ENCLOSURE 4

Request for Additional Information – Technical Review of STP
RMTS Initiative 4B Full Plant Pilot

1. **RAI #1 requested clarification of the risk calculations planned for the RMTS program to assure Regulatory Guide 1.174 criteria for acceptably small risk increases was being met. The response stated that the total ICCDP and ICLERP would be "automatically determined as the risk is being accumulated...". Please provide additional detail as to how this automatic calculation is physically accomplished.**

RESPONSE:

The approach used at STP for Configuration Risk Management employs pre-solved configuration-specific Level 1 PRA calculations. The PRA scope and quality is structured to satisfy RG 1.200 requirements and also be acceptable for calculating the change in risk due to the removal of equipment from service. Only the equipment within the scope of the CRMP can be evaluated in terms of delta risk (i.e., change in core damage frequency). The CRMP processes are procedurally controlled using station procedure 0PGP03-ZA-0091, Configuration Risk Management. This procedure establishes the organizational requirements and responsibilities for administering the CRMP. The automatic calculations are physically performed by the Risk Management organization as part of the proceduralized PRA update process. All the existing configurations (>20,000) are individually calculated, verified, and the results stored in a database. Station personnel can then access the pre-calculated results using the Risk Assessment Calculator (RAsCal) software tool. This software tool is LAN based and uses a centralized database. The software program complies with the station's software QA program. In the event a configuration is entered into the RAsCal program which is not represented the pre-solved configuration database, then an error message ("unquantified maintenance state") is displayed and information detailing the specifics of the configuration are captured. A member of the Risk Management team is on duty or on call at all times. They are trained in calculating plant configurations. Once an unquantified maintenance state error message is received the configuration is calculated and added to the pre-solved configuration database. This process can take up to an hour but is rare for an actual plant condition.

It is the staff's understanding that the accumulated risk, tracked from the point when the front stop CT is first exceeded until all extended CTs are exited, and based on actual plant configurations, will be cumulatively tracked and periodically reviewed to determine that the overall RITS program application meets the criteria in Regulatory Guide 1.174 for small risk increases. Please confirm.

RESPONSE: The staff's understanding as described is correct.

Further, it is the staff's understanding that the actual integrated risk (either ICDP or ILERP) will be tracked during use of the RICT and will be used to determine the amount of time available to reach the integrated risk limits for the RICTs (i.e., $10^{-6}/10^{-7}$ ICDP/ICLERP for RMA threshold RICT; $10^{-5}/10^{-6}$ ICDP/ICLERP for the maximum safety limit RICT). That is, the calculated RICT is dependent upon the actual configuration which currently exists, and on the actual accumulation of risk which has occurred from the point the equipment was declared inoperable. Please clarify.

RESPONSE: The staff's understanding as described is correct.

Finally, it is also the staff's understanding that once the RICT is entered, accumulation of risk toward the $10^{-5}/10^{-6}$ ICDP/ICLERP for the maximum safety limit RICT continues until all LCOs for which the front stop CTs have been exceeded have been restored to a MET status (components fully operable). Please confirm.

RESPONSE: The staff's understanding as described is correct.

2. **RAI #3, in part, requested the requirements for crediting compensatory measures and contingency actions in risk assessments performed for RICT calculations. In response, it was stated that only actions in the PRA model would be credited, typically, and that special emergent conditions would require procedural and administrative controls. This seems to contradict the guidance provided in Attachment 3 of the licensee's August 2, 2004 submittal, used by the operators to determine functionality, which implies that SSCs can be considered functional with manual operator actions "...contained in approved written instructions..." (item 1), and that realignment from surveillance testing can be credited if included in the test procedure. Considering such equipment functional appears to be the expected outcome of the guidance, and effectively assigns an HEP of zero to those manual actions. The staff believes that credit should be taken in accordance with the applicable PRA standards after a realistic or bounding human reliability analysis is used to quantify the action, and an assessment of potential dependencies with other actions is considered. Further, the relevant procedures should be part of the expected plant response to accidents or transients (i.e., emergency or abnormal operating procedures), or to component failure (alarm response procedures), to assure that a direct cue is available which directs the operator to the applicable procedure. The mere existence of written instructions does not assure timely implementation of recovery actions. Please discuss in detail how manual actions are credited for functionality determinations for RICT calculations.**

3. **RAI #4 asked for clarification of the STP process for assessing common cause failure potential. Additional information is required for the staff to understand how STP assesses CCF within the context of a RMTS program.**

   a. **STP identified their Corrective Action Program as providing guidance for the CCF assessment. Please discuss the specific technical guidance provided to the operators which would apply to an emergent failure or condition of components within the scope of the RMTS. Does the CCF assessment require testing, inspections, or other activities to reach a determination? How is the time frame for this assessment determined within the Corrective Action Program (i.e., within the front stop CT?).**

   RESPONSE:

   The CCF assessment is more accurately described as an "extent of condition" assessment. The STP Condition Report procedure requires evaluation of extent of condition for emergent issues that could affect plant reliability. In addition, Licensed Operators recognize that an emergent condition identified on a TS component may have the potential to affect a redundant component or similar components. In addition to a determination of operability on the affected component, the Operator is expected to make a judgment with regard to whether the operability of similar or redundant components might be affected. In accordance with the guidance of Part 9900 of the NRC Inspection Manual (originally provided in Generic Letter 91-18) for degraded and

nonconforming conditions, the determination of operability is to be done promptly, commensurate with the safety significance of the affected component. Part 9900 references the allowed outage time as guidance for performing the evaluation. The STP procedure direction is that initial Operability screening is to be commensurate with the safety significance of the Condition, but should normally not exceed one work week. Initial Operability screening for Conditions with allowed outage time less than 72 hours, and which have a shutdown action statement, should normally be completed within 24 hours.

b. From Attachment 3 of the licensee's August 2, 2004 submittal, it is stated that SSCs are considered functional if it is "reasonably assured" that they can perform intended functions. If an emergent failure of one of three redundant components occurs, would all trains be declared inoperable, but the unfailed components be considered "reasonably assured" of being functional unless they specifically exhibited symptoms of the failure mode?

RESPONSE:

Based on the information available, the Licensed Operator is often able to make an immediate determination that there is reasonable assurance that redundant or similar components are not affected. Using his judgment with regard to the specific condition, the Operator may direct that similar or redundant components be inspected for evidence of the degradation. For conditions where the Operator has less information, assistance from other organizations, such as Engineering, is typically requested. The organization continues to perform the evaluation promptly, as described above. However, unless there is clear evidence otherwise, the Operator will typically consider the redundant or similar components to be operable. The guidance contained in Part 9900 of the Inspection Manual is used as well as conservative decision-making for extent of condition evaluations. The components are considered functional in the PRA unless the operability evaluation determines otherwise.

c. It is stated that if a CCF issue is determined to exist, "it will be accounted for in the operability determination". Please clarify – does this mean that the components will be considered inoperable or non-functional?

RESPONSE: No. See the response to 3.b. above.

d. It is stated that the PRA and CRMP are used to provide safety significance insights "for components that might affect more than one train or function". Please clarify – should this refer to "component failure modes" instead of "components"? How are the insights used in the RMTS program for RICT calculation?

RESPONSE:

A component's failure mode is intended to be implicit with respect to the associated component. With regard to how insights are used in the RMTS program for RICT calculations, the following is offered. The RMTS is a programmatic document that defines the organizations, responsibilities, and processes used to administer the configuration risk management program. Contained within the RMTS program documents are process steps that define risk threshold criteria (an insight), compensatory measures (i.e, insights), and required actions (e.g., communication,

notifications) under certain risk related conditions. Although this response can not address all situations where risk insights might or could be used, the intent of the statements referred to by this portion of question 3 was structured to highlight these types of programmatic features.

The insights may be used to facilitate and prioritize the determination of the extent of condition, as discussed in the response to Question 3a. The RICT may be affected if other SSCs are determined to be affected.

e. It is stated that the PRA "includes the effect of a component failure in the CCF of similar components", but then states that the failure rate of "cross-train" components is not adjusted. Please clarify exactly what the PRA calculation is doing for CCF rates when an emergent SSC failure occurs.

RESPONSE:

The failure rates for cross train equipment within the same system are not adjusted under the assumption that a "train" is removed from service (voluntarily or involuntarily). The common cause treatment is changed. The RISKMAN software is designed to account for removing a train or trains from service (i.e., guaranteeing failure of one or more trains). The common cause treatment is adjusted mathematically by the software. The following illustrates in general how the software treats these conditions:

Assume a two train system, where A and B represent a motor operated valve common cause group with success criteria being one out of two. Failure of the system would be equal to

[A] * [B] + [AB], where [AB] represents a common cause failure of the two components.

The failure equation for the system would be as follows:

$(1-\beta)\lambda * (1-\beta)\lambda + \beta\lambda,$,

where the component failure rate is represented by λ and the common cause failure fraction is represented by β, the common cause factor for this common cause group. $(1-\beta)\lambda$ represents the corrected independent failure rates of A and B.

Since A and B are in the same common cause group (i.e., same component type), they have the same failure rate designator (we will use a RISKMAN motor operated valve failure rate designator, ZTMOVD).

Using Boolean logic, if A is removed from service, then the equation is reduced to:

~~$(1-\beta)\lambda$~~ * $(1-\beta)\lambda + \beta\lambda,$

This equation now reduces to:

$\lambda - \beta\lambda + \beta\lambda = \lambda$

or the failure rate of the remaining component (i.e., ZTMOVD).

The mathematical treatment described above is incorporated into the RISKMAN software. Whenever a component is removed from the equation for modeling conditions where a component is removed from service, this reduction takes place.

f. **It is stated that the CRMP "...requires *consideration*..." of risk reduction actions including plant shutdown if the risk crosses the 1E-5 threshold. It is understood that the 1E-5 risk is the RICT limit, which would *require* applicable TS shutdown actions. How could such actions only be "considered" in a RMTS program?**

RESPONSE:

At this time, prior to implementation of the risk-informed TS, the CRMP considers shutdown if the risk crosses the 1E-05 ICDP threshold. When the proposed risk-informed TS is implemented, TS 3.13.1 will require application of the pertinent TS ACTION from the referencing TS if the 1E-05 threshold is crossed. If that ACTION requires shutdown, then that will be the action required by TS 3.13.1. In accordance with TS 3.0.2, the shutdown action may be exited if the limiting condition is restored.

4. **RAI #7 requested clarification of the assessment of LERF within the RMTS program. In response it was stated that CDF is the only required metric "for nearly all evaluations", then described the capability to perform such assessments with the PRA model. Please clarify under what configurations would a LERF assessment be performed. The RMTS guidelines require the LERF evaluation for all RICT calculations, so it is not clear how LERF could not be required.**

RESPONSE:

The term "for nearly all evaluations" is based on STP's current experience with our RAsCal program which shows that CDF is almost always the limiting figure-of-merit for a RICT calculation. Only the equipment that is important for containment performance and has little or no role in the likelihood of core damage is equipment for which LERF would be more limiting. STP's PRA will have an update to its Level 2 PRA in 2005. Once the Level 2 update is completed, a study will be performed to determine what configurations or equipment are more limited from a LERF perspective as opposed to CDF. The results of this study will be a key input to the final resolution of this issue. Should the occurrence of LERF limited components be relatively small or few (<10), then a logical solution would be to incorporate the LERF calculation directly into the RAsCal database. Should the occurrence of LERF limited components be relatively high (>10), then it could be more cost effective to augment the RAsCal database with LERF calculations for all configurations. In either case, the CRMP will be designed to select the more limiting of the two figures-of – merit, CDF or LERF, for the appropriate RICT calculation.

5. **RAI #8 requested clarification of the RMTS program treatment of planned vs. emergent configurations. In response, it was stated that a threshold CDF of 10^{-6} was established for planned configurations, consistent with the generic guidelines, but then identified that a higher risk level could be used by duty manager approval. It was not stated if this approval is used only to address emergent conditions or if it could be part of the normal planned maintenance practices. It is the staff's understanding that planned use of RICTs would be applicable to preventive as well**

as emergent corrective maintenance, and will not exceed thresholds of 10^{-6} for CDF and 10^{-7} for LERF. It is also the staff's understanding that the use of the higher RICT limits would only be used for emergent failures of equipment or other unanticipated conditions which occur during implementation of an RICT. Please clarify.

RESPONSE:

The staff's understanding is generally correct with the exception that emergent conditions are not necessarily only those that occur during implementation of a RICT. STP plans routine maintenance not to exceed the 1E-06 ICDP threshold in accordance with the configuration risk management procedure. However, the procedure allows planned exceedance of this threshold with Plant General Manager approval. Although it is not a procedure or program limitation, the most likely reason for a planned exceedance would be to address an unexpected condition identified during operation.

6. **RAI #9 requested clarifications of the risk assessments documented in Table 2 of the licensee's August 2, 2004 submittal. Table 2 includes the column "Risk Basis Calculated STP AOT Before Backstop (base case)" which is further clarified in footnote 1 as the calculated time to reach an ICDP of 1E-5. Each of the technical specification LCOs includes actions for one or more of the redundant trains being inoperable, but only a few of the table entries provide the corresponding RICT for each separate configuration. Please provide an expansion of this table to provide the calculated RICT for each number of trains being inoperable within the proposed scope of the submittal. If there is a significant difference in the RICT depending upon which train(s) is inoperable, identify each RICT and provide the basis for the asymmetry in the calculated RICT.**

RESPONSE:

Table 2 is being revised to include additional cases. Note that Table 2 is not intended to be all-inclusive. Its purpose was to provide the reviewer with a general insight with regard to the margin to the existing allowed outage times.

STP's CRMP program uses an approach where pre-solved configurations are retained in database for the RAsCal program. There are over 20,000 individual configurations and their associated CDF values contained in this database. All train combinations are included. If the Staff requires this information, STP will make arrangement s for the entire database to be sent to the staff for review. This would be a voluminous RAI response. In Table 2 of STP's August 2, 2004 submittal an attempt was made to provide configuration risk information based on current Technical Specification structure, so not all possible configurations were included; however, that information is available for staff review. STP will make the information available to the NRC but will need input as to which items are requested.

7. **The staff has no additional questions regarding RAI #10, except to confirm our interest in seeing the STP program demonstrate application of the RMTS for several plant configurations.**

RESPONSE: STP can arrange to demonstrate the application either at the STP site or in the NRC offices.

8. RAI #12 requested further explanation of the distinction between "inoperable" and "non-functional" components within the RMTS process. In response, Attachment 3 of the licensee's August 2, 2004 submittal was referenced. The staff requests additional clarification of the use of functionality to determine RICTS for TS.

a. The licensee submittal identifies a differentiation between the definition of OPERABILITY applied to the technical specification LCOs, and the term "functionality", which is not defined in technical specifications, to be applied to components for calculating RICTs. When a component is INOPERABLE, due to the inability to perform a limited portion of its intended functions, and these functions are distinguishable in the PRA model and can therefore be quantified while taking credit for those functions which the component is still able to perform, it may be acceptable for the RICT to be longer than would otherwise be calculated if the component is assumed to be completely non-functional. However, if one or more components are determined to be INOPERABLE, but the loss of functionality is (1) not known or uncertain, or (2) not capable of being addressed in the PRA model, then the component should be assumed to be non-functional for purpose of calculating a RICT. This would typically arise with emergent issues associated with design issues of components which impact all safety trains, and would currently require entry into TS 3.0.3. Please discuss in detail how components which are inoperable may be evaluated as fully or partially functional in the calculation of RICTs. Several examples which cover the spectrum of possible conditions may be beneficial to the staff's understanding of this issue.

RESPONSE:

STPNOC agrees that if a component is determined to be inoperable and there is not reasonable assurance of its functionality or it is not capable of being addressed in the PRA model, it should be assumed to be non-functional for calculating the RICT. As discussed in the response to Question 3.b, the redundant or similar components may still be considered operable and functional.

The August 2, 2004 application provides the CRMP requirements for a component to be considered functional. The criteria described in the CRMP typically apply to situations affecting a single component, not conditions where TS 3.0.3 would apply. In no case is a component determined to be functional without authorization from the Shift Supervisor.

Other examples of where a component might be considered functional or partially functional such that the condition could be quantified in the determination of an allowed outage time are listed below.

- SSCs that don't meet seismic requirements but are otherwise capable of performing their design function.
- SSCs that are inoperable but secured in their safe position (e.g., a closed containment isolation valve).
- SSCs powered from a source other than their normal power source, provided the alternate power source is modeled in the PRA.
- An SSC with an inoperable automatic function if the manual actuation of the SSC is modeled in the PRA (e.g., a diesel generator with an inoperable sequencer).

- A valve that is inoperable because it doesn't meet closure time requirements but the closure time is not important to the accident analysis.

b. With regards to functionality vs. operability, it is understood that functionality will only address requirements modeled in the PRA. Some mitigating functions are reviewed and screened out in the development of a PRA model due to low frequency of demand for the particular function, or the low probability of failure of the function. For specific configurations which may be encountered during planned maintenance or testing, combined with possible emergent conditions, these screened functions could become more important, and would potentially impact the calculation of a RICT. For each of the TS LCOs for which the RMTS will apply, (1) identify the PRA function(s) which are modeled including success criteria if different than the design basis, and (2) identify any design basis functions not modeled, and (3) justify that these should not significantly impact the calculated RICT under configurations covered by the RMTS.

RESPONSE:

The response to this question will be addressed in parts. However, prior to each of the three sections some background information is provided.

1). STP's PRA has undergone several independent reviews for scope and quality. In general, PRA functions modeled are contained in the system and event tree notebooks documentation. In this regard, the documentation of PRA functions is required by PRA standard's requirements. In STP's peer review there was not an observation documented on the lack of this information but that the information was dispersed in numerous system and event tree notebooks. STP will be providing a Success Criteria notebook with the upcoming Revision 5 of its PRA to place modeled PRA functions and associated success criteria in a more reviewer friendly format.

2). It is important to note that only those safety functions which are within the PRA scope (or which can be directly linked to a PRA scoped function) are in the RMTS scope. In general there are very few design basis functions not within the PRA scope. An example of a design basis function not modeled in the PRA is radiological detection systems.

3). As mentioned in 2) above, only those systems within the PRA scope are in the RMTS scope. Those systems which are not in the scope of the PRA will not be a part of the RMTS and, thus, will retain their current TS allowed outage time requirements.

c. Further with regards to functionality vs. operability, Attachment 3 of the licensee's submittal identified procedural requirements for functionality. The staff requests additional clarifications of the application of these requirements in RMTS:

Item 1 states that a component is functional without automatic actuation if "prompt restoration" by the control room operator or a dedicated local operator is available, with written instructions provided for actions not involving complex repairs or diagnostics. Similarly, item 9 allows actions in surveillance procedures to be similarly credited. The staff assumes that such recovery actions would not normally be part of the baseline PRA model, but would be specific to the configuration. Crediting such manual recovery actions, without a

quantitative consideration of the human error probability, or of dependencies on other actions which may be required in specific sequences, would not be appropriate for calculation of RICTs. This also appears to conflict with responses made to NRC RAI 3, that only PRA modeled actions are typically credited in the RICT calculations.

Item 4 identifies examples of alterations which affect functionality. Some can be directly evaluated as to impact (i.e., jumpers or lifting electrical leads), but the others are somewhat uncertain as to the impact on functionality.

Item 5 allows an SSC to be functional if there is "reasonable assurance" that it can perform its intended functions. The staff is concerned that two standards are being applied with regards to the operators' confidence in assessing the status of SSCs, one to determine operability and a lesser standard to determine functionality.

Items 5 and 8 identify that, if the functionality determination is later determined to be in error, "non-functional time will be corrected accordingly". This implies that the determination of functionality need not be rigorous and can have some degree of uncertainty, since it can be later modified if found to be incorrect. This would not be appropriate for RICT determination.

RESPONSE:

The standards for determining a component is functional with manual action in lieu of automatic action are identical to the standards applied in Part 9900 of the Inspection Manual for determining a component is operable with manual action in lieu of automatic action. For an operator action to be credited to maintain functionality, it must be modeled in the PRA.

The response to Question 8.a. describes the standards for functionality, which clearly require the component to be able to perform its function and requires the degradation to be quantified in the PRA. If the degradation can not be modeled in the PRA then the component would be considered not functional for purposes of calculating a RICT. The requirements for operability as it is defined in the TS have not changed.

The functionality determination is expected to be correct. The functionality determination is performed in accordance with regulatory inspection guidance as mentioned above. The likelihood of the functionality determination being wrong would be considered a rare event unless new information was discovered that had a direct impact. In the event that this occurs, the RICT calculation would be corrected and incorporated. Other actions that may be required as a result of the revised RICT calculation would be processed in accordance with station procedures. The intent is not to relax the rigor of the determination, but only to prescribe how the component is to be treated in tracking the cumulative risk in the unlikely event that the determination is found to be incorrect.

9. **RAI #24 requested justification of proposed changes which involved application of the RMTS to loss of function conditions. The staff requests additional discussion of these configurations, and refers to new RAIs #25 through #38.**

10. The licensee proposes to apply a RICT to the reactor trip breakers (TS 3.3.1.20) and to the automatic trip and interlock logic (TS 3.3.1.21). It is therefore critical to this application that the PRA modeling and success criteria for ATWS sequences be thorough and comprehensive, unless bounding analyses are applicable.

a. In the development of accident sequences, it is not unusual to screen out failure to trip the reactor for some initiating events, such as LOCAs, steamline breaks, or SGTRs, since the combination of the low frequency initiator and the failure of the reactor trip system, as well as the potential for adequate negative reactivity from ECCS flow, make these sequences very low frequency. However for this application, such a screening process may not be appropriate. Please discuss.

RESPONSE:

STP has elected to remove the reactor trip breakers (TS 3.3.1.20) from the scope of the application.

b. The success criteria for mitigation of an ATWS event is dependent upon the specific point in each operating cycle, as well as the cycle-specific core reactivity design characteristics (i.e., moderator temperature coefficient and the unfavorable exposure time). It is not unusual that the risk calculations performed to support the CRMP for Maintenance Rule a(4) would not specifically account for the time in the operating cycle, but instead use a cycle-average risk calculation. In order to support the calculation of a RICT for these TS, such an average calculation may not be appropriate, and the configuration-specific risk should account for this time-dependent impact. Please discuss.

RESPONSE:

See response to RAI #10a above.

As general information to the Staff the following is provided:
For purposes of the RICT calculation, the PRA does not use cycle averaged risk values for core reactivity design characteristics. Instead conservative or bounding values are used for establishing success criteria for equipment required in ATWS scenarios. Therefore, the maintenance states and subsequent RICT calculations used in STP's CRMP are not varied based on operating cycle core reactivity design characteristics.

c. The existing technical specifications do not address the operability of the AMSAC. Since the AOT is only six hours when the reactor trip function is unavailable, it is not critical that AMSAC be considered. However, if a RICT is implemented, then the operability of AMSAC should be required so that there is some mitigation immediately available in the event of a demand for a reactor trip. Please discuss how AMSAC is addressed in the PRA model, and whether a new TS for AMSAC should be required given the proposed modifications to these TS requirements.

RESPONSE:

See response to RAI #10a above.

As general information to the Staff the following is provided:

AMSAC does not meet the 10CFR50.36(c)(2)(ii) criteria necessary for a limiting condition for operation. AMSAC; however, is included in the PRA and its contribution is calculated for all maintenance states. It should be noted that its quantitative effect is negligible in terms of a RICT.

d. **The emergency boration system (EBS) was deleted from the STP design based on acceptable fuel performance in the event of a return to criticality for a steamline break accident. STP is proposing to apply a RICT to the trip logic and breakers, and the MSIVs and actuation logic. How does the STP PRA model address steamline break accidents with regards to the synergies between reactor trip and steamline isolation functions? Is the model detail able to distinguish concurrent unavailability of these related functions with regards to the potential for core damage due to return to criticality?**

RESPONSE: See response to RAI #10a above.

11. **The licensee proposes to apply a RICT to the steam line isolation actuation logic and relays (TS 3.3.2.4.b), to the turbine trip and feed water isolation actuation logic and relays (TS 3.3.2.5.a), to the main steam line isolation valves (TS 3.7.1.5), and to the main feedwater isolation valves (TS 3.7.1.7). These LCOs exist to limit the reactor cooldown transient, and such events are not typically modeled in PRAs as being relevant to core damage. Please describe how the STP PRA models these functions such that an RICT is appropriate.**

RESPONSE:

The Staff is correct that cooldown transients are not always modeled in PRAs; however, STP's PRA does include cooldown events. Cooldown events are modeled for General Transients (i.e., turbine-generator trip) since this initiator is relatively frequent in a probabilistic sense and for the Small LOCA and SGTR initiating events. Cooldown events are not modeled under other initiators such as large/medium LOCA since decay heat removal is a part of the initiator itself or is not applicable to the initiator. For any excessive cooldown, the effect of the cooldown is modeled under pressurized thermal shock event tree top events. In summary, cooldown events are included in STP's PRA, their contribution is small and, therefore, their contribution to a RICT is very small.

12. **The licensee proposes to apply a RICT to the pressurizer code safety valves (TS 3.4.2.2). There are no tests or maintenance performed on these valves during operation, and no challenges occur which would reveal an INOPERABILITY. Therefore, the only application of the RICT would be to allow extended time to deal with an emergent issue causing INOPERABILITY of all three valves.**

a. **Does the scope of the STP PRA model include all design basis events which result in a challenge to the code safety valves? If not, please identify those events not modeled, discuss the plant response to the event under these conditions, discuss why continued plant operation is appropriate with no code safety valves OPERABLE to mitigate those events, and identify what compensatory measures would be applicable during such operation.**

RESPONSE:

STP has elected to remove the pressurizer code safety valves (TS 3.4.2.2) from the scope of the application.

b. The submittal states that the pressurizer PORVs and sprays provide overpressure protection. Is the mitigating capability of these components (e.g., capacity, response time, availability during design basis events) equivalent to the code safety valves? Are these components able to provide equivalent overpressure protection to the reactor coolant system pressure boundary for the spectrum of design basis events which challenge the code safety valves? The pressurizer spray valves are not included in the scope of technical specifications, and indefinite power operation with both PORVs isolated is permitted under TS 3.4.4; should this specification include a requirement for OPERABILITY of one or both PORVs and/or the pressurizer spray valves? Does the STP PRA model include both the PORVs and spray valves as an alternative to the code safety valves?

RESPONSE: See response to RAI #12a above.

c. The proposed changes to TS 3.4.2.2 do not include any assurance of the OPERABILITY of any component(s) which are capable of providing overpressure protection to the reactor coolant system pressure boundary to assure that the safety limit for maximum RCS pressure is not exceeded. Please identify how the integrity of the RCS as a fission product barrier is assured under such operations.

RESPONSE: The STP application has been revised to remove TS 3.4.2.2 from its scope.

13. The licensee proposes to apply a RICT to the pressurizer power-operated relief valves and their associated block valves (TS 3.4.4). The submittal identifies a RICT of 352 days with one PORV inoperable, and 349 days with both PORVs inoperable. It is not clear why these RICTs are so similar. Please clarify:

a. What accident sequences take credit for operation of the PORVs?

RESPONSE:

ATWS and Feed & Bleed scenarios both incorporate the contribution of PORV operation in their accident sequences. SGTR sequences question the pressurizer PORVs as an alternate to the pressurizer spray valves.

b. What is the success criteria for the PORVs for each accident sequence?

RESPONSE:

Feed and Bleed requires two of two pressurizer PORVs, ATWS overpressure response requires one of two PORV's depending upon the status of the AFW pumps. SGTR sequences require one of two PORV's for RCS pressure reduction.

c. If the PORVs are credited for overpressure protection of the RCS, as a redundant capability to the code safety valves, discuss if operator action is credited in the event of (1) the failure of the automatic function or (2) if the PORV is isolated due to seat leakage.

RESPONSE:

The PORV's are not credited as redundant capability to the pressurizer code safety valves.

14. The licensee proposes to apply a RICT to the safety injection system accumulators (TS 3.5.1).

a. Confirm that the success criteria and the required accident sequences for the accumulators is consistent with the design basis analyses, or provide a sensitivity study of the calculated RICTs for one or more accumulators inoperable using the design basis criteria.

RESPONSE:

The accumulator success criteria for injection is the same as the design basis. Two accumulators inject into intact loops, one accumulator injects into the broken loop.

b. For action b when boron concentration is not within limits, the submittal states that the RICTs presented for action a apply. This seems inconsistent with other parts of the submittal where it is stated that the functionality of the INOPERABLE components is used to determine the RICT. Please discuss how the RICT would be applied to action b.

RESPONSE:

Unless the PRA can quantify the specific effects of the boron concentration, STP will consider the accumulator made inoperable to be non-functional. However, a RICT for one or more non-functional accumulators will be substantially longer than the current allowed outage time and application of TS 3.13.1 is appropriate for ACTION b.

15. For TS 3.5.2 for ECCS, with two or more subsystems INOPERABLE, the proposed change requires restoration of at least one ECCS train to OPERABLE status within one hour. In Table 2 for this LCO, it states that a risk-informed AOT is appropriate with no OPERABLE trains. However, the RICT could not apply since the proposed action requirement is to restore one train within one hour. Is this the intent of the changes to TS 3.5.2? Please clarify.

RESPONSE:

The proposed change to TS 3.5.2.b has been revised to change "and" to "or". For a condition where all three trains of HHSI are inoperable and non-functional, the configuration will exceed the 1E-03/yr instantaneous core damage frequency criterion and the shutdown action of TS 3.5.2.b will be required.

16. For TS 3.6.2.3 for the reactor containment fan coolers, the calculated RICT is stated to be based on CDF and there was no impact on LERF. Please clarify how the fan coolers are credited in the PRA model for mitigation of core damage given that the

design basis function is containment heat removal, and identify the basis for the success criteria (i.e., judgment or specific calculations).

RESPONSE:

17. **For TS 3.7.1.5 and 3.7.1.7, the wording of the action requirement includes a note which states: "Separate condition entry is permitted for each MSIV (MFIV)." This wording is inconsistent with other action statements being revised, as is noted in Table 2. Introducing a new phrasing would seem to be an unnecessary complication and distraction to the operators applying the technical specifications. Further, as worded the proposed action could be interpreted to allow a new 30 day backstop AOT to be constantly applicable without restoration of all MSIVs or MFIVs to OPERABLE status. Please confirm that inclusion of this note is not intended to create any unique interpretation of the application of a RICT for these specifications, with regards to applying the 30 day backstop. Specifically, confirm that it is not intended to have a separate 30 day backstop for each individual MSIV or MFIV, but only a single 30 day backstop applicable to all valves.**

RESPONSE:

TS 3.7.1.5 and TS 3.7.1.7 have been revised to be consistent with the format of the other TS that reference TS 3.13.1. The provision for separate condition entry has been eliminated.

18. **For TS 3.7.14 for chilled water, which supplies room cooling to safety-related equipment, it is typical that the PRA model would only include a subset of the components supported, based on room heatup evaluations. It is also typical to include time-of-year flag events to turn off the ventilation models when cooler outside temperatures exist. These PRA model conventions would result in a 30 day LCO for large portions of the system, and during winter months. Please discuss STP plans in this regard.**

RESPONSE:

19. **For TS 3.8.1.1 for AC sources, Table 2 states that the STP switchyard is served by 8 incoming lines. However, there is no control in the technical specifications requiring these 8 separate lines. Please describe how the STP PRA model accounts for the unavailability of one or more incoming lines. Describe also the plant configuration controls on the incoming lines.**

RESPONSE:

RESPONSE:

The 8 incoming lines feed the STP switchyard and are part of the off-site electric power grid. As such, they are not subject to Technical Specification requirements. Technical Specification 3.8.1.1 requires two independent circuits between the off-site transmission network and the on-site Class 1E distribution system in accordance with GDC-17. Attachment 1 discusses the TS treatment for the required off-site circuits. The STP PRA models two of the 8 lines to account for maintenance on the North Bus or South Bus in the STP switchyard. Otherwise, the 8 lines are not specifically modeled in the PRA.

STPNOC is not the controlling authority for the off-site transmission network. However, STP has direct communications with the controlling authority and may coordinate activities with the system operator. The controlling authority will not perform switching operations or restoration that affects STP without first contacting the STP control room. In addition, STP has agreements with the operator for early power restoration should there be a loss of off-site power. The controlling authority will notify STP regarding status of grid restoration should the grid be lost.

20. **For TS 3.8.1.1, Action d, which applies concurrently with actions b and c, is inconsistent with those actions with regards to the application of 3.13.1. Specifically, action d requires that 3.13.1 be applied within 24 hours. The requirement to apply 3.13.1 at 14 days (action b) is unnecessary since 3.13.1 was already in effect from action d. Similarly, the requirement to apply 3.13.1 at 12 hours (action c) renders action d unnecessary.**

RESPONSE:

The submittal has been revised to delete TS 3.8.1.1.d. New TS 3.13.2 is proposed that requires a risk assessment any time Limiting Conditions for Operation are entered for PRA modeled TS SSCs on different trains. The conceptual wording for TS 3.13.2 is provided below.

3.13.2 Application of the specified allowed outage times for inoperable equipment in different safety trains shall meet the criteria of the Configuration Risk Management Program

APPLICABILITY: Entry into the ACTION statements for two or more components associated with different safety trains and to which Specification 3.13.1 may be applied

ACTION: Determine the configuration is acceptable for the application of at least the specified allowed outage times for the affected components within the shorter of 24 hours or the shortest affected allowed outage time. For configurations where the specified allowed outage time is not acceptable, restore one or more of the affected components to OPERABLE status within or declare the LCO not met for the most limiting affected component and apply its associated ACTION.

21. **For TS 3.8.1.1 Action d, the defense-in-depth requirement that, for a loss of offsite power, at least one safety train of equipment is OPERABLE and powered from an OPERABLE EDG is eliminated, as is the requirement for OPERABILITY of the steam driven AFW pump for station blackout mitigation. In response to related RAI #20, STP stated that existing procedures "require very similar compensatory actions". It is not clear why an existing requirement is proposed to be eliminated from TS control within the context of RMTS 4b initiative. Please discuss, and provide examples of the RICT for cases involving EDGs and other supported equipment.**

RESPONSE:

Proposed new TS 3.13.2 will replace TS 3.8.1.1.d. TS 3.13.2 has broader applicability than TS 3.8.1.1.d. since it is not limited to conditions where an EDG is affected but will require a

risk assessment whenever more two or more cross-train components are inoperable.

If there are inoperable cross-train components, the AOT should depend on the risk significance of the specific configuration. For instance, an inoperable cross-train accumulator or reactor containment fan cooler would be of low significance and additional time up to the 30 day backstop can be justified if necessary. Concurrent inoperability of an EDG and the turbine-driven auxiliary feedwater pump is more limiting but still has over 20 days to cross the 1E-05 threshold (see Example 2 in the August 2, 2004 application). Example 1 in the August 2, 2004 application quantifies a configuration with a Train A maintenance outage (including EDG A, and HHSI A) and a concurrent failure of Train B HHSI. Train C is unaffected in this example. The calculated time to cross the 1E-05 threshold is also over 20 days.

22. **For TS 3.8.1.1 Action e, which applies when two of the two required offsite AC circuits are INOPERABLE, Table 2 of the submittal states that STP will maintain in this configuration at least one ESF bus with offsite power. This requirement is not found in the technical specifications. Please confirm if this is intended as a commitment.**

RESPONSE:

The application of TS 3.13.1 to TS 3.8.1.1 ACTION a and ACTION e is discussed in detail in Attachment 1.

23. **For TS 3.8.3.1 (onsite power distribution), Table 2 states that the loss of a single ESF bus does not result in a plant trip. If the ESF bus is de-energized, the battery chargers for that train would be lost, and after a period of time the batteries would deplete. Does the loss of one DC train cause a plant trip? If so, wouldn't the application of 3.13.1 for this LCO (and for TS 3.8.2.1 for batteries and chargers) potentially lead to a plant transient?**

RESPONSE:

Implementation of the energize to actuate modifications in both units has removed the immediate plant trip associated with the loss of one DC channel. However, for loss of the Channel I or Channel III DC bus, a plant trip on low steam generator level will occur within a short time as the hydraulic pressure bleeds down for the feedwater isolation valves associated with those channels and the valves go closed.

It is not STPNOC's intent to use TS 3.13.1 to extend the allowed outage time for configurations where the Channel I, Channel III, or Channel IV battery bank is the sole source of power for the loads on the DC bus. A note has been added to TS 3.8.2.1 to restrict the application of TS 3.13.1 for these conditions.

Operator action can be taken to energize the ESF bus from alternate sources, such as the Emergency Transformer, its own EDG or the opposite unit Standby Transformer. In addition, STP has procedures to enable cross-train feed to an ESF bus for some configurations. AC vital distribution panels can be energized from same-train Class 1E AC power apart from the normal power to their associated inverters. The DC bus could be energized through its associated batteries with its associated charger powered from an alternate source or from a temporary charger. With inoperable batteries, the DC bus can be energized through an operable charger or a temporary charger. Most of the example

alternatives could be implemented in either a planned or emergent condition and none would result in a plant transient. TS 3.13.1 would allow appropriate consideration of these alternatives in determining an allowed outage time.

See Attachment 1 for additional discussion.

RG 1.200 PRA Quality

NOTE: During the staff review of Regulatory Guide 1.200 conducted at STP, the reviewers encountered difficulty in assessing how the STP PRA complied with the elements of the standard. This was based in part on the staff's unfamiliarity with the support state methodology; however, it was also attributed to the lack of adequate documentation. The staff is currently assessing how to assure a thorough review and assessment of STP PRA quality per the requirements of Regulatory Guide 1.200, and considers the following RAIs to be gathering preliminary information leading to a more detailed assessment.

24. **Regulatory Guide 1.200 sections 1.2.4 and 1.2.5, and section 1.3 Table 3, identify attributes of a fire PRA and external events PRA, which are not addressed by existing PRA standards. The licensee is requested to describe the scope and quality of their fire and external events PRA models, addressing the attributes identified in the guide.**

    RESPONSE:

25. **Regulatory Guide 1.200 section 4.2 requires the licensee to submit "... a discussion of the resolution of the peer review comments that are applicable to the parts of the PRA required for the application." Two options are identified, one to provide a discussion of how the PRA model has been changed, and the second to provide a sensitivity study that demonstrates the particular issue does not impact the significant accident sequences or contributors. The licensee has provided only the numerical identification of their peer review facts and observations, and identified which were categorized as level 'A' or 'B' (Attachment 5, Resolution of Peer Review Comments, to submittal letter dated 10/28/2004). Therefore, the licensee is requested to submit the information required by the guide to address the resolution of peer review comments.**

    RESPONSE:

26. **Regulatory Guide 1.200 section 4.2 requires the licensee to submit the identification of the key assumptions and approximations relevant to the results used in the decision-making process, along with the peer reviewers' assessment of those assumptions. Reference is made to Regulatory Guide 1.174 in section 3.3 for applicable guidance on addressing the impact of these assumptions on uncertainty as it relates to the decision-making process. Only four areas were identified by the licensee, and the peer review assessment was not provided (Attachment 4, Key Assumptions and Approximations, to submittal letter dated 10/28/2004). Since this is a "whole plant" application of risk-informed TS initiative 4B, it is expected that there would be something more than four key assumptions/approximations applicable. Therefore, the licensee is requested to submit additional information regarding the key assumptions and approximations in their PRA model, along with the peer reviewer assessments.**

RESPONSE:

27. **Regulatory Guide 1.200 section 4.2 requires the licensee to submit documentation that the PRA is consistent with the standard as endorsed in the appendices to the guide, and the identification of the parts of the PRA that conform to the less detailed capability categories and the limitations which this imposes. The licensee did not identify how their PRA model conforms to the capability categories identified in the ASME Standard as endorsed by the appendices to Regulatory Guide 1.200 (Attachment 3, Conformance to Standards, to submittal letter dated 10/28/2004). Further, during the NRC staff review of the STP PRA for the Regulatory Guide 1.200 pilot, the reviewers noted that the STP self assessment documentation was "difficult to discern their conclusions about their PRA". Therefore, the licensee is requested to submit the information required by the guide, and their plans and schedules (if applicable) to address identified deficiencies which are relevant to this application.**
RESPONSE:

28. **Regulatory Guide 1.200 section 1.2.6 describes the characteristics of PRA model documentation. During the NRC staff review of the STP PRA for the Regulatory Guide 1.200 pilot, deficiencies in the documentation were specifically noted, and it was further identified that STP placed excess reliance on one particular experienced staff member. Because the nature of this application is to place ongoing reliance on the accuracy and quality of the PRA model to calculate RICTs for the technical specifications, robust documentation of the PRA model is essential to assure the capability of the licensee to properly maintain the fidelity of the model, without undue reliance on specific staff members. The licensee is therefore requested to describe the current capability of their PRA model documentation, and to identify a schedule for updates and upgrades to assure their documentation is adequate to permit ongoing maintenance of their PRA models for the following key areas:**

    a. **Key assumptions and approximations applicable to system and event tree models.**

       RESPONSE:

    b. **Screening of sequences or failure modes from the model.**

       RESPONSE:

    c. **Quantification instructions, including recovery rules and their bases, mutually exclusive event combinations and their bases, and truncation levels.**

       RESPONSE:

PRA Technical Questions

29. **During the NRC staff review of the STP PRA for the Regulatory Guide 1.200 pilot, issues with the adequacy of the common cause failure modeling were noted during very brief reviews of system modeling. The methods were not using the most recent available information, and some CCF modes were not considered (i.e., batteries, chargers). The licensee is requested to describe the development of CCF models for**

their PRA, and provide a listing of the CCF modes considered, the components which are modeled for CCF, and the sources of data used.

RESPONSE:

30. **For use in the configuration risk management program, the baseline PRA model requires changes to account for the real time nature of the calculations, compared to the average annual risk calculation of the baseline model. The licensee is requested to describe the process of making changes to the baseline PRA model for the CRMP, including the following key areas in their discussion:**

    a. **Alignment of operating train(s), including swing or spare components.**

    RESPONSE:

    STP's baseline PRA employs a maintenance pre-tree to establish a specific configuration. This pre-tree establishes the initial alignment of running and standby trains of equipment for systems which are under continuous duty (e.g., Essential Cooling Water, Component Cooling Water). All reasonable initial configurations (based on plant operating experience) are included in the pre tree quantification. For the CRMP, the actual equipment configurations are set by event tree macros (the equivalent of fault tree flags). Maintenance equipment macros are defined for all trains/components included in the RICT calculations. Given an initial operating support system configuration, e.g., A and B operating, C in maintenance, all affected initiating event rules and train top event rules are defined by the status of the pre tree maintenance macros.

    b. **Disallowed maintenance (i.e., multiple trains in maintenance typically removed from final results, should be retained in CRMP model).**

    RESPONSE:

    No post-processing of disallowed maintenance states is performed in the STP PRA model. Any possible maintenance configuration can be set by the equipment configuration macros and the PRA model quantified. Therefore multiple trains in maintenance are not disallowed by the CRMP PRA model. Typically however, once the initial alignments are established planned maintenance events are modeled in accordance with station procedures and work planning guidelines (i.e., two trains out of service for planned maintenance is not permitted). NOTE: Unplanned maintenance events due to hardware failure, etc. are included in the system level models.

    c. **Maintenance impact on initiating events for systems.**

    RESPONSE:

    Maintenance unavailabilities are specifically incorporated for impact on initiating events frequencies.

    d. **Adjustment of initiator frequencies (i.e., average CDF model includes unit availability factor, not applicable to CRMP model).**

    RESPONSE:

Initiating event frequencies are all adjusted to represent annual operation (i.e., per operating year (8760 hours)). The at-power average PRA specifically adjusts for station availability factors. For purposes of configuration risk calculations, no initiating event adjustment is performed.

e. Seasonal dependencies, or point-in-cycle dependencies (e.g., seasonal HVAC requirements, ATWS success criteria).

RESPONSE:

Currently, STP's CRMP model does not incorporate seasonal dependencies or point-in-cycle dependencies.

f. Repairs of failed components (should be removed in CRMP model).

RESPONSE:

STP's PRA model does not take credit for equipment repair as a recovery action for configuration risk calculations.

31. During the NRC staff review of the STP PRA for the Regulatory Guide 1.200 pilot, issues with the adequacy of the LERF model were identified and require resolution:

a. The STPNOC self-assessment of LERF did not include an explicit review of the LERF elements of the PRA. Rather, reliance was placed on results of the independent peer review and an STPNOC contractor's proposal for addressing the peer review comments. However, the technical issues and criteria used to conduct the peer review do not fully cover the areas addressed in the ASME standard. As a result, the assessment of PRA capability in the area of LERF is incomplete. Please complete the self assessment of LERF, and identify the results and corrective actions from that assessment.

b. The attributes used to distinguish large, early releases from other source terms is insufficient to discern a "potential for early health effects" as required by the Standard. With the exception of containment bypass and induced steam generator tube rupture (ISGTR), the sole characteristic of large early release (LER) sequences is the size of the opening in the containment pressure boundary. Although this attribute is typically an important contributor, it is not the only one. Some of the sequences assigned to the LER category involved long-term operation of containment sprays and have wet cavities (i.e., quenched debris ex-vessel). Conversely, some of the small early release (SER) sequences involve dry containments (no sprays and dry cavities). A technical basis for this counter-intuitive grouping scheme is not offered in PRA documentation.

Further, the simplistic method of assigning release categories does not appear to be supported by results of plant-specific MAAP calculations of radionuclide release. Consider the following two damage states:

- **SGTR (fast station blackout with induced SGTR during core damage).**
- **07SU (fast station blackout with pre-existing containment leakage).**

According to the attributes used to assign accident sequences to release categories, the first of these is allocated to LER (RC-I), whereas the second is classified as SER (RC-II). However, the MAAP results indicate the following actual release fractions within the first 5 hours of the event:

Fission product group	Percent of Core Inventory Released to Environment	
	ISGTR	R07SU
Xe, Kr	20	50
I	9	3
Cs	8	2

c. A systematic search for, and evaluation of, plant-specific containment failure modes was not evident in PRA documentation. As assessment of containment failure modes was performed as part of the STP IPE. However, much of the IPE analysis relied on adapting the structural evaluation of the Zion containment. Although adaptation of reference plant analysis is acceptable for determining the ultimate strength of the containment pressure boundary under quasi-static loads, a plant-specific evaluation of alternative failure modes was not found in PRA documentation.

d. Actions to mitigate the effects of core damage recommended in the STP severe accident guidelines (SAGs) are not addressed in the PRA. For example, successful implementation of the guidelines offered in SCG-1 could alter the magnitude of radiological releases.

e. The effects of major assumptions, simplification and uncertainties on LERF have not been evaluated.

f. The effects of adverse environmental conditions in containment and physical effects of structural failure(s) of the containment pressure boundary on long-term spray recirculation operation are not addressed. STPNOC documentation provided during the review indicates the minimum NPSH required by containment spray pumps (operating in recirculation mode) is 20 ft-H_2O.

RESPONSE:
The elements in this question are being addressed in the update of STP's Level 2 PRA which is currently underway. The Level 2 update is scheduled for completion in 2005. Thus, the responses to each of the items in this RAI items will be provided at that time.

Additional Electrical Questions

32. This is a followup question on the STP response to RAI 19 on compensatory measures, as it would apply to Technical Specification (TS) 3.8.2.1, DC Sources,. Following the December 15, 2004 public meeting at NRC, the licensee provided a copy of procedure 0POP01-ZO-0006, Extended Allowed Outage Time.

The risk informed completion time (RICT) for two out-of-service battery chargers for this TS is 140-1042 days with a proposed 30 day back-stop. A backstop time of 30 days by itself is not acceptable for the following reasons:

a. The battery, without a battery charger, will continue to discharge at a rate related

to the normal dc operating load. This may result in a deep discharge damaging the connected battery cells by a reverse polarity to the weakest cells. This could be irreversible.

b. The battery is sized for a limited time discharge of 2 hours. If a battery charger is not restored within that time, loss of a complete protection channel will result. Also, possible loss of a complete ac power train could result because dc control is required for the ac power system to be operable.

c. Typical battery manufacturer's operating manuals state that damage may occur to an open circuited (unloaded) after some time (months) without the battery being on charge.

RESPONSE:

The 30 day backstop is proposed as the backstop that will apply to all of the risk-informed TS in this application. The responses to Questions 23 and 34 and Attachment 1 are also relevant to the applicability of TS 3.13.1 to batteries.

The calculated allowed outage time for the batteries includes the risk associated with the consequential failures from the unavailability of the batteries, including the loss of a protection channel. Loss of a protection channel is addressed in the proposed changes to TS 3.3.2 and the calculated AOT also allows application of the 30 day backstop. The length of the AOTs reflects the very small effect on CDF.

For planned configurations involving application of TS 3.13.1 from TS 3.8.2.1 for an inoperable battery, STPNOC would be able to plan the work to prevent damage to the batteries. For emergent conditions where TS 3.13.1 might be applied from TS 3.8.2.1, STP procedures recognize the potential for battery depletion or damage from discharge and require appropriate action to minimize this potential.

33. Procedure 0POP01-ZO-0006, Extended Allowed Outage Time, does not address the DC system. Please identify all compensatory measures for the DC system when removing a required battery charger from service. Also, please address how the following items, including required action time, will be accomplished when battery charging capability is not available:

a. Limit the immediate discharge of the affected battery.

b. Recharge the affected battery to float voltage conditions using a spare battery charger.

c. Confirm that the partially discharged battery has sufficient capacity remaining to perform its safety function.

d. Periodically verify battery float voltage is equal to or greater than the minimum required float voltage.

RESPONSE:

STPNOC does not intend 0POP01-ZO-0006 to be a comprehensive listing of compensatory actions.

The actions listed in 33.a – d are all actions that could be applied to manage the risk associated with an inoperable battery. The response to Question 23 and Attachment 1 also address options for managing the risk associated with inoperable batteries or DC power alignment.

34. The original allowed outage times (AOTs)/completion times (CTs) established in the technical specifications were, in part, based on realistic industry standards for maintenance time intervals for equipment under test or maintenance. It is the staff's understanding that the additional optional extended AOTs based on the risk management techniques will not be entered as a standard operating practice but will only be entered when the maintenance or test conditions can not be completed because of some extraordinary circumstance. This being the case;

RESPONSE: Use of the risk-informed completion times is not limited to extraordinary circumstances. They may be used for planned or emergent activities.

a. Please identify those electrical components where you believe this extended AOT/CT may be necessary, identify the length of the extended AOT/CT and provide justification why such an extended AOT/CT would be required. A 30 day extended outage should not be required based upon past industry experience for the following equipment: Circuit breakers and other switchgear components, transformers, motors, cables, battery chargers, inverters, control and protective relays and associated circuits.

RESPONSE:

The STP application specifically identifies the electrical system TS to which TS 3.13.1 may be applied and includes all the electrical TS that apply in MODE 1-4. Table 2 in the application identifies example AOTs associated with those TS, assuming the condition identified in the table is the only inoperable TS component.

TS 3.8.2.1 and TS 3.8.3.1 have particularly short completion times for one inoperable channel or train that are not commensurate with their risk significance. All of the STP electrical TS for a condition where more than one of the three ESF trains is inoperable currently require entry into TS 3.0.3 even though an intact ESF train remains operable and safety function is not lost. These are valid reasons for the application of risk-informed completion times for either planned or emergent work.

The extended completion time, up to the 30 day backstop, allows time to obtain parts for work on emergent conditions or for the work to be deferred to a normal work week schedule, or to obtain an emergency or exigent TS change if necessary. There is no technical or risk basis to limit the components to which it may be applied if the extended completion time is managed in accordance with the Configuration Risk Management Program.

It is not STPNOC's intent to use TS 3.13.1 to extend the allowed outage time for configurations where the Channel I, Channel III, or Channel IV battery bank is the sole source of power for the loads on the DC bus. A note has been added to TS 3.8.2.1 to restrict the application of TS 3.13.1 for these conditions.

Additional information on the application of TS 3.13.1 to electrical systems TS is

provided in Attachment 1.

b. In as much as an extended AOT/CT based on risk management techniques would be the exception rather than the rule, please describe the record keeping system identifying the following items to verify application for the risk-informed process: (1) each application of risk management techniques to extend the AOT/CT, (2) any contingency actions or compensatory measures used during the extended time, and (3) the analysis that justified the extension.

RESPONSE:

Although it is expected that most work activities will continue to be performed within the existing allowed outage times, there is no restriction on how often the risk-informed completion times may be applied. They may be applied for routine planned or emergent conditions.

1. The Control Room logs show the entry and exit time for each TS action and will reflect the application of a RICT.
2. Any compensatory action that requires a temporary modification will be documented in accordance with the Temporary Modification procedure. Required contingency actions are normally documented in the work instructions.
3. A record of the risk profile for the configuration will be retained. STPNOC routinely compares the actual configuration risk for each week to the projected risk for the week.

c. Will the risk-informed extension of the AOT result in a 30 day extension to a 10CFR 50.72 or 50.73 reporting requirements if the 30 day backstop is invoked?

RESPONSE:

If a component in the scope of TS 3.13.1 is discovered to have been inoperable beyond its frontstop completion time, an evaluation may be performed to determine if the completion time could have been extended in accordance with TS 3.13.1. If the 1E-06 threshold was crossed and the required risk management actions were not taken, the condition would be reportable as operation prohibited by the Technical Specifications. If there was no configuration that crossed the 1E-06 threshold, no violation of TS would have occurred and the condition would not be reportable. Conditions resulting in loss of function or involving common mode failure still meet the reporting requirements of 10CFR50.73 even if the CRMP would permit an extended completion time.

The risk-informed provision to extend the AOT has no bearing on the time required to issue the event report if the condition is determined to be reportable. The 60 day clock for submitting the event report would start at the time the condition is determined to be reportable. If a notification is required by 10CFR50.72, its time clock would also start at the time the condition was determined to be reportable.

35. 10 CFR 50, Appendix B, states that:

"This appendix establishes quality assurance requirements for the design, construction, and operation of those structures, systems, and components. The pertinent requirements of this appendix apply to all activities affecting the safety-related functions of those structures, systems, and components; these activities

include designing, purchasing, fabricating, handling, shipping, storing, cleaning, erecting, installing, inspecting, testing, operating, maintaining, repairing, refueling, and modifying.

As used in this appendix, "quality assurance" comprises all those planned and systematic actions necessary to provide adequate confidence that a structure, system, or component will perform satisfactorily in service."

Please confirm that the STP Configuration Risk Management Program (CRMP) and associated procedures fall under the 10 CFR 50 Appendix B. If STP believes these programs and procedures are not subject to the Appendix B requirements, please justify any exceptions to those requirements.

RESPONSE:

STPNOC agrees that 10CFR50 Appendix B applies to the CRMP and its implementing procedures.

36. **In Table 2, Specifications 3.3.2.8.a-c, new Action 20.A.b states, "with the number of operable channels more than one less than the Total Number of Channels, within one hour apply the requirements of specification 3.13.1, or be in at least Hot Standby within the next 6 hours and be in at least Hot Shutdown within the following 6 hours, and be in Cold Shutdown within the subsequent 24 hours."**

    a. **How long does it take to update the CRMP database regarding plant equipment configuration changes? Is it credible that the implementation of T.S. 3.13.1 can be accurately accomplished within one hour? Would not the loss of the second channel fall into the "emergent conditions" that would not be expected to require an extension of the AOT (page 2 of license submittal dated August 2, 2004)?**

    RESPONSE:

    Since STP's CRMP approach is based on pre-solved Level 1 CDF calculations, the information to calculate a RICT is essentially instantaneous. For items with very short allowed outage times, these will be specifically targeted to ensure those configurations are immediately available to control room personnel. In general, the time to update the CRMP database is usually less than one hour although it is acknowledged that it could take longer in certain situations. In the event that an unquantified maintenance state occurs for an item with a short allowed outage time, then the control room staff will attempt to get the required information or perform the actions required by the Technical Specifications.

    b. **During the five year history of the use of the CRMP to make risk assessments, has there been any instances where the initial assessment significantly differed from the final assessment?**

    RESPONSE:

    Since STP's CRMP uses pre-solved Level 1 CDF calculations, differences between initial and final assessments are not the result of PRA modeling errors. Differences have occurred in the past 5 years as a result of planning or scheduling changes, changes in operator functionality calls, or equipment clearance timing issues such that the

maintenance states (i.e.,configurations) that were planned ended up being different. These events have also occurred for actual risk profiles when new or discovery information is identified which impacts a maintenance state (i.e., configuration). When these events happen, condition reports are generated and corrected risk profiles are generated.

With regard to this pilot application, the determination of maintenance states is predicated on OPERABILITY determinations. The process for OPERABIITY determinations follow both industry and regulatory guidance. Log entries for Tech Spec equipment will be entered into the CRMP with the same controls.

c. The primary function of the loss-of-power instrumentation system is to assure the independence between offsite and onsite systems. This independence, pursuant to GDC 17 of 10 CFR Part 50, Appendix A, minimizes the probability of losing electric power from the onsite electric supplies as a result of, or coincident with, the loss of power from the offsite power supply. Loss-of-power instrumentation initiates load shedding to prevent overloading of the stand-by diesel generators (SDGs). It also supports independence between redundant ac systems and, together with automatic load sequencing, assures the capacity and capability of the offsite and onsite ac power supplies. Please confirm that the proposed changes in T.S. 3.2.2.8.b and .c will not reduce this independence between power sources.

RESPONSE:

The proposed changes affect the required completion time for restoring inoperable loss of power instrumentation. The UFSAR design function of the components is not affected and no physical changes are involved. Implementation of the proposed change will permit a longer allowed outage time and eliminate the potential for entry into TS 3.0.3 for more than one inoperable channel. As described in Table 2 of the application, the extended completion time evaluation for inoperable loss of power instrumentation is bounded by the evaluation performed for an inoperable standby diesel generator.

37. In Table 2, Specification 3.8.1.1, New Action Requirement, specifies restoration of at least one SDG to operable status within 12 hours whereas the existing Action requirement calls for restoration of at least one standby diesel generator within 2 hours and two standby diesel generators within 24 hours. Please explain why this change was not submitted separately in accordance with Regulatory Guides 1.174 and 1.177 since the technical basis provided does not justify this change.

RESPONSE: The requirement should have stated 2 hours and has been corrected.

38. New Action Requirement 3.8.2.1 implies that one battery bank and one battery charger can be inoperable indefinitely. Please clarify whether Action is initiated only if multiple components are inoperable. In addition, please address concerns stated in question 36 for Specification 3.8.2.1.

RESPONSE:

The TS require operability of only one of the two full capacity chargers for each battery bank; consequently, one charger for each battery bank can be inoperable indefinitely. The

LCO still requires entry into the ACTION if less than the required 4 battery banks are operable; therefore, even if only one battery bank is inoperable the action must be applied. The ACTION is worded such that it applies until all the battery banks are operable. The phrase "battery bank" in the ACTION has been changed to "battery bank(s)" to make the requirement clearer.

The electrical components within the scope of the application are modeled in the STP PRA; therefore, configurations involving these components are included in the configuration risk monitor. Thus, the responses to Question 36.a and 36.b also apply to this question.

39. **New Action Requirement 3.8.3.1.a implies that one battery bank and one battery charger can be inoperable indefinitely. Please clarify Action if only one train of the AC power ESF busses is inoperable. In addition, please address concerns stated in question 36 for Specification 3.8.3.1.a.**

RESPONSE:

As indicated in the response to Question 38, the TS do not allow one battery bank to be inoperable indefinitely. LCO 3.8.3.1.a, b, & c require three energized ESF busses. ACTION a must be entered if one or more of the three busses are not energized and may not be exited until all three busses are energized. The phrase "reenergize the train" has been revised to "reenergize the train(s)" to make the requirement clearer.

The electrical components within the scope of the application are modeled in the STP PRA; therefore, configurations involving these components are included in the configuration risk monitor. Thus, the responses to Question 36.a and 36.b also apply to this question.

40. **Please address concerns stated in question 36 for Specifications 3.8.3.1.b and 3.8.3.1.c (Re. the one hour risk assessment.)**

RESPONSE:

The electrical components within the scope of the application are modeled in the STP PRA; therefore, configurations involving these components are included in the configuration risk monitor. Thus, the responses to Question 36.a and 36.b also apply to this question.

41. **Please clarify how the proposed changes will differentiate between degraded vs. inoperable systems, trains, channels or components.**

RESPONSE:

The proposed change does not affect the definition of OPERABLE or how an affected SSC is determined to be operable. The SSC's TS ACTION will be entered when it is determined to be inoperable and will not be exited until the SSC meets the requirements for operability. Application of TS 3.13.1 will permit the allowed outage time to be calculated based on the risk associated with the inoperability of the component. Unless the condition of the affected SSC can be quantified in the PRA, it will be considered to be non-functional and unavailable.

The risk imposed by an inoperable SSC can depend on the nature of the inoperable condition. Examples of degraded conditions that can be quantified to determine a risk-informed completion include:

- SSCs that don't meet seismic requirements but are otherwise capable of performing their design function.
- SSCs that are inoperable but secured in their safe position (e.g., a closed containment isolation valve).
- SSCs powered from a source other than their normal power source, provided the alternate power source is modeled in the PRA.
- An SSC with an inoperable automatic function if the manual actuation of the SSC is modeled in the PRA (e.g., a diesel generator with an inoperable sequencer).
- A valve that is inoperable because it doesn't meet closure time requirements but the closure time is not important to the accident analysis.

General Questions

42. LCO 3.13.1 specifies that when referred to this specification, equipment that has been declared inoperable shall be evaluated for its impact on risk and AOT determined accordingly. The first two actions require the determination of the acceptability of the configuration for AOT beyond the frontstop AOT when equipment is declared inoperable, and for the continued operation beyond the frontstop AOT whenever the configuration changes, respectively. In response to previous RAI 22 to specify the allowable time to complete the required determination process, the licensee stated that this time will be defined in the implementing procedure for the Configuration Risk Management Program and will be consistent with the generic industry guidance. However, each referencing Action specifies that within a specific frontstop completion time (e.g., 1 hour) ... apply the requirements of Specification 3.13.1. Also Section 1 of Attachment 1 (Description of Changes and Safety Evaluation) stated that the frontstop time also provides the operator sufficient time to determine and apply an appropriate extended time from the application of the CRMP for those situations where it is determined that an extended AOT is necessary.

a. Explain and justify why it is acceptable to specify the allowable time in the implementing procedure for the CRMP, rather than in TS 3.13.1 or the referencing TSs?

RESPONSE:

The CRMP has sufficient quality to determine the risk-informed completion time based on the plant configuration and is also of sufficient quality to determine the time allowed to calculate changes in the completion time. Allowing the CRMP to be applied to determine how quickly this calculation needs to be done is preferable to fixing the time in the Technical Specifications since the time will vary with the risk significance of the change in plant configuration.

b. Clarify whether the frontstop time specified in the referencing TS is also the allowable time to complete the required determination process in Specification 3.13.1.

RESPONSE:

As discussed in the response to Question 42.a, the time to determine the new completion time due to changes in plant configuration is determined by the CRMP. The

frontstop time only applies to the time to determine the initial RICT.

43. Some ACTION statements are revised and some new ACTION statements are created to deal with cases with more than one channel, component, train, or subsystem inoperable, which currently do not have a associated ACTION statement and would be subject to TS 3.0.3. These revised or new Action statements generally require that within one hour restore at least one inoperable channel, component, train, or subsystem to OPERABLE status or apply the requirements of Specification 3.13.1, or be in HOT STANDBY within the next 6 hours and in COLD SHUTDOWN within the following 30 hours. Examples of these revised or new ACTION statements are Action 3.4.2.2 (pressurizer code safety valves), 3.4.4 Actions c and e (PORVs), 3.5.1.a and b (Accumulators), 3.5.2.b (ECCS subsystems), 3.6.2.1.b (containment spray systems),3.6.2.3.b (containment fan coolers), Table 3.3-1 (RTS Instrumentation) Actions 9, and 9A.b, Table 3.3-3 (ESFAS Instrumentation) Action14.b, 17.b, 19.b, 20A.b, and 22.b.

a. Since these revised or new Action statements have a frontstop AOT of only one hour, is one hour sufficient to apply LCO 3.13.1 requirements, which include the use of CRMP to determine AOT extension and the need for corrective or compensatory actions?

RESPONSE: As discussed in other responses, the STP CRMP can readily be applied to determine the appropriate revised completion time.

b. Could there be cases where it takes longer than one hour to determine that an AOT extension for the configuration is not acceptable, and therefore the frontstop AOT is exceeded without implementing subsequent actions?

RESPONSE:

STP's evaluations have not identified a condition where the extension of the completion time could not be completed within the frontstop time. STPNOC has not identified any configuration that would exceed the 1E-06 threshold within one hour. A condition that exceeds the threshold within an hour would almost certainly involve serious degradation of multiple cross-train SSCs such that the first priority for the operator would be to place the plant in a safe condition.

44. For these conditions that could result in the loss of the required safety function, compensatory actions are most likely required as a defense-in-depth consideration. Section 4 of Attachment 1 (Description of Changes and Safety Evaluation) discussed the use of the CRMP to determine the safety implications associated with multiple inoperable components, and to assist the operator in identifying effective corrective or compensatory actions for various plant configurations to maintain and manage acceptable risk levels. It is said that these compensatory actions may be incorporated in procedures, work instructions, or other station media. To support this TS amendment, please identify all TS changes (especially for those conditions where two or more channels or trains are inoperable) that require compensatory actions to reduce risk significance, describe each compensatory action and where it is incorporated.

RESPONSE:

STP's CRMP requires the implementation of the risk management actions listed below if the configuration risk will exceed the non-risk-significant threshold (Incremental Core Damage Probability > 1E-06). Except for extensions of the allowed outage time for the standby diesel generator and the auxiliary feedwater, configuration-specific compensatory actions are not prescribed at STP. Compensatory action would be determined on a case by case basis.

Risk Management Actions:

The Shift Supervisor performs the following actions:

Notifies the Duty Operations and Duty Plant Manager of the expected exceedance.

Identifies and implements compensatory measures approved by the Duty Plant Manager. Compensatory measures may include but are NOT limited to the following:

- Reduce the duration of risk sensitive activities.
- Remove risk sensitive activities from the planned work scope.
- Reschedule work activities to avoid high risk sensitive equipment outages or maintenance states.
- Accelerate the restoration of out-of-service equipment.
- Determine and establish the safest plant configuration.
- Establish contingency plan to reduce the effects of the degradation of the affected SSC(s) by utilizing the following:
  - Operator actions
  - Increased awareness of plant configuration concerns and the effects of certain activities and transients on plant stability
  - Administrative controls
  - Ensure availability of functionally redundant equipment
- Ensures any measures taken to reduce risk are recorded in the Control Room Logbook.
- Evaluates whether heightened station awareness is acceptable while attempting to return components or systems to functional status. Duty Plant Manager approval is required to solely implement heightened station awareness.

45. In WCAP-15773-P, Rev. 0, supporting TSTF-424, it is stated in Section B3.2, "Scope and Structure of the Flexible AOT Concept," that typically, AOTs/CTs less than one day are associated with loss of system function and extension beyond the existing AOT may incur significant risks. Therefore, shorter term Action Statements, such as those associated with complete system inoperability or loss of an entire safety function will retain an Action Statement with a fixed AOT/CT value based on the system's or function's risk importance. ... The flexible AOT concept would also not apply to TS associated with plant operational limits." However, in the STP's application of LCO 3.13.1 for AOT extension, many referencing TSs have 24-hour

frontstop AOT (e.g., Table 3.3-1, Actions 9A.a) and some have one-hour frontstop AOT (e.g., TS 3.5.1 Actions a and b, TS 3.5.2 Action b). Explain why the application of LCO 3.13.1 for those TSs with frontstop AOT of one and 24 hours is not contradictory to TSTF-424.

RESPONSE:

From Table 2 in STPNOC's application, it can be seen that there are many exceptions to the position that short allowed outage times are typically associated with significant risk. In addition, there are conditions involving a loss of function that do not incur significant risk (e.g. loss of all containment spray or a seismic related deficiency that affects all trains of a function).

STPNOC has proposed a 1 hour frontstop for conditions where the current TS would require application of TS 3.0.3. This time was proposed to avoid the need to justify a new frontstop time and thereby complicate the review of the application and because STP's program can be applied within that time.

46. **In TS Table 3.3-3, Action 19.a specifies the action with the number of OPERABLE channels less than the Minimum Channels OPERABLE requirement, and therefore appears to cover Action 19.b, which specifies the action with the number of OPERABLE channels more than one less than the Minimum Channels OPERABLE requirement. Is there a typographic error in Action 19.a in that it is intended for the number of operable channels one less than the minimum channels operable requirement?**

RESPONSE: Yes. The word "one" has been inserted in ACTION 19.a.

Attachment 1

Application of Risk-Informed Completion Times to Electrical Components

12/13/2005

In the review of risk-informed Technical Specification (TS) changes proposed by STPNOC that would allow a "floating" risk-informed completion time with a 30 day backstop (Initiative 4B), the NRC Electrical Systems Branch reviewers asked several questions related to the application of the proposed TS to electrical systems. STPNOC agreed to prepare a response that describes how the Initiative 4B changes will be applied to electrical components.

General Comments on Application of TS 3.13.1

Events that result in a de-energized bus or discharging batteries will be addressed and the plant stabilized before there would be any consideration of whether the allowed outage time for the component can be extended.

Application to an ESF Bus (TS 3.8.1.1 ACTION a and ACTION e)

STP Normal Configuration Description:

Each of the three Class 1E 4.16 kV busses for each STP unit is fed from its associated non-class 13.8 kV Standby bus through its associated non-class 1E 13.8 kV – 4.16 kV Auxiliary ESF Transformer. Two of the three 13.8 kV Standby busses are energized from the Unit's Standby Transformer and the other 13.8 kV Standby bus is energized from the Unit Auxiliary Transformer (UAT). Power to the Unit 1 Standby Transformer comes from the North Bus in the switchyard. Power to the Unit 2 Standby Transformer is from the South Bus. Power to each unit's UAT is from the unit's main transformer. The generator breaker arrangement is such that on generator trip the generator breaker opens and provides immediate offsite power connection to the ESF bus that is energized from the UAT. The Standby Transformers and the busses they supply are not affected by the trip.

Each UAT is capable of supplying all three of the unit's ESF busses. Each Standby Transformer is capable of supplying all three ESF busses on both units. Although a unit's ESF busses are normally aligned to its own associated UAT and Standby Transformer, the ESF busses may also be aligned to the other unit's Standby Transformer. All line-ups are done manually from the control room.

An off-site source is operable if it is capable of supplying the required power to one or more ESF busses. The off-site sources are independent as long as all of a unit's ESF busses are not powered from a single UAT or Standby Transformer and the switchyard configuration or condition is not such that a single fault will cause a loss of both transformers supplying the ESF busses.

Alternate Sources of Power for the ESF Bus:

In addition to the alignments described above, the Station Emergency Transformer is capable of powering one ESF bus on each unit. STP has conservatively not credited the Emergency Transformer as an independent off-site source. Emergency power to the ESF bus is provided by its associated standby diesel generator (SDG).

Conditions for Entry into TS 3.8.1.1 ACTION a:

ACTION a establishes a 72 hour required completion time if one of the two required circuits between the off-site transmission network and the on-site Class 1E distribution system is inoperable.

ACTION a may apply for either planned work or an emergent condition. The conditions that would require entry into the action include the following:

- Loss of one 13.8 kV Standby Bus to 4.16 kV ESF Bus feed (per Note 1 to TS 3.8.1.1)
- A configuration where an ESF bus is powered from a source other than a Standby Transformer or the UAT (e.g. from the Emergency Transformer or its associated SDG)
- A configuration where all the ESF busses on a unit are powered from a single UAT or Standby Transformer
- A condition or configuration in the switchyard where a single fault will cause a loss of power to all ESF busses on a unit
- A condition where a properly aligned and energized ESF bus is determined not to be in conformance with its design basis such that it is inoperable (e.g., found not to be seismically qualified)

The first bullet above could involve a de-energized 4.16 kV ESF bus. A loss of off-site power to the bus will cause the associated SDG to start and load, which is included in the second bullet. STPNOC would not normally plan an at-power work activity that de-energizes the 4.16 kV ESF bus.

The other examples describe conditions where the ESF bus is energized, but the TS action must be applied because the off-site sources are aligned such that they not independent or an ESF bus is degraded. Although entry into the TS action may be caused by a degraded or non-conforming condition of the ESF bus, the most likely reason for entering the action is a condition or work activity involving the switchyard or one of the transformers.

Proposed changes to ACTION a would permit STPNOC to extend the 72 hour allowed outage time in accordance with the requirements of proposed TS 3.13.1.
Table 2 of STPNOC's August 2, 2004 application depicts a 30-day backstop risk-informed completion time for a configuration involving loss of a single ESF bus. The calculation for the completion time is based on the availability of an alternate source to energize the 4.16 kV ESF bus. TS 3.13.1 will be applied only in those cases where the availability of the alternate source of power is modeled and the risk assessment can be quantified. The STP PRA model includes the preferred sources (Standby Transformers, UAT), the SDG, and the Emergency Transformer.

Conditions for Entry into TS 3.8.1.1 ACTION e:

ACTION e establishes a 24 hour required completion time if two required circuits between the off-site transmission network and the on-site Class 1E distribution system are inoperable.

Two required circuits would be considered inoperable if any of the following conditions are met:

- Loss of two 13.8 kV Standby Bus to 4.16 kV ESF Bus lines (per Note 1 to TS 3.8.1.1)
- Loss of a 13.8 kV Standby Bus to 4.16 kV ESF Bus line while in a configuration where ACTION a applies
- A condition where two or more properly aligned and energized ESF busses are determined not to be in conformance with the design basis such that they are inoperable

TS Note 1 (cited above) does not reflect STP's three train design. With the loss two 13.8 kV Standby bus to 4.16 kV ESF lines, STP still has one 13.8 kV Standby to 4.16 kV ESF connection.

STPNOC believes any condition where entry into ACTION e is required would be the result of

an emergent condition.

The first two conditions would result in either a de-energized ESF bus or one or more ESF busses powered from their associated SDG. If the condition involves a loss of the UAT, the SDG will pick up the ESF loads; however, the reactor will trip on low flow because the reactor coolant pumps will lose power and coast down. Loss of the Standby Transformer does not directly result in a reactor trip.

If the condition is the result of a LOOP or partial LOOP, the operators will be taking action to establish stable plant conditions from the transient as a priority before any consideration of applying TS 3.13.1 to extend the completion time. One of those actions will most likely be securing the SDG and energizing the ESF bus from a preferred source, at which time the configuration will be the same as the condition addressed by ACTION a. ACTION e also imposes a 72 hour completion time, consistent with ACTION a. STPNOC proposes to delete the 72 hour portion of ACTION e as an administrative change that eliminates the potential for being in ACTION a and ACTION e at the same time.

STPNOC proposes to allow application of TS 3.13.1 to TS 3.8.1.1.e.

Application to Batteries and Battery Chargers (TS 3.8.2.1):

TS 3.8.2.1 requires 4 channels of batteries and associated chargers. If a required battery bank is inoperable or if the battery bank has no operable charger, the TS requires the function be restored in 2 hours or the plant must be shutdown. TS 3.0.3 currently applies in the event of inoperability of more than one channel.

STPNOC proposes to allow the application of TS 3.13.1 to extend the 2 hour completion time for batteries or battery chargers.

Since the batteries provide the power for the field flashing for the emergency diesel generator, an emergent condition where a train of batteries is carrying the associated DC bus with no power to either of the battery chargers could indicate an in-progress loss of off-site power transient in which the emergency diesel generator for the affected ESF train did not start or is not available. STPNOC does not believe it is appropriate to apply TS 3.13.1 to extend the allowed outage time during an ongoing emergent transient condition.

Discharge of the battery banks supporting the Channel II and Channel IV DC loads will not result in a plant trip or transient; however, STPNOC would not normally permit continuous discharge of a battery in an emergent condition (provided power to one of the chargers is available) or plan a work activity that involved an extended discharge of a battery bank. Discharge of the battery banks supporting Channel I and Channel III will not result in an immediate plant trip; however, a plant trip on low steam generator level will result after a loss of DC power as the Feedwater Isolation Valve hydraulic control system pressure bleeds off and the valves close. The evolution of the event provides the operators with an opportunity to anticipate this trip and it can be avoided with timely local operator action. As discussed in the General Comments, it is not STPNOC's intent to use TS 3.13.1 to extend the allowed outage time for configurations where the battery bank is the sole source of power available for the loads on the DC bus. A note has been added to TS 3.8.2.1 to restrict the application of TS 3.13.1 for these conditions. The note states:

> Specification 3.13.1 may not be entered for batteries or chargers when the batteries are the sole source of available power to their DC bus. If the batteries discharge for more

than 2 hours as the sole source of power to their DC bus while Specification 3.13.1 is being applied and no alternate source of power is available, the Specification 3.13.1 LCO shall be considered not met.

As stated in the response to Question 23, the DC bus could be energized through its associated batteries with its associated charger powered from an alternate source or from a temporary charger. With inoperable batteries, the DC bus can be energized through an operable charger or a temporary charger. TS 3.13.1 would allow appropriate consideration of these alternatives in determining an allowed outage time.

Application to Onsite Power Distribution (TS 3.8.3.1):

ACTION a establishes a completion time of 8 hours to restore a train of AC ESF busses that is not fully energized. STP has three independent trains of ESF busses and there is no action for more than one train de-energized, so TS 3.0.3 would apply for that situation. For an emergent condition on either Train A or Train B, the consequences of a de-energized ESF train include the loss of power to the Channel I or Channel III battery chargers, respectively. As discussed above, without operator intervention a plant trip can result after the batteries discharge.

The Class 1E 480 volt AC distribution system is powered through a double ended load center which is supplied by separate breakers from the 4.16kV Class 1E load center via independent step down transformers. The step down transformers and breakers are sized to allow either transformer to carry the entire load center. The load center includes a tie breaker that allows powering of both sides of the load center from either transformer. Individual motor control centers and loads are fed from either side of the load center.

The design of the distribution system is such that each of the two battery chargers is supplied by motor control centers that are supplied by different sides of the 480 volt load center. The 125 VDC bus can be powered from either of the two battery chargers. This allows one side of the 480 volt load center to be taken out of service without affecting the operability of the DC system which only requires one charger for the system to be operable.

Conditions may arise where ACTION a is entered because a "downstream" bus (e.g. one half of the double ended 480V load center) has been de-energized by a fault or needs to be de-energized to perform maintenance. Due to the previously described redundancy, the 8 hour completion time of ACTION a, is unnecessarily restrictive and application of TS 3.13.1 is appropriate.

Each NSSS class 1E 120VAC distribution panel (DP1201, 1202, 1203 and 1204) is normally supplied by a dedicated static inverter. Backup power to the panel is supplied via an automatic bus transfer switch from a dedicated voltage regulating transformer. The inverter and the voltage regulating transformer are supplied via motor control centers from opposite sides of the 480 volt double ended load center. In the event AC power is lost to the inverter or the inverter AC-DC power section is lost, inverter loads are instantaneously picked up by the class 1E DC system. The class 1E DC system battery chargers are sized to carry the inverter load in addition to the other normal loads while keeping the battery fully charged.

Each TMI (post accident monitoring) class 1E 120VAC distribution panel (DP001 and 002) is normally supplied by a dedicated static inverter. Backup power to the panel is supplied via a manual bus transfer switch from a dedicated voltage regulating transformer. The inverter and the voltage regulating transformer are supplied from the same motor control center. In the event AC power is lost to the inverter or the inverter AC-DC power section is lost, inverter loads

are instantaneously picked up by the class 1E DC system. The class 1E DC system battery chargers are sized to carry the inverter load in addition to the other normal loads while keeping the battery fully charged.

ACTION b applies when a 120 VAC vital distribution panel is not energized from its associated inverter or with the inverter not connected to the DC bus. The action requires the panel to be energized within 2 hours and energized through its inverter and DC bus within 24 hours. These completion times may be extended with the application of TS 3.13.1. The preceding discussions describe the redundancy that enables STPNOC to manage the configuration risk when ACTION b applies.

ACTION c applies when a DC bus is not energized from its associated battery bank and requires it to be re-energized from the battery bank within 2 hours. Power to the DC bus can also be provided by either of its associated chargers. The 2 hour allowed outage time is not consistent with the redundancy available from the other DC channels and the low likelihood of a LOOP. TS 3.8.3.1 ACTION c should be consistent with the ACTION for TS 3.8.2.1 for batteries and chargers. Consequently, it is appropriate to be able to apply TS 3.13.1 to extend the 2 hour allowed outage time for either an emergent condition or a planned maintenance evolution for which the corrective action requires the battery bank to be disconnected from the DC bus.

16. **For TS 3.6.2.3 for the reactor containment fan coolers, the calculated RICT is stated to be based on CDF and there was no impact on LERF. Please clarify how the fan coolers are credited in the PRA model for mitigation of core damage given that the design basis function is containment heat removal, and identify the basis for the success criteria (i.e., judgment or specific calculations).**

RESPONSE:

The reactor coolant fan coolers (RCFCs) are included in the PRA in the Late Event Response event trees. With an intact containment (i.e., no large opening), the heat removal capacity of the RCFCs is such that long-term decay heat removal can be accomplished using two of six RCFCs. This decay heat removal function is only credited on sequences where a sump recirculation flow path is established but normal decay heat removal using the residual heat removal heat exchangers is not available. This was verified during the Sandia review of the original PRA. The RCFCs also provide containment cooling, the status of which is tracked in the Level 2 PRA model.

18. **For TS 3.7.14 for chilled water, which supplies room cooling to safety-related equipment, it is typical that the PRA model would only include a subset of the components supported, based on room heatup evaluations. It is also typical to include time-of-year flag events to turn off the ventilation models when cooler outside temperatures exist. These PRA model conventions would result in a 30 day LCO for large portions of the system, and during winter months. Please discuss STP plans in this regard.**

RESPONSE:

The safety related chilled water system (essential chilled water) in the STP PRA includes cooling to the two major ventilation systems, Electrical Auxiliary Building HVAC and Control Room HVAC, and room coolers associated with the safety injection pumps and the essential chillers. Not included are several smaller room coolers such as the penetration space coolers, reactor make-up water pump cubicle, boric acid transfer pump cubicle, radwaste control room AHU, CVCS valve room coolers, etc. These smaller coolers either do not support continuously operating equipment that is modeled in the PRA or only support components that are not modeled in the PRA.

Room heat-up calculations have been used to modify the success criteria for the safety injection pump rooms which are supplied by the essential chilled water system.

The PRA does not include time of year flags for ventilation cooling requirements for any of the modeled ventilation, chilled water, or room cooling systems.

24. Regulatory Guide 1.200 sections 1.2.4 and 1.2.5, and section 1.3 Table 3, identify attributes of a fire PRA and external events PRA, which are not addressed by existing PRA standards. The licensee is requested to describe the scope and quality of their fire and external events PRA models, addressing the attributes identified in the guide.

RESPONSE:

This response will be provided as the current model update is being completed.

25. Regulatory Guide 1.200 section 4.2 requires the licensee to submit "... a discussion of the resolution of the peer review comments that are applicable to the parts of the PRA required for the application." Two options are identified, one to provide a discussion of how the PRA model has been changed, and the second to provide a sensitivity study that demonstrates the particular issue does not impact the significant accident sequences or contributors. The licensee has provided only the numerical identification of their peer review facts and observations, and identified which were categorized as level 'A' or 'B' (Attachment 5, Resolution of Peer Review Comments, to submittal letter dated 10/28/2004). Therefore, the licensee is requested to submit the information required by the guide to address the resolution of peer review comments.

RESPONSE:

Please see the attached Table 1 for set of Facts and Observations (F&Os) generated by the Peer Review and the current status of all F&Os.

26. Regulatory Guide 1.200 section 4.2 requires the licensee to submit the identification of the key assumptions and approximations relevant to the results used in the decision-making process, along with the peer reviewers' assessment of those assumptions. Reference is made to Regulatory Guide 1.174 in section 3.3 for applicable guidance on addressing the impact of these assumptions on uncertainty as it relates to the decision-making process. Only four areas were identified by the licensee, and the peer review assessment was not provided (Attachment 4, Key Assumptions and Approximations, to submittal letter dated 10/28/2004). Since this is a "whole plant" application of risk-informed TS initiative 4B, it is expected that there would be something more than four key assumptions/approximations applicable. Therefore, the licensee is requested to submit additional information regarding the key assumptions and approximations in their PRA model, along with the peer reviewer assessments.

RESPONSE:

Table 1 (attached) provides the status of the peer review F&Os. Key sources of uncertainty and key assumptions will be included in the update of the STP PRA currently in progress. The update will include the latest guidance from the Westinghouse Owner's Group (June 2005) for the identification of the assumptions. The model update is expected to be completed by the end of 2005.

27. Regulatory Guide 1.200 section 4.2 requires the licensee to submit documentation that the PRA is consistent with the standard as endorsed in the appendices to the guide, and the identification of the parts of the PRA that conform to the less detailed capability categories and the limitations which this imposes. The licensee did not identify how their PRA model conforms to the capability categories identified in the ASME Standard as endorsed by the appendices to Regulatory Guide 1.200 (Attachment 3, Conformance to Standards, to submittal letter dated 10/28/2004). Further, during the NRC staff review of the STP PRA for the Regulatory Guide 1.200 pilot, the reviewers noted that the STP self assessment documentation was "difficult to discern their conclusions about their PRA". Therefore, the licensee is requested to submit the information required by the guide, and their plans and schedules (if applicable) to address identified deficiencies which are relevant to this application.

RESPONSE:

The current model revision that is being performed is intended to ensure that issues identified during peer review, the RG 1.200 Self-Assessment, and reviewers comments on the PRA. The response to this RAI will be provided at the completion of the model update.

28. Regulatory Guide 1.200 section 1.2.6 describes the characteristics of PRA model documentation. During the NRC staff review of the STP PRA for the Regulatory Guide 1.200 pilot, deficiencies in the documentation were specifically noted, and it was further identified that STP placed excess reliance on one particular experienced staff member. Because the nature of this application is to place ongoing reliance on the accuracy and quality of the PRA model to calculate RICTs for the technical specifications, robust documentation of the PRA model is essential to assure the capability of the licensee to properly maintain the fidelity of the model, without undue reliance on specific staff members. The licensee is therefore requested to describe the current capability of their PRA model documentation, and to identify a schedule for updates and upgrades to assure their documentation is adequate to permit ongoing maintenance of their PRA models for the following key areas:

RESPONSE:

The intent of this RAI item appears to question the long term technical adequacy of STP's Risk Management programs relative to the availability of knowledgeable practitioners and the adequacy of PRA documentation facilitate long term maintenance and knowledge of STP PRA models. STP PRA models are maintained and updated in accordance with station procedures. PRA models are procedurally required to be updated at least every 3 years for plant modifications and procedure changes and at least every 5 years for performance data updates. The documentation of the model is performed by each team member of the PRA group and is readily available on STP's local area network. Thus, access to the documentation is protected and available to PRA personnel. Each team member is responsible for multiple PRA areas and therefore have familiarity with the documentation over a large scope of the PRA. Long term familiarity and experience with the PRA models by senior personnel presents itself in their ability to readily recall information or other probabilistic bases for certain modeling aspects. This does not imply that other PRA group members are not familiar or unable to retrieve the documentation or be cognizant of the probabilistic bases for any area in the PRA including the areas listed below. Currently, STP's PRA documentation is considered to be more than adequate for knowledgeable RISKMAN practitioners and meets the needs of STP's risk informed

programs and applications. With the completion of the PRA update scheduled for completion in 2005, STP's PRA documentation is targeted to meet available industry standards (Capability Category 2) and Regulatory Guide 1.200 such that the documentation of the PRA, including the areas listed below, are more robust to greater ensure that the long term maintenance and knowledge transfer activities are satisfactorily performed.

a. Key assumptions and approximations applicable to system and event tree models.

RESPONSE:

See response to item # 26.

b. Screening of sequences or failure modes from the model.

RESPONSE:

This portion of this question may require additional clarification. "Screening of sequences" is not performed on STP's PRA. All sequences are included as generated by the event tree structures. Failure modes are listed in system notebooks for each system within the PRA scope. Failure modes not listed would not be included. The documentation contained in STP's system notebooks includes this information at a system level. This includes the system boundary conditions, split fraction rules, and specific sources of system unavailability. At a plant level, the event tree notebooks contain the documentation for sequence structure, logic rules, binning rules, etc. Recovery top events specifically contain the conditions necessary for operator actions to be successful or failed. All this information and more resides in the event tree notebooks. The documentation is considered more than adequate for STP PRA work activities associated with model maintenance and transfer of model knowledge. It is, however, important to note that several Peer Review open items were associated with documentation and will be closed with the upcoming PRA update. Documentation will continue to be an area of focus, scrutiny, and continued improvement as it is recognized that long term workforce management STP's Risk Management group will essential to accommodate personnel changes over the next decade.

c. Quantification instructions, including recovery rules and their bases, mutually exclusive event combinations and their bases, and truncation levels.

RESPONSE:

All of the personnel assigned to the PRA are capable of quantifying STP's risk models at any level (system or plant) and do so as a part of regular work activities (e.g., Significance Determination Process, Risk Ranking, Maintenance Rule, On-line Maintenance). Recovery rules, mutually exclusive event combinations, truncation levels and associated bases are all contained in STP's PRA documentation either in system notebook or event tree notebook documentation. In general, event tree rules are used to address recovery and mutually exclusive event combinations. Complicated event combinations are usually discussed in the event tree notebooks. Since STP uses event tree linking instead of linked fault trees, mutually exclusive events can be addressed in more direct means. For example, Loss of AC power leading to a loss of DC power is explicitly treated with Event tree rules and recovery analysis. Conversely,

Loss of DC power prior to a loss of AC power is addressed by specific event tree rules. Loss of Essential Cooling Water after emergency diesel generators are questioned (diesels require the cooling water), specific event tree macros map these failures to failure of the affected downstream components (CCW, ECH, SI, AFW, etc.). All systems in the PRA scope are evaluated and treated in similar manners but in each case a specific treatment will be used which is documented in the event tree notebooks. This information is available for Staff review or discussion for any area within the PRA.

29. **During the NRC staff review of the STP PRA for the Regulatory Guide 1.200 pilot, issues with the adequacy of the common cause failure modeling were noted during very brief reviews of system modeling. The methods were not using the most recent available information, and some CCF modes were not considered (i.e., batteries, chargers). The licensee is requested to describe the development of CCF models for their PRA, and provide a listing of the CCF modes considered, the components which are modeled for CCF, and the sources of data used.**

RESPONSE:

Common cause update of generic prior data is included in the general update of the STP PRA currently in progress. This response will be provided after the model update is complete.

Table 1 – STP PRA Peer Review Facts and Observations

F&O OBS ID	LEVEL OF SIGNIFICANCE	OBS TEXT	PLANT RESPONSE	STATUS
HR-04	A	The STPEGS HRA was performed in 1988 and has not been updated. An update for SGTR sequences was performed in 1999, but has not been incorporated into the model. The underlying basis of the HEP values is the operator interviews conducted in 1988. These provide the operator assessment of the PSF for each event. The resultant HEPs reflect the procedures, training, and experience of STP which were in place in 1988. The actual operator interviews may have been done prior to the plant going critical. It is very probable that the collective knowledge and experience of the operating staff is very different today than in 1988. FLIM also uses a "calibrating curve" for calculation of the final HEP. The calibrating curves for STP are derived from PRA's completed prior to 1988. The final HEPs for STP may not be indicative of current plant conditions and operating practices. This comment also applies to the pre-initiator HEPs. The quantification of these events was based on maintenance procedures in effect in 1988. They should be reviewed to see if they have changed since then.	Operator actions (all risk significant actions plus selected additional actions not just SGTR actions) were updated at the end of 1999 by an HRA team which included STP and contractor personnel involved in the original HRA. The review of the calculation had not been completed by the time of the data freeze date of the Revision 3 PRA model. The updated HRA data were reviewed during the Revision 3 update process. Because the results of the operator error requantification were not significantly different than what was being used in the PRA, a decision was made to defer using this data until a review of event trees and ESDs was also complete. This was explained to the peer review team at the beginning of the peer review process and the results of the calculation were made available to the peer review team. The updated HRA data is included in the Revision 4 PRA model. A larger scale HRA update using the HRA calculator is planned for the Revision 5 PRA model	Closed
HR-06	A	There is no process developed in the HRA to perform a systematic examination of dependent human actions, credited on individual sequences. Current HRA practices generally require a systematic process to identify, assess and adjust dependencies between multiple human errors in the same sequence, including those in the initiating events.	There is no documented process, however part of model signoff is a review of PRA accident sequences to ensure that they accurately reflect the plant and that no errors such as this finding describe exist. As part of the risk ranking, sensitivity analysis on operator actions are also performed and are described in the risk ranking procedure. Selected sequences (down to 1E-11) were re-reviewed as a result of this finding, and no instances of linked operator actions that are not accurately quantified could be found. STP accident sequences are dominated (>90%) by single operator actions with equipment failure or multiple (e.g., common cause) equipment failures. An HRA guidance document will be prepared as part STP_REV5 that discusses sensitivity analysis that may be used to discover these type of operator linkages through event sequences.	Partial

Table 1 – STP PRA Peer Review Facts and Observations

F&O OBS ID	LEVEL OF SIGNIFICANCE	OBS TEXT	PLANT RESPONSE	STATUS
MU-03	A	Prior PRA applications have not yet been evaluated qualitatively or quantitatively with the 1999 updated model to ensure that the conclusions of those applications remain valid. In addition, STP is still using the 1996 PRA model results for all ongoing PRA risk ranking and risk categorization applications due a limitation in the component risk-ranking feature in the newer version of the RISKMAN code. The current RISKMAN code can calculate basic event importances; however, it cannot correctly calculate component importances for module events. Therefore, the 1997 and 2001 PRA model results have not been utilized in any risk ranking or risk categorization applications to date. The STP personnel indicate that a corrective action item has previously been entered into their corrective action process to track this issue and the delay is due to RISKMAN software problems. Also, STP Procedure 0PGP01-ZA-0305 "PRA Model Update and Maintenance" indicates that prior PRA applications must be "updated" as a part of each model update, but this is not required by the NEI Peer Review process guidance. Instead, the NEI Peer Review Process allows the use of qualitative assessments to screen prior PRA applications which may be affected by a PRA model update; for those applications which cannot be screened out by qualitative evaluation a quantitative assessment is to be performed to ensure the conclusions of the PRA application are not impacted. The vagueness of the wording in procedure 0PGP01-ZA-0305 in terms of the scope and content of the evaluation of prior PRA applications may be contributing to the ongoing delay in the evaluation of prior PRA applications.	Problems within RISKMAN prevented performing basic event importance using the previous PRA model update. The problem had to do with size limitations on output results. The limitations were such that basic event importance results could not be generated for results of the model at STP model cutoff of 1E-12. Results could be obtained at 1E-10, but the number of basic events truncated out of the results would have affected component risk ranking for several tens of components with low failure frequencies and at the margin of the GQA risk ranking procedure criteria. Basic event risk ranking with STP_REV4 indicates the RISKMAN problems have been resolved. In addition, RISKMAN now allows the development of component risk ranking from basic event data (components and failure mode). The model update procedure will be revised to ensure that the requirement for the update of applications is performed, or if computer problems, etc. preclude an update, an alternative will be developed and documented for the application review.	Closed
IE-02	B	The Interfacing Systems LOCA - V Sequence Analysis notebook (vseqrev3.doc) does not provide a clear definition of the ISLOCA pathways modeled, nor does it provide the development of the frequency for each pathway. The supporting local variables and basic events are tabulated in the notebook, but there is no indication of how they are combined to calculate the frequency of ISLOCA through each pathway. It is not clear where the value for Gross Leakage through check valves (ZTVMCX) comes from; it does not appear to match the value used in the IPE. The ISLOCA analysis takes no credit for relief valves in the low pressure systems.	Changes made to model and documentation to clarify process. The RISKMAN system notebook provides the details of the quantification of the likelihood of an interfacing systems LOCA analysis.	Closed

Table 1 – STP PRA Peer Review Facts and Observations

F&O OBS ID	LEVEL OF SIGNIFICANCE	OBS TEXT	PLANT RESPONSE	STATUS
IE-03	B	The ISLOCA initiating event analysis does not produce the correct cutsets for the configuration of the system. The ISLOCA notebook shows 3 types of cutsets: MOV-60-Fail* MOV-61-Fail*MOV-18-HEP-FTC, MOV-60-Fail*MOV-61-Fail*CKV-30-FTC* MOV-18-HEP-FTC, CKV-32-FTC*CKV-38-FTC*CKV-65-FTC*MOV-18-HEP-FTC*MOV-31-HEP-FTC. Observations are: 1. The first cutset does not credit Check valve 30, which is necessary to cause a low pressure pipe overpressurization. 2. The second cutset is correct. 3. The third cutset includes a failure of CKV-65, which has nothing to do with overpressurization of the LHSI system. The event does not make sense according to the system configuration. 4. The "fault tree" in the system notebook, which describes the flow paths for ISLOCA, does not appear to be correct.	Comment 1 - The cutsets portrayed in the certification findings are correct as presented in the model. The LOCA path identified is through the CCW piping which the reviewer missed. Comment 3 - The failure of the check valve in question determines whether the LOCA is inside or outside containment and is correct as stated. The cutset makes sense according to the system configuration. Comment 4 - The fault tree is somewhat confusing, since success of a basic event in some cases leads to failure of the top event through another path. However, "Does Not Appear to be Correct" is wrong, as the fault tree is correct. We have an unusual design that the reviewer was not familiar with.	Closed
IE-04	B	The loss of ECW initiating event frequency fault tree includes a common cause strainer clogging event. However, this is modeled as a 24-hour mission time event, under the assumption that such a failure would be recognized and dealt with promptly. While this is likely a reasonable assertion, it violates the premise of an initiating event fault tree: each resulting failure combination must represent an annual frequency. The assignment of a 24-hour mission time to this failure means that it does not represent the full mission time; it is missing a factor of 365, since, over the course of a year, there would be that many times the "daily frequency" of occurrence for such an event.	Initiating event models have been modified to include component repair times, versus "exposure time" identified in certification finding for the second and third failures. Initiating event models are availability models instead of post trip response reliability models which creates confusion in model developers and reviewers. The mission time that was used previously with basic event failures was a surrogate repair time. The models have been modified to use component repair times rather than the 24 hour mission time substitute. The IE frequencies calculated in STP_1999 and earlier models are slightly higher (more conservative) than the frequencies determined with the current model, STP_REV4. See the system initiating event RISKMAN notebooks. The ECW plugging basic event also uses a repair time rather than a reliability mission time. The repair time is based on ECW train repair times. Strainer plugging is not considered a common cause failure because of the unique STP Essential Cooling Pond layout and operating experience.	Closed
AS-04	B	Hot leg recirculation is not modeled in the large LOCA event tree. No justification is provided for omitting this node from the large LOCA success paths.	Hot leg recirculation has been added to STP_REV4.	Closed

Table 1 – STP PRA Peer Review Facts and Observations

F&O OBS ID	LEVEL OF SIGNIFICANCE	OBS TEXT	PLANT RESPONSE	STATUS
AS-08	B	The reactor coolant pump seal LOCA model used in the STP PRA is outdated. Plant PRA staff have indicated to the reviewers that an up-to-date seal LOCA model has been prepared and documented, but has not been integrated into the PRA model yet.	At STP, seal LOCA is not as important as at other facilities. The high pressure injection pumps are not supported by other cooling systems such as CCW and ECW. A single pump train can be operated in excess of 24 hours with no room cooling. The low pressure injection system, which provides long term core decay heat removal through the RHR heat exchanger, does require CCW and ECW for decay heat removal. Upon loss of CCW or ECW, operator action to secure the running RCPs, trip the reactor, and initiate a plant cooldown prior to a seal LOCA occurring is highly likely. A non-safety diesel generator, the TSC diesel, provides power to a positive displacement charging pump, which has the capability to provide seal cooling in the event of a station blackout or loss of CCW or ECW. An improved Rhoades RCP LOCA model is included in offsite power and station blackout modeling in STP_REV4. the WOG approved Seal LOCA model will be used as one of the sensitivity cases to evaluate Key Model Assumptions	Partial
AS-10	B	The second highest ranking core damage sequence set (3.6% of total CDF) is an ATWS with loss of secondary heat sink scenario. The transient is initiated by loss of control room envelope ventilation with one train out of service for maintenance. The loss of control room ventilation initiating event is assumed to result in spurious equipment start/stop signals while disabling the solid state protection system. Operator action to recover these sequences is also assumed to fail due to the nature of the initiating event. This sequence is very unusual in PWR PRAs. The heat-up of the control room and spurious equipment operation would not be expected prior to trip of the unit due to loss of control room habitability and evacuation of the control room. Nevertheless, assuming the sequence is appropriate, the sequence set does not consider the impact of AMSAC in mitigating this dominant scenario. AMSAC automatically actuates on low steam generator level (15% narrow range) when the reactor power level reaches 30% of nominal. AMSAC is independent of the solid state reactor protection system, located in the QDPS cabinets outside of the control room boundary, and is designed for operation to 50 degC.	Mapping is corrected in STP_REV4. An AMSAC "black box" was added to STP_REV4.	Closed

Table 1 – STP PRA Peer Review Facts and Observations

F&O OBS ID	LEVEL OF SIGNIFICANCE	OBS TEXT	PLANT RESPONSE	STATUS
TH-01	B	(1) The Level 1 Quantification Notebook for the STP_1999 PRA revision provides the following definition of core damage: "The PRA assumes that any scenario in which the loss of core heat removal progressed beyond the point of core uncovery, and core exit temperatures exceeded 1,200 degF, is a core damage scenario. Any sequence that terminates in stable plant conditions or that exhibits a transient in core heat removal in relation to heat generation that is recovered before the core exit temperatures reach 1,200 degF is classified as success." This is a reasonable definition of core damage for use in performing PRA analyses with codes such as MAAP, and is consistent with definitions commonly used in other PRAs. The reviewers note that much of the STP PRA model success criteria are derived from design basis rather than PRA-specific analyses, and this definition does not really apply to sequences for which success is based on UFSAR calculations (which use 10CFR50.46 App. K criteria). This should be clarified in the Quantification Notebook. (2) A 24-hour mission time is defined in the STP IPE (section 3.1.1), but the reviewers did not find this definition in the current PRA documentation. This should be included in the Quantification notebook (or the appropriate current PRA document) along with the core damage definition.	Success Criteria - Use of UFSAR criteria - The single train success criteria used for most PRA sequences is based primarily on UFSAR criteria, Fire Hazards Safe Shutdown, and SBO calculations. Use of more realistic criteria, as suggested in the reviewer comments and as a general rule, will not significantly affect accident sequence modeling in the PRA. Alternative criteria, such as crediting RCFCs for decay heat removal or success criteria for the containment spray system, are based on reasonable assumptions concerning success criteria and are documented in either the IPE or the PRA. Detailed calculations support modeling of operator response where appropriate. Where detailed alternative calculations are required, they are included or referenced in the PRA. Examples include room heat-up calculations for establishing ventilation success criteria. Mission time definition is included in all system analysis notebooks and in the various initiating event model notebooks. Mission time and the definition of core damage will be included the System Success Criteria Notebook for STP_REV5.	Partial
TH-03	B	For the MLOCA and LLOCA initiating events, SI accumulators have been determined not to be required for success. In the LLOCA ESD description in the 1997 model (Rev. 1, dated 2/26/97), it is stated that the accumulators do not significantly alter the time of core uncovery for LLOCA events, based on analyses with the MAAP computer code. Several points should be considered to better justify this modeling feature: a) The MAAP code results that are used to justify this modeling feature are not referenced and not readily available, b) There are known limitations (published by EPRI) of the MAAP3b code for modeling certain features of large LOCA sequences. A companion document is not available for the MAAP4 code. Any use of the MAAP code to justify deletion of accumulators from the large and medium LOCA event trees should be documented in light of these identified limitations. Elsewhere in the STP PRA documentation, there is a statement that: "analyses for Beznau plant showed that no accumulators were required to prevent core damage." There are significant differences between the South Texas and Beznau plants that require assessment before results from Beznau can be applied to South Texas, including the core power density (Beznau is a 350 MWe, 2-loop Westinghouse PWR with a 10 foot core).	Accumulators have been added to the large and medium LOCA event tree models.	Closed

Table 1 – STP PRA Peer Review Facts and Observations

F&O OBS ID	LEVEL OF SIGNIFICANCE	OBS TEXT	PLANT RESPONSE	STATUS
TH-05	B	The Thermal-hydraulic Analysis Notebook documents the results of MAAP analyses used for establishing the time available for operator actions. However, the results presented for the analyses are given in terms of the total time from beginning of the accident that is available for the results of the operator action to be successful. This neglects the time into the accident at which cue is provide to the operator to take that action. It appears that the analyses took into account the time required for the system to respond after the action is taken. An example of this is the time available for operator action to initiate bleed and feed when AFW is not available to the SGs. The analysis documented in the notebook concludes that 60 minutes is available for this operator action. However, bleed and feed according to the FR-H.1 EOP is not prescribed until the SG level drops below about 10% wide range which is typically about 30 minutes after the initiation of the accident. Prior to this, the operators are performing EOP steps to try to re-establish auxiliary feedwater or an alternate means of feed to the steam generators. Thus, only 30 minutes would be available for the operators to diagnose the need for and then perform the bleed and feed operation. The level of detail from the MAAP runs provided in the Thermal-hydraulic Notebook is minimal so that the times for success criteria cannot be validated from the Notebook.	Updated operator actions incorporated into the model resolve the apparent issues. A re-evaluation of the HRA models is in progress for STP_REV5 using the HRA calculator and additional HRA experts.	Closed
TH-07	B	The Reactor Coolant System Notebook defines success criteria for pressure relief during ATWS as 3 safety valves or 2 PORVs and 2 safety valves. The reference for this is NUREG/CR-4550 (Sequoyah). The model assumes the pressure relief capacity requirements are independent of core reactivity feedback throughout the cycle. Such as assumption is contrary to other "standard" ATWS models (e.g., NRC SECY-83-273, Westinghouse WCAP-11992), in which it is acknowledged that there may be some fraction of the cycle in which, for limiting transient initiators (e.g., loss of main feedwater), either moderator temperature coefficient (MTC) is not sufficiently negative (NRC model) or the integrated core reactivity feedback is insufficient (WCAP model) to prevent RCS overpressure even with operation of all PORV and safety valves. In the WCAP model, the pressure relief requirement is further a function of the amount of AFW available, and whether there is successful insertion of control rods using the rod control system. It is possible that the STP design is such that this fraction of the cycle is zero, but no such information is provided.	ATWS modeling described in WCAP 15831 has been incorporated in STP_REV4	Closed
SY-06	B	Justification for not modeling Power Conversion System (PCS) (Main Feedwater, Condensate, and steam dump to the condenser) was not provided. It is not typical among other similar PWR PRAs to have excluded the PCS from the scope of modeled systems.	Will be added to STP_REV5 based on guidance provided in the ASME standard.	Open

Table 1 – STP PRA Peer Review Facts and Observations

F&O OBS ID	LEVEL OF SIGNIFICANCE	OBS TEXT	PLANT RESPONSE	STATUS
SY-08	B	System success criteria in most cases appear to be reasonable, but there are, in general, no specific references given in the system notebooks or the accident sequence notebooks to provide the bases for the criteria used. (Specific exceptions to this that were noted during the review are the Essential Cooling Water notebook and Component Cooling Water notebook, in which success criteria are referenced to applicable analyses.) The IPE, in Section 3.2.1.1.3, includes a general statement that system success criteria were initially taken to be the UFSAR success criteria, and might be later modified if determined to be unrealistic. In many cases in the current PRA, system success criteria can be readily inferred to be design basis (e.g., requiring one train of AFW for decay heat removal following reactor trip, requiring one train of ECCS injection for small LOCA response), but this is not always the case. For example, the AFW success criterion for ATWS response is stated in the AFW system notebook to be success of at least 2 AFW top events (AFA-AFD), with no basis provided. There is a general statement given in the ATWS event tree notebook indicating that this is based on generic Westinghouse analyses, but no reference is provided. The generic 4-loop Westinghouse ATWS analysis requires "full" AFW flow for the limiting case, corresponding to 3 AFW pumps (typically 2 motor-driven and 1 turbine driven with a capacity double that of a single motor-driven) providing flow to 4 steam generators. Since the STP motor-driven AFW pumps have a capacity equal to that of the turbine driven pump, which has a capacity roughly equivalent to that of turbine driven pumps at other plants, the 2-pump requirement for STP appears to be reasonable. But determining that it is reasonable should not require a knowledgeable analyst to make assumptions based on having other knowledge, and making evaluations. Additional analysis information should be provided. Another example is the lack of modeling of accumulators as part of ECCS response to large and medium LOCAs. This is based on a distinction between core damage and "onset of" core damage, and is based on analyses performed for another plant. Rev. 1 of the LOCA event tree notebook indicates, for medium LOCA: "If the accumulators fail to inject, some transient fuel cladding damage may occur, but no significant fuel damage is expected before RCS pressure falls below 300 psig. Since LHSI makeup is always required for long-term success during the MLOCA events, the accumulators are therefore not considered in the model." This is insufficient basis for a system (and accident sequence) success criterion that is different than that used in most plant PRAs. STP PRA personnel indicated that this has been discussed with NRC and found to be acceptable, but it appears that the basis for NRC acceptance was low incremental CDF for a sensitivity case where accumulators were included.	Corrected in STP_REV4. See previous comments	Closed

Table 1 – STP PRA Peer Review Facts and Observations

F&O OBS ID	LEVEL OF SIGNIFICANCE	OBS TEXT	PLANT RESPONSE	STATUS
		In discussions about the accumulator modeling, STP personnel indicated that they have developed an accumulator model for use in the large and medium LOCA event sequences, and intend to incorporate this into the baseline model in a future PRA update. Specific analyses have not been performed for that model, but the criteria used in a recent application of the model (Analysis PRA-01-010, Probabilistic Risk Study for changing Accumulator Allowed Outage Time) appear to be consistent with UFSAR for LLOCA and reasonable for MLOCA.		
DA-01	B	The common cause MGL parameters are based on outdated generic data, available at the time of the IPE. The common cause analysis included plant specific screening of generic common cause events and mapping to plant specific system sizes, but does not include any plant specific collection of common cause data.	A limited review of the INEEL database for diesel generators, essential cooling water (ECW) pumps, and check valves was performed. No significant changes were identified for the current diesel generator or ECW pumps common cause factors given the factors currently in use. The check valve review indicated that the practice of not modeling common cause failure of fresh water check valves in the PRA is valid. Based on this review, the INEEL database was not reviewed for the STP_REV4 update. A more complete review will be completed for the STP_REV5 update which should slightly reduce the effects of common cause failure of mechanical components. A previous review of common cause factors for motor-operated valves was completed for the STP_1996 model.	Partial
DA-02	B	The data update of May 2001 included derivation of 28 new failure elements. Each failure rate was developed using Bayesian update. Priors were selected from the RISKMAN database. The observation is that in several cases, the point estimate of the plant specific data was outside the bounds of the posterior limits. This is due to the very skinny distributions on the priors. Some of the priors are not true data, but are posteriors from the 1997 STP data update. The elements where this occurs are: 480v breaker fail to close, EDG output breaker fail to close, EDG Output breaker transfer open, EDG failure during the first hour, EAB fan fail to run, ECH Pump fail to start. None of these elements were off by more than a factor of 2 from the 95th or 5th bound. Some of the elements were too	These data variables have been corrected in the STP_REV4 model. A data analysis guidance document to be generated in support of STP_REV5 will reduce the likelihood of these types of data analysis errors.	Closed

Table 1 – STP PRA Peer Review Facts and Observations

F&O OBS ID	LEVEL OF SIGNIFICANCE	OBS TEXT	PLANT RESPONSE	STATUS
		low, but most were too high.		
DA-03	B	There is no specific guidance document developed for the data analysis. The data analysis notebook and IPE data analysis sections provide guidance for the data analysis. But, the component boundaries were not defined, the method used for plant data collection and analysis was not described, and the generic data sources used for the 1999 model update were not presented in the notebook.	In general, generic data sources have not been used for data update since the original IPE. Operating experience data is reviewed for every model update and a decision on update based on plant operating experience is made. Initiating event data update for STP_1999 used the latest NRC NUREG on initiating event frequencies for data update as described in the IE notebook. As generic sources are published (such as the IE data), they are reviewed for inclusion in the PRA as part of the model update process. As a generic source is identified, a tracking CR is generated under an update CR to review the data for applicability to the current or next PRA model. General component boundaries for use in data collection will be developed for use in STP_REV5.	Partial
HR-02	B	The STP PRA uses the FLIM (Failure Likelihood Index Method, which is a variation of the Success Likelihood Index Method, SLIM) methodology to quantify the post initiator human actions. The HRA quantification currently in use in the STP PRA was completed in 1988 and has not been updated. Since then, there have been improvements to the SLIM/FLIM method to address some of the identified limitations. Specifically, the early method (believed to be in use at STPEGS) can only combine the performance shaping factors (PSFs) linearly to develop the overall FLI for each action. A more realistic approach is to allow PSFs can have non-linearities. For example if a particular action is rated poorly for a given PSF and moderately in all the others, "middle of the road" (i.e., averaged-out) HEPs tend to result even though poor performance in only one PSF may be indicative of poor human reliability irrespective of what is going on with the other PSFs. Dr. Ali Mosleh of University of Maryland has addressed this issue in a refinement of the FLIM method (which allows assignment of importance to PSFs) in an update of the Calvert Cliffs PRA, the earlier version of which used a version of FLIM similar to what is used in the Diablo Canyon PRA.	An updated HRA using an improved FLIM is incorporated into STP_REV4. The HRA update project for STP_REV5 is using the EPRI HRA calculator and its included HRA modeling techniques. The update is being performed under the guidance of an external HRA expert.	Partial

Table 1 – STP PRA Peer Review Facts and Observations

F&O OBS ID	LEVEL OF SIGNIFICANCE	OBS TEXT	PLANT RESPONSE	STATUS
HR-03	B	There were two sets of HEPs in the STPEGS PRA. One set is the HI's dictated by the Emergency Procedures. These are designated with an "H" and are quantified by the FLIM method. The other set of HI's involve component start or restoration. They are dictated by the abnormal or operating procedures and are designated "ZH". Examples are: ZHEPR1-Human Action- 5.96E-3. ZREAS – Reasonable Human Action = 9.7E-3. ZHEEW1 – Align the off CEW train 4.93E-5. The basis/method for quantification of the "ZH" HI's was not found. It is not known if the quantification basis for these two sets of HI's is compatible. It is also not known if the two types of HI's appear together in the same sequences. If they do, how they relate to each other?	This is an editorial issue. In the PRA, the operator actions that were developed in response to a plant initiating event (usually those covered by the emergency procedures) are designated as an "H___" in the PRA database. Those operator actions that are not related to a specific plant procedure or are "generic" are designated as "Z____". Three exceptions exist. The plant specific operator response actions for three support system initiating events have a "Z____" designator rather than an "H____" designator. The actions are described in the IPE and are based on operator interviews and plant specific procedures. The variables were developed correctly and are used appropriately. In order to eliminate confusion, these three data variables were redesignated to "H____" in the Revision 4 model.	Closed
HR-07	B	It is not apparent that the use of sequence timing in the development of HEPs is done. The HEPs were based on operator interviews, for which the input and output information is not available for this review. The available documentation for sequence timing is simplistic. The reference for the timing is not stated. Whether the "available time" was subdivided into fractions for diagnosis, action, and execution is not documented in the analysis. The time for the first "cue" is not stated. The only available data is the time from reactor trip to the time of the undesired event.	Sequence timing is included in all plant specific operator response actions in the PRA. The time availabilities listed on each HRA worksheet. This time is based upon the identified need for the action (a cue, plant conditions, etc.) and the time to damage once the condition occurs. For example, feed and bleed is based upon the time available once steam generator low level occurs until the steam generator inventory is essentially gone (dryout). The worst case time is used in almost all cases. Loss of offsite power recovery uses time of failure modeling (e.g., for EDGs). Clarification in an HRA guidance document would eliminate the confusion that this finding indicates. Will be included in the guidance document for STP_REV5.	Partial
DE-01	B	Propagation pathways: Flood propagation through drains, stairwells, and cracks under doors were considered. It is not apparent that pathways such as HVAC ducts, pipe chases and penetrations, pipe tunnels were considered in the same detail. All flood barriers were assumed to be in their functional position. That is, doors being open, structural failure of doors, dikes being removed for maintenance were not considered. Drains being blocked or drain line check valves being failed open were not considered. All rooms were screened based on the room alone. No propagation analysis was done.	Flooding has been reanalyzed in support of STP_REV5. A spatial interactions database from the IPEEE has been recreated electronically. All areas containing PRA modeled equipment have been walked down. New data sources have been reviewed. No areas reviewed resulted in greater than 1E-07 CDF in a screening analysis. A more detailed analysis could further reduce any potential contribution from credible (likely) floods. Incredible floods (e.g., double ended shear that results in a theoretical maximum flood rate) in safety systems like essential cooling water are not included in the screening process.	Closed
DE-02	B	It appears that all flood sources from safety related components and external reservoirs were identified. It is not apparent that the water volumes of each flood source were factored into the analysis. It is not clear that non-safety systems were considered.	Water volumes from the various sources are included in the flood analyses. Non-safety systems, specifically the fire protection system, are included in the flood evaluation.	Closed

Table 1 – STP PRA Peer Review Facts and Observations

F&O OBS ID	LEVEL OF SIGNIFICANCE	OBS TEXT	PLANT RESPONSE	STATUS
DE-03	B	Pipe breaks and tank ruptures appear to be the only cause of flooding considered in the 1988 analysis. Floods caused by human errors during maintenance, water hammer, and failures during off-normal operations were not considered as flooding initiators.	Operator errors leading to flooding are one of the sources for the potential initiating events used. Design to minimize water hammer has been aggressively pursued. For the potential flooding scenarios that affect PRA modeled equipment, with the exception of the ECW system and fire water storage, water volumes are limited to piping and expansion tank volumes. Fire protection and ECW as potential flooding sources are explicitly considered in the analysis.	Closed
DE-04	B	The maximum flow rate of the flood was not considered. The screening analysis appears to be based on the flood water volume caused by the design basis flood. Flow rates, duration of the flow rates and ultimate water volumes produced during the flood were not stated. Reference to the drain size was not mentioned.	See flooding reanalysis	Closed
DE-07	B	Flooding frequencies were based on a 1983 paper, which provided an overall frequency for flooding in the Aux. Building, DG building, turbine building. These frequencies were apportioned to rooms of interest based on square footage. Continued use of flooding frequencies based on 19-year-old data is not appropriate. Further, the method of apportioning the data may no longer reflect current industry experience.	Flood frequency updated during the flooding reanalysis. Screening analysis considered systems associated with areas rather than room sizes.	Closed
DE-09	B	All potential flood rooms were screened away based on analysis of a single room. The flooding screening criteria were qualitative and quantitative. The final screening criteria was the flooding CDF of 2E-7. 13 sequences were screened based on the estimate of CDF being less than 2E-7. The total plant CDF is now 1E-5, whereas in 1988, the CDF was greater than 1E-4. Based on the current CDF, the 2E-7 screening criterion is no longer appropriate.	Reanalysis used 1e-07 as a screening criteria.	Closed
ST-01	B	The ISLOCA analysis does not consider probabilistic failure of pipes and other components. The fault tree includes "success events" for the rupture of the RHR HX tubes or the RHR pump seals. The assumption is that failure of the RHR seals or RHR HX will relieve pressure in the system thus preventing the ISLOCA pipe failure. This is not substantiated and may be not true. The pressure relief provided by these failure paths are not sufficient to reduce pressure in the event of the complete check valve failure. Probability of pipe rupture should address the design margins in the pipe, as indicated in NUREG/CR-5102 and other documents. The method used in the PRA increases the probability of certain valve failures by a factor of 10 to account for the higher pressure. No basis or justification for this approach is provided.	There is a misunderstanding the South Texas interfacing systems LOCA model. The STP RHR system is contained entirely within the containment building. Any failure of the RHR piping within the containment building with a concurrent overpressure event from the RCS will result in a LOCA inside containment. For this reason, failure of the RHR piping is not considered. This event is similar to the LOCAs already modeled and not included in the interfacing systems LOCA analysis. An interfacing system LOCA at STP that results in a containment bypass can only result from an RCS pressure boundary failure AND: 1: Failure of RHR heat exchanger tubes such that the overpressure event carries over into the CCW system, or; 2. failure of the containment isolation check valves for the LHSI trains. The most likely scenario quantified is the failure of the RHR heat exchanger tubes with consequential failure of the CCW system outside containment with failure of the operator to isolate. Operator action to isolate the CCW system after tube failure (value equal to 0.1) or isolation of the LHSI piping after piping is considered in the model. Failure of the RHR heat exchanger tubes serves to direct an interfacing systems LOCA to the CCW system. Success of the heat exchanger tubes challenges the LHSI piping. An updated notebook that more completely describes the interfacing systems LOCA with more clarity will be developed for STP_REV5.	Closed

Table 1 – STP PRA Peer Review Facts and Observations

F&O OBS ID	LEVEL OF SIGNIFICANCE	OBS TEXT	PLANT RESPONSE	STATUS
QU-02	B	The Level 1 quantification summary document provides the top sequences and the contribution to CDF from individual initiators and initiator groups. It also provides a comparison of results between the current model and the previous version of the PRA model. The summary document does not, however, provide any sensitivity analyses for the PRA model. Further, textual descriptions are provided in the summary for only a few of the top sequences and should be included for more of the important sequences. The above are important aspects to examine in order to gain a full understanding of the results.	Additional sequence detail has been included in the Revision 4 update. Additional sensitivity studies still needed (above those performed to support GQA risk ranking).	Partial
QU-03	B	Uncertainty analysis was performed by using RISKMAN. The statistical parameters such as mean, variance and 5th, 50th and 95th percentile were calculated (CNAQ 01-17305-1, Uncertainty Analysis for STP 1999). Five sensitivity studies were performed and the results were documented (0PGP01-ZA-0304, PSA Risk Ranking Sensitivity Study). However, there is no evidence that the causes of uncertainty in the model (e.g., associated with data, modeling assumptions, success criteria analyses, etc.) were studied and were linked to the sensitivity analysis	Key sources of uncertainty will be identified and selected sensitivity studies etc. to bound these assumptions will be included in the STP_REV5 model. The key assumption and uncertainty analysis will use the recently published WOG guideline (WCAP-16432-NP).	Open
L2-01	B	The Level 2 assessments that impact LERF from early containment failures (vessel thrust, steam explosions, DCH, hydrogen burns, etc.) rely heavily on the containment loads estimated for Zion in the NUREG-1150 (and the NUREG/CR-4551 series). These loads are then combined with the containment structural capability results for South Texas, using the STADIC code. This provides a conservative assessment of LERF contributions from early containment failures. Later information on the potential for early containment failures from DCH (NUREG/CR-6338), steam explosions (NUREG-1524), etc. has not been considered in the STP LERF model. This later information indicates that these phenomena do not present as severe a challenge to containment integrity as previously suspected. Also see F&O L2-02 for further information related to conservative assessments of LERF.	Newer information is included in the updated LERF analysis	Closed

Table 1 – STP PRA Peer Review Facts and Observations

F&O OBS ID	LEVEL OF SIGNIFICANCE	OBS TEXT	PLANT RESPONSE	STATUS
L2-02	B	The Level 2 assessments that impact LERF from thermally induced SGTR are based on NUREG-1150 (NUREG/CR-4551 series) expert elicitation of thermal induced steam generator tube rupture (TISGTR). Additional conservative MAAP analyses were performed for the SG replacement for Unit 1. These analyses show that TISGTR will occur for tubes degraded substantially past the current tech spec limit of 40% remaining tube wall thickness. More recent generic assessments of TISGTR in EPRI report TR-107623-V1 can be used to conclude that the likelihood of TISGTR is very small for Westinghouse NSSS configurations. The SG replacement analyses provide a conservative assessment of LERF contributions from early containment failures. TISGTR is the dominant LERF contributor in STP-1999 model. The Level 2 assessments that impact LERF are generally based on a very conservative assessment of phenomena that can challenge the plant fission boundaries. For the current STP PRA-1999 model, the TI SGTR dominates the LERF by contributing over 75%. Other conservatively assessed LERF contributors such as DCH contribute another 5 to 6% to the total LERF. The issue with conservative analyses for dominant contributors to LERF is that they can mask the real risk importance of other contributors. For example, consider risk importance of an ISLOCA SSC. If the "always fail" condition (RAW importance) for this SSC tripled the ISLOCA LERF value, then the RAW that would be computed is 1.10. On the other hand, assume that a more realistic overall LERF assessment for STP shows a 50% contribution from ISLOCA. For the same SSC, the new RAW value would be 15.0. In the case of LERF, the risk importance measures for LERF can be significantly impacted by the conservatism inherent in the analyses.	The latest Level 2 update addresses this question.	Partial
L2-04	B	There are few success criteria in the Level 2 analysis that impact LERF. The primary success criterion is the RCS depressurization after core damage that helps to reduce the LERF contribution from TI SGTR. In this case, an estimate is made for success without any analytical basis.	The updated Level 2 analysis provides a more robust basis for LERF success criteria.	Closed
L2-05	B	The impact of severe accident environment on continued operability of the pressurizer PORV was assessed from the perspective of sticking open. This provided a benefit for RCS depressurization. However, the failure to open or remain open was not assessed. This would be a negative impact in terms of RCS depressurization. Also the impact of severe accident environment on the continued operation of the containment fans coolers is not documented in the Level 2 assessment. The containment loads used to assess LERF challenges to the containment consider operation of the fan coolers. The conditional LERF containment failure probability could be impacted by inability of fan coolers to survive during a severe accident.	Continued fan cooler operability is documented in the updated Level 2 analysis.	Closed

Table 1 – STP PRA Peer Review Facts and Observations

F&O OBS ID	LEVEL OF SIGNIFICANCE	OBS TEXT	PLANT RESPONSE	STATUS
L2-06	B	The Level 2 endstates include all key LERF contributors found in most PRAs with the following exceptions: Pre-existing containment leakage is not considered in the containment isolation failure model. The basis for this is not documented. The peer review team was told that they have to vent containment every two or three days to prevent pressure buildup to the tech spec limit due to leakage from compressed air systems inside containment. A pre-existing opening would prevent such a buildup and be noticed by the plant operating staff. Thus pre-existing openings would not exist for extended periods of time. The reviewer questions what would happen if the leakage from the compressed air system is fixed. Would this be picked up in a modification to PRA? All SGTR core damage sequences are assessed to be late core melts. Thus they are excluded from LERF. There are two issues here: 1) this is in complete contrast to NRC positions stated in their SDP on the Indian Point 2 Tube failure event in 2000 and their draft guidance on Tube Inspections (3/2002), and 2) there is no basis for the time of fission product release in relation to the potential order for radiological protection actions in the STP Emergency Plan.	Small pre-existing containment leakage is included specifically in the containment isolation system notebook as a failure mode. Large pre-existing containment leakage is excluded because of the containment venting performed during normal plant operation. This venting is required as a result of the normal operation of numerous air-operated valves inside containment. The purge history was presented to the reviewers but was not understood. The binning of SGTR sequences has been evaluated as part of the Level 2 update project and will be incorporated into STP_REV5.	Partial
L2-07	B	The LERF model does not incorporate the Emergency Action Levels (EALs) into the evacuation model. The LERF model assumes all SGTR sequences that lead to core damage will be late releases. To classify as a late release, it is necessary to show evacuation was started 4-6 hours prior to the release. Without designated EALs for evacuation, it is not possible to justify all SGTR sequences being "late".	Incorporation of the EALs into the Level 2 analysis is included as part of the Level 2 update project and will be included in STP_REV5.	Partial
MU-01	B	STP Procedure 0PGP01-ZA-0305 "PRA Model Update and Maintenance" does not ensure that the current state of PRA technology or "accepted industry approaches" are used in updating the PRA. There is no reference in the PRA maintenance and update procedure to prompt the analyst to consider the possibility that methods used in the PRA may no longer be accepted. Several of the F&Os from this review identify methods used in the PRA which are no longer widely accepted PRA technology (e.g., common cause modeling factors, human reliability analysis, flooding analysis).	See attached Response to F&O MU-01 (MU-01 Response)	Closed

Table 1 – STP PRA Peer Review Facts and Observations

F&O OBS ID	LEVEL OF SIGNIFICANCE	OBS TEXT	PLANT RESPONSE	STATUS
MU-05	B	STP PRA procedures specify a fixed PRA update schedule (3 years for plant changes, 5 years for data update) and also indicate that as plant changes are identified, they are to be reviewed for PRA impact. PRA impacts are determined by a PRA analyst and categorized as no significant impact (estimated delta-CDF less than 10%, no immediate action required), or significant impact (estimated delta-CDF 10% or greater, PRA manager/supervisor determination of need for immediate PRA update to address). 1. The guideline as written does not require the evaluation of the cumulative (or combined) effects of multiple pending changes. It would appear to allow the accumulation of multiple changes, each with baseline CDF impact of up to 10%, for a period of up to 3 years (i.e., between regular updates). 2. The guide does not require the evaluation of the impact of minor changes between scheduled PRA update, or the cumulative or combined effects of such pending changes, on existing PRA applications. It is possible that a number of individually minor impact changes that are awaiting implementation could have a cumulative significant impact on an application.	The findings described in MU-05 come from Section 4.2 of 0PGP03-ZA-0305 which describes how to disposition changes to references used in the PRA utilizing the database of inputs. Sub-steps also describe how the model change should be dealt with if there is a quantifiable impact to the model. Step 4.4 of 0PGP03-ZA-0305 states "if system or model changes are made within a maintenance model, in order to track cumulative changes, the responsible PRA analyst Shall:" Sub-steps go on to describe exporting changes to the reference model coordinator for cumulative impact assessment between model updates. Risk management guideline 002 goes into much more detail on this topic as well. See response to MU-02. Additionally, analysis assessments are performed per 0PGP05-ZE-0001 on quantifiable changes. In these assessments, the impact on the PRA is documented and the maintenance models created for these assessments are saved for further evaluation and exporting to a new reference model. The reference model coordinator is responsible to track cumulative effects on the model. Should cumulative effects cause a change of greater than 10% to the PRA, then an evaluation will be done to determine if a revision to the reference model should be generated before the next PRA reference model update. Therefore quantifiable changes to the PRA are documented and their cumulative effects are monitored by procedure. We disagree with the finding level of significance.	Closed
IE-01	C	In the support system initiating event models, only basic events involved in common cause groups have the year long exposure time applied to them. Other basic events may be minor contributors to the initiating event frequency, but should have the long exposure time applied for completeness.	Initiating event models have been modified to include component repair times, versus "exposure time" identified in certification finding. Initiating event models are availability models instead of post trip response reliability models which creates confusion in reviewers and model developers. The mission time that was used previously with basic event failures was a surrogate repair time. The models have been modified to use component repair times rather than the 24 hour mission time substitute. The IE frequencies calculated in STP_1999 and earlier models are slightly higher (more conservative) than the frequencies determined with the current model, STP_REV4. See the system initiating event RISKMAN notebooks.	Closed
AS-01	C	The RCP Seal LOCA initiating event is designated as RCPL in the PRA model and RCPS in the initiating event notebook.	Changed in the initiating events notebook. Editorial.	Closed
AS-02	C	Some top event split fraction rules use the "all support available" split fraction as the default split fraction. Other top events do not have a default split fraction. It is good practice to use the guaranteed failure split fraction as the default split fraction to highlight logic combinations not captured by the split fraction rules.	When building a new PRA model using RISKMAN, a method typically used to find logic errors in split fraction rules is to use a "Guaranteed Failure" split fraction as the last rule in the split fraction definition set. This method allows event tree processing to continue in the event a valid split fraction is not found in the split fraction set. This has severe limitation. If the sequences which contain the "Guaranteed Failure" split fraction are low in frequency, the split fraction logic error may never be found. In the South Texas PRA, a concerted effort has been made to assure the correct assignment of split fractions to the event tree rules. In the case of complicated logic, all split fraction logic is completely defined. Although the "All support Available" split fraction is the last one in the split fraction set, the logic used to define this split fraction assignment is specific. "Guaranteed Failure" is not used as a default split fraction. This allows any split fraction logic errors to halt processing of the event trees. Given the mature state of the South Texas PRA, the "Guaranteed Failure" split fraction is not appropriate	Closed

Table 1 – STP PRA Peer Review Facts and Observations

F&O OBS ID	LEVEL OF SIGNIFICANCE	OBS TEXT	PLANT RESPONSE	STATUS
			as the last split fraction logic rule in the split fraction set.	
AS-03	C	Reactor trip is not modeled for several of the initiating events, including the SGTR and MLOCA. In the case of the SGTR initiating event, this has been identified as an open item in the SGTR Notebook documentation (page v of FNTLSGTR.DOC, Rev. 1, 4/30/97). However, in the case of the MLOCA, no justification for its deletion is provided. Generic analyses have shown that trip is required at the lower end of the medium LOCA break range, especially for the case of MLOCA without auxiliary feedwater available because the amount of borated RWST water that can be injected into the RCS is limited.	At a high level, the likelihood of reactor trip failure and MLOCA occurrence is approximately 1E-10. With successful safety injection, no core damage would be expected. Based on frequency, inclusion of reactor trip failure (ATWS) in Medium LOCA is not necessary. Inclusion of reactor trip failure for other LOCA initiating events is still under review, but reactor trip failure during LOCAs would not be risk significant because of the low frequency of occurrence. Incorporate into REV4 modification (SLOCA and SGTR). Extended to Revision 5 model.	Open
AS-09	C	The S2 event tree does not address core cooling recovery (CCR). The SGTR tree, which is similar to S2, does include CCR. CCR is in the STP procedures.	Recovery of core cooling (recirculation cooling) is modeled in the LOCA recovery event tree for small SLOCA events. Detailed treatment of other core cooling recovery scenarios in the small LOCA event trees is not considered necessary because of the low frequency associated with possible recovery actions. It is considered in the SGTR event tree because of the release consequences associated with the SGTR event. The same recovery action currently modeled in the LOCA recovery event tree is not possible in the SGTR event tree.	Closed
TH-02	C	The IPE system notebooks include reference to room heat-up analyses that were performed using an STP code called HEATUP. No documentation of this code was available for the peer review. The HEATUP analyses appear to still be the basis for the current PRA room cooling modeling decisions for some rooms. If this is the case, the analyses, including documentation of the HEATUP code capabilities and limitations, should be retrieved and retained with the PRA documentation.	Added as an action for the REV 5 model	Open
TH-04	C	The traceability of the success criteria documentation that is not provided in the Thermal-hydraulic Analysis Notebook is not well laid out. While many of the systems success criteria are based on the FSAR requirements for the system, the references are not provided in many cases. Some of the Systems Notebooks have criteria embedded in the Notebook (e.g. AFW), again with no reference to the basis for the success criteria. There are other instances in the Event Sequence Diagrams and Event Trees where the event sequence is stated with no reference to the basis.	A success criteria notebook was created for STP_REV4. Additional success criteria calculations/bases will be added as appropriate in STP_REV 5	Partial

Table 1 – STP PRA Peer Review Facts and Observations

F&O OBS ID	LEVEL OF SIGNIFICANCE	OBS TEXT	PLANT RESPONSE	STATUS
TH-06	C	The IPE notes that accident sequence and system success criteria were initially established using design basis criteria (e.g., operating support system continues to operate for 24 hours; one train of a 3-train mitigating system starts and operates for 24 hours). In specific cases, e.g., CCW and ECW system success criteria, the success criteria have been based on better estimate analyses that better reflect the conditions modeled in the PRA. There is no specific guidance for these analyses, but the approach used can generally be discerned from the referenced analyses. In some cases, MAAP plant-specific analyses have been performed to define success criteria for specific accident scenarios and to support the HRA. The Thermal-hydraulic Analysis (TH_Calcs) notebook, which was prepared prior to but incorporated as part of the 1999 model update, documents these analyses, and provides a limited but sufficient set of guidance to allow an experienced analyst to perform such analyses.	Actions related to this finding are incorporated into STP_REV4. See previous responses to TH-04 and TH-05.	Closed
SY-01	C	Formal guidance describing the current process for updating and revising fault trees was not found. In addition, guidance for generic modeling assumptions (e.g., when to model diversion flow paths), naming conventions or standard component failure modes was not found.	The current STP fault tree models and system notebooks are used to train new PRA engineers. As part of the training cycle, new engineers are given responsibility for several of the system model notebooks and associated documentation. However, the suggestion is well founded in that a guide for new and recently qualified PRA engineers will ensure consistent standards for fault tree models. System modeling guidance will be developed in STP_REV5.	Partial
SY-03	C	Simplified schematics (piping & instrumentation diagrams) of systems showing system boundaries were not found during the review.	P&IDs were included with the model up until Revision 3 (STP_1999). Given the flexibility of LAN access to P&IDs, etc, and concerns about maintaining marked-up drawings current, these drawing were removed from the system notebooks. The descriptions in the notebooks concerning boundaries are sufficient for a qualified reviewer/analyst to mark up the P&IDs if necessary. P&IDs and descriptions will be added to STP_REV5 based on guidance provided in the ASME standard.	Partial
SY-05	C	No evidence was found that operating experience with each system was reviewed to ensure that important system characteristics were modeled appropriately.	Operating experience review is incorporated in the GQA process. A PRA member is also a member of the GQA working group. Actual review experience indicates questions concerning operating experience effects on the PRA model is being incorporated into the PRA as necessary from this process. Will be considered as an addition to the system analysis guidance process for STP_REV5.	Partial

Table 1 – STP PRA Peer Review Facts and Observations

F&O OBS ID	LEVEL OF SIGNIFICANCE	OBS TEXT	PLANT RESPONSE	STATUS
SY-07	C	Traceability of basic events to modules and cutsets is not transparent to the reviewer. Modules may limit ability to discern between components in a module that are characterized as high risk importance for Fussell-Vesely only, unless special steps are taken to do this.	There are no modules in the STP PRA fault trees. The reviewer comment relates to the grouping of series components into a single basic event to ensure generation of system level cutsets. Previous versions of RISKMAN fault tree codes imposed time or cutset generation limits on cutset generation and quantification. Each system analysis attempted to generate all cutsets or used a sufficiently low cutset truncation value to ensure accurate representation of system level cutsets. Each use of a composite basic event to represent a series of component failures was reviewed in light of the reviewer comments. The composite basic events were used correctly in the system models. Concerns about risk ranking of components is valid, however as noted by the reviewer, the risk ranking results would be conservative in that each component in a composite basic event would have the risk rank of the basic event. With the exception of the AFW pump composite events, all composite basic events contain only passive components. A new version of the RISKMAN code increases the cutset limits and cutset element limits. A revision 4.1 STP PRA model expanded most of the composite basic events to individual component basic events with no significant change in cutset generation times. The RAW component risk ranking was not affected by these changes, while the F-V risk ranking for individual component and failure mode basic events decreased as expected.	Closed
SY-09	C	Basis for not modeling ECW screen clogging during internal events due to screen wash failures is not adequately justified. The operating experience with the ECW screens was not provided as a basis for not modeling.	The STP ECP is a open loop cooling system with it's own cooling pond which is not connected to the main cooling reservoir or its make-up source (the Colorado river). The ECW system is chemically treated to reduce (or eliminate) the likelihood of screen plugging from plant growth. Several incidences in plant history have indicated the potential for water borne grass formation, which led to the current treatment cycle. Evidence from plant operation indicates that screen plugging (or strainer plugging) is not an issue of concern at STP. The screen wash system is designed to mitigate the consequences of an upstream dam failure that overtops the ECP embankment with the potential for concurrent excessive waterborne debris.	Closed
DA-04	C	Although generic and plant specific databases are available for use, the data sources used for the generic database is not easily traceable. The generic data used for the Bayesian update in the current model update has been updated few times since the first PRA model was developed.	Creating a direct link to data used in the original IPE for select variables has been noted in past updates. In general, the data in the current PRA is based on an extensive data update for the 1994 model update and is documented in that data notebook. Since the 1996 update, the link to data is documented in the data analysis notebook and also noted in the PRA data module. An attempt to document potential errors in the data variables will be made. The creation of a data analysis guide will enhance the documentation of the update process and the generic variables used.	Partial
HR-01	C	Pre-initiator operator errors are included in the model and the method for quantifying these error rates is sufficiently documented in the IPE. However, there is no written evidence of a systematic approach for identifying which pre-initiator errors to include in the model.	The screening method currently in use is not described well in the documentation. In general, each system notebook contains a review of all plant procedures with a potential to affect the system as modeled in the PRA. The effect of the procedure is identified during the review and modeled as appropriate (see the AFW system). Potential miscalibration for actuation systems is included in the reactor protection notebook. Miscalibration of individual sensors is implicitly included in the component failure rate if applicable. The HRA update process for STP_REV5 will correct this issue.	Partial

Table 1 – STP PRA Peer Review Facts and Observations

F&O OBS ID	LEVEL OF SIGNIFICANCE	OBS TEXT	PLANT RESPONSE	STATUS
DE-08	C	Although the walkdown documentation is extensive, it does not discuss the screening criteria used for flooding, nor does it discuss the results of the walkdown with respect to what information was included in the PRA.	The new area walkdowns and the screening criteria used is included in the flood re-analysis.	Closed
QU-01	C	At the present time, the system module of the RISKMAN computer code is somewhat limited in the size of fault trees that can be quantified, causing some consolidation of component failures into supercomponents (modules). This can have an impact on the risk ranking of equipment. It has been indicated that a newer version of RISKMAN is soon to be released that will address this limitation. Also, there is no evidence of written guidance concerning how to deal with code limitations such as this one.	See response to SY-07	Closed
QU-04	C	The use of the maintenance/operating configuration top event divides sequences into three similar sequences. The summary document for Level 1 results presents approximately the top 170 sequences, but this is only equivalent to the top 60 or since the sequences were subdivided by the configuration top event. More sequences should be included in the summary.	Additional sequence detail has included in the Revision 4 update.	Closed
QU-05	C	There was no evidence that a comparison of STP important sequences with important sequences from other plants was made.	See Attached Response to Peer Review (QU-05 Response)	Closed
MU-02	C	STP Procedure 0PGP01-ZA-0305 "PRA Model Update and Maintenance" and 0PGP04-ZA-0604 "Probabilistic Risk Assessment Program" do not address operational experience, new maintenance policies, operator training program changes, technical specification changes, emergency plan changes, and industry studies, as specified in the sub-element.	See attachment to MU-01	Closed
AS-07	D	The Event Sequence Diagrams lay out a very detailed accident sequence model. Some of the ESD model is based on assumptions and conceptual strategies that were not carried forward into the PRA event tree models due to lack of analytical basis or their perceived lack of benefit for the intended purposes of the PRA. Some of these are very "cutting-edge" modeling assumptions, such as using RV head vents to supplement PORVs for RCS depressurization and draining the containment sump to the radwaste system to prevent flooding vital containment equipment. As a result, their future incorporation into PRA models for risk informed applications could be done without a very thorough review of the capabilities and limitations. This F&O is documented because the South Texas PRA documentation already includes a discussion of these strategies which may imply that there is more of a basis for these than for conceptual strategies that were captured in the ESDs for posterity.	This finding relates to potential success paths described in the event sequence diagrams for the South Texas PRA that were not incorporated into the actual event trees. The concern appears to be that caution is necessary before these alternatives are included in the PRA model. Changes to the PRA event tree models are based on changes to plant procedures, TH calculations that support new success criteria, and new finding in plant behavior under accident conditions. The ESDs contain large numbers of potential success paths that were considered during the original development of the South Texas PRA. Inclusion of these paths will only be made if supported by changes in plant procedures, TH calculations, or new information from industry research. A caution is not required.	Closed

Table 1 – STP PRA Peer Review Facts and Observations

F&O OBS ID	LEVEL OF SIGNIFICANCE	OBS TEXT	PLANT RESPONSE	STATUS
SY-02	D	The following are editorial comments identified during the System Notebook review: (1) In the Reactor Containment Fan Coolers notebook, the success criteria discussion (section 3.1.2) refers to the "single train shutdown letter ST-YB-HL-13518, dated November 17, 1986 [Ref. 5.11.b]"; there is no Ref. 5.11.b in the References section, but this letter is listed as Ref. 5.10.c, following Ref. 5.10.a (there is no Ref. 5.10.b). (2) The Safety Injection System Notebook includes, in Section 3.1.2, a reference to Ref. 5.1(b) for basis for not requiring room coolers for 24 hours for a single SI train. Ref. 5.1(b) is a reference to the plant Tech Specs. It is likely that the correct reference is 5.1(d), which is listed as an internal memo about SI room cubicles.	Corrected in STP_REV4.	Closed
SY-04	D	No evidence that a search for plant specific failure modes was performed for PRA updates subsequent to the IPE. STP PRA staff indicates that feedback from Maintenance Rule operating experience has been factored into the PRA as a means of capturing plant-specific failures.	A guidance document for reviewing MR failures is not necessary. The PRA staff sits on the MR expert panel and reviews all MR failures for inclusion in the PRA. Each failure is coded as PSAFF (a PSA functional failure), kept for general PRA data update, or not applicable to PRA. Given the emphasis in the ASME standard on guidance documents, and the expectation for qualifying new data analysts, a guidance document for data analysis will be created for STP_REV5 model.	Partial
AS-05	S	Failure of turbine trip or failure of the MSIVs to close is modeled in the STP PRA as a possible event sequence pathway that can result in a PTS failure of the vessel, based on the resultant excessive plant cooldown. In addition, these failures are also modeled to potentially fail the turbine driven auxiliary feedwater pump based on low SG pressure to drive the steam turbine.		n/a
AS-06	S	The Event Sequence Diagrams are constructed to show a very large number of possible accident sequence progressions based on operator actions specified in the EOPs as well as interactions between systems and components. These were then used to construct the Event Trees, which are subsequently quantified for core damage and fission product releases. A discussion is provided concerning the tracking between event sequence diagram and the event tree, including the elimination of event sequence diagram nodes for the event tree. The event sequence diagrams show that a thorough effort was completed to identify the applicable operator actions from the EOPs and the system interactions. In addition, very detailed dependency matrices document the support system requirements and other dependencies between systems. These dependencies are translated into event tree logic by way of the event tree structure and split fraction rules.		n/a

Table 1 – STP PRA Peer Review Facts and Observations

F&O OBS ID	LEVEL OF SIGNIFICANCE	OBS TEXT	PLANT RESPONSE	STATUS
HR-05	S	The HRA analysis develops PSF's for 7 factors. The process for quantification of each PSF involved multiple operator interviews (25). To the extent the reviewers could assess the interview process, it appeared to provide unbiased questioning of operator's opinions. The insight and opinions resulting from the PSF questionnaires is invaluable.		n/a
DE-05	S	A dependency matrix is available to describe the dependency relationship among systems. The level of detail is at the train level with quite thorough documentation. The initiating event effects on front line and support systems were described through the analysis of event tree and top event split fraction, and were well documented. The treatment of system-to-system dependencies was modeled and there is clear traceable documentation.		n/a
DE-06	S	In all aspect of spatial dependencies, the STPEGS PRA (in 1988) performed a rigorous hazard analysis which considered jet water, spray water, explosive canisters, equipment drops, high temperatures and missiles. The work was largely completed in an extensive walk down. All rooms were walked down and documented.		n/a
L2-03	S	The use of a methodology such as the STADIC code to determine the probability of containment challenges permits the correct assessment of two probability events. This methodology requires the determination of probability distributions for both containment loads and containment response and permits the assessment of the impact of distribution "tails".		n/a
MU-04	S	STP Procedure 0PGP01-ZA-0305 "PRA Model Update and Maintenance" specifies that the models shall be stored on permanent media (e.g., CD ROM) in accordance with quality documents (i.e., copy placed in a secure vault). 0PGP04-ZA-0604 "Probabilistic Risk Assessment Program" references 0PGP07-ZA-0014 "Software Quality Assurance" for the controls on the PRA software. Code and model software control is very good, with controlled copies of the model stored on the local area network. The model naming convention ensures that correct versions of the code and models are used. Procedures require copying down current version from local area network before performing any calculation to ensure current version of the model being used. Hard copies of results and calculations, including sensitivity runs, are transmitted to Records for permanent retention.		n/a

Response to MU-01:

There are four documents that outline expectations of analysts when updating the PRA. The global document that explains general expectations and processes is the Living PRA Policy Document (Ref. 1). The parent procedure for all work performed using the PRA by the Risk Management Department is 0PGP04-ZA-0604, Probabilistic Risk Assessment Program (Ref. 2), which specifically assigns duties and responsibilities to individuals within the group and outlines licensing commitments and other departmental requirements. The procedure that controls the PRA model configuration and update process is 0PGP01-ZA-0305, PRA Model Maintenance and Update (Ref. 3). PRA analysts at STP are trained and qualified to use these documents and procedures in unison in performing daily tasks with regard to the PRA. Finally Risk Management Guideline 002, User Manual for the PRA Database of Inputs (Ref. 4) describes how to maintain the Database of Inputs which includes reviewing and dispositioning all known references currently in the PRA, and integrating new references including external industry documentation into the PRA.

Starting with Ref. 1, a general mindset is created with regard to maintaining a "Living PRA" under the guidance of NRC GL 88-20 and NUREG CR-2300. Two prime directives are defined which specifically address using up to date tools and methodologies when updating the model to provide a current and up to date assessment. In the realm of Technical Quality Assurance all changes to the PRA must be value added, optimizing resources towards those areas of highest safety significance. Though the Living PRA Policy Document is slightly outdated (currently under revision) with regard to current programs and capabilities of the PRA, the concepts set forth by this document to update the PRA with current methodologies is clearly implied.

The Probabilistic Risk Assessment Program Procedure (Ref. 2) takes what is outlined in the Ref. 1 and becomes more specific. Step 5.3 Maintenance and Control clearly outlines departmental expectations and licensing commitments with regard to the PRA reference model. Step 5.3.3 States "Scheduled PRA Reference Model Updates SHALL have a clearly defined and documented scope. An update should reassess PRA figures of Merit periodically incorporating applicable plant modifications, procedure changes, Risk Management guideline revisions, advances in PRA Methodology, and plant configuration data collected since the previous update." Combining concepts from Ref. 1 and Ref. 2 one can see that if the methodology change is value added, and in the scope of the PRA model update, then it will be incorporated in the model by procedure. Since STP has UFSAR section 13.7 requirements to update certain aspects of the PRA at different frequencies all details of the model will be reviewed and changes will be implemented at a frequency of every 36 to 60 months.

Taking the input from the two previous references, the PRA Model Maintenance and Update Procedure (Ref. 3) becomes very specific in how to update the PRA model to meet departmental and licensing commitments. Again responsibilities are clearly defined for individuals performing this procedure. The PRA Model Maintenance and Update Procedure is broken up into two parts, maintaining the PRA on a daily basis which includes revisions to the model, and formal reference model updates. Section 4.0 PRA Database of Inputs and System Update Process describes the daily maintenance and update requirements of the PRA. The PRA Database of inputs is an Access database that tracks all changes to references used in the PRA, which includes a review of all "external" industry documents. The PRA Database of inputs also has a departmental guideline Ref. 4, which is referenced in Ref. 3, and is an integral part of a departmental expectation to review all reference changes to assigned PRA Model notebooks on a monthly basis, and disposition the effect those changes have on the PRA. Sub-Steps of 4.0 will lead the annalist to perform a revision of the PRA Reference Model for changes to a reference, methodology, discrepancy, or error. No

matter what caused the change to the model, if there is an increase to CDF of greater than 10% a condition report SHALL be generated and the process of updating the model to account for this change will be evaluated. Additionally, since many changes to the PRA do not meet the 10% trigger for an update, cumulative effects are also captured in Step 4.4. The Reference Model coordinator is required to monitor the cumulative effects of minor changes and evaluate whether a revision to the model should be made prior to a complete reference model update.

The PRA database of Inputs Risk Management Guideline (Ref.4) is a highly detailed and outlined user manual. Section 2 Background, states:

Another source of documentation that may generate a requirement or a desire to modify the STPEGS PRA not captured in the PRA Database of Inputs are "external" industry documents. The Manager, Risk Management will, at times he deems appropriate, assign PRA Analysts to review and determine if these documents generate a requirement or desire to change the PRA. Examples of external industry documents include the following:

U. S. Nuclear Regulatory NUREG reports
Nuclear Energy Institute (NEI) documents
Institute for Nuclear Power Operations (INPO) documents
Industry owners group (i.e., Westinghouse Owners Group, etc.) documents
Electric Power Research Institute (EPRI) reports
Industry professional society (i.e., ASME, ANS, IEEE, etc.) documents
Other external documents and databases identified by the Manager, Risk Management.

Both internal and external documents that should be referenced or applied to the PRA should be added to the PRA Database of Inputs. A tracking (CNAQ) Condition Report action should be used to insure the documentation is referenced and discussed in the relevant PRA documentation. In this way, new documents that affect the PRA models are identified during the periodic PRA update process.

It was discovered during the update of STP_1999 that the issues commented on by the Peer Review Team were a concern, and the procedures and guidelines were revised at that time to account for all the concerns described in MU-01. Therefore we disagree with the finding level of significance. Prior model revisions did not have the detailed procedures and guidelines that are now used in performing a PRA reference model update or revision. It should not be assumed that new methodologies have not been reviewed or implemented in the PRA as condition reports have been generated to track implementation of the needed changes. However, the observation brings to light that STP Risk Management should do a better job of documenting these reviews.

Response to QU-05:

Accident sequences from other plants are not readily available. WOG has provided a PSA survey database that contains some useful information on PRA results but not sequences.

Compared results from other Westinghouse PWRs using RISKMAN. The comparison involved initiating event contribution to CDF and system importance (risk reduction).

Reference W PSA model method and results comparison database - Rev 2. Information for database obtained in 1997.

Sequence comparison - physical sequence comparison is not possible, however, information can be gleaned from other available information.

Comparison made between the following similar plants: Diablo Canyon, Seabrook, Beaver Valley, Sequoyah and Watts Bar.

Comparison of table 9.2 CDF by IE - in large part STP's value were different due to incorporation of generic initiating event information from NUREG/CR-5750, February 1999. Information other plants did not have access to. This issue also hampers comparison of other available tables like CDF by sequence type.

Comparison of Table 9.5 system importance can be made. For the most part system importance compares favorably (i.e., within 10%) except the following:

AF for Diablo Canyon (11% dec) , Seabrook (17% inc) and BV (17% inc) - each plant has 2 MD and 1 TD

DG for Diablo Canyon (33% inc) and Sequoyah (12% dec) – Diablo Canyon - 3 diesel and ESF bus cross-tie, Sequoyah - two DG per unit and ESF bus crosstie.

DJ for Sequoyah (27% inc) - 2 DC buses

RC (pressure relief) for Seabrook (13% inc) and Beaver Valley (14% dec)

EW for Beaver Valley (24% inc) - 2 cross-tied MD trains. STP has 3 non cross-tied EW trains each with a MD.

It is difficult to make a direct comparison with the limited information provided in W database. However, 2 STP engineers participated in 4 WOG PRA peer certification reviews. This provides confidence that STP PRA is comparable to other PRAs.