recovery actions. Please provide separate lists of the response and recovery actions considered in the analysis. If response or recovery actions were not considered, please justify. If response and recovery actions are used, are they proceduralized? If not, please justify any credit taken for such actions.

Response actions are listed in Tables 3.3-3 and 3.3-10 of the IPE report while recovery actions are listed in Table 3.3-4 of the IPE report. As stated in question 6 above, response actions are those actions taken in response to

written procedures such as normal, abnormal and emergency operating procedures. Recovery actions are those actions in which procedural guidance may not be available but an operators training is assumed to be sufficient to enable him to perform the required action. Recovery actions were only added to cutsets in which it was apparent that an operator would have sufficient time to perform the additional action. MAAP runs were used to provide the timing in which the recovery action would need to be performed. All of the recovery probabilities were derived from NSAC-161, "Faulted Systems Recovery Exper. nce".

Local recovery of valves that had failed to open or close was only applied if there was control room indication that the valve was in the incorrect position and the valve was easily accessible to operators. In these cases, the non recovery probability applied was 0.25. In the case where equipment such as pumps were recovered, the same criteria was applied as for valves, but the non recovery probabilities were approximately 0.5.

There was one action listed in Table 3.3-4 of the IPE report that was calculated differently. This actions was H8182XXRCV (Local Recovery of MV-32079 or MV-32080 after MV-32081 and MV-32082 Have Both Failed to Open). This event involves the control room operators following an EOP checklist in the control room following a safety injection (SI) signal. This checklist verifies that all of the automatic actions that should occur following a SI signal have occurred. In this case an automatic action has not occurred and the operator is modeled as completing the action by opening one of two motor operated valves from the control room. This action was calculated using a screening HEP value rather than a non recovery probability.

HRA Question 11: Treatment of Post-Initiator Human Error Dependencies

It is not clear from the submittal how dependencies were addressed and treated in the post-initiator HRA. The performance of the operator is both dependent on the accident under progression and the past performance of the operator during the accident of concern. Improper treatment of these dependencies can result in the elimination of potentially dominant accident sequences and, therefore, the identification of significant events. Section 3.3.4 of the submittal provides the following human dependency related information, "The cutsets were reviewed after sequence quantification and when more than one human error appeared in the same cutset, either independence of the human actions was confirmed, or a change was made to correctly model dependence between the human errors." Please provide a concise discussion and examples illustrating how dependencies were addressed and treated in the post-initiator HRA such that important accident sequences were not eliminated. There are several ways post-initiator dependencies can be treated, namely, modeled in fault trees and event trees. If the submittal did not address dependencies in the quantification, please justify. The discussion should address the two models below:

> **Human events are modeled in the fault trees as basic events such as failure to manually actuate. The probability of the operator to perform this function is dependent on the accident in progression - what symptoms are occurring, what other activities are being performed (successfully and unsuccessfully), etc. When the sequences are**

quantified, this basic event can appear, not only in different sequences, but in different combinations with different systems failures. In addition, the basic event can potentially be multiplied by other human events when the sequences are quantified which should be evaluated for dependencies.

Human events are modeled in the event trees as top events. The probability of the operator to perform this function is still dependent on the accident progression. The quantification of the human events needs to consider the different sequences and the other human events.

Post-initiator human events were modeled in the IPE at both the fault tree level (as basic events) and the event tree level (in the event tree heading quantification).

In the fault trees, dependencies were addressed in two ways: dependencies based on the initiating event were addressed through assignment of separate basic events for the same operator action. For example, separate basic events were modeled for failure of the operator to perform transfer to recirculation depending on whether the transfer was to high head recirculation or to low head recirculation. The transfer is performed using the many of the same emergency procedures, however, the operator is under different time constraints and different stress levels. Similarly, different basic events are required (and were modeled) for failure of the operator to restore main feedwater if auxiliary feedwater is unavailable, depending on whether an S-signal is present. The S-signal trips the feedwater pumps and condensate pumps, and causes a feedwater isolation which must be reset at the control board. Reestablishing feedwater under transient conditions (no S-signal) requires only reopening the feedwater bypass control valves from the control board. Operator stress levels would also be different for these two events.

The reference made to Section 3.3.4 of the submittal addresses the other concern with operator actions when modeled in fault trees, namely multiplication of human events together when the sequences are quantified. For example, many cutsets involved the combination of operator errors (failure to restore main feedwater - no S-signal) with (failure to align the Unit 2 motor driven auxiliary feedwater pump to Unit 1 - no S-signal). In this case, the operator would attempt to restore main feedwater before attempting to locally, manually cross-tie the Unit 2 motor driven auxiliary feedwater pump. However, since both actions involve control room manipulations and both are directed from the same emergency procedure, the second action (the Unit 2 pump cross-tie) was given a higher probability (a conditional probability) of failure than would be applied if no other operator failure had occurred.

As noted in HRA Question #7, the process used to keep multiple operator actions from being truncated was as follows. First, only those operator actions necessary for system operation were included as a part of the accident sequence quantification. Operator actions in response to a failed automatic signal and repair actions were added following cutset generation. Next, truncation was very low throughout the quantification (at or less than 1E-9) including the fault trees, event tree headings and the accident sequences.

In the event trees, operator actions were included as part of the event tree heading quantification. However, human error dependencies on the events in progress and on other human errors were taken into account. For example, this was done in the steam generator tube rupture event tree, if secondary cooling (through the steam generators) and short term inventory (high head injection) functions are available, and the intact steam generator is isolated from the ruptured steam generator. In this case, operator action to perform RCS cooldown and depressurization is necessary to stop the primary to secondary leak before the ruptured steam generator overfills, to preserve the secondary side integrity (prevent development of a large release path to the environment). If this action fails, then operator action to perform RCS cooldown and depressurization is again required, to stop the leakage and to achieve RHR shutdown cooling conditions before the RWST is depleted. Given that the first chance for the operator to perform the cooldown and depressurization had failed, a higher probability (a conditional probability) of operator failure was applied than would have been if no previous operator failure at the task had occurred.

For those events that received detailed human error analysis (Table 3.3-3 of the IPE report), dependency between the actions of the various control room crew personnel were also taken into account. This is discussed further in the response to HRA Question #9.

Note that, although this discussion centers on the operator failures, failures of equipment required to perform these operations was also included in the event tree heading development. Therefore, equipment which had caused a failure of the former cooldown/depressurization function would also cause the failure of the latter cooldown/depressurization function.

HRA Question 12: Discuss Key HRA Assumptions Including Walkdowns and Operator Interviews

Please discuss the process used to assure that key HRA assumptions about operator actions, information available to operators, plant environment, etc., represent the conditions in the as-built, as-operated plant. In particular, please discuss information related to interviews with operators and plant walkdowns.

All important human error calculations were performed while following through the current plant procedures. They were all reviewed by a previously SRO licensed engineer. The human factors review in support of the HRA included the following three tasks:

1. Review of the "Control Room Design Review" documents for factors not previously considered in the Prairie Island PRA HRA.
2. Walkdowns of selected local operator actions and control room panels to verify assumptions made during the HRA, and to look for factors not previously considered in the HRA.
3. Interviews with control room personnel to discuss roles and responsibilities of specific actions important to the PRA.

The walkdowns of the plant included both a control room walkdown, and plant walkdowns for local actions. This included a walk through of the operator

actions, taking into account timing, distances, environmental factors, required controls, location of indications, etc. Actions and procedures verified include:

1) Crosstie of the AFW Pumps from Unit 2 to Unit 1 (local actions).
2) Manual operations for High Head and Low Head Recirculation (local actions).
3) Feed and Bleed control room actions.
4) High Head and Low Head Recirculation control room actions.
5) Steam Generator Tube Rupture control room actions for procedures 1E-3, 1ECA-3.1, and 1ECA-3.2.
6) Response to loss of Reactor or Secondary Coolant procedure 1E-1.
7) Crosstie of Unit Emergency Power during an SBO, control room actions.

Interviews with operations personnel included informal interviews with one Reactor Operator (RO), the Shift Supervisor (SS), and the Shift Manager (SM). Additionally, when required, questions were raised to other control room personnel and a local auxiliary building operator. NSP PRA staff familiar with the plant operations also assisted in the walkdowns, and answered questions about equipment location and local operations.

Most questions during the interviews dealt with operator actions and timing of the key actions discussed above. Walk through of all of the above actions were performed and the operations personnel were questioned about critical steps during the walk through. Additionally, the SM was questioned in length about balancing the roles of both the STA and Emergency Director (ED) during the initial phases of an accident.

HRA Question 13: Justify HRA Modeling Assumptions Regarding Symptom-Based Procedures

Please provide specific information describing the process used to access the use of symptom-based procedures in the current plant. The information should focus specifically on justification of assumptions used in the HRA modeling.

Most of the important human error probabilities were calculated using the ASEP methodology described in NUREG/CR-4772. As is discussed in NUREG/CR-4772, Table 8-1, item 9.d, if symptom-oriented EOPs are available and if the criteria listed in 9.d are met, the diagnosis HEP is adjusted downwards by using HEPs from the lower bound curve given in Figure 8-1 of the NUREG.

HRA Question 14: Sequences Screened Due to Credit for Human Recovery Actions

As requested in NUREG-1335 "Individual Plant Examination: Submittal Guidance", please provide a listing and a discussion of any sequences that drop below the applicable core damage screening criteria because the frequency has been reduced by more than an order of magnitude by credit taken for human recovery actions (not to exceed 50 of the most significant sequences).

Please note that the Prairie Island IPE reported all functional accident sequence types regardless of whether they met the screening criteria of NUREG/CR-1335. The discussion includes identification of important operator actions for each functional sequence type. In addition, Section 3.4.2.16 of the IPE report contains a discussion of the method used to determine which core damage sequences had been reduced by an order of magnitude due to recovery actions. Table 3.4-3 of the IPE report lists the two sequences whose magnitude had been reduced by an order of magnitude and Table 3.3-4 of the IPE report provides the values of the recovery actions, the time available to perform the action and the complexity of the action.

Finally, detailed HEPs were performed on all operator actions which by themselves contribute to accident sequences totaling 1% of the core damage frequency or could result in an accident sequence frequency of 1E-6/yr if the action was not taken (equivalent to Birnbaum importance of 1E-6/yr). Human actions meeting this criteria are listed in Table 3.3-3.

HRA Question 15: Discuss How Diagnosis Was Considered in the HRA Analysis

The submittal is not clear if the need to diagnose an event (i.e., to figure out what is to be done in any given situation) was considered in the HRA analysis. The diagnosis in NUREG/CR-1278, "Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Plant Applications", includes the actions to "perceive, discriminate, interpret, diagnose" an event and the operators "first-level of decision making". While using symptom-based emergency operating procedures (EOPs) removes the need to identify the type of accident, such as a LOCA, their use does not remove the need for other aspects of diagnosis. Please discuss how diagnosis was considered in your analysis. If it was not considered, please justify this omission .

Most of the important human error probabilities were calculated using the ASEP methodology described in NUREG/CR-4772. ASEP gives three general diagnosis response options. The option used most in the HRA calculations is the Time-Based Crew Response Model. This option is discussed further below. The second option is the Annunciator Response model. In this case the operator or crew responds procedurally to an alarm or annunciation, without significant interpretation. The last case is the case where no diagnosis is required. For this last case, ASEP states that there is a negligible probability of diagnosis error given that the operators are well trained to quickly respond to a signal or alarm.

ASEP allows for some interpretation of which diagnosis model to use. The general guidance is that the Annunciator Response Model (ASEP Table 8-4) is used to estimate the probability of detecting a second or subsequent abnormal event during an ongoing accident sequence. Typically, the annunciator response error probabilities given by ASEP are lower than the diagnosis error rates. NUREG/CP-1278 expands on the idea in that a diagnosis error should only be included in a sequence for one HEP, with subsequent operator actions using either no diagnosis or the Annunciator Response Model. For this analysis, the Annunciator Response Model is used only when the HEP analyzed is in response to subsequent system failures, and a diagnosis error is already included in the HEP for a previous related operator action.

Recovery is not credited for the diagnosis failure HEPs analyzed using the Time-Response Models, since the ASEP figure already accounts for a crew response. HEPs analyzed using the alarm response model can be recovered if recovery possibilities exist and are expected.

The main time dependency included in the HRA are in the diagnosis modeling. The general time dependence model provided by ASEP and used in the IPE is discussed in the response to HRA Question #8. ASEP provides some guidance on establishing the time windows (T_m) and response time (T_a). The resulting diagnosis time (T_d) is then used in conjunction with ASEP Figure 8-1 (note that this figure is incorrectly shown on page 7-6 as Figure 7-1 in ASEP) to determine the probability of non-response for a control room crew. ASEP also provides very good guidance on using upper bounds and lower bounds of this figure. In general, an upper bound value is used if the event is unfamiliar to the operators. A lower bound HEP for diagnosis is used if the event is considered "well-recognized" by the operator and the stimulus for the event is clear. Otherwise, the nominal (median) diagnosis HEP should be used.

Level 2 Question 1: External Vessel Cooling Effects on Source Term Definition

According to the IPE, the containment water level will be more than 7 feet above the bottom of the reactor vessel if the RWST [refueling water storage tank] content is injected to the containment, either through core injection and subsequent condensation or through containment spray. This is several feet higher than the depth of the debris inside the vessel if all of the core material were to slump to the bottom of the vessel, assuring that any portion of the vessel wall in contact with the debris can transfer heat directly to coolant in which the vessel is submerged. In-vessel recovery by this heat removal mechanism is considered in the containment event tree (CET) as one of the top events and its effect on CET quantification is evaluated in the sensitivity studies. Since this mechanism may terminate or delay vessel penetration, fission product production and release path are consequently affected (e.g., in-vessel release from a dry debris bed versus ex-vessel release from a debris bed covered by water). Please discuss the effect of external vessel cooling on source term definition. Please also discuss whether this mechanism is included in the MAAP model used for the base case source term analysis, and if not, then please discuss how the source terms are modified by the inclusion of this mechanism.

Prevention of reactor vessel lower head failure would retain the debris within the vessel, and prevent core-concrete attack and the associated sparging mechanisms for release of non-volatile fission products from the debris. This has a first order influence on limiting the source term to the containment atmosphere for those sequences where the containment integrity would be jeopardized (such as a failure to isolate), thereby limiting the radiological source term which could be released to the environment. In addition, the prevention of core-concrete attack removes two mechanisms for threatening the containment integrity: overpressurization by noncondensible gases and overpressurization by hydrogen combustion with the added contribution of ex-vessel steam explosions. This removes mechanisms which have been postulated to result in early containment failure and direct releases of large

quantities of radionuclides to the environment. Therefore, prevention of the lower head failure by external RPV cooling would have a first order influence on reducing the source term and challenges to the containment integrity. As a result, the majority of accident sequences in which core melt progression is terminated in-vessel do not lead to containment failure.

Successful external vessel cooling leading to in-vessel recovery was not included in the MAAP base case model for source term analysis. MAAP source term results for end states which include vessel failure were assumed to bound the results for end states which do not include vessel failure. For example, the X-XX-X end state, in which neither the vessel nor the containment have failed, was binned together with the L-XX-X and H-XX-X end states. All of these end states resulted in no containment failure except for leakage. The source terms calculated for the H-XX-X were conservatively assumed to apply to the other two end states. This is indicated on Tables 4.7-1, 4.7-2 and 4.7-3 of the IPE submittal. Also, the frequency of the X-XX-X was added together with the L-XX-X and H-XX-X end states in determining the overall source term categorization, as shown in Table 4.7-4 and in Figures 1.4-7 and 1.4-8 of the submittal.

Level 2 Question 2: Treatment of Availability of Containment Systems in CET Quantification

The front-to-back end interfaces are provided in the IPE by the definition of 14 accident classes. These accident classes are identified by a three-character designator addressing the following parameters: The accident initiator, core melt timing, and reactor pressure at the time of core melt. The availability of containment systems (e.g., containment fan coil units and containment spray) are not explicitly included in the definition of the accident classes. Since each accident class may include many core damage sequences (or cutsets), the availability of containment systems may not be the same for all the core damage sequences in an accident class. Please provide a more detailed discussion of how the availability of containment systems is determined and how this information is used in CET quantification for the various accident classes. Please illustrate this process with a few examples.

Containment system fault trees (for containment spray injection, containment spray recirculation, and containment fan coil units) were quantified as frontline systems along with the Level 1 frontline and support system fault trees using linked fault tree models. No credit for operation of containment systems is given in the Level 1 analysis for prevention of core damage or decay heat removal. However, the containment systems fault tree cutsets were input to the CET branches as necessary to support the CET quantification. The availability of containment systems is not required to be known for binning of the Level 1 results into damage classes, since the damage class cutsets and the containment systems cutsets both define the availability of the containment systems support systems (e.g., AC and DC power, cooling water, component cooling water, etc.). The containment systems cutsets are combined with the accident class cutsets in the appropriate branches of the CETs. Boolean reduction of these combined equations correctly identifies those sequences in which failures of support systems have caused failures of containment systems.

The "Containment" event tree headings shown on many of the Level 1 event trees in Figures 3.1-1 through 3.1-9 were used in the calculation for information only. Sequences involving failure of this heading were binned into accident classes whose three-character designators end in "C" (e.g., TLC, RLC, etc.). However, since the CETs identify which sequences require operation of containment systems, these bins were quantified for review only. They were not directly input to the CET quantification.

Level 2 Question 3: CET Branch Probabilities Used and Basis/Survivability of Equipment

The CETs used for the Prairie Island Level 2 analysis were discussed in Section 4.5 and the results of Level 2 sequence quantification were presented in Section 4.6 of the submittal. Although the top events of the CETs, the CET end states, and the dominant sequences were discussed in relative detail in these sections, the discussions are of qualitative nature and the quantitative values used for the CET branches were not presented. Please provide the probability values allocated to each of the CET branches and discuss the basis for these values. Please include in the discussion the basis for the values used for human actions as well as how the availability and survivability of systems and components with potentially significant impact on the CET or the radionuclide release were considered.

Based on the 2/1/96 conference call between NSP and Ed Chow, NRR Research branch, this question was clarified to request a discussion of the types of point values used in the CET branch probabilities (including examples), and a discussion of how the other non-point value branch probabilities were quantified (with examples). NSP requested clarification of this question because the non-point value branch probabilities (the vast majority) are not a normal output of the quantification, and a significant effort would be required to recalculate and report each of them.

Point values were used in some of the CET branch probabilities. These point values can be divided into three categories: unity/null (true/false) based on CET phenomenological modeling assumptions, quantitatively evaluated events, or qualitatively evaluated phenomena. Examples of these are described below:

CET Branches Assigned as Unity/Null: An example of CET branches assigned as unity are the in-vessel recovery branches for the early core damage accident classes (TEH, SEH, BEH and SEL). These accident classes all lead to core damage resulting from inability to inject water to the reactor early in the event. Core damage is assumed to occur for these sequences without RWST water in the containment . Containment spray is an alternate means of injection of water into containment independent of the reactor. However, for transients in which reactor inventory is lost through the pressurizer PORVs, and small LOCAs, the FCUs remove sufficient heat to keep containment pressure below the actuation setpoint for containment spray (23 psig). Only during medium or large LOCAs with early injection failure would containment spray be available for submerging the lower vessel head to prevent vessel penetration. However, this was not credited (no credit for in-vessel recovery for early core damage sequences). Therefore, in-vessel recovery for these sequences were assigned as unity, and their complement branches were assigned as null.

Another example is reactor depressurization through RCS hot leg creep rupture on early core damage sequences at high pressure (accident classes TEH, SEH and BEH). For these sequences, if the lower head is not submerged, it is assumed that debris penetration of the lower head occurs prior to RCS hot leg creep rupture. This assumption, which is conservative based on MAAP sensitivity studies, results in high pressure melt ejection rather than depressurization of the RCS with the core in the vessel. Had hot leg creep rupture been credited in the analysis of these sequences, vessel failure would have been assumed at low pressure, resulting in a majority of the debris being retained in the reactor cavity (as opposed to ejection at high pressure, which distributes it throughout the upper compartments of containment in a less coolable geometry).

The in-vessel recovery and reactor depressurization CET headings (which contain the ex-vessel cooling and RCS hot leg creep rupture phenomena) are discussed in Section 4.5.3.1 of the IPE submittal. The unity values are signified by the "1.0" notation below these CET branches on Figures 4.5-1 and 4.5-2.

CET Branches with Quantitatively Evaluated Point Values: An example of the use of point values determined quantitatively is the value used for the Containment Isolation function in the CETs. The evaluation of this point value is described in the response to Level 2, Question #4 below.

CET Branches with Qualitatively Evaluated Point Values: Examples of the use of point values determined qualitatively are the values used for the probabilities of containment post-core damage phenomena. These phenomena are Ex-Vessel Cooling, Failure of Hot Leg Creep Rupture and the early containment failure phenomena which were analyzed to be credible challenges (In-Vessel Steam Explosion, Ex-Vessel Steam Explosion, Hydrogen Combustion, and Direct Containment Heating). A discussion of the evaluation of each of these phenomena and their quantitative point values are given in Sections 4.4.3 (early containment failure phenomena) and 4.5.3 (Ex-Vessel Cooling, Failure of Hot Leg Creep Rupture) of the IPE submittal. The point value for one qualitatively evaluated phenomena, Debris Cooling, was not explicitly given in the submittal: Given the relatively thin layer of debris expected on the containment floor following vessel penetration, the baseline quantification for the Level 2 PRA assumed that the debris would be in a coolable geometry. Sensitivity analysis regarding this and other selected phenomena was discussed in Section 4.8.1.

Non-Point Value Branch Probabilities:

Most of the CET branch probabilities used in the IPE analysis were not point values but were equations developed for the CET event tree headings from linked fault tree models. This process was identical to that used in the Level 1 event tree quantification. However, the quantification of each CET started with a Level 1 accident class (a group of Level 1 core damage sequences binned together into one Boolean equation), rather than an initiating event as was done in the Level 1 event tree quantification. This method maintains the availability of frontline and support systems correct throughout the CET analysis, an advantage which is not available with the split fraction analysis method. These event tree branch equation probabilities

by themselves (without consideration of the Level 1 system failures which have occurred) have relatively little meaning. Therefore, these intermediate probabilities were not quantified in the original IPE and would require much effort to reproduce.

Examples of this type of branch probability quantification used in the CET analysis are for the Containment Pressure Control (CPC) and Containment Spray (CSS) headings which appears on all of the CET diagrams (Figures 4.5-1 through 4.5-5). As is shown on the diagrams, the Boolean combination of fault tree top event failure equations that comprise each CET branch under these headings are dependent on accident class and failures that have occurred.

Level 2 Question 4: Containment Isolation Failure Analysis

With respect to the analysis of containment isolation failure probability, NUREG-1335 (Section 2.2.2.5, page 2-11) states that "the analyses should address the five areas identified in the Generic Letter, i.e., (1) the pathways that could significantly contribute to containment isolation failure, (2) the signals required to automatically isolate the penetrations, (3) the potential for generating the signals for all initiating events, (4) the examination of the testing and maintenance procedures, and (5) the quantification of each containment isolation failure mode (including common-mode failure)." Although the materials presented in the IPE submittal cover most of the above areas, some of the items in the above list are not addressed. Please discuss your findings related to all of the above five areas.

(1) The IPE submittal gives a detailed discussion of the methods used in the containment isolation failure probability quantification. All containment penetrations were examined against the criteria identified in Section 4.4.3 of the submittal. Those which remained following this initial screening (the pathways that could significantly contribute to containment isolation failure) are identified in Table 4.4-2. This table gives the configuration of the valves, their normal positions, the signals required to close the valves, and the dependencies of the valves on support systems for motive and control power. Table 4.4-3 gives the resulting containment isolation failure probabilities, arranged by availability of support systems. The highest probability value, 5.8E-4, was conservatively selected for use in the CETs due to the diverse range of support system availability that exists in the binned accident class cutsets.

(2) The automatic containment isolation valves are closed upon receipt of a "T" signal. A "T" signal is generated from manual containment isolation from actuation of one of two control switches in the control room. The other way a "T"signal is generated is by an SI signal. An SI signal is created either from 1/2 manual control board switches, or from 2/3 containment pressure high, 2/3 pressurizer pressure low, or 2/3 low steam line pressure on either steam generator.

The only notable exception to this is for the containment instrument air isolation valves, which close on receipt of a "T" signal and a coincident "M" signal. An "M" signal is generated by coincident SI, Low-Low T_{avg} and high

steam flow signals, by coincident SI and high-high steam flow signals, or by a high-high containment pressure signal.

(3) All of the analyzed initiating events result in containment isolation prior to core damage occurring. Many of the initiating events generate signals based on the normal plant response to the events themselves, while others (transients, for example) require further functional failures to occur before containment isolation signals are generated. The potential for generating signals for the initiating events are as follows:

a. Large LOCA - Yes (Low Pressurizer Pressure).

b. Medium LOCA - Yes (Low Pressurizer Pressure).

c. Small LOCA - Yes (either Low Pressurizer Pressure or Manual SI/containment isolation due to successful operator action in response to the event).

d. Interfacing Systems LOCA - Yes (Low Pressurizer Pressure).

e. Steam Line/Feed Line Break - Yes (High Containment Pressure for breaks inside containment or low steam line pressure for any break location).

f. Steam Generator Tube Rupture - Yes (Low Pressurizer Pressure).

g. Inadvertent SI Signal - Yes (initiating event definition requires SI-signal).

h. Transient - Yes (high containment pressure following loss of secondary cooling and initiation of bleed and feed).

i. Internal Flooding - Yes (high containment pressure following loss of secondary cooling and initiation of bleed and feed).

j. Loss of DC Bus A - Yes (high containment pressure following loss of secondary cooling and initiation of bleed and feed, plus normally open control valves with a containment isolation function fail closed on loss of DC).

k. Loss of DC Bus B - Yes (high containment pressure following loss of secondary cooling and initiation of bleed and feed, plus normally open control valves with a containment isolation function fail closed on loss of DC).

l. Loss of Offsite Power - Yes (high containment pressure following loss of secondary cooling and initiation of bleed and feed).

m. Loss of Cooling Water - Yes (high containment pressure following loss of secondary cooling and initiation of bleed and feed).

n. Loss of Component Cooling Water - Yes (high containment pressure following loss of secondary cooling and initiation of bleed and feed).

o. Loss of Instrument Air - Yes (high containment pressure following loss of secondary cooling and initiation of bleed and feed, plus normally open control valves with a containment isolation function fail closed on loss of instrument air).

(4) Preventive maintenance of containment isolation valves is normally performed when the unit is off-line. Inservice testing of containment isolation valves is performed per the ASME Sect XI Code that is currently in force at the plant. Verification of valve closure is performed per the Code on a frequency required by the Code and is a signoff point on the procedure. No changes to the IPE models were required as a result of the review of test and maintenance performed on the containment isolation valves.

(5) The quantification of each containment isolation failure mode (including common-mode failures) was provided in the IPE submittal as summarized in (1) above.

Level 2 Question 5: Liner Meltthrough Considerations on High Pressure Melt Ejection

It is assumed in the IPE that during a high pressure vessel blowdown, a significant amount of core debris is carried out of the reactor cavity, through the instrument tunnel, to the upper compartment. Because Prairie Island uses a steel containment and the seal table is situated outside the secondary shield wall, a high pressure blowdown could lead to corium coming into contact with the containment steel shell. This failure mode is discussed briefly and dismissed as a potential failure mode in the IPE. Please provide a more detailed discussion of the analytical model used to determine the flow paths and distribution of the discharged debris during a high pressure melt ejection. Please discuss the impact of the two personnel entry hatches on corium dispersal and disposition. According to the IPE, these two hatches are located on the instrument tunnel and are left slightly ajar during normal operation.

The amount of core debris carried out of the reactor cavity and the amount then de-entrained during the 90° turn into the in-core instrument tunnel was determined by applying the methods in NUREG/CR-5039 to a high-pressure melt ejection at the Prairie Island plant. These calculations indicate that approximately 4850 kg of core debris, or roughly 0.7 m^3, would make the turn into the instrument tunnel. The majority of this debris would then be de-entrained at the seal table, leaving very little available to contribute to liner melt-through. This would be composed of only the smallest entrained particles, since it could not otherwise have remained entrained through the second 90° turn. Given in addition the many pipes, structures, and other obstacles between the seal table and the steel liner, it is not reasonable to suppose that debris could collect against the liner in a sufficiently large and coherent mass to melt the steel.

The access hatches to the instrument tunnel are in an open area on the basement level of the containment, and for both of the reactor units one of the two hatches faces toward the steel containment, about 30 feet away, with a

largely unobstructed path in between. Because more of the entrained material could reach the steel wall in this case than in the area around the seal table, a scoping study was done to determine whether this could pose a threat to containment integrity. It was found that even with conservative assumptions about the mass, distribution, and heat generation of the debris expelled from the instrument tunnel, the temperature generated by debris adhering to the steel wall would be insufficient to melt the steel and breach containment. Liner melt-through is therefore still not considered a credible threat to the Prairie Island containment.

Level 2 Question 6: Probability of SG Valve Failure for Induced SGTR Events

In most of the temperature-induced steam generator tube rupture (SGTR) failures reported in the submittal, the valves which open to relieve the steam generator pressure are assumed to reclose successfully . This limits the release to a relatively short duration puff, followed by a series of shorter puffs, and all releases are terminated upon vessel failure when the primary system depressurizes to containment pressure. Please discuss how the probability of steam generator valve failure is determined in the analysis and whether the harsh operating conditions (e.g., the flow of extreme high temperature gases with entrained debris) is considered in the analysis.

Environmental conditions experienced by the steam generator relief valves following temperature-induced SGTR (termed steam generator tube creep rupture or SGTCR in the IPE submittal) were assumed to have little effect on the ability of the valves to operate. No degradation of the failure to open or close rates were assumed based on relief of gases as opposed to steam. The main steam power-operated relief valves (PORVs) are Copes-Vulcan model D-100 valves, and the main steam safeties are Consolidated model 3787A Maxiflow valves. Although the valves are not designed for high temperature gas relief in this installation, there is some assurance that they would likely relieve the gases just as well as steam without significant degradation. All valves have metallic seats and have few other non-metallic parts that have a pressure retaining function. The safety relief valves employ a seat design which, according to the technical manual, are "giving excellent results at 5500 psi and 1150 °F". Very little entrained debris would be likely due to the path from the core to the steam generators and through the U-tubes, through the steam generator moisture separators, the other upper steam generator components and the flow restricting nozzle in the steam line at the outlet of the steam generator. Also, the expansion of the gases into the steam generator after exiting the ruptured tube(s) would significantly reduce the velocity of the gases, which would further de entrain the debris.

However, the concern over temperature-induced steam generator tube rupture (SGTCR) is moot at this point, due to changes made to the EOPs since the IPE was submitted (see the response to Level 2, Question #7).

Level 2 Question 7: CET End State Matrix

Table 4.6-1 shows the frequencies of the dominant CET sequences that contribute to the CET end states (i.e., containment failure modes). This

provides partial information on the conditional probabilities of the failure modes for an accident class (or plant damage state). Please provide the C-Matrix which provides a complete account of the conditional probabilities of the failure modes for all accident classes evaluated in the Level 2 analysis. Since the probability of temperature-induced SGTR is excluded in the calculation of the probability values presented in Table 4.6-1, please also provide the C-Matrix with the temperature-induced SGTR included in the evaluation.

The requested C-Matrix for the case with induced steam generator tube rupture events excluded is provided in the next page.

Based on the 2/1/96 conference call between NSP and NRC Research, it was agreed that NSP would not need to provide the C-Matrix that reports the probabilities of the various Level 2 plant end states versus accident class for the case which includes core damage followed by induced steam generator tube rupture (termed steam generator tube creep rupture or SGTCR in the IPE submittal). Based on recommendations from the Westinghouse Owners Group, the emergency procedures have been changed prohibiting restart of a reactor coolant pump with a dry steam generator under severe accident conditions. This procedure change effectively precludes the contribution of SGTCR to containment failure as described in the IPE report.

PRAIRIE ISLAND IPE C-MATRIX

LEVEL 1 ACCIDENT CLASS VS. LEVEL 2 PLANT END STATE

ACCIDENT CLASS	X-XX-X	X-DH-L	X-H2-E	L-XX-X	L-DH-L	L-CC-L	L-H2-E	H-XX-X	H-DH-L	H-OT-L	H-H2-E	X-CI-E	L-CI-E	H-CI-E	GLH[1]	GEH[1]	ISLOCA[1]	TOTALS[2,5]
SEH	0E+00	0E+00	0E+00	0E+00	0E+00	0E+00	0E+00	2E-06	2E-06	5E-06	7E-08	0E+00	0E+00	1E-09	N/A	N/A	N/A	8E-06
TEH	0E+00	0E+00	0E+00	0E+00	0E+00	0E+00	0E+00	6E-06	5E-07	4E-06	7E-08	0E+00	0E+00	6E-10	N/A	N/A	N/A	1E-05
FEH[3]	0E+00	0E+00	0E+00	0E+00	0E+00	0E+00	0E+00	1E-05	5E-08	1E-08	1E-07	0E+00	0E+00	6E-09	N/A	N/A	N/A	1E-05
BEH[4]	0E+00	0E+00	0E+00	0E+00	0E+00	0E+00	0E+00	3E-06	1E-08	2E-07	2E-08	0E+00	0E+00	2E-10	N/A	N/A	N/A	3E-06
REP	0E+00	0E+00	0E+00	0E+00	0E+00	0E+00	0E+00	1E-07	0E+00	4E-08	6E-11	0E+00	0E+00	0E+00	N/A	N/A	N/A	2E-07
SLH	3E-06	0E+00	2E-08	2E-08	0E+00	0E+00	0E+00	0E+00	0E+00	0E+00	0E+00	2E-10	0E+00	0E+00	N/A	N/A	N/A	3E-06
TLH	1E-06	0E+00	1E-09	1E-09	7E-09	0E+00	0E+00	0E+00	0E+00	0E+00	0E+00	0E+00	0E+00	0E+00	N/A	N/A	N/A	1E-06
FLH	0E+00	0E+00	0E+00	0E+00	0E+00	0E+00	0E+00	0E+00	0E+00	0E+00	0E+00	0E+00	0E+00	0E+00	N/A	N/A	N/A	0E+00
RLO	2E-07	0E+00	1E-09	1E-09	9E-10	0E+00	0E+00	0E+00	0E+00	0E+00	0E+00	0E+00	0E+00	0E+00	N/A	N/A	N/A	2E-07
SEL	0E+00	0E+00	0E+00	4E-08	0E+00	4E-08	6E-10	0E+00	0E+00	0E+00	0E+00	0E+00	0E+00	0E+00	N/A	N/A	N/A	8E-08
SLL	8E-06	0E+00	7E-08	3E-08	0E+00	0E+00	2E-10	0E+00	0E+00	0E+00	0E+00	3E-09	0E+00	0E+00	N/A	N/A	N/A	8E-06
GLH[1]	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	6E-06	N/A	N/A	6E-06
GEH[1]	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	6E-07	N/A	6E-07
ISLOCA[1]	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	2E-07	2E-07
TOTALS[2,5]	1E-05	0E+00	9E-08	6E-08	8E-09	4E-08	8E-10	2E-05	3E-06	9E-06	3E-07	4E-09	0E+00	8E-09	6E-06	6E-07	2E-07	4E-05

NOTE: All frequencies are per reactor year.

[1] These accident classes represent both core damage and containment bypass. Therefore, they were quantified in the Level 1 analysis rather than in the Level 2 (CET) analysis.

[2] The totals shown for the SLH accident class and the H-OT-L end state add to slightly more than the totals listed in the IPE submittal (Tables 3.4-1 and 4.6-1) due to rounding.

[3] The FEH accident class includes the FEH-TB1 accident class listed in the IPE submittal Table 3.4-1.

[4] The BEH accident class includes the BEH-NOPWR accident class listed in the IPE submittal Table 3.4-1.

[5] The sum total of all the accident classes and end states is less than the reported core damage frequency (5E-5/rx-yr) due to truncation in the CET quantification.

Level 2 Question 8: Provide Plant Data Suggested in NUREG-1335 in Tabular Form

The plant data that are of interest to the Level 2 analysis are provided in Section 4.1 of the IPE submittal. Although this section provides the essential data for the accident progression discussion, it lacks the detail suggested in NUREG-1335. Please provide in tabular form the data described in Table A.1 of NUREG-1335.

The MAAP PWR Rev. 19.0 computer code was used to perform success criteria and timing calculations for the Prairie Island IPE. Many of the values on this table are from the parameter file for the MAAP code, which were the values used for all MAAP analysis and were current at the time the parameter file support files were prepared. Values denoted with an asterisk (*) are not from the parameter file, but were taken from current plant documentation. The MAAP parameter file contains plant specific pump curve data which it uses to calculate pump flows. The internal structural heat sinks table was taken from the historical Prairie Island Reactor Data Package NSPNAD-8311P Volume 1, Table 4.1-1 Rev. 2, 1/23/86.

1. Reactor Core, Vessel and Primary System

A. Core and Vessel Data

Core Full Power	1.65E9 J/sec
Mass of UO_2	49,301 kg
Mass of Zr in Core	11,241 kg
Mass of Zr in Cladding	11,087 kg
Mass of Steel:	
Upper Plenum Structures	13,520 kg
Upper Core Support Plate	12,426 kg
Lower Core Support Plate	1,134 kg
Core Barrel including Thermal Shield, Baffle, and Former Plates	70,126 kg
Mass of Reactor Vessel Below the Flange including Nozzles and Lower Head	165,300 kg
* Bottom Head Diameter	133.86 inches
Bottom Head Thickness	0.113 m
Fuel Enrichment	3.8 w/o
Mass of Control Rod Constituents	1,279.1 kg

B. Primary System Data

* Total Water Inventory	5938 ft^3
* Total Water and Steam Volume	6191 ft^3
* Type of Steam Generators	Vertical U-tube
* Number of Steam Generators	2
* Model of Steam Generators	Westinghouse Model 51
Total Flow Rate	198,203 gpm
PORV Capacities	22.6 kg/sec
PORV Settings	16.2E6 Pa
Safety Valve Capacities	4..47 kg/sec

Safety Valve Settings	16.96E6 Pa, 17.41E5 Pa
Reactor Coolant Temperature	566.48 °K
Reactor Coolant Pressure	1.55E7 Pa
* Reactor Coolant Enthalpy	699.6 Btu/lb

C. Accumulator System

* Volume of Water	1270 + or - 20 ft^3
Inventory Temperature	305 °K
Initiating Pressure	5.27E6 Pa

2. Containment System

A. Containment Structure

* Containment Type	Free Standing Steel Shell
* Type of Concrete in Base Mat	Basaltic Concrete
* Weight Fraction of Free H_2O	2.9 w/o
* Weight Fraction of Bound H_2O	2.0 w/o
Free Volume	37,393 m^3
* Design Pressure	46 psig
Normal Pressure	0.102E6 Pa
Normal Temperature	310.9 °K
Area of Reactor Cavity Floor	27 m^2
Shield Building Wall Thickness	2.5 ft
* Containment Shell Thickness:	
Cylinder Shell	3/4 inches
Dome	1-1/2 inches
Ellipsoidal Basemat	1-1/2 inches
* Basemat Thickness	9.8 ft

B. Containment Spray System

Number of Pumps	2
Total Design Flow Rate	1300 gpm per pump
Containment Pressure Setpoint	23 psig
* Spray Additives	Borated water mixed with Sodium Hydroxide

C. Containment Fan Coolers

Capacity	14.5 MW per fan
Number of Fans	4
Flow Rate per Fan	29,000 cfm
Primary Inlet Temperature	85 °F

D. Interior Structural Heat Sinks

Thickness (inches)	Paint Thickness (inches)	Unpainted Area (ft^2)	Painted Area (ft^2)	Total Area (ft^2)
1.5 Steel	0.011		41,300	41,300
0.75 Steel	0.011		32,000	32,000
0.25 Steel / 12 Concrete		7,860		7,860
0.375 Steel	0.011		6,800	6,800
0.25 Steel		32,000		32,000
0.5 Steel	0.011		44,000	44,000
0.145 Steel	0.011		1,695	1,695
0.09 Steel		12,400		12,400
0.1 Steel		6,000		6,000
0.1875 Steel	0.011	22,000	13,125	35,125
1.44 Steel	0.011		2,200	2,200
12 Concrete	0.018	36,720	4,080	40,800
6 Concrete	0.018		25,070	25,070
3 Concrete	0.018		7,570	7,570

3. <u>ECCS and Other Injection / Recirculation Systems</u>

A. Volume / Chemistry Control Charging Pumps

Total Flow Rate (per pump)	60.5 gpm
Number of Pumps	3 (positive displacement)
Discharge Relief Valve Setpoint	2735 psig

B. High-Pressure Injection

Total Flow Rate (per pump)	700 gpm @ 2760 ft
Number of Pumps	2
Shutoff Head	5100 ft

C. Low-Pressure Injection (RHR Pumps at Prairie Island)

Total Flow Rate (per pump)	2000 gpm @ 280 ft
Number of Pumps	2
Shutoff Head	340 ft

D. Residual Heat Removal (RHR)

Total Flow Rate (per pump)	2000 gpm @ 280 ft
Number of Pumps	2
Shutoff Head	340 ft

E. Upper Head Injection (ice condenser containments)

Not Applicable at Prairie Island

4. Auxiliary Building

The auxiliary building was not modeled as a barrier to fission product release in the Prairie Island Level 2 IPE analysis. All releases from containment into the auxiliary building were assumed to lead directly to the environment, without credit for further scrubbing in the auxiliary building.

Level 2, Question 9: Containment Equipment Survivability

The effects of harsh environmental condition on the operation of containment sprays and containment fan cooler units are not discussed in the CET quantification of the IPE submittal. Please discuss the survivability of these components under severe accident conditions. Please include in the discussion the environmental conditions (e.g., temperature, pressure, radiation, aerosol plugging and debris effects) derived and used in the evaluation.

The following summarizes assumptions made regarding the survivability of containment spray and fan cooler systems under severe accident conditions.

Pressure and Temperature

From an equipment qualification standpoint, only the fans themselves are located in the containment. All other active components in these two systems are located outside containment and are not exposed to the steam environment. If either the fan coolers or sprays are in operation, then the containment environment is likely to be within the fan motor qualification envelope for most of the accident scenarios quantified in the PRA.

From a containment sump water temperature standpoint, long term containment spray operation in the recirculation mode is assumed not to be available if water in the containment sump is saturated for a significant period. RHR pump operation is assumed to be impaired due to lack of NPSH under these conditions. Keeping containment water subcooled requires heat removal through the RHR heat exchanger. Fan cooler unit operation is not assumed to be sufficient to maintain the sump water subcooled. However, fan cooler operation is sufficient to prevent containment over pressure due to steam generation from the reactor or water covering the debris on the containment floor.

Radiation

The only components in fan cooler and containment spray systems credited following exposure to radiation resulting from a severe accident are the fans (located in the containment), the RHR and containment spray pumps (located outside the containment but exposed to fluids containing fission products). Each of these components is qualified for exposure to TID source term as a part of the equipment qualification program. As this source term is similar to that expected for a full core melt, radiation is assumed to have little effect on the operation of the fan cooler and containment spray systems.

Aerosol and Debris Effects

The accident sequence quantification for the Level 2 PRA was performed assuming there was little effect on the operation of containment spray and fan cooler units due to aerosols and debris. However, the sensitivity studies described in Section 4.8 bound the possible effects of aerosol and debris on these systems. Two types of accident scenarios affect the amount of debris that may be located in the containment; those in which the core is retained within the vessel and those in which lower head penetration occurs allowing the core debris to enter the reactor cavity and possibly other parts of containment. In the first scenario, the majority of the debris is retained within the primary system and it is assumed that there is limited potential for nozzle plugging or plate out of materials on fan cooler tube surfaces. The majority of sequences in the second group are high pressure melt ejection scenarios in Prairie Island Level 2 results. The sensitivity study performed regarding the ability to provide cooling to the debris during this type of accident sequence also applies to the loss of containment heat removal from any cause, including nozzle plugging or plate out. The sensitivity study suggests that the conditional containment failure probability might rise from 21% to 63% if sprays were not available for some reason. However, this particular failure mode takes a significant time to evolve, on the order of days, and has no impact on the potential for large early releases.

Level 2, Question 10: Localized Hydrogen Combustion

The generic letter containment performance improvement recommendation for pressurized-water reactor dry containments is the evaluation of containment and equipment vulnerabilities to localized hydrogen combustion and the need for improvements (including accident management procedures).

> **Please discuss whether plant walkdowns have been performed to determine the probable locations of hydrogen releases into the containment. Discuss the process used to assure that: (1) local deflagrations would not translate to detonations given an unfavorable nearby geometry, and (2) the containment boundary, including penetrations, would not be challenged by hydrogen burns.**
>
> **Please identify potential reactor hydrogen release points and vent paths. Estimates of compartment free volumes and vent path flow areas should also be provided. Please specifically address how this information is used in your assessment of hydrogen pocketing and detonation. Your discussion (including important assumptions) should cover the likelihood of local detonation and the potential for missile generation as a result of local detonation.**

The plant walkdowns identified the most likely places for hydrogen to be released to the containment, depending on the type of accident. For transient-induced core damage sequences, where there is no leak in the primary system, hydrogen within the vessel would be directed through the pressurizer PORVs or safety valves into the pressurizer relief tank (PRT) and then into containment. The PRT is on the basement floor in an open area which communicates freely with the rest of containment, so hydrogen released from

the PRT cannot collect in local pockets, but would disperse throughout the containment.

For LOCA events, hydrogen would be released directly to the containment through the break in the primary system. The primary system piping is protected by shield walls, but these areas nevertheless communicate with the rest of containment through sizeable openings such as those surrounding the steam generators. Since the fan cooler units are also expected to operate during a LOCA, good mixing should occur among the containment regions. Local pocketing of hydrogen is therefore not expected to occur during LOCA events.

Hydrogen Detonation: Hydrogen detonation by direct ignition is not possible because even the largest ignition source in containment, a 12 kV arc, is several orders of magnitude too small to cause detonation. The potential for hydrogen detonation initiated by deflagration-to-detonation transition (DDT) was assessed using NUREG/CR-4905 and NUREG/CR-4803. First, the mixture was characterized by conservatively assuming a dry containment atmosphere and an amount of hydrogen equal to the amount which would be generated by 100% oxidation of the zirconium and the core lower plate, and assuming uniform mixing throughout containment. A hydrogen concentration of 15% is calculated for these conditions, and per NUREG/CR-4905, the equivalence ratio is 0.4.

Using the method in NUREG-4803, this hydrogen mixture is classified as Mixture Class 4, unlikely to detonate. Geometrically, the lower and annular compartments of the Prairie Island containment (free volumes approximately 2851 m^3 and 5451 m^3, respectively) are characterized as channels with transverse venting, since an upward propagating flame in either of these is free to expand in a transverse direction; this is Geometry Class 4, unfavorable to flame acceleration. The upper compartment (approximately 28,952 m^3) is characterized as an unconfined geometry at large scale, or Geometry Class 5, which is very unfavorable to DDT. All regions of the containment therefore fall into Result Class 5, meaning that DDT is highly unlikely to impossible.

Hydrogen Deflagration: A bounding assessment was done to ensure that a hydrogen burn cannot fail the containment. First, the amount of hydrogen in containment was conservatively assumed to be the amount generated by 100% oxidation of all zirconium in the core and all metallic constituents of the lower core plate; this far exceeds the amount actually predicted due to metal oxidation and core-concrete interaction during the most severe station blackout sequence. The effects of steam inerting were neglected, and complete combustion of the hydrogen was assumed to occur. Next, the changes in gas composition following complete combustion of the hydrogen were then evaluated to determine the ratio of the number of moles of gas in the containment before and after the burn. The post-burn temperature was then determined by assuming that the heat of combustion goes entirely to heating the containment atmosphere - that is, neglecting both the passive and active heat sinks in containment. Finally, a post-burn pressure was determined based on the containment volume, post-burn temperature, and number of moles of gas in containment. This conservative assessment leads to an estimated post-burn pressure of 95 psia, which is well within the containment's ultimate capacity. Hydrogen burns are therefore not expected to cause containment failure.

Level 2, Question 11: Containment Spray Recirculation and System Availability

It is assumed in the IPE that containment spray is required to cool the debris that has been relocated out of the reactor cavity to the upper areas of the containment following a high pressure melt ejection. The results of the sensitivity studies presented in the submittal show that the probability of late containment failure increases significantly (from 21 percent to 63 percent) if the relocated debris is not coolable. A similar change in containment failure probability is expected if containment spray is not available for all accident sequences. Please discuss whether containment spray in recirculation mode is required to prevent containment failure in the cases with relocated debris, and discuss how the data for spray availability is derived in the IPE. Please discuss the effect of maintenance schedules and harsh environmental conditions on the availability and continuous operation of the containment spray.

The Level 2 analysis assumed that a means to provide long term cooling of the relocated debris following a high pressure melt ejection (HPME) must be available in order to prevent eventual failure of containment. Containment failure would otherwise occur many days after the event due to overpressurization from the noncondensible gas generation produced through core concrete interaction. It is believed that containment spray recirculation is the only means available to provide long term cooling of the dispersed debris. Therefore, the CET quantification assumed that containment failure occurs several (3 to 4) days after the HPME occurs if containment spray recirculation is unavailable.

At the time the IPE was submitted transfer to containment spray recirculation was proceduralized in the plant EOPs. Recently, changes to the EOPs have been made which has removed this guidance. These changes were made in response to design basis analysis which shows that containment spray recirculation is not required following any analyzed accident to prevent the containment from exceeding design pressure (46 psig). However, it is stressed again that containment failure occurs on the order of 3 to 4 days following the event. Therefore, ample time would be available to align the system for operation despite the unavailability of procedures. Time would also be available to effect repair and recovery of the system if failures did occur following initiation of containment spray recirculation. (No credit for repair and recovery of containment spray recirculation was given in the baseline IPE analysis, or in the sensitivity analyses described in Section 4.8 of the IPE report.) Also, it must be stressed that the offsite release consequences of containment spray recirculation failure are not large. Since containment fails so late in the event, most of the radionuclides have been removed, either through decay, settling in the containment or through the scrubbing action of the spray fluid itself. Only noble gases are available for release once containment failure does occur. Therefore, the effects of these EOP changes are not significant in the consideration of either the probability or consequences of containment failure during HPME events.

Also, note that our assumption that RCS hot leg creep rupture does not depressurize the reactor for most high pressure core melt sequences is very conservative. If we had assumed that this does occur, then unavailability of

containment spray recirculation would have had a minor effect on long term containment challenges.

Data for spray availability was derived consistent with the way availabilities were derived for other systems in the IPE. Plant specific failure data were collected and analyzed as described in Section 3.3.3 of the IPE report. Maintenance and testing unavailability data was collected and analyzed as described in Section 3.3.4 of the IPE report.

Survivability of containment systems under harsh environmental conditions is addressed in the response to Level 2 Question #9 above.

Disposition of IPE Recommendations

The following is a description of the IPE recommendations as contained in the IPE Report (NSPLMI-94001, Rev. 0) in italics, and the disposition of each recommendation to date - 11/28/95:

The following recommendations are generated based on the results of the Level 1 IPE analysis:

1. ***a)** Proceduralize the cross-tie from station air to instrument air such that C34 AOP1, Rev 0, "Loss of Instrument Air" utilizes the cross-tie. The station air compressors are cooled from loop B cooling water and would not be affected by a LOOP A CL pipe break. If the cross-tie could be accomplished within 1 hour after the flood initiator, main feedwater or bleed and feed cooling could be restored and core melt could be prevented. **b)** The instrument air operating procedure should also be more emphatic in stating that the station air cross-tie should be used whenever an instrument air compressor is out of service for maintenance. It is recognized that this recommendation will only restore instrument air if the flood occurs as a result of a Loop A CL pipe break. However, this recommendation would be effective for many other events in which instrument air was lost.*

   DISPOSITION: a) C34 AOP 1, Rev. 4 incorporates this action (Step 2.4.6).
   b) C34, Rev. 12 incorporates this recommendation (Section 1.0).

2. *Revise C35 AOP1, Rev 2, "Loss of Cooling Water Header A or B" such that it addresses the problem of closure of the turbine building cooling water header isolation valve and the subsequent loss of cooling water to the main feedwater lube oil coolers and condensate pump oil coolers. Analysis has shown that the main feedwater pumps can conservatively operate without cooling water for approximately 20 minutes before possible pump damage.*

   DISPOSITION: This recommendation relates to the continued availability of cooling water to the main feedwater and condensate pumps following the postulated auxiliary feedwater pump room cooling water header rupture event. Therefore, this recommendation is addressed through the disposition of #3 below.

3. *To limit the impact of AFW pump room flooding due to Cooling Water System header rupture, provide a means to either allow additional water flow out of the room (through modifications to the Unit 1 and Unit 2 side doors, for example) or to segregate the room into two compartments (close the fire door between the two halves of the AFW pump room and upgrade the ability of the door to block water flow, for example).*

   DISPOSITION: Calculation ENG-ME-148, Rev. 1, "Cooling Water Header Pipe Failure Causing Flooding in the Auxiliary Feedwater Pump/Instrument Air Compressor Room", addresses this recommendation. This position paper documents the qualifications, design features and periodic inspections in place which provide confidence that the probability of occurrence of the pipe rupture is negligible. The design and construction standards are much more stringent than are the standard quality used in industrial and fossil plant design and construction. The CL header piping was completely replaced during the November, 1992 dual-unit outage. The new piping is 33 percent thicker (1/2" compared to the original thickness of 3/8"). The internal surface of the new pipe is coated with an epoxy coating to inhibit microbiologically induced corrosion (MIC). Also, it is likely that a substantial piping leak (which could eventually lead to a larger piping failure) would be noticed by operators, engineering or maintenance staff, or security personnel who periodically walk though these rooms.

4. *Emphasize in training the importance of bleed and feed and the operator actions that are necessary for success as bleed and feed is a significant contributor to class TEH and the overall CDF.*

DISPOSITION: This recommendation is addressed by the following:

1) Letter 2/21/94, M. Wadley to D. Reynolds, asking Training to take the necessary actions to ensure the operators receive periodic training on the IPE recommended training actions. The letter identifies the actions and a suggested frequency for giving training on them.

2) Request for Training 94-25 from J. Sorensen - Requal/NLO training on IPE and bases. Training completed during cycle 94-09.

3) Course Outline for Simulator Continuing Training: P9160S, Rev. 4. Record of Individual Plant Manipulations includes each of the IPE recommended training items at the frequency requested in the Wadley letter.

4) NLO Training Program P8400, Rev. 9: Outplant actions required to successfully establish low head recirculation and to cross-connect the MDAFWP to the opposite unit are IPMs (SI-3 and AF-7), required biennially.

5) Lesson Plan P8161L-003, Rev. 1, Introduction to Accident Analysis for license candidates: In addition to USAR accident analysis topics, students are trained in how PRA techniques are used to determine risk, and on the results and uses of the PINGP IPE in the operation and maintenance of the plant.

5. *Emphasize in training the importance of the crosstie between the motor driven AFW pumps and the operator actions that are necessary for success as the AFW crosstie is a significant contributor to class TEH and the overall CDF.*

DISPOSITION: See #4 above.

6. *Emphasize in training the importance of switchover to high and low head recirculation and the operator actions that are necessary for success as switchover to recirculation is a significant contributor to class SLL and the overall CDF.*

DISPOSITION: See #4 above.

7. *Emphasize in training the importance of RCS cooldown and depressurization to terminate SI before ruptured SG overfill and the operator actions that are necessary for success this action is a significant contributor to class GLH and the overall CDF.*

DISPOSITION: See #4 above.

Since the starting point of the Level 2 analysis is the Level 1 core damage sequences, the preceding Level 1 recommendations will also have a positive effect on the Level 2 release frequency. The following recommendations are generated based on the results of the Level 2 analysis:

1. *Revise FR-C.1, Rev 5, "Response to Inadequate Core Cooling" step 18 such that the operator checks for adequate steam generator level before attempting to start an RCP. If the RCPs are started with a "dry" steam generator with core exit thermocouples greater than 1200°F, hot gases could be pushed up into the steam generator tubes causing creep rupture of the tubes and a possible containment bypass if one of the steam generator relief valves were to lift.*

DISPOSITION: FR-C.1, Rev. 6, Step 18 (and bases for Step 18) implement this recommendation.

2. *The in-core instrument tube hatches for both units should be secured open during normal operation. This could be accomplished by using a solid bar or other device, instead of a chain, to keep the hatch open but still prevent inadvertent entry during normal operation. Having this hatch open greatly improves the probability of recovering from a core damage event in-vessel (without vessel rupture), by allowing injection water from the RWST to flow into the reactor cavity and to provide cooling to the lower vessel head.*

DISPOSITION: The Sump C hatch doors on both units were reopened during recent containment entries. Options for maintaining the door in the partially open position are being considered. Final disposition of this recommendation will be implemented as early as possible, but prior to the completion of the next refueling outage for each unit.