September 11, 2002

MEMORANDUM TO: James Lyons, Director
New Reactor Licensing Project Office
Nuclear Reactor Regulation

FROM: F. Mark Reinhart, Section Chief /**RA/**
Probabilistic Safety Assessment Branch
Division of Systems Safety and Analysis
Nuclear Reactor Regulation

SUBJECT: REQUEST FOR ADDITIONAL INFORMATION ON AP1000 LEVEL 1 PRA FOR OPERATION AT POWER (TAC NO. MB4683)

Attached is a set of request for additional information (RAIs) prepared by the Probabilistic Safety Assessment Branch (SPSB) regarding the AP1000 Level 1 PRA for power operation. If you have any questions regarding these RAIs, please contact Nick Saltos at 415-1072.

Attachment: As stated

cc: Michael Johnson
Lawrence Burkhart
Robert Palla
Marie Pohida
Yi-Hsiung Hsii
Walton Jensen

September 11, 2002

MEMORANDUM TO: James Lyons, Director
New Reactor Licensing Project Office
Nuclear Reactor Regulation

FROM: F. Mark Reinhart, Section Chief /**RA/**
Probabilistic Safety Assessment Branch
Division of Systems Safety and Analysis
Nuclear Reactor Regulation

SUBJECT: REQUEST FOR ADDITIONAL INFORMATION ON AP1000 LEVEL 1 PRA FOR OPERATION AT POWER (TAC NO. MB4683)

Attached is a set of request for additional information (RAIs) prepared by the Probabilistic Safety Assessment Branch (SPSB) regarding the AP1000 Level 1 PRA for power operation. If you have any questions regarding these RAIs, please contact Nick Saltos at 415-1072.

Attachment: As stated

cc: Michael Johnson
Lawrence Burkhart
Robert Palla
Marie Pohida
Yi-Hsiung Hsii
Walton Jensen

Accession#MLML022540132 NRR-096
DISTRIBUTION: SPSB r/f
G:\\spsb\saltos\AP1000RAIS.wpd

OFFICE	SPSB	SC:SPSB
NAME	NSaltos:nyc	FMReinhart
DATE	09/10/02	09/10/02

OFFICIAL RECORD COPY

SPSB REQUEST FOR ADDITIONAL INFORMATION
ON
AP1000 LEVEL 1 PROBABILISTIC RISK ASSESSMENT
FOR
OPERATION AT POWER

720.27 The staff review identified several differences between the AP600 and the AP1000 probabilistic risk assessments (PRAs) in the assumed initiating event frequencies for several accident categories. These differences are related to (a) various loss of coolant accident (LOCA) categories, (b) steam generator tube rupture (SGTR) accidents, and (c) passive residual heat removal (PRHR) tube rupture accidents.

For the LOCA categories, these differences are primarily due to the selective use in the AP1000 PRA of operating experience data reported in NUREG/CR-5750 for pipe breaks as opposed to data from a pipe break analysis used in the AP600 PRA. In the AP1000 PRA, operating experience data are used for some pipe break frequencies (e.g., pipe breaks contributing to medium and large LOCAs) but not for others (e.g., pipe breaks in the direct vessel injection lines). Similarly, the frequencies of contributors to the various LOCA initiating event categories other than pipe breaks, such as stuck-open pressurizer valves, were calculated in the AP1000 PRA while operating experience data are reported in NUREG/CR-5750 for these contributors.

The initiating event frequency for SGTR events is assumed in the AP1000 PRA to be 3.88E-3 events/year as opposed to 5.2E-3 events/year used in the AP600 and 7E-3 events/year reported in NUREG/CR-5750. In attachment 2A, it is stated that the AP1000 SGTR frequency is based on 1.94E-7 failures per tube-year instead of 1.25E-6 failures per tube year used in the AP600 PRA because the AP1000 steam generator will be manufactured using Alloy 690 which is more resistant to stress corrosion cracking than the Alloy 600 assumed in the AP600 design. It is argued that due to this design improvement the SGTR frequency is smaller for the AP1000 design than the AP600 design even though the AP1000 steam generators have many more tubes (i.e., 20,000 for AP1000 versus 12,614 for AP600). Please explain how the SGTR frequency per tube year for AP1000 was calculated, including data and assumptions.

The initiating event frequency for PRHR tube rupture events is assumed in the AP1000 PRA to be 1.34E-4 events/year as opposed to 2.5E-4 events/year used in the AP600 PRA even though there are more and longer tubes in the AP1000 design. Statements made in section 2.3.1.4 imply that the reliability of the AP1000 design PRHR tubes has improved because the reliability of the AP1000 SGTR tubes has improved with respect to the AP600 design. Please explain or re-calculate the PRHR tube rupture frequency to address these comments.

The frequency of PRHR tube rupture events is shown in the associated event tree (page 4-185) as 2.83E-4 events/year which is different from 1.34E-4 events/year reported in Chapter 2. Please explain and revise appropriately.

The staff believes that a better understanding is needed of the impact of these new frequencies, including uncertainties, on PRA results and insights which were derived from the AP600 PRA and assumed to be valid also for AP1000. Examples of insights and conclusions that may need to be revised are the identification of low thermal margin but risk significant success sequences for thermal-hydraulic uncertainty assessment and the level of availability control for non-safety-related equipment. Please provide information addressing this issue.

720.28 The staff review identified two potentially significant differences between the AP600 and the AP1000 PRAs in the categorization of LOCA initiating events. One difference involves combining two AP600 PRA LOCA categories into one AP1000 PRA category. In the AP600 PRA, a medium LOCA (MLOCA) and an intermediate LOCA (NLOCA) categories were defined. The MLOCA involved break sizes between six and nine inches equivalent diameter and the NLOCA involved break sizes between two and six inches equivalent diameter. In the AP1000 PRA, however, these two categories were combined to one category (MLOCA which range from two to nine inches equivalent diameter. The other difference involves the splitting of one AP600 PRA LOCA category into two categories in the AP1000 PRA. In the AP600 PRA, the large LOCA category included both pipe breaks and spurious opening of the automatic depressurization system (ADS) valves. In the AP1000, there is one large LOCA category for pipe breaks and another large LOCA category for spurious ADS actuation.

Thermal-hydraulic (T-H) analyses performed for the AP600 design have identified bounding parameters (e.g., break size and location) for each LOCA category. The success criteria for systems and operator actions used in the AP600 PRA were determined by studying the plant response given such bounding parameters. For example, in the AP600 PRA, the success criteria for a MLOCA (i.e., six to nine inches equivalent diameter) are based on a cold leg break while for an NLOCA (i.e., two to six inches equivalent diameter) they are based on a hot leg break. These two AP600 LOCA categories which are associated with different plant responses were combined in the AP1000 PRA. Since the AP1000 PRA success criteria are based to a certain extend on information from analyses performed for the AP600 design, please explain the following:

a. Why these different initiating event categorizations were needed;

b. How information from AP600 design T-H analyses is used to support AP1000 design criteria; and

c. The approach that was followed, including new analyses beyond those performed for AP600, to ensure that the AP1000 success criteria are valid for all break sizes and locations in each category and that the thermal-hydraulic (T-H) uncertainties for risk-significant sequences are bounded.

720.29 In Section 6.3.2.5, the time windows available for several operator actions associated with specific LOCA sequences are discussed. They include operator

actions to actuate the core makeup tanks (CMTs), depressurize the reactor coolant system (RCS) , and actuate the normal residual heat removal (NRHR) pumps. In many cases, more than one time windows (success criteria for operator action) are defined depending on the success or failure of other systems. For example, for medium LOCAs and CMT line breaks it was determined that the time available for operator action to manually actuate CMT injection (from the time the first signal that would alert the operators to the fact that CMT actuation should have occurred) is 10 minutes without accumulator injection and 20 minutes with accumulator injection. Similarly, for medium LOCAs and CMT line breaks it was determined that the time available for operator action to manually depressurize the RCS is 20 minutes for cases with successful accumulator injection and passive residual heat removal (PRHR) injection but too short to take credit for operator action for cases without accumulator injection or PRHR operation. The success criteria for operator actions used in the AP1000 human reliability analysis (HRA) are summarized in Table 6.3. For the specific example of medium LOCAs and CMT line breaks, two operator actions are listed: (1) Manually actuate the CMTs if automatic actuation fails (event CMN-MAN01); and (2) recognize need for RCS depressurization (event LPM-MAN02). It appears from the HRA, documented in Chapter 30, that the human error probabilities for the events CMN-MAN01 and LPM-MAN02 were calculated assuming a 20 minutes time window, independently of the success or failure of the accumulators and PRHR (actually, the PRHR is not modeled at all in the MLOCA and CMT line break event trees). Please explain how the various success criteria for operator actions (time windows), determined by thermal-hydraulic analyses of the various accident sequences, were modeled in the PRA.

720.30 The AP1000 PRA event trees include a top event for containment cooling (event CHR). In Chapter 4 (Event Tree Models) it is stated that this top event models the need to successfully remove thermal energy from the containment atmosphere to the environment via the containment vessel following events that cause a significant increase in containment pressure and temperature, such as a LOCA and main steam line break accident inside containment. However, several statements made in Chapter 6 (Success Criteria Analysis) imply that the passive containment cooling system (PCS) water is not needed to prevent core damage. For example, on page 6-8 it is stated: *"Therefore, sequences in which core damage has been avoided with successful IRWST injection and recirculation represent success (i.e., no core damage) regardless of the status of containment integrity or PCS water."* Furthermore, on page 6-9 it is stated: *"For success paths that result in steam release to the containment, the success of containment cooling (PCS or RNS) is modeled. If containment cooling is successful, then the path ends in an OK state. If PCS water cooling is not successful, then the path goes to a special OK end state to allow containment integrity sensitivity studies to be made."* This "special OK" end state is labeled "late containment failure (LCF)" end state on page 4-141 and defined as an end state *"...where the containment heat removal by either passive containment cooling system (PCS) or component cooling water (CCS) heat exchangers via normal residual heat removal (RHR) fails."* These and other similar statements throughout the PRA create some confusion regarding what constitutes the PCS and what the criteria for its success are. In addition, no attempt is made to assess the impact of the "special OK end state" on PRA results and insights.

Please address the following items:

a. Is containment cooling by heat transfer through the containment shell to the outside air included in the functions of the PCS system? Some parts of the PRA imply that containment cooling by air flow is part of the PCS while elsewhere in the PRA it is stated that the PCS is identical with the passive containment system water. If the answer is yes, please revise the system description and success criteria accordingly. Otherwise, include a statement at the beginning of each chapter discussing containment cooling, such as Chapter 4 (event tree models) and chapter 6 (success criteria), to clarify that air cooling is not part of PCS.

b. The success criteria for containment cooling are included in section 6.3.1.5 under "Containment Isolation." Please include a separate section discussing the success criteria for "Containment Cooling."

c. In Chapter 13, on Passive Containment Cooling System (PCS), three fault tree models are listed. One, labeled PCT, is for all transients and LOCA events. Another, labeled PCP, is for loss of offsite power accidents. A third, labeled PCB, is for station blackout accidents. Table 13-2 summarizes the success criteria for fault tree PCT only. Since the PCS is a passive system, loss of offsite power or station blackout should not have an impact on the fault tree of this system. Please explain how fault trees PCP and PCB are different from PCT.

d. It is stated in Chapter 13 on Passive Containment Cooling System (PCS) that blockage or plugging of the air flow paths is not modeled in the PRA because of the many design features that make such failure mechanisms highly unlikely (e.g., fifteen air flow path inlets covered by screens, each provided with a heating source to prevent blockage due to buildup of snow or ice). The staff believes that even "highly unlikely" failures should be included in the PRA models when such failures are associated with certain systems, structures and components (SSCs) whose unavailability or degradation would increase significantly the plant's risk (i.e., SSCs associated with high risk achievement worth). An SSC's risk achievement worth is used to identify operational requirements, such as requirements for surveillance and maintenance, to ensure that failure rates for these SSCs do not increase and remain "highly unlikely." In the case of containment air flow cooling paths, is air blockage highly unlikely when the availability of the heating sources to prevent buildup of snow or ice is not properly monitored and maintained? This issue maybe more significant for AP1000 than it is for AP600 because of the higher power and, thus, lower thermal margin associated with AP1000 as compared to AP600. Please provide a discussion on how this issue is being addressed in the AP1000 PRA.

e. On page 6-9 it is stated that *"If PCS water cooling is not successful, then the path goes to a special OK end state to allow containment integrity sensitivity studies to be made."* This "special OK" end state is labeled

"late containment failure (LCF)" end state on page 4-141. Please explain the reasons for considering containment integrity sensitivity studies but not core damage sensitivity studies. Would not the assumed late containment failure cause core damage and large release? Also, is containment cooling by air flow alone adequate for long-term operation of the passive residual heat removal (PRHR) system even in the presence of an open or failed containment? Please explain and provide supporting analyses, as necessary.

f. The success criteria for containment heat removal, as listed in Table 6-2 and associated footnote #17, indicate that heat transfer through the containment shell to the outside air is sufficient to cool the containment atmosphere even with an open containment. According to Table 6-2, the success criteria for containment cooling by air flow for all accident sequences are based on thermal-hydraulic analyses documented in Appendix A of the PRA. However, the staff was not able to locate such analyses. Please explain.

g. If there is significant uncertainty whether the "late containment failure (LCF)" end state can lead to core damage, please perform a sensitivity study to assess the potential impact of this uncertainty on PRA results and insights, including insights related to the identification of non-safety-related equipment for availability control as well as the level of availability control for such equipment.

720.31 The success criteria listed in Table 6-2 for the "containment integrity" function appear to apply to the "core cooling" function. Please explain and revise accordingly.

720.32 In Section 6.3.1, General Sequence Success Criteria, it is stated (page 6-3): *"In general, if the reactor achieves a stable shutdown condition without core damage, and this condition can be maintained for at least 24 hours following event initiation without further action or system operation, the sequence is categorized as successful. It is not sufficient to avoid core damage during the first 24 hours if conditions have not stabilized and core damage is anticipated shortly following 24 hours. That is, core damage is assumed if the RCS conditions are not stabilized in 24 hours, or if core damage is anticipated following 24 hours without further system or operator action."* Please describe the accident sequences where the conditions are not stabilized in 24 hours or core damage is anticipated following 24 hours without further system or operator action.

720.33 Several statements and common cause failure (CCF) probabilities related to explosive (squib) valves, included in Chapter 12 on Passive Core Cooling/In-Containment Refueling Water Storage Tank and in Chapter 29 on Common Cause Failure Analysis, appear to be conflicting each other. For example, in section 12.6.1 (page 12-6) it is stated: *"Common cause failures of the valves in the*

injection paths are modeled separately or independently of common cause failure of the valves in the recirculation paths." However, in section 29.3.1 (page 29-6, assumption #9) it is stated: *"The IRWST injection system consists of four high-pressure (HP) explosive valves (EV). The IRWST recirculation system consists of two HP EVs and two low-pressure (LP) EVs. For this analysis, these valves are grouped into one common-cause failure group of six HP EVs and one common-cause failure group of two LP EVs."* Another example of conflicting statements is the definition of event IWX-EV3-SA which in Table 12-8 is defined as the CCF of two squib valves in the recirculation lines while in Table 29-2 it is defined as the CCF of three out of six HP EVs. Please explain and revise appropriately such statements in Chapters 12 and 29. In addition please provide information to clarify the following items:

a. The staff was not able to find a description of the design and operational differences between HP and LP explosive (squib) valves. Please explain what makes these valves "diverse" so that CCF between them is considered negligible.

b. The calculation of CCF probabilities for several sets of explosive and check valves is documented in Chapter 29 and summarized in Table 29-2. Several discrepancies appear in the assessed probabilities for the various sets of valves. For example, the CCF of all six HP EVs (event IWX-EV-SA) was assessed to be 2.6E-5/demand while the CCF probability of only two HP EVs (event IWX-EV1-SA) was assessed to be 5.8E-6 per demand (i.e., smaller than the CCF probability of all six valves in both injection lines). Similarly, the CCF probability of all four injection check valves (event IWX-CV-AO) was assessed to be 3.0E-5/demand while the CCF probability of only the two check valves in one injection line (event IWX-CV1-AO) was assessed to be 5.4E-7/demand. It appears that this discrepancy resulted from an erroneous application of the methodology used to assess CCF probabilities. These CCF probabilities have a significant impact on PRA results and insights as the importance analyses reported in Chapter 50 indicate. Please explain and revise as necessary.

c. The HP EVs were grouped into one common-cause failure group when both injection lines are available but not when only one injection line is available, as is the case of a direct vessel injection (DVI) line break accident. Please explain the basis for this apparent discrepancy and revise as necessary.

720.34 The sensitivity of the PRA results to the unavailability of the non-safety related standby systems was investigated and the results are summarized in section 50.5.4 (sensitivity case # 36). However, two different CDF numbers are reported in page 50-14. A CDF of 2.92E-5/year is reported at the end of section 50.5.4 while in section 50.6 (Results) a CDF of 7.345E-6/year is reported. Please explain and revise as necessary.

720.35 In Chapter 26 on the Protection and safety Monitoring System (PMS), in Chapter 27 on the Diverse Actuation System (DAS) and in Chapter 28 on the Plant Control System (PLS), the following statement is made: *"Because of the rapid changes that are taking place in the digital computer and graphic display technologies employed in the modern human systems interface, design certification of the AP1000 focuses upon the process used to design and implement instrumentation and control systems for the AP1000, rather than on the specific implementation."* To be able to take advantage of such changes in technology, design options in additions to the ones used in the AP600 design certification are proposed for the safety-related PMS and the non-safety related DAS and PLS. For the safety-related PMS, the option to use the Common Qualified Platform (Common Q) is proposed. For the non-safety-related DAS and PLS, the option to use commercial off-the-shelf hardware and software which will be current at the time of construction is proposed. Please provide more detailed information regarding the implementation of the proposed options by responding to the following questions:

a. Regarding the PMS, it is stated that the AP600 I&C functional requirements, which have received design certification, will be retained to the maximum extent compatible with the Common Q hardware and software. Also, it is stated that although the details of the AP1000 PRA model follow the AP600 design, the Common Q hardware and software provide a degree of redundancy that is equivalent to the redundancy modeled in the AP1000 PRA. Please explain the process that will be used to verify that a PMS designed with the "Common Q" option will have equivalent or better reliability with the system modeled in the PRA. Also, please explain how the introduction of the "Common Q" option will affect important PRA-based insights about the PMS, such as the ones identified during the AP600 PRA review (i.e., the design certification information "PRA-based insights" documented in Table 19.59-29 of the AP600 DCD).

b. Regarding the non-safety-related DAS and PLS, it is stated that the AP1000 PRA is based on *"one possible ....configuration designed to meet the requirements of DCD Chapter 7"* and that *"the functional requirements and the degree of redundancy modeled in the PRA are representative of the expected final ....design."* Please explain the process that will be used to verify that the DAS and PLS ,designed with the "commercial off-the-shelf hardware and software current at the time of construction" option, will have equivalent or better reliability with the systems modeled in the AP1000 PRA. Also, please explain how the introduction of such an option will affect important PRA-based insights about the DAS and PLS, such as the ones identified during the AP600 PRA review (i.e., the design certification information "PRA-based insights" documented in Table 19.59-29 of the AP600 DCD).

720.36 In Appendix A (page A-29), several accident sequences, which were identified in the AP600 PRA as "low T/H margin, risk important" scenarios, are discussed with respect to their potential applicability to AP1000 design. While the first three cases discussed concern small LOCAs (SLOCAs), it is stated that *"The PRHR HX is*

included for the AP1000 because the success criteria has been changed to require PRHR HX operation for MLOCAs with failure of CMTs." Please clarify and revise accordingly.

720.37 In Appendix A (pages A-28 and A-29) it is stated that a process to evaluate thermal-hydraulic (T/H) uncertainty was developed for the AP600 design certification. This process included the identification of "low T/H margin PRA important accident scenarios" which were analyzed with design basis accident analysis computer codes to bound the T/H uncertainty. It is argued that no additional sequences can be classified as "low T/H margin PRA important accident scenarios" for AP1000 beyond those identified and analyzed for the AP600 design because the AP1000 plant/systems are very similar in design and capability to the Ap600's and the PRA results are similar. The staff believes that additional analysis is needed to support this argument. Even though the two designs use similar systems with comparable capabilities to respond to design basis accidents, differences in sizes, flow rates, heat transfer areas and decay heat production exist between the two designs. The impact of such differences to plant response can be significant for beyond design basis accident scenarios involving multiple failures and potentially system interactions. In addition, changes in initiating event categories, initiating event frequencies and success criteria in the AP1000 PRA, as compared to the AP600 PRA, could have increased the risk significance of accident scenarios. Please use a systematic approach to identify "risk significant low margin" sequences for detailed T-H uncertainty assessment.

720.38 An important objective of the AP600 design certification PRA was to identify important PRA insights and assumptions and make sure that they have been addressed in the design certification through design certification requirements, such as requirements for inspection, tests, analyses and acceptance criteria (ITAAC), the requirement for a design reliability assurance program (D-RAP) and combined operating license (COL) action items. These requirements were incorporated in the Design Control Document (DCD), Table 19.59-29 "PRA-based insights," to ensure that any future plant which references the design will be built and operated in a manner that is consistent with important assumptions made in the design certification PRA. Please provide similar information for AP1000. Since the major part of this information is expected to be the same as for AP600, please start with DCD Table 19.59-29 and highlight the differences in "insights" between the two designs.

720.39 An important objective of the AP600 PRA was to provide input to the design certification process regarding the need for regulatory oversight of certain non-safety-related systems. The process used to identify systems, structures and components (SSCs) for regulatory oversight as well as the type and level of such oversight was called Regulatory Treatment of Non-Safety-Related Systems (RTNSS) in the AP600 certification. The end result of this process were the "availability controls" documented in Section 16.3 of the DCD. Please provide similar information for AP1000. This information should account for uncertainties in

the AP1000 PRA so that it can be used by the staff to make similar conclusions, about the need for non-safety-system oversight, to those made for the AP600 design (e.g., as documented in the AP600 FSER Chapter 19.1.7 “PRA input to the RTNSS Process.)”

720.40 Please provide representative examples of PRA use in the AP1000 design process to achieve each of the following objectives: (a) enhance the AP1000 design by adding or modifying design features or operational requirements; (b) quantify the effect of new design features and operational strategies on plant risk to confirm the risk reduction credit for such improvements; (c) select among alternative features, operational strategies or design options.