Request for Additional Information No. 2, Revision 0

4/10/2008
U. S. EPR Standard Design Certification
AREVA NP Inc.
Docket No. 52-020
SRP Section: 19 - Probabilistic Risk Assessment and Severe Accident Evaluation
Application Section: 19
SPLA Branch

QUESTIONS

19-1

Section 19.0.1, "NRC Regulatory Requirements and Related Policies," does not include several items listed in Section 19.0 of the Standard Review Plan (SRP). For completeness, please confirm in Section 19.0.1 that the following requirements and guidance either were considered or are not applicable: (1) Title 10 of the Code of Federal Regulations (10 CFR) 52.47(a)(8); (2) 10 CFR 52.47(a)(23); (3) 10 CFR 52.47(a)(27); (4) NRC Policy Statement, "Regulation of Advanced Nuclear Plants"; (5) SECY-96-128 and the related Staff Requirements Memorandum (SRM); (6) SECY 97-044 and the related SRM.

19-2

Footnote 8 in RG 1.206, Section C.I.19, Appendix A, states that: "'PRA [probabilistic risk assessment]-based insights' are those insights identified during the DC [design certification] process that ensure that assumptions made in the PRA will remain valid in the as-to-be-built, as-to-be-operated plant and include assumptions regarding SSC [structure, system, and component] and operator performance and reliability, ITAAC [inspections, tests, analyses, and acceptance criteria], interface requirements, plant features, design and operational programs, and others. The usage of the phrase is intended to be consistent with its use in Table 19.59-29 of the AP600 design control document [DCD]." In the AP600 DCD, each insight receives a disposition such as a reference to another portion of the DCD, an ITAAC, or a combined license (COL) information item. Table 19.1-102, "Summary of Insights from the PRA of the U.S. EPR," does not include a similar disposition for each insight to ensure that the assumptions remain valid in the as-to-be-built, as-to-be-operated plant. For example, the diversity of the station blackout diesel generators is an important assumption that must be retained by future COL holders. Please update Table 19.1-102 to include a disposition for each insight and ensure that the table reflects all important assumptions and insights that must remain valid for future plants.

19-3

Section 19.1.4.1.1.4, "Data Analysis," lists unavailabilities of equipment due to testing and maintenance as a type of data required for the probabilistic risk assessment (PRA), but does not provide the source of test and maintenance unavailability estimates. Please discuss how test and maintenance unavailabilities were derived. Please discuss how plans for online maintenance (given the four-train redundancy of most systems) were addressed if generic data was used.

19-4

Please provide the generic failure probabilities and distribution parameters used for components in the PRA, with references to the data source, so that the NRC staff can confirm the statement in section 19.1.4.1.1.4, "Data Analysis," that the data is "comparable to other U.S. data sources."

19-5

The values presented in the "Risk Metrics" sections throughout Chapter 19 appear to be point estimates. NRC guidance, as well as the American Society of Mechanical Engineers (ASME) PRA standard, specifically requests mean values rather than point estimates. (See Regulatory Guide (RG) 1.174, section 2.2.5.5; RG 1.206, Section C.I.19, Appendix A; SRP 19.0, section III; ASME RA-Sb-2005, Supporting Requirement QU-A2b; and RG 1.200, Table A-1, clarification of requirement QU-A2b.) Therefore, the final safety analysis report (FSAR) should be revised to reflect: (a) Mean values for risk metrics (i.e., core damage frequency (CDF) and large release frequency (LRF)) in all appropriate sections (b) Any changes to risk insights as a result of using the mean value (c) Clarified discussion of the impact of redundant equipment with the same state-of-knowledge-based probability distribution (d) Discussion of why the impact is different for the internal events, fire, flooding, shutdown and Level 2 PRA elements. Additionally, the response to this RAI should include a list of the correlation classes used in the PRA model and the components that are assigned to each class. If there is any difference between the correlation class grouping and common cause grouping (especially for the emergency and station blackout diesel generators), please identify and justify these differences.

19-6

Section 19.1.4.1.1.4 states that point estimates (not mean values) were used for frequency inputs to the CDF quantification for initiating events whose frequencies were calculated using fault trees. Please provide the mean frequencies for all initiating events evaluated using fault trees. Please discuss how the state-of-knowledge correlation described above is addressed for these frequencies.

19-7

Please provide system information (including a description and system drawing or fault tree) as assumed in the PRA for the closed cooling water system, auxiliary cooling water system, and operational chilled water system. These systems appear to be modeled in the PRA, but no information on the systems could be found in the rest of the FSAR.

19-8

Section 19.1.4.1.1.3, "Systems Analysis," states that the Babcock & Wilcox (B&W) design most closely resembles the U.S. EPR in terms of total number of control rods and success criteria. Appendix C of NUREG/CR-5500, Volume 11, indicates that the control rod drive and rod failure data is based on pooled testing and unplanned trip data from B&W, Combustion Engineering (CE), and Westinghouse. Please discuss whether this pooling affects the conclusion that the B&W data is applicable to the U.S. EPR.

19-9

Please provide more justification for the statement in section 19.1.4.1.1.3 that the control rod failure probability of 4.1E-8/demand from NUREG/CR-5500, Volume 11, is conservative for the U.S. EPR. The FSAR states that the U.S. EPR has 89 control rods, and analysis has shown that at least 38 control rods must fail to insert during a reactor trip before there is insufficient shutdown margin. This fraction—38 of 89 rods—corresponds to approximately 43%. It is not immediately obvious whether the common cause failure probability of 50% of 41 rods is greater than the failure probability of 38 of 89 rods. For comparison, Table E-7 of NUREG/CR-5500, Volume 11, provides a mean failure probability of 8.4E-7 for failure of 20% of rods (8/41) to insert.

19-10

Please provide justification for changing the level of dependence between post-maintenance testing and independent verification from complete to medium (section 19.1.4.1.1.5).

19-11

Please provide a more detailed description of Plant Operating State (POS) D, which section 19.1.6.1.2 describes as "RHR [residual heat removal] heat removal at mid-loop with RPV [reactor pressure vessel] head off." Commonly, water level is increased to the height of the RPV head flange before lifting the head, and the filling and draining POS are assessed separately from the mid-loop POS. Please describe any plans to operate at mid-loop with the RPV head off.

19-12

Please explain how the U.S. EPR design has considered the Shutdown Management Guidelines in NUMARC 91-06, including how containment closure can be achieved in sufficient time to prevent potential fission product release (NUMARC Guidelines 4.5).

19-13

Please provide a justification for not including support system failures, such as loss of component cooling water (CCW) or loss of essential service water (ESW), as initiating events in the shutdown PRA, as described in section 19.1.6.1.3. If support system failures are included as part of the loss of RHR initiating event, please discuss how the model accounts for the subsequent unavailability of these support systems after their failure causes a loss of RHR.

19-14

Please provide further justification for not including low temperature overpressure events as initiating events in the shutdown PRA, as described in section 19.1.6.1.3. What would the impact be of the inadvertent start of a charging pump, given that charging pumps are not required to be isolated per LCO 3.4.11? The statement in section 19.1.6.1.7 that charging is not credited in shutdown does not imply that charging is not available. The probabilities of both the initiator and subsequent relief valve failures should be considered in the assessment.

19-15

Is the loss of offsite power (LOOP) frequency in the shutdown PRA assumed to be the same as the at-power LOOP frequency? Please describe any related assumptions, such as switchyard maintenance during shutdown.

19-16

How does the shutdown PRA model account for both system-related failures (e.g., pump failures) and LOOP-related failures of the RHR system, and how are these failures separated to provide statements about the contribution of LOOP to shutdown risk?

19-17

How does the shutdown PRA model account for the subsequent unavailability of offsite power to support systems following a LOOP-induced loss of RHR?

19-18

Please justify the assumption in section 19.1.6.1.6 that all performance shaping factors (PSF) for operator actions are assumed to be optimal.

19-19

Please clarify the assumed refueling cycle and duration of shutdown. Table 19.1-91 indicates 18 days shut down per year, and the technical specifications (TS) bases in Chapter 16 refer to a 24-month refueling cycle. How have forced outages and maintenance outages, with or without entry into mid-loop conditions, been considered?

19-20

Section 19.1.6.1.8 states that transient combustibles and maintenance activities are judged not to be significant for the protected RHR trains providing decay heat removal during shutdown. What is the impact of transient combustibles and maintenance activities on the fire and flood frequency for RHR support systems (such as CCW or ESW)? Are these systems similarly protected during shutdown? How are fire and flood barriers controlled during shutdown? How are transient combustibles controlled during shutdown?

19-21

Please provide additional detail on the modeling of low-probability human failures in the shutdown PRA. What assumptions (such as procedures, cues, and timing) have been made, and how will these conditions be ensured in the as-to-be-operated plant? At a minimum, discuss the failure of the operator to isolate the chemical and volume control system (CVCS) low pressure reducing station (OPE-ISOCSLPRS) and the failure of the operator to start maintenance heating, ventilation, and air conditioning (HVAC) trains after failure of normal safety air chiller (SAC) safety train (OPF-SAC-1H).

19-22

Please describe the proposed sequence of events during shutdown between entry into MODE 5 and installation of nozzle dams in the steam generators and during startup between removal of nozzle dams and entry into MODE 4.

19-23

Table 19.1-87 indicates significant differences between the sub-states of POS CA (CAd1, CAd2, and CAd3), especially the mode, availability of steam generators for heat removal, and TS requirements. Therefore, please justify the modeling of POS CA as a single state and describe how available mitigation strategies in each of the sub-states are addressed in the detailed system modeling.

19-24

Please clarify when the steam generators can be used for heat removal, by both MODE and POS. Discuss how the availability of the steam generators will be ensured, given that: (a) The steam generator tubes (LCO 3.4.16), emergency feedwater (EFW) system (LCO 3.7.5), and EFW storage pools (LCO 3.7.6) are required by TS only in MODES 1-4 (b) Steam generator pressure and level sensors, main steam safety valves (MSSVs), and main steam relief trains (MSRTs) are required by TS only in MODES 1-3 (LCOs 3.3.1, 3.7.1, and 3.7.4) (c) Table 19.1-87 indicates that the RCS is vented in POS CAd2, CAd3, CB, and CAu

19-25

Is reflux cooling via the steam generators at mid-loop credited in the shutdown PRA? If so, please provide a justification.

19-26

Discuss how the repressurization (if any) required to use the steam generators for heat removal during shutdown challenges temporary pressure boundaries such as nozzle dams or thimble seals.

19-27

Sections 5.4.7.2.1 and 19.1.6.1.7 describe design features to address shutdown and mid-loop operations. However, most of these features appear to have limited or no coverage in TS, as presented in the attached table (Table RAI-19-1). Considering this table, please: (a) Confirm the apparent treatment in TS and justify the inclusion or exclusion of the referenced systems and signals

according to the four criteria in 10 CFR 50.36. If the analysis determines that the system or signal should not be included in TS, discuss how the availability of these features designed to reduce shutdown risk will be ensured. (b) Discuss how each feature is credited in the shutdown PRA. (c) Provide a sensitivity study for the shutdown PRA that credits only the mitigating systems that are required to be operable according to TS. This request is related to SECY-97-168, in which the staff concluded that the current level of shutdown safety was achieved by voluntary measures that are not required by current regulations, and that these measures could be withdrawn by licensees without NRC approval.

19-28

Section 19.1.3.4.3 states that MHSI is actuated on either low level in the RCS loops or LHSI/RHR pump low suction pressure. Low loop level is addressed by the previous question on TS coverage. However, no discussion of the low suction pressure actuation signal could be found elsewhere in the FSAR. Please provide additional information on this diverse MHSI actuation signal and discuss how the availability of the sensor and actuation signal is ensured during shutdown.

19-29

Table 19.1-102 is missing key U.S. EPR features that reduce shutdown risk and their disposition (e.g., Tier 2, Tier 1, TS, or emergency response guidelines). Please augment this table in the following areas of shutdown risk (the examples are not inclusive): (a) Key design features or structures, systems, and components (SSCs) that reduce the potential of reactor coolant diversion from the vessel through the RHR/CVCS systems (b) Key design features, if any, that automate the response to losses of RHR (c) Key design features, if any, that automate RCS injection following loss of RHR, reactor coolant diversions, and LOCAs (d) Key operator actions and key pieces of instrumentation that are needed to support the associated operator actions (e.g., operator opening a gravity injection flow path) (e) Key SSCs that need to be available at shutdown to provide an alternate decay heat removal path using low pressure makeup and primary pressure relief (f) Key SSCs that are needed to reduce fire risk at shutdown and validate fire risk estimates (e.g., capability of fire watches when fire barriers are not intact)

19-30

Please document the status of containment during cold shutdown (MODE 5) when the RCS is completely intact and how these assumptions will be met (e.g., TS, administrative controls). This explanation should include the status of the equipment and personnel hatches, penetrations for operating systems, and temporary instrument and electrical penetrations. This explanation should also describe the operator's ability to close containment should a core damage event occur.

19-31

Please document in the status of containment during cold shutdown (MODE 5) up to when the refueling cavity is flooded with an open RCS (mid-loop operation is a subset of this phase of

shutdown) and how these assumptions will be met (e.g., TS, administrative controls). This explanation should include the status of the equipment and personnel hatches, penetrations for operating systems, and temporary electrical and instrument penetrations. This explanation should also describe the operator's ability to close containment before steaming through an open RCS makes containment conditions intolerable to the operator.

19-32

Please identify the probabilities assumed for containment isolation during all phases of MODE 5.

19-33

Please provide a complete electrical dependency matrix including all major accident mitigating systems to supplement Figure 19.1-3. This figure does not include, for example, electrical dependencies of the severe accident heat removal system (SAHRS).

19-34

The list of major modeling assumptions in Section 19.1.4.1.2.5 states that breaks are always assumed to occur in Train 4. However, the large break loss-of-coolant analysis in Chapter 15 appears to assume that the break occurs in Train 3 (see Table 15.6-8). Please discuss whether this difference in assumptions has any impact on the PRA results and insights.

19-35

Please describe how the treatment of induced steam generator tube ruptures, as described on page 19.1-22, considers the potential for multiple tube ruptures.

19-36

Please clarify whether the loss of a single switchgear, said on page 19.1-23 to "bound electrical failures," bounds alternating current (ac) failures only or both ac and direct current (dc) failures. If only ac failures are bounded, please discuss how the risk from dc bus failures is addressed, given that Table 19.1-3 states that the loss of a vital dc bus is not modeled.

19-37

Please clarify why HVAC recovery times "are expected to be site-specific," as stated on page 19.1-23, rather than design-specific. For example, are different procedures, training, or plant layouts expected among sites?

19-38

COL information item 19.1-9 states that the COL applicant must confirm that assumptions used in the PRA remain valid. Several areas for which the modeling is not complete or for which assumptions have been made (such as HVAC recovery times, instrumentation and controls (I&C) details, calibration errors, station blackout human errors, CVCS supply availability, and cooldown operator actions) are in different locations in Chapter 19. Please describe the strategy for

communicating these assumptions to the COL applicants (e.g., collection of all assumptions in a single area in the PRA documentation).

19-39

Please provide additional information on the EFW pressure boundary conditions (EFW PBF) top event. The event tree success criterion is that four of four EFW storage pools maintain integrity, but Chapter 10 and TS appear to indicate that three pools or a minimum of 300,000 gallons are necessary for success.

19-40

Please provide additional detail on the "high-level review" for inter-system common-cause failures, as stated on page 19.1-41. Are there any cases in which the same parts (such as valves or pumps) are expected to be used in different systems? If so, how is the potential for common manufacturing defects or other common-cause failures removed?

19-41

Please provide additional information on the full-load-rejection capability of the U.S. EPR and the planned actions following a LOOP. Page 19.1-12 states that the "design includes the capability to withstand a full load rejection without tripping the reactor" and that the design reduces "the potential for reactor trip and challenge to onsite emergency power systems for grid-centered [LOOP] events." However, page 19.1-23 states that a LOOP event results in a unit trip and affects mitigation response by placing demands on the onsite power system. If the LOOP event includes only events for which a reactor trip must occur, please discuss how the LOOP frequency was modified to account for this condition and how full-load rejection and a subsequent partial trip (as discussed on page 7.7-12) is modeled.

19-42

Please clarify the first bullet on page 19.1-57 on the difference in modeling CCW and ESW losses between the system fault trees and the initiating event models. Why was a loss of a CCW train assumed to cause a loss of the corresponding ESW train in the initiating events model?

19-43

Please provide additional information on what types of electrical interdependencies between HVAC divisions may not be included in the model, as mentioned on page 19.1 57. What effect is this omission expected to have on the overall risk insights and conclusions?

19-44

Please clarify the statement on page 19.1-58 that "some simplifying assumptions are used for the inter-dependent support systems." Does this statement refer to the removal of circular logic, or have additional assumptions been made? What is the overall effect on the risk insights and conclusions?

19-45

Please clarify the statement on page 19.1-58 that an electrical realignment of the main steam relief isolation valves (MSRIVs) would cause a 16 percent improvement in the CDF. Table 19.1-15 appears to indicate a 7% decrease in CDF for this case. Additionally, please discuss other design changes that were considered to potentially improve risk; this MSRIV change appears to be the only change included in Table 19.1-15.

19-46

Please provide additional detail on the modeling uncertainty cases discussed on page 19.1-59 and 19.1-60. How was the probability of each success criterion derived? How is the subsequent weighted average modeled?

Table RAI-19-1. Treatment of Shutdown Design Features in the U.S. EPR

Design Feature Identified in Section 5.4.7.2.1	Apparent Treatment in Technical Specifications
Inherent redundancy in the design of the four trains safety-related U.S. EPR safety injection system (SIS)/RHRS, with each train having separate RCS connections.	• LCO 3.4.6, 3.4.7, and 3.4.8 address operability of two or three trains of RHR in MODES 4 and 5 • MHSI, in-containment refueling water storage tank (IRWST), CCW, ESW, safeguard building controlled area ventilation system (SBVS), and safeguard building ventilation system electrical division (SBVSED) are only required to be operable in MODES 1-4 per LCO 3.5.3, 3.5.4, 3.7.7, 3.7.8, 3.7.12, and 3.7.13.
Automatic stop of the LHSI [low head safety injection] pumps in RHR mode in the event of a low loop level or low delta-Psat (difference between the RCS hot leg temperature and the RCS hot leg saturation temperature).	• No reference to either signal or to an RHR pump trip caused by either signal could be found in Table 3.3.1-1 of LCO 3.3.1.
Manual opening and closure of the RHR suction isolation valves (in addition of interlocks) prevent unwanted RHR connection or isolation on irregular RCS pressure.	• LCO 3.3.1 requires the inputs to the P14 permissive (wide range hot leg temperature and pressure) in MODE 3, which includes the pressure-temperature condition at which P14 is satisfied.
Safety injection via MHSI with reduced discharge head during low loop level ensures availability of the LHSI pumps for RHR function.	• LCO 3.3.1, Table 3.3.1-1, requires SI manual actuation only in MODES 1-4, does not require an engineered safety features actuation system (ESFAS) signal based on low loop level in any MODE, and does not require a sensor for RCS loop level. • LCO 3.4.11 requires that miniflow lines be open for any MHSI pump capable of injecting into the RCS in MODE 4 (when pressure is less than the low temperature overpressure (LTOP) arming temperature), MODE 5, and MODE 6 (when the reactor vessel head is on).
The RHR connection will be automatically isolated in the event of a break outside of the containment, based on the safeguard building sump level and pressure sensors.	• Section 9.3.3 on equipment and floor drains mentions double sump level measurement in the safeguard buildings, but no indication of a sump level signal or automatic RHR isolation could be found in TS or elsewhere in the FSAR.
Spring-loaded safety relief valve, located at the RHR hot leg suction line, protects the SIS/RHRS against over-pressurization when in RHR mode.	• LCO 3.4.11 does not require RHR suction relief valves as an alternative to pressurizer safety relief valves or an RCS vent.
Redundant hot leg level sensors that initiate RCS make-up when the RCS hot leg has reached low level.	• LCO 3.3.1, Table 3.3.1-1, does not require a sensor for RCS loop level.
During mid-loop operation, the RCS loop level is controlled by the CVCS low pressure reducing valve to ensure there is sufficient RCS water inventory for operation of the LHSI pumps in RHR mode.	• Section 7.7.2.3.13 describes RCS loop level limitation, which is classified as a “control system not important to safety” and is not referred to in either TS or Tier 1.
The reactor pressure vessel (RPV) water level is continually monitored during outage with a level sensor.	• LCO 3.3.1, Table 3.3.1-1, does not require a sensor for RPV water level. • Section 7.1.1.5.7 indicates that the RPV level measurement system uses three temperature sensors at different heights in the hot leg. However, LCO 3.3.1, Table 3.3.1-1, requires hot leg temperature sensors only in MODES 1-3. Cold leg temperature sensors are required in MODES 1-6.
Temperature sensors, located at the RCS hot legs, allow temperature measurement of each hot leg when in a reduced inventory condition.	• LCO 3.3.1, Table 3.3.1-1, requires hot leg temperature sensors only in MODES 1-3. Cold leg temperature sensors are required in MODES 1-6.