

Response to

Request for Additional Information No. 26, Revision 1

7/16/2008

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: FSAR Ch. 19

SPLA Branch

Question 19-162

Diversity assumptions for the station blackout diesel generators (SBODG) and the emergency diesel generators (EDG) are stated differently in various sections of the FSAR. For example:

- Table 19.1-102 states that “the SBODGs are diverse from the EDGs in design, manufacturer, cooling, actuation and control, fuel oil and operating environment.”
- Section 8.4.1.1 states that “[t]he SBODGs do not share control power, heating, ventilation and air conditioning (HVAC), engine cooling, or fuel systems with the EDGs.” The section goes on to state that “[t]o minimize the potential for common cause failure with the onsite emergency alternating current power sources, the SBODGs are of a different model than the EDGs.”
- Section 2.5 of Tier 1 states that “[t]he SBODG air start system is independent of the [EDG] air start system.” An ITAAC is provided to verify this statement after construction.

The staff needs further information to conclude that separation of the SBODGs and EDGs into different common cause groups and correlation classes is an appropriate assumption in the probabilistic risk assessment (PRA). For each major subsystem (e.g., starting, control power for startup, fuel, lubrication, cooling, combustion air, exhaust, emission control, and ventilation), provide an engineering assessment of the diversity between the SBODGs and the EDGs and/or how the potential for common cause failures (CCF) is limited. If information on the two models is not yet available and assumptions are necessary, provide specific combined license (COL) items and/or inspections, tests, analyses, and acceptance criteria (ITAAC) in the Final Safety Analysis Report (FSAR) so that these assumptions will be verified in the as-to-be-built, as-to-be-operated plant. Additionally, revise the FSAR so that the diversity discussions in chapters 8 and 19 are consistent.

Response to Question 19-162:

As discussed in the response to NRC RAI No. 11, Question 08.04-3,¹ due to the large difference in nominal size between the SBODG and the EDG, the two types of diesel generator will be different models. As noted in U.S. EPR FSAR Tier 2 Section 8.4.1.1, the two types of diesel generators are located in separate areas, and do not share control power, HVAC, engine cooling, or fuel systems. For example, the cooling system for the emergency diesel generators, transfers heat through a water-to-water heat exchanger, while the corresponding system for the station blackout diesel generators transfers heat by a water-to-air radiator. There are no single active failures that can simultaneously disable the station blackout and emergency diesel generators.

Specific diesel generator models have not yet been selected; therefore, comparing specific engines, generators, or support system components is not currently possible. However, the differences in size, location, and support systems minimize the probability of common mode failures.

The diesel generator diversity discussions in U.S. EPR Tier 2 Chapter 19 will be revised to be consistent with U.S. EPR Tier 2 Chapter 8. A revision to U.S. EPR FSAR Tier 2 Table 19-102 will be provided in AREVA NP’s response to RAI No. 26 Questions 19-166 and 19-167.

¹ See e-mail from Ronda Pederson (AREVA NP Inc) to Getachew Tesfaye (NRC), “Response to U.S. EPR Design Certification Application RAI No. 11, FSAR Ch. 8” dated June 20, 2008.

FSAR Impact:

U.S. EPR FSAR Tier 2 Sections 19.1.3.1.2, 19.1.3.4.1, 19.1.4.1.1.3, and 19.1.4.1.2.5 will be revised as described in the response and indicated in the enclosed markup.

Question 19-163

(Follow-up to Question 19-71) The response to Question 19-71 states that the process information and control system (PICS) and the safety information and control system (SICS) are implemented on diverse I&C platforms and are not vulnerable to the same CCF. Provide the results of a sensitivity study in which PICS and SICS can fail due to a common cause. Also, include this assumption as an insight in Table 19.1-102 of the FSAR.

Response to Question 19-163:

A sensitivity case is defined in which PICS and SICS are assumed to be vulnerable to a common cause failure (CCF). If such a CCF occurred, the operators could lose plant status indication on the displays in the Main Control Room (MCR) and Remote Shutdown Station (RSS), as well as the ability to perform any actions on these systems from those locations.

This sensitivity case is modeled by adding to the probabilistic risk assessment (PRA) model a PICS/SICS CCF undeveloped event that would fail all operator actions. The probability for this event is set to 1.0E-05, which is consistent with the value used in the PRA model for software CCFs with no credit given for recovery.

The results of the sensitivity case (see Table RAI 19-163-1) show an increase in core damage frequency (CDF) of less than one percent.

The assumption that the PICS and the SICS are not vulnerable to CCF is based on the diversity of the PICS and the SICS instrumentation and controls (I&C) platforms that are described in U.S EPR FSAR Tier 2 Section 7.1 and the U.S. EPR Instrumentation and Control Diversity and Defense-in-Depth Methodology Topical Report (ANP-10284, see U.S EPR FSAR Tier 2 Table 1.6-1). A revision to U.S EPR FSAR Tier 2 Table 19.1-102 to reflect this assumption will be provided in AREVA NP’s response to RAI No. 26 Questions 19-166 and 19-167.

Table RAI 19-163-1—Sensitivity Case Results for Modeling CCF of PICS and SICS

Risk Measure	Base Case	Sensitivity Case	Change in CDF
Total CDF (internal events, fire, and flood; per year)	5.26E-07	5.27E-07	+0.2%

FSAR Impact:

The U.S. EPR FSAR will not be changed as a result of this question.

Question 19-164

(Follow-up to Question 19-58) Clarify how the PRA models cooling of the reactor coolant pumps (RCP) by the component cooling water system (CCWS) common headers (CH). The response to Question 19-58 indicates that CH1 cools RCPs 1 and 2, while CH2 cools RCPs 3 and 4. However, Section 7.6.1.2.3 states that “[e]ither the Common 1b or 2b headers can provide cooling to the RCP thermal barriers.” How is the crosstie between CH1 and CH2 controlled? How many RCPs trip on the loss of a CCWS CH? How many RCPs must trip to cause a reactor trip?

Response to Question 19-164

A response to this question will be provided by September 30, 2008.

Question 19-165

(Follow-up to Question 19-43) Clarify how electrical dependencies are modeled in the “circular logic equivalent” fault trees in the PRA. Section 19.1.4.1.2.5 of the FSAR and the response to Question 19-43 indicate that the failure of power supplies is not modeled as a failure mode of HVAC, CCWS, and the essential service water system (ESWS). Compare the probability that an electrical bus fails to other failure modes modeled for these systems. Is power to these systems modeled as a zero-probability basic event or as an undeveloped event with a probability derived from the fault tree for that power supply? If the former approach was used, provide the results of a sensitivity study using the latter approach.

Response to Question 19-165

Failures of power supplies are not modeled in the circular logic equivalent fault trees that are used in the probabilistic risk assessment (PRA) heating, ventilation, and air conditioning (HVAC) model to represent the component cooling water system (CCWS) and ESWS. Rather, the power supplies are represented by zero-probability undeveloped basic events. Due to the high reliability of the power supplies, this is a reasonable approach to a circular logic problem (i.e., the function of these power supplies is to support HVAC which support the electrical system).

A sensitivity case is evaluated by replacing the power supply’s zero-probability basic events by unavailability values calculated from the corresponding fault trees. The unavailability of electrical buses, as calculated from their Risk Spectrum fault trees, are shown in Table RAI 19-165-1. Division 1 and 2 buses are shown in the table; the results for Division 3 and 4 are the same as Division 2 and 1, respectively.

The results of the sensitivity case are shown in Table RAI 19-165-2. An increase in core damage frequency (CDF) of one percent occurs if the zero-probability undeveloped events are replaced by the quantified values for the power supplies.

For the trains identified in the question (i.e., CCWS, HVAC, and ESWS), Table RAI 19-165-3 compares the train unavailabilities without power supplies, and the corresponding power supply unavailabilities. This comparison shows that an independent failure of the power supply is not always negligible, compared to the other causes of train unavailability. However, the combined error made by omitting these power supplies is small, as shown in the sensitivity case results discussed above.

Table RAI 19-165-1 Electrical Buses Unavailabilities for Division 1 and Division 2

Electrical Bus	Mean Unavailability
Division 1	
31BDA	2.8E-05
31BDB	6.7E-05
31BDD	6.6E-05
31BMD	1.3E-04
31BNB01	1.6E-04
31BNB02	1.9E-04
31BNB03	2.3E-04
31BRA	3.1E-05
Division 2	
32BDA	3.1E-05
32BDD	6.9E-05
32BMD	1.3E-04
32BNB01	1.4E-04
32BNB02	1.7E-04

Table RAI 19-165-2 Sensitivity Case Results for Replacing Zero-Probability Undeveloped Events for Power Supplies with Quantified Unavailabilities

Risk Measure	Base Case	Sensitivity Case	Change in CDF
Total CDF (internal events, fire, and flood; per year)	5.26E-07	5.30E-07	+1%

Table RAI 19-165-3 Comparison between Selected Train Unavailabilities without Power Supplies and the Corresponding Power Supply Unavailabilities

Train	Train Unavailability w/o Power Supplies	Corresponding Power Supply	Power Supply Unavailability
CCW Train 1	3.3E-04	31BDA	2.8E-05
HVAC Train 1	4.1E-04	31BDB	6.7E-05
ESW Train 1	1.5E-04	31BDD	6.6E-05

FSAR Impact:

The U.S. EPR FSAR will not be changed as a result of this question.

Question 19-166

(Follow-up to Question 19-2) The disposition of risk insights added to Table 19.1-102 in response to Question 19-2 is helpful for both staff review and future use of the FSAR. However, the insights should be tied to the portion of the FSAR that provides the strongest assurance that the insight will remain valid in the as-to-be-built, as-to-be-operated plant. In many cases, the revised Table 19.1-102 refers to a portion of FSAR Tier 2 when the insight is also addressed in Tier 1 system descriptions; specific ITAAC; or a specific COL information item. Revise Table 19.1-102 in the FSAR to refer to Tier 1, ITAAC, and COL items where applicable.

Response to Question 19-166

A response to this question will be provided by October 31, 2008.

Question 19-167

(Follow-up to Question 19-38) The response to Question 19-38 states that the communication of assumptions to COL applicants is achieved by FSAR Table 19.1-102 and actions related to COL items. To ensure that these mechanisms are as useful as possible to COL applicants and the staff, revise Table 19.1-102 to include all key assumptions identified in the PRA documentation (such as in system analyses) and all assumptions alluded to in the FSAR text. For example, the following assumptions are in the FSAR text but not in the table:

- Heating, ventilation, and air conditioning (HVAC) recovery times (see FSAR page 19.1-23)
- Instrumentation and controls (I&C) details (see FSAR page 19.1-32)
- Calibration errors (see FSAR page 19.1-42)
- Additional training for certain evolutions (see FSAR page 19.1-44)
- Station blackout human errors (see FSAR page 19.1-56)
- Chemical and volume control system (CVCS) supply availability (see FSAR page 19.1-56)
- Cooldown operator actions (see FSAR page 19.1-57)

Also, revise the text of COL information item 19.1-9 to add a reference to the insights and assumptions listed in Table 19.1-102.

Response to Question 19-167

A response to this question will be provided by October 31, 2008.

Question 19-168

(Follow-up to Question 19-59) Question 19-59 asked for additional information on the pressurizer safety relief valve (PSRV) spurious opening frequency indicated in FSAR Table 19.1-4. The staff needs further information in several areas. Note that if the approach is changed in response to sub-part (a), responses to (b) and (c) are not needed.

- a. The response appears to discuss failures of safety valves to reseal after opening during a transient, rather than spurious opening while at power. It is unclear how this frequency addresses both spurious opening of a PSRV and its subsequent failure to reseal. It is also unclear how the frequency accounts for all three PSRVs. Discuss how the PSRV spurious opening frequency modeled in the PRA addresses both of these subjects.
- b. Provide additional information to support the conclusion that transients such as loss of an electrical bus or a turbine trip would not result in PSRV opening. The safety analyses in Chapter 15 indicate that the PSRVs open in many scenarios, including after a turbine trip.
- c. Justify the use of 0.1 failure events over 500 reactor critical years. The value of $5.0E-3$ /yr listed in NUREG/CR-5750 results from an analysis of two failures over approximately 500 reactor critical years. The update in NUREG/CR-6928 also uses the two failures, but over 866.6 reactor critical years, and uses a simplified constrained non-informative (SCNI) prior distribution with the Jeffreys mean and an alpha value of 0.5. The resulting mean value is $2.88E-3$ /yr with alpha and beta values of 0.5 and 173.3, respectively. Even if the approach of excluding the two failures as not applicable to the U.S. EPR were appropriate, a similarly updated gamma distribution would be $5.8E-4$ /yr with alpha and beta values of 0.5 and 866.6, respectively.

Response to Question 19-168

- a. U.S. EPR FSAR Tier 2 Table 19.1-4 incorrectly lists the $2E-4$ contribution as pertaining to spurious PSRV operation (this frequency accounts for one or more PSRVs). This contribution is actually from failure of safety valves to reseal after opening during a transient, which is discussed in the response to NRC RAI No. 7, Question 19-59². U.S. EPR FSAR Tier 2 Table 19.1-4 will be revised accordingly.

A spurious opening of a PSRV is unlikely since it has two solenoid-operated pilot valves in series, and each one is powered from a different power supply. This prevents spurious opening of the valve at lower pressures. During normal operations, the valve setpoint is approximately 300 psi higher than the operating pressure of the plant and the valve is medium operated (operated by the system fluid and pressure) during these conditions.

- b. The frequency of $2E-4$ for failure of safety valves to reseal after opening during a transient takes credit for design improvements in the U.S. EPR that reduce the likelihood that a turbine trip or loss of an AC bus would challenge the PSRVs. (The credit assumes 0.1 events, rather than the two events that have occurred.) The frequency also takes credit for

² See e-mail from Ronda Pederson (AREVA NP Inc) to Getachew Tesfaye (NRC), "RE: U.S. EPR Design Certification Application RAI No. 7" dated June 16, 2008.

design improvements that reduce the probability that a safety valve would fail to reseal after one of these transients. These improvements include:

- A relatively large pressurizer.
- Water seals to prevent steam and noncondensable gases from leaking past the PSRV seats.
- The PSRV is designed to avoid unnecessary cavities where particles suspended in the process fluid can settle and collect.
- The PSRV is qualified to operate in saturated steam, water, and any steam/water mixture in hot or cold conditions.
- The PSRV clearances within the valve allow it to function under all modes of operation at the specified temperatures.

In the U.S. EPR FSAR Tier 2 Chapter 15 analyses, the turbine trip is the limiting transient event for the PSRV design (i.e., a turbine trip causes the PSRVs to lift). However, this deterministic analysis is conservative since it takes no credit for pressurizer spray, partial trip, or turbine bypass. Furthermore this analysis assumes that five percent of the steam generator tubes are plugged and it assumes a loss of offsite power occurs 0.41 seconds after the reactor trip signal is generated from high pressurizer pressure.

- c. The use of 0.1 failure events over 500 reactor critical years for one or more PSRVs failing to reseal is based on data in NUREG/CR-5750. These data show two failure events over 500 reactor critical years. As discussed in the response to part b of this question, these two events would not cause a PSRV failure to reseal. The first failure was counted as one-tenth of an event, or 0.1 failure events. The leak rate for the second event was smaller than the capacity of one U.S. EPR charging pump and does not constitute a challenge to the U.S. EPR shutdown capability. This failure was not counted as a failure event for the U.S. EPR.

The use of $5.8E-04/\text{yr}$ as a mean value would be appropriate to represent zero events in 866.6 reactor critical years, if the PSRV failure to reseal was treated as a separate initiating event. However, this would produce overly conservative results for the U.S. EPR PRA because the PSRV failure to reseal is added to the small break loss of coolant accident (SBLOCA) initiating event frequency, and the alpha value of 0.5 (as described in the question) would be counted twice. The SBLOCA frequency data from NUREG/CR-6928 includes the simplified constrained noninformative (SCNI) prior distribution alpha of 0.5. To add the PSRV failure-to-reseat data to the SBLOCA frequency requires adding 0.1 to the SBLOCA alpha value, rather than $(0.5 + 0.1)$. Therefore, using 0.1 failure events over 500 reactor critical years is justified.

FSAR Impact:

U.S. EPR FSAR Tier 2 Table 19.1-4 will be revised as described in the response and indicated on the enclosed markup.

Question 19-169

(Follow-up to Question 19-62) The response to Question 19-62 indicates that no single ventilation failure would result in the loss of more than one building and that support system failures would fail the front-line system as well as ventilation. However, the response does not address the impact of individual ventilation component failures (e.g., failure of a ventilation fan in an SBODG building) on equipment in that building. Provide a quantitative justification for exclusion of these ventilation failures, with reference to failure probabilities, room heat-up assumptions, and operator actions that are possible.

Response to Question 19-169

The response to NRC RAI No.7, Question 19-62³ indicates that no significant dependency had been overlooked by not modeling heating, ventilation, and air conditioning (HVAC) systems outside of the Safeguard Buildings. Detailed design information for most of the systems discussed in the response to Question 19-62 is not available, with the exception of the HVAC for the Emergency Power Generation Building (EPGB) and the Essential Service Water (ESW) Pump Building.

The design of these two systems includes four identical chiller unit trains. The EPGB HVAC also includes two supply and two exhaust fans. The approximate unavailability of these HVAC systems can be estimated based on the following data:

- Chiller failure to run over 24-hour mission time: 7E-04.
- Fan failure to run over 24-hour mission time: 4E-04.
- Human recovery action (opening doors if possible, using portable fans) with a human error probability (HEP) of 1.E-02.

Based on the above values, the average HVAC train unavailability is estimated at $2.3E-05 (7E-04 + (4 \times 4E-04)) \times 1E-02$.

This value is small compared to the dominant failure modes of the systems in these buildings:

- Diesel generator failure to run over 24-hour mission time: 3E-02
- ESW pump failure to run over 24-hour mission time: 1E-04

Thus, an HVAC failure would not be a significant contributor to the overall unavailability of these two systems. A similar conclusion would apply for the other HVAC systems outside of the Safeguard Buildings.

FSAR Impact:

The U.S. EPR FSAR will not be changed as a result of this question.

³ See e-mail from Ronda Pederson (AREVA NP Inc) to Getachew Tesfaye (NRC), "RE: U.S. EPR Design Certification Application RAI No. 7" dated June 16, 2008.

Question 19-170

(Follow-up to Question 19-63) The response to Question 19-63 states that the alternate feed connection is credited in some cases as a response to loss of power. The bases for technical specification (TS) 3.8.1 state that “[i]f one EDG is inoperable and the alternate feed is not aligned, certain required safety systems, safety support systems, and components that do not have adequate redundancy to support maintenance, do not have sufficient AC power source availability to ensure the completion of all safety functions for a postulated accident coincident with a single failure and the loss of offsite power.” Provide a quantitative discussion of the risk benefit of the alternate feed connection when an EDG is out of service for maintenance. If the benefit is large, the connection should be modeled in the PRA and included as a risk insight in Table 19.1-102 of the FSAR.

Response to Question 19-170

A sensitivity case is defined to evaluate the risk benefit of the alternate feed connection when an emergency diesel generator (EDG) is out of service. The base case is defined with the Division 4 EDG in preventive maintenance with no alternate feed. The sensitivity case is defined as the base case with the alternate feed configuration established (i.e., the 6.9 kV switchgear 34 BDB is fed from switchgear 33 BDA instead of switchgear 34 BDC).

The PRA model used for both the base case and the sensitivity case was updated to include a design change that was not implemented in the probabilistic risk assessment (PRA) model (see item 5 in U.S. EPR FSAR Tier 2 Section 19.1.2.4). Specifically, this design change allows for a direct connection of the station blackout (SBO)-backed buses 31/32 BBH to Division 2, and Division 3 buses 32/33 BDB. As a result of this change, the PRA-modeled operator action to establish cross ties and provide SBO-backed power to Division 2 and 3 is removed from the model. This design change is incorporated because it relates to the current electrical connection and therefore affects potential insights from the alternate feed configuration.

The results of these sensitivity cases are shown in Table RAI 19-170-1. These results reflect a core damage frequency (CDF) improvement of four percent due to the alternate feed configuration, if one EDG (Train 4) is assumed to be in preventive maintenance (PM) for all year. For the EDG maintenance duration of just over two weeks per year assumed in the PRA model, a corresponding improvement in the CDF will be negligible. Therefore, the comparison between the base case (no alternate feed) and the sensitivity case (alternate feed in place), when scaled down to an actual time period during a year when one of EDGs will be out for maintenance, shows that there is a less than one percent decrease in the risk if the alternate feed configuration is in place.

Table RAI 19-170-1—Sensitivity Case Results at Power – Without (Base Case) and With (Sensitivity Case) the Alternate Feed Configuration when EDG Train 4 is Out for Maintenance

Risk Measure	Base Case	Sensitivity Case	Change in CDF
Total CDF (internal, fire, and flood, per year) with EDG Train 4 in PM for all year	4.9E-7	4.7E-7	-4%

FSAR Impact:

The U.S. EPR FSAR will not be changed as a result of this question.

Question 19-171

(Follow-up to Question 19-66) The response to Question 19-66 indicates that pipe break frequencies based on the number of pipe segments and the Electric Power Research Institute (EPRI) TR-102266 Pipe Break Failure Study may be much lower than the initiating event frequencies assumed in the PRA. Has the number of reactor coolant system (RCS) and steam line pipe segments been reduced significantly for the U.S. EPR design compared to operating plants? If so, discuss how using generic initiating event frequencies affect the U.S. EPR risk profile and associated risk insights.

Response to Question 19-171

The response to NRC RAI No. 7, Question 19-66⁴ does not indicate that the number of RCS and steam line pipe segments has been reduced for the U.S. EPR. The reference to a small number of segments (“only four”) refers to a small number of steam line segments inside containment. The comparison with the segments failure frequency is presented to illustrate the possibility that a generic frequency for a steam line break inside containment may be conservative, even without crediting improvements in the piping materials for the advanced plants.

FSAR Impact:

The U.S. EPR FSAR will not be changed as a result of this question.

⁴ See e-mail from Ronda Pederson (AREVA NP Inc) to Getachew Tesfaye (NRC), “RE: U.S. EPR Design Certification Application RAI No. 7” dated June 16, 2008.

Question 19-172

(Follow-up to Question 19-17) The response to Question 19-17 states that loss-of-offsite-power (LOOP) events recovered in less than one hour are not considered in the analysis. Provide justification for this assumption. Do any LOOP-initiated loss-of-residual-heat-removal (RHR) scenarios result in boiling in the RCS in less than an hour? If so, describe the scenario and provide a description and results of the time-to-boil calculation. Describe procedures and training related to closure of the equipment hatch and other containment penetrations without offsite power. State how long containment closure is expected to take both with and without offsite power.

Response to Question 19-172

LOOP-initiated loss-of-residual-heat-removal (RHR) scenarios in plant operating state (POS) D (midloop) would result in boiling in the reactor coolant system (RCS) in less than one hour (27 minutes in POS Dd and 37 minutes in POS Du). This allows the operators sufficient time to recover RHR. The input parameters and the time to boil are discussed in the response to NRC RAI No. 14, Question 19-133 (see Table 19-133-1)⁵. However, if the RHR recovery fails, operators can recover core cooling by initiating a feed and bleed action. The time used for this action is the time to uncover the core (or the active fuel), which is much longer in both of these POS (146 minutes in POS Dd, and 203 minutes in POS Du). The one hour used for a LOOP recovery is based on the time-to-top-of-active-fuel.

If time-to-boil was used as a base for the LOOP recovery time line, and a recovery in one half-hour is used, the LOOP (in 24 hours) basic event value would change from 2.2E-4 to 3.3 E-4. A sensitivity case run with the new LOOP recovery value (see Table RAI 19-172-1) shows a moderate increase in the total shutdown CDF (<20%).

The equipment hatch is powered from a bus backed by an emergency diesel generator (EDG). In addition, the hatch is designed with the capability to be closed manually in the event of a complete power loss. The hatch is designed to be closed manually in less than one hour and fully secured in less than two hours.

The containment status in shutdown will be further evaluated in the response to NRC RAI No. 22, Question 19-158⁶. Procedures and training related to closing the equipment hatch and other containment penetrations will be developed by the COL applicant.

⁵ See e-mail from Ronda Pederson (AREVA NP Inc) to Getachew Tesfaye (NRC), "Response to U.S. EPR Design Certification Application RAI No. 14, FSAR Ch 19" dated July 11, 2008.

⁶ See e-mail from Ronda Pederson (AREVA NP Inc) to Getachew Tesfaye (NRC), "Response to U.S. EPR Design Certification Application RAI No. 22, FSAR Ch. 19" dated July 31, 2008.

**Table RAI 19-172-1—Sensitivity Case Results in Shutdown - for the LOOP Recovery
Change from One Hour (Base Case) to One Half Hour (Sensitivity Case)**

	Base Case	Sensitivity Case	Change in CDF
Shutdown CDF (one per year)	5.8E-8	6.8E-8	17.2%

FSAR Impact:

The U.S. EPR FSAR will not be changed as a result of this question.

Question 19-173

(Follow-up to Question 19-32) The response to Question 19-32 states that “containment availability as modeled in the PRA is based on administrative controls” and that “the shutdown PRA uses the same model for containment status as the at power PRA.” Assumptions about containment closure are critical to the assessment of radioactive release during shutdown. Revise Table 19.1-87 for all plant operating states (POS) to include the status of the equipment hatch, personnel airlock, and other permanent and temporary containment penetrations (e.g., open, closed, or an assumed probability of failure following a severe accident during shutdown), and include these assumptions as a risk insight in Table 19.1-102.

Response to Question 19-173

U.S. EPR FSAR Tier 2, Chapter 16, Technical Specification (TS) 3.9.3, Containment Penetrations, addresses the required penetration configuration during the handling of recently irradiated fuel assemblies within containment. This TS permits the equipment hatch and personnel air locks to be open and the penetrations to be under manual control. The term “recently irradiated fuel” is defined as fuel that has been part of a critical reactor core and has decayed for less than 34 hours. Since the time required to cool down from a reactor subcritical state to 131°F for head stud de-tensioning is approximately 34 hours, and additional time is needed to de-tension the reactor vessel head, remove the head, upper internals and components, and fill the pool, handling recently irradiated fuel is not expected to occur.

The containment status was not analyzed in the U.S. EPR FSAR Tier 2 Section 19 because shutdown Level 2 analysis was not performed. Rather, a bounding analysis was used based on the at-power Level 2 results. This bounding analysis will be updated and the containment status in shutdown will be further evaluated in the response to Question 19-158, including a revision to U.S. EPR FSAR Tier 2 Table 19.1-87 and Table 19.1-102.

FSAR Impact:

The U.S. EPR FSAR will not be changed as a result of this question.

Question 19-174

(Follow-up to Question 19-22 and 19-26) Section 6.7 of NUREG-1449 describes instances in which the failure of temporary RCS boundaries (such as freeze seal, which is used to temporarily isolate fluid systems, temporary plugs for neutron instrument housing, and nozzle dams installed in the hot-leg and cold-leg penetrations to steam generators) can lead to a rapid non-isolable loss of reactor coolant. Therefore, the decision to use these temporary boundaries is an important component of the U.S. EPR shutdown risk assessment. (See section 19.3.3 of NUREG-1512, the Final Safety Evaluation Report (FSER) on the AP600 design, for a previous discussion of this topic.) In response to Questions 19-22 and 19-26, AREVA stated that the use of nozzle dams and temporary pressure boundaries, respectively, will be decided by the COL applicant. Postponing this decision means that the shutdown risk assessment is not complete enough for the staff to develop risk insights. Provide the following additional information:

- a. Are nozzle dams used in the U.S. EPR steam generators at shutdown?
- b. At what point during shutdown will the nozzle dams be installed and removed?
- c. What is the design pressure of these nozzle dams? Discuss the analysis performed to calculate this pressure. Compare this pressure to the pressure expected following a loss of RHR in all POS.
- d. How are nozzle dams and their impact on steam generator availability modeled in the PRA?
- e. Are freeze seals used during shutdown? If so, revise the FSAR to include a COL item for applicants to develop plant-specific guidelines that would reduce the potential for loss of RCS boundary and inventory when using freeze seals.
- f. Will any other temporary pressure boundaries, such as plugs in neutron instrument housings, be used?

Response to Question 19-174

A response to this question will be provided by September 30, 2008.

Question 19-175

(Follow-up to Question 19-74) The response to Question 19-74 is not complete enough for the staff to understand the U.S. EPR shutdown strategy. Describe the approach taken (e.g., tasks performed, systems and equipment used) for each of the following steps:

- a. Depressurization before draining the RCS
- b. Reduction of RCS level to mid-loop
- c. Draining the steam generator tubes (e.g., whether nitrogen is injected to speed draining)
- d. Level control during mid-loop
- e. Draining the refueling cavity after refueling
- f. Vacuum fill of the RCS

Response to Question 19-175

- a. After the reactor coolant system (RCS) is cooled, the pressurizer (PZR) level is increased to approximately 90%, and pressure control is shifted from the PZR steam space to the chemical and volume control system (CVCS) high pressure (HP) reducing station. The residual steam bubble above the PZR spray nozzles is vented through the degas line to the nuclear island drain and vent system (NIDVS). One safety injection system (SIS) accumulator will have its nitrogen pressure reduced to 320 psia and will be connected to the RCS. The SI accumulator is used to prevent an inadvertent de-pressurization of the RCS below the requirements for the reactor coolant pump (RCP) 1 seal. RCS spray lines from the RCS loops are opened in order to cool the upper portion of the PZR.

The PZR pressure is approximately 390 psia and PZR water temperature at the end of the PZR cooldown is approximately 160°F. When cooldown is complete, pressure control is transferred from the CVCS HP reducing station to the CVCS low pressure (LP) reducing station (from residual heat removal), and the RCPs are secured. The SI accumulator is isolated and depressurized. Nitrogen gas is lined up to the PZR and the regulator is set for atmospheric pressure (to prevent drawing a vacuum in the RCS during draining). RCS pressure is then reduced manually by using the CVCS LP reducing station (from RHR) to atmospheric pressure.

The RCS is drained via the letdown system to the CVCS letdown system storage tanks. As the PZR level is lowered, its pressure will be reduced below atmospheric and this will allow nitrogen to enter the PZR. The RCS level is monitored via the RCS wide range level indicator (from the bottom of hot leg to the top of PZR). The PZR level is initially lowered to the reactor pressure vessel (RPV) flange level.

- b. The PZR level is initially lowered to the RPV flange level. Only the PZR has nitrogen gas. Once conditions have been established for the RCS to enter reduced inventory, the level is lowered to the mid ($\frac{3}{4}$) loop position. When level is reduced below the top of the RCS hot leg the steam generator (SG) tubes will drain and water is allowed to enter the loops. Once the RCS level is stabilized (when SG tube draining is complete), the level control system is placed in the $\frac{3}{4}$ loop level control mode. The nitrogen will pass from the PZR and hot legs to the SG tubes. Once the RCS draining is complete and RCS level is stabilized at the $\frac{3}{4}$ loop level, a nitrogen sweep of the RPV closure head and PZR is performed, followed by an

air sweep to remove the nitrogen. During a mid-cycle SG maintenance shutdown, the RPV vessel head is not removed; RCS level is reduced to the flange level, after conditions have been established to enter reduced inventory the RCS level is reduced to $\frac{3}{4}$ loop level a nitrogen sweep and air purge are performed. After the SG tubes have completed draining the SG manways will be removed and the nozzle dams will be installed, RCS level is then increased above the reduced inventory level. SG inspections and repairs are performed. Once repairs are complete, the RCS level is reduced to $\frac{3}{4}$ loop (with automatic loop level control) and nozzle dams are removed and SG manways are re-installed and the RCS vacuum re-filled.

- c. See the above response to part b of this question. The nitrogen gas is added but it prevents a vacuum from being formed in the PZR and maintains atmospheric pressure during the draining process. It does not apply excess pressure and is not used to speed the draining process.
- d. The automatic mid-loop level control is manually activated during cold shutdown. The control level is 23.6 inches above the bottom of the RCS loop piping (charging pump must be in operation and the volume control tank (VCT) must not be bypassed). The level is maintained ± 2 inches by controlling letdown and there are high and low RCS level alarms to assist the operator. If the RCS loop level decreases below 18.9 inches an SIS pump will recover the level.
- e. Once the reactor is refueled, the cavity level is lowered to just below the RPV flange level, the Reactor Building (RB) cavities (reactor cavity, core internal storage area, and RB transfer compartment) are drained to the in-containment refueling water storage tank (IRWST) via the fuel pool cooling and purification (FPPS) system.
- f. With the RPV head in place, the head bolts are installed, including the SG primary and secondary manways. The RCS level is stable at the $\frac{3}{4}$ loop position. One charging pump is running during the vacuum process and applying a positive pressure to all RCP 1 seals. The NIDVS vacuum pump is aligned to the RPV closure head vent and the PZR. RCS pressure is reduced to 24 inches of Hg. The RCS level is increased to a PZR level of 20 percent by adding borated water through the CVCS charging and seal injection lines from the CVCS or IRWST. When the level approaches the RPV head vent, the vacuum vent line from the RPV is isolated. When the PZR is at the 20 percent level, the vacuum is reduced. As the vacuum reduces, the water level in the PZR also reduces as the water is transferred to the SGs and RPV head. When the RCS is at atmospheric pressure and the PZR water level is stabilized at 20 percent, the fill is complete and the heat-up of the PZR commences.

FSAR Impact:

The U.S. EPR FSAR will not be changed as a result of this question.

Question 19-176

(Follow-up to Question 19-27) The response to Question 19-27 identifies several design features (e.g., safety injection (SI) signal, CVCS letdown isolation, and medium head safety injection) that would increase average shutdown core damage frequency (CDF) to a value comparable to the Commission's safety goals if they were not available during shutdown. Neither the low loop level SI signal nor the medium head safety injection (MHSI) system is required by TS in MODES 5 and 6. The letdown isolation valves are required to be operable by TS 3.1.8, which relates to boron dilution, not loop level. The loop level sensors are used to isolate letdown, stop the low head safety injection (LHSI) pumps, and start makeup with the MHSI pumps on low loop level. Although they were not included in the list of RAW values in response to Question 19-27, Table 19.1-98 indicates that CCF of these sensors is of high importance. The in-containment refueling water storage tank (IRWST) was also not included in this list, but Table 19.1-97 indicates that CCF of the IRWST (because of check valve or strainer failure) is extremely important.

Standard Review Plan (SRP) Section 19.0 states that the design-phase PRA is used to demonstrate whether the plant design, including the impact of site-specific characteristics, represents a reduction in risk compared to existing operating plants. The PRA is also used to identify and support the development of specifications such as ITAAC, reliability assurance program (RAP), TS, and COL items. The staff must be able to make these conclusions in its FSER.

Therefore, as requested in Question 19-27, provide a sensitivity study by specifying guaranteed failure for all operator actions, equipment, and sensors related to systems that are not required to be operable during shutdown. If neither TS nor procedures detailing availability controls are available for the important features discussed above, the staff will need to use the results of this sensitivity study in its safety evaluation.

Response to Question 19-176

A response to this question will be provided by October 31, 2008.

Question 19-177

Provide the assumed contents of the steam generator tubes during all phases of plant shutdown. Will nitrogen be injected in the steam generator tubes to speed draining? If so, how does the nitrogen content impact the steam condensing surface for reflux cooling and any subsequent repressurization?

Response to Question 19-177

From power operation to RCS depressurization, the steam generator (SG) tubes are filled solid with RCS fluid. From RCS depressurization to mid ($\frac{3}{4}$) loop condition, the SG tubes are partially filled with RCS fluid and will have a vacuum due to the reduced reactor coolant system (RCS) level. This condition may exist for 24 to 48 hours as the plant is preparing to enter the reduced inventory phase.

Once at mid ($\frac{3}{4}$) loop, the SG will drain completely and empty the remaining reactor coolant system (RCS) fluid from the SG tubes. A nitrogen sweep is performed on the RCS, in which nitrogen is injected and the vacuum system draws a negative pressure on the reactor pressure vessel (RPV) head vent and the pressurizer (PZR). When the nitrogen sweep is complete, air is introduced to sweep the nitrogen from the RCS.

The SG tubes will have air throughout the refueling process until the RCS is vacuum filled and the tubes reach the second $\frac{3}{4}$ loop condition. At that point most of the SG tubes will be filled with RCS water; however, the top of the SG tubes may not be completely solid; this condition can exist for 24 to 48 hours.

The SG tubes are considered water solid only after the reactor coolant pump (RCP) on the SG loop is started and RCS fluid has fully displaced the air at the top of the tubes.

Nitrogen is not used to speed draining. Rather, it replaces the air in the SG tubes once the SG is drained in order to prevent a vacuum during pressurizer draindown.

FSAR Impact:

The U.S. EPR FSAR will not be changed as a result of this question.

Question 19-178

TS 3.9.5, on RHR with low water level during MODE 6, requires containment closure within four hours whenever no RHR loops are available. The bases for this TS state that “[t]he Completion Time of 4 hours allows fixing of most RHR problems and is reasonable, based on the low probability of the coolant boiling in that time.” Provide descriptions and results of time-to-boil calculations from the shutdown PRA that support this statement.

Response to Question 19-178

A response to this question will be provided by September 30, 2008.

Question 19-179

Discuss any design improvements made to the RCS and RHR system to reduce shutdown risk, such as self-venting suction lines, suction nozzle modifications, or vertically offset hot and cold legs.

Response to Question 19-179

The discussion of design improvements made to the U.S. EPR to reduce shutdown risk is provided in the U.S. EPR FSAR Tier 2 Section 5.4.7.2.1. The low head safety injection (LHSI) pump suction piping from the reactor coolant system (RCS) hot legs to the LHSI pump is designed to be self-venting by either a continuous downward slope or a continuous vent line, which prevent the formation of loop seals (voids) within the piping.

FSAR Impact:

The U.S. EPR FSAR will not be changed as a result of this question.

Question 19-180

Define “mid-loop” for the U.S. EPR. To what elevation will the RCS be drained to allow steam generator maintenance and nozzle dam installation? Provide the location and elevation of the RHR hot leg suction nozzle (e.g., bottom or side of pipe, +X feet).

Response to Question 19-180

The U.S. EPR control level is 23.6 inches in the 31 inch diameter hot leg piping, hence mid-loop is the $\frac{3}{4}$ loop level. Steam generator (SG) maintenance will be performed at $\frac{3}{4}$ loop with no fuel in the vessel. Nozzle dams are discussed in the response to Question 19-174.

The residual heat removal (RHR) suction piping is connected to the bottom of the RCS hot leg piping, and is orientated down (

90 degrees to the RCS pipe). The RHR suction pipe is a 10 inch diameter, schedule 160 pipe, and the entrance of RHR suction nozzle is at elevation 17.22 feet.

FSAR Impact:

The U.S. EPR FSAR will not be changed as a result of this question.

Question 19-181

Discuss the mass or energy input that would cause the low temperature overpressure (LTOP) PSRV to open when the RCS is water-solid during shutdown. Provide the likelihood that the PSRVs will stick open, and discuss how the shutdown PRA handles this scenario.

Response to Question 19-181

The mass or energy inputs that were analyzed to determine their impact on system pressure when the pressurizer is solid are described in FSAR Section 5.2.2.2.2. The inputs are:

- Mass addition due to the charging pumps starting.
- Mass addition due to the medium head safety injection pumps starting.
- Energy addition due to the reactor coolant pumps starting with the steam generator temperature higher than the primary system temperature.

In the U.S. EPR probabilistic risk assessment (PRA) model, a probability of failure to re-close the pressurizer safety relief valves (PSRV) after they open is assumed to be $3E-03$, which is based on generic industry data (U.S. EPR FSAR Tier 2 Section 19.1.9, References 22, 23, and 24). The PSRVs are designed to reduce the likelihood that they will fail to re-close. For example, the specifications for this valve states that it will be designed to avoid unnecessary cavities where particles suspended in the process fluid can settle or collect. Also, the PSRVs are designed to operate in saturated steam, water, and any steam and water mixture and in both hot and cold conditions. Additionally, the solenoid-operated pilot valves that control the valve during low-temperature overpressure conditions are from different power supplies and close at a given setpoint, providing single failure re-closing protection for the PSRVs.

PSRVs remaining open are analyzed as a LOCA event in the shutdown PRA after a loss of residual heat removal (RHR) cooling. However, this event is not specifically analyzed for low temperature overpressure protection (LTOP) conditions. As noted above, this is an unlikely event, and is considered even less likely when its occurrence frequency is combined with the small time when the pressurizer is full. Additionally, the plant operating state with the pressurizer full is a transition state, during which the primary system is depressurized to atmospheric pressure. After depressurization, the pressurizer is drained down in plant operating state CBd. During this time the pressurizer level and pressure are closely monitored, and the safety impacts of a PSRV failing to reseat are diminished.

FSAR Impact:

The U.S. EPR FSAR will not be changed as a result of this question.

Question 19-182

Section 7.3.1.2.1 of the FSAR states that “[a] manual bypass of SIS [safety injection system] actuation on low RCS loop level is provided for protection of personnel working in the RCS components during outages.” Discuss how this manual bypass is controlled during shutdown and when it would be used. Given the high importance of the SI signal cited in response to Question 19-37, control of this bypass is a risk insight that should be documented FSAR Table 19.1-102.

Response to Question 19-182

The SIS pumps are capable of both manual and individual operations from the Main Control Room (i.e., manual bypass of the safety injection (SI) signal). U.S. EPR FSAR Tier 2 Table 19-102 will be changed to reflect the availability of the SIS actuation function on low loop level during mid-loop operations. Additionally, U.S. EPR FSAR Tier 2 Section 19.1.2.2 contains a COL information item to confirm that assumptions used in the PRA remain valid (see FSAR Tier 2 Table 1.8-2 COL information item 19.1-9).

The revision to U.S. EPR FSAR Tier 2 Table 19-102 will be provided in AREVA NP’s response to RAI No. 26 Questions 19-166 and 19-167.

FSAR Impact:

The U.S. EPR FSAR will not be changed as a result of this question.

Question 19-183

Provide additional information on the RHR relief valves, including their relief setpoint and capacity. These relief valves are not discussed in detail in FSAR Section 5.4.7 and are not included in the equipment list in Tier 1 Section 2.2.3. Discuss how the relief capacity of these valves designed to protect the RCS pressure boundary during shutdown will be ensured in the as-to-be-built, as-to-be-operated plant. Describe how these valves are modeled in the shutdown PRA.

Response to Question 19-183

The relief valves protect the residual heat removal system (RHRS) pressure boundary. The reactor coolant system pressure boundary is protected by the low temperature overpressure protection (LTOP) functions provided by the pressurizer safety relief valves, as discussed in U.S. EPR FSAR Tier 2 Section 5.2.2.2.2.

The relief setpoint and capacity of the main RHR relief valve designed to protect the RHR pressure boundary during shutdown are:

- Setpoint pressure = 800 psig
- Relief capacity = 700 gpm

The RHR relief valve is sized to provide protection against the spurious actuation of a medium head safety injection pump with its large miniflow line closed, when the RHRS is aligned to the reactor coolant system during plant cooldown.

In the probabilistic risk assessment, the RHR system relief valve is modeled for premature opening (creating a potential LOCA) with a probability of 3.0E-06 per hour. They are also credited in the screening of the LTOP events, as described in the response to NRC RAI No. 2, Question 19-14.⁷

FSAR Impact:

The U.S. EPR FSAR will not be changed as a result of this question.

⁷ See e-mail from Ronda Pederson (AREVA NP Inc) to Getachew Tesfaye (NRC), "U.S. EPR Design Certification Application RAI No. 2" dated April 10, 2008.

Question 19-184

What indication of RCS temperature, pressure, and level is available to the operators during shutdown? For each, state the type of sensor, its location in the RCS, any associated alarms and trips, and the controls that ensure the indication is available during shutdown. Discuss whether these sensors are susceptible to errors identified at current plants (e.g., errors in differential pressure caused by RCS inventory swept into the pressurizer, failures of tygon tubing, and inaccurate hot leg temperature measurement after a loss of flow).

Response to Question 19-184

Reactor coolant system (RCS) temperature, pressure, and level indications are available to the operator during shutdown operations (Modes 4 – 6). Administrative controls for the availability of the temperature, pressure, and level sensors during shutdown operations will be established by the COL applicant (see U.S. EPR FSAR Tier 2 Table 1.8-1, COL information item 13-1).

Temperature Indication

Shutdown RCS operations rely on the cold leg and hot leg wide range (WR) temperature sensors to provide temperature indication. Temperature measurement inside the reactor pressure vessel (RPV) is not available when instrumentation is disconnected from the top of the RPV in preparation for head removal.

The cold leg WR temperature measurement is located between the residual heat removal system/low head safety injection (RHRS/LHSI) injection nozzle to the RCS and the RPV inlet. The instrument well, located at 135 or 225 degrees (with zero degrees being at the top of the pipe), permits the instrument to be fully submerged during mid-loop operation. The cold leg WR indication is available to the operator through the process information and control system (PICS) and the safety information and control system (SICS). Detection of a faulty cold leg WR temperature sensor generates an alarm. There are no equipment trips that use input from the cold leg WR temperature measurement sensors during shutdown operations.

The hot leg WR temperature measurement is located between the RPV outlet and the RHRS suction nozzle. The instrument well, located at 135 or 225 degrees (with zero degrees being at the top of the pipe), permits the instrument to be fully submerged during mid-loop operation. The hot leg WR indication is available to the operator through PICS and SICS. Detection of a faulty hot leg WR temperature sensor generates an alarm. The hot leg WR temperature measurement is used to determine the margin to saturation in the hot leg so that the RHRS/LHSI pump can be tripped in order to avoid cavitation.

Pressure Indication

Shutdown RCS operations rely on the hot leg narrow range (NR) and hot leg WR pressure sensors to provide pressure indication. The hot leg WR pressure sensors can provide pressure indication during all modes of operation, while the hot leg NR pressure sensors are only used during low pressure operating states. The hot leg NR sensors are required to have a range from 0–870 psia to provide more accurate information during low pressure operations. Switching sensor input from the WR to the NR sensors is performed automatically with the sensor selector. The selected primary pressure input is displayed on PICS.

The hot leg WR pressure sensors are located in the RHRS suction line prior to the first isolation valve, and hot leg WR pressure indication is available to the operator through PICS. When automatic RCS pressure control is engaged, alarms are generated when the RCS pressure deviates from the control band. Alarms are also generated when pressure limitation functions actuate. Although safety functions take precedent, the hot leg WR pressure sensors provide high pressure trip signals for the medium head safety injection (MHSI) pumps, the extra borating system (EBS) pumps, the chemical and volume control system (CVCS) charging pumps, and the pressurizer (PZR) heaters, when RPV brittle fracture protection is enabled to limit pressure increases potentially caused by operation of these components. The hot leg WR pressure sensor is used to determine the margin to saturation in the hot leg so that the RHRS/LHSI pump can be tripped in order to avoid cavitation.

The hot leg NR pressure sensors are located in the RHRS suction line prior to the first isolation valve. Hot leg NR pressure indication is available to the operator through PICS. When automatic RCS pressure control is engaged, alarms are generated when the RCS pressure deviates from the control band. Alarms are also generated when pressure limitation functions actuate. Although safety functions take precedent, the hot leg NR pressure sensors provide high-pressure trip signals for the MHSI pumps, the EBS pumps, the CVCS charging pumps, and the pressurizer heaters, when RPV brittle fracture protection is enabled to limit pressure increases potentially caused by operation of these components.

Level Indication

Mid-loop RCS operations rely on the RCS loop level sensors to provide loop level indication. The RCS loop level is derived from differential pressure measurements between the top of the hot leg pipe and the bottom of the hot leg pipe. Measurement at these two points avoids erroneous indication due to potential differences in PZR and RCS loop pressures. The RCS loop level sensors are located between the steam generator (SG) and the RHRS suction line, in order to provide a conservative indication of the loop level at the RHRS suction line, considering the effects of flow-induced level change.

Each of the four loops of the RCS contains a level measurement sensor. These sensors are located in the hot leg between the SG and the RHRS suction nozzle. These sensors are permanently installed with metal tubing to avoid the use of tygon tubing, which is susceptible to collapse during vacuum sweeping and to improper routing that can trap air causing an erroneous level indication. Since Loop 3 contains the surge line, an additional level sensor is placed between the bottom of the hot leg and the top of the pressurizer. This provides WR level indication so that RCS level is known during the process of draining to mid-loop. RCS loop level indication is available to the operator through PICS and SICS. When RCS loop level control is in the manual control mode, alarms are generated when the loop level deviates from the desired range. When RCS loop level control is in the automatic control mode, alarms are generated when the loop level limitation functions are actuated. The RCS loop level measurement is used to trip the RHRS/LHSI pump in case of low loop level, in order to prevent air ingestion.

U.S. EPR FSAR Tier 2 Section 5.4.7.2.1 provides details on the design features that address shutdown and mid-loop operations.

FSAR Impact:

The U.S. EPR FSAR will not be changed as a result of this question.

Question 19-185

Discuss whether any gravity-driven sources of borated water are available for injection following a loss of inventory during shutdown. At operating plants, the ability to inject from the refueling water storage tank (RWST) is an important mitigation strategy during shutdown, but the IRWST at the U.S. EPR is below the RCS elevation. Discuss how this design feature, which enhances safety by eliminating the need for recirculation switchover following a loss-of-coolant accident (LOCA), affects shutdown risk.

Response to Question 19-185

A response to this question will be provided by September 30, 2008.

Question 19-186

Provide the assumed water volume in the IRWST during shutdown and the assumed water volume that is transferred to the refueling cavity. Do LHSI and MHSI draw from the IRWST following a LOCA in POS E? If so, clarify, with supporting drawings as needed, whether the suction point from the IRWST remains covered with water in POS E.

Response to Question 19-186

A response to this question will be provided by September 30, 2008.

Question 19-187

Clarify the success criteria for RHR in all POS (both in the initiating event assessment and as a mitigating system). Provide a description and results of the calculations performed to justify these success criteria. If the number of trains required is different from the numbers used to support system analyses and/or development of TS, state why.

Response to Question 19-187

A response to this question will be provided by September 30, 2008.

Question 19-188

The staff needs additional information on the interfacing system LOCA (ISLOCA) analysis in the internal events PRA. It is not clear how the analysis progressed from a set of "ISLOCA systems and associated containment penetrations" to a set of systems requiring detailed modeling (SI, CVCS, and component cooling water system (CCWS)) to the list of initiating events in Table 19.1-4 of the FSAR. Provide a more detailed discussion of this analysis in the FSAR, including:

- a. A general discussion of the analysis progression above, including a justification for pathways that were screened out
- b. Development of the ISLOCA initiating event frequency for each pathway, including the pipe rupture and other failure rates used, with sources for each
- c. The mitigation strategy (e.g., isolation or depressurization) credited for each pathway
- d. Key assumptions related to both the initiating event frequencies and the mitigation options
- e. Risk insights regarding the preventive design features (such as in-series check valves, motor-operated valves, pipe strength, control room alarms, and control room indications, as stated on page 19.1-21 of the FSAR) that contribute to the low risk associated with ISLOCA

Response to Question 19-188

- a. The ISLOCA analysis is performed as follows:
 - A screening analysis of all the possible ISLOCA pathways is performed.
 - The pathways that are not screened out are evaluated and an ISLOCA initiating event frequency is calculated using a fault tree method.

Identifying potential ISLOCA pathways begins with identifying all systems that interface with the reactor coolant system (RCS) and could get exposed to normal RCS operating pressure. Containment penetrations in these systems are reviewed to identify whether an RCS connection could cause an ISLOCA outside containment. Penetrations are screened out if they cannot result in an event challenging the safe shutdown of the plant. For example, pathways are screened out if:

- The associated piping diameter for the penetration is 0.6 inches or less (see Key Assumptions in part d) below).
- The system does not have a direct connection to the RCS (e.g., sump system).
- The system is isolated from the RCS and is designed for the RCS pressure.

After screening, pathways affecting three systems are selected for further evaluation:

- Safety Injection System (SIS)

- Medium Head Safety Injection (MHSI) lines: These lines are isolated from the RCS by three check valves in series, and rupture of these valves would expose the safety injection (SI) piping to RCS pressure.
 - Low Head Safety Injection (LHSI) lines: These lines are isolated from the RCS by three check valves in series, and rupture of these valves would expose the SI piping to RCS pressure
 - Residual heat removal (RHR) suction lines: These lines are isolated from the RCS by closed isolation valves during normal operation, and rupture of these valves would expose the SI piping to RCS pressure.
- Component Cooling Water System (CCWS)
 - Tube ruptures in the thermal barrier cooling coil would expose the low-pressure CCWS to RCS pressure.
 - Rupture of a high-pressure cooler tube would expose the CCWS to RCS pressure via the chemical and volume control system.
 - Chemical and Volume Control System (CVCS)
 - Failure of the high-pressure reducing valves would expose the low-pressure portion of the letdown line to RCS pressure.
 - The charging line is connected to the RCS during normal operation. An unisolated break in this line could result in RCS backflow outside of containment.
- b. For each of the pathways identified above, an initiating event frequency is derived using a fault tree. The following elements are used in the fault tree analysis:
- Component failure probability (motor-operated valve (MOV) or check valve rupture, tube leakage): The failure probabilities of these components are obtained from the main data sources used in the model and are calculated for a yearly mission time.
 - Break isolation: For each path, automatic or manual isolation of the break is modeled. Given successful isolation, component failures are modeled for a 24-hour mission time (which is the assumed time to bring the plant to safe shutdown).
 - Pipe rupture probability: The failure probability of low pressure piping is assumed to be one (i.e., guaranteed failure) if exposed to RCS pressure. For the charging line (connected to the RCS during normal operation), which is designed for RCS pressure, the failure rate is estimated based on the pipe failure study in EPRI TR-102266 (U.S. EPR FSAR Tier 2 Section 19.1.9, Reference 40).
- c. The ISLOCA mitigation strategy modeled in the PRA depends on the pathway considered.
- For the safety injection pathways, where an ISLOCA requires failure of several redundant isolation valves, the modeled operator action is to diagnose the failure of the first valve and perform a controlled shutdown in 24 hours to prevent an ISLOCA.
 - For the other pathways, the modeled operator action is to isolate the pathway once the break occurs.

If the ISLOCA isolation fails, the PRA models ISLOCA mitigation by depressurizing the RCS to RHR entry conditions, and switching to RHR using the unaffected trains. This mitigation strategy is modeled for the smaller size pathways; ISLOCAs in the safety injection and the charging line are conservatively modeled as leading directly to core damage.

d. Assumptions in the ISLOCA analysis are:

- Pathway screening: Systems that penetrate the containment through pipes with an inside diameter less than or equal to approximately 0.6 inches are excluded from consideration, since the maximum RCS flow rate through these pipes is less than the capacity of the normal charging system.
- Un-isolated ISLOCAs affecting the SIS and the charging line are conservatively assumed to result in core damage.
- Upon diagnosing an ISLOCA, the operators are assumed to perform a controlled shutdown within 24 hours.

e. The probabilistic risk assessment identifies several design features that contribute to the low risk associated with ISLOCAs, including:

- The presence of sensors and alarms that will alert the operator of a valve failure and initiate automatic isolation in case of a break.
- High redundancy and diversity of isolation valves. For example, three valves in series separate the RHR suction line from the RCS.
- Diversity in isolation valve design.
- High piping design pressure for systems that are not qualified for RCS pressure. For instance, the RHR suction line has a design pressure of 930 psig and is vented to the in-containment refueling water storage tank, decreasing the risk of rupture.

U.S. EPR FSAR Tier 2 Section 19.1.4.1.1.2 will be revised to reflect the information provided in this RAI response.

FSAR Impact:

U.S. EPR FSAR Tier 2 Section 19.1.4.1.1.2 will be revised as described in the response and indicated on the enclosed markup.

U.S. EPR Final Safety Analysis Report Markups

- If the pending change does not impact the PRA, no further action is needed.

A COL applicant that references the U.S. EPR design certification will describe the applicant’s PRA maintenance and upgrade program.

19.1.3 Special Design/Operational Features

The U.S. EPR is a 4590 MWt evolutionary pressurized water reactor (PWR) that combines proven technology with innovative system configurations to enhance safety. The EPR was originally developed through a joint effort between Framatome ANP and Siemens KWU in the 1990s by incorporating key technological and safety features from the French and German reactor fleets. The U.S. EPR version is an adaptation of the EPR to conform to U.S. codes, standards, and regulatory requirements. The design features that contribute to the low frequency of core damage and low frequency of large release compared to the current operating fleet of PWRs are described in the sections that follow.

19.1.3.1 Design/Operational Features for Preventing Core Damage

The U.S. EPR design incorporates many features that reduce the potential core-damage accidents that have been assessed to be important for current-generation PWRs. These features are summarized below. Their relevance to the low CDF for the U.S. EPR is described in more detail in Section 19.1.4.

19.1.3.1.1 High Level of Redundancy and Independence for Safety Systems

The U.S. EPR design incorporates four trains of safety systems, including the emergency core cooling systems (ECCS), the EFW system, and the support systems needed to allow these systems to function. In addition to being highly redundant, these trains are housed in four separate buildings. This separation reduces the risk of common failure of multiple trains due to postulated internal or external hazards.

19.1.3.1.2 Highly Redundant Onsite Power System

19-162

The U.S. EPR design includes four EDGs, one supporting each safety division. In addition to the four EDGs, there are two backup SBO diesel generators. The SBO diesel generators are diverse from the EDGs in ~~design, manufacturer, cooling, actuation and control, fuel oil and operating environment~~ model, control power, HVAC, engine cooling, fuel system, and location. This U.S. EPR electrical design reduces the risk associated with loss of offsite power (LOOP) and SBO.

19.1.3.1.3 Stand Still Seal System for Reactor Coolant Pumps

The potential for leakage or small LOCAs (SLOCA) due to failure of reactor coolant pump (RCP) shaft seals has been an important risk contributor for many PWRs. The U.S. EPR design includes a stand still seal for each RCP. The stand still seal is a

the U.S. EPR relative to the weaknesses they are intended to reduce or eliminate. These features are primarily those identified in NUREG-1560 (Reference 11) and NUREG-1742 (Reference 12).

Throughout the design process, the PRA plays an important role both in identifying features that merit consideration with respect to opportunities to reduce risk, and to review proposed design changes to evaluate the potential risk impact. As indicated earlier, PRA review of design changes is incorporated into the AREVA NP design change control process.

AREVA NP has also used insights from the PRA to identify specific improvements to reduce the contribution to risk due to some aspects of the design. The specific areas of improvement include the following:

19.1.3.4.1 SBO Diesel Generators

19-162

The SBO diesel generators were added to reduce the contribution of SBO events initiated by a LOOP. The PRA also identified the need for the SBO diesel generators to be independent and diverse from the EDGs. To that end, the SBO diesel generators differ from the EDGs in manufacturer, control logic, starting and control batteries, fuel oil, cooling mechanism, and location model, control power, HVAC, engine cooling, fuel system, and location.

19.1.3.4.2 Cooling of Low Head Safety Injection Pump Motors

Cooling water for the motors for two of the four low head safety injection (LHSI) pumps (Pumps 1 and 4) were permanently aligned to the safety chilled water system (SCWS). The original configuration entailed cooling of all four pumps by the component cooling water system (CCWS), with chilled water available as backup cooling to pumps 1 and 4. This change added diversity in the motor cooling and eliminated the need for manual alignment of backup cooling. Since Divisions 1 and 4 of the chilled water system are air cooled, the diversity extends to the heat sink used for cooling. The change in configuration also eliminates the potential that common cause failure (CCF) of the three-way valves supplying cooling water could affect two of the LHSI pumps.

~~**19.1.3.4.3 Reliability of Safety Injection Actuation During Mid-Loop Operation**~~

~~A diverse signal consisting of LHSI residual heat removal (RHR) pump low suction pressure has been added to actuate the MHSI pumps to reduce the potential for overdraining the RCS during mid-loop operation. Thus, MHSI is actuated on either low level in the RCS loops or LHSI/RHR pump low suction pressure.~~

RCS flow rate from a postulated 0.6-inch diameter (or smaller) break is not expected to exceed the make-up capacity of the chemical volume control system (CVCS). Several industry studies including NUREG/CR-5744 (Reference 15) and EPRI-NSAC-154 (Reference 16) have concluded that ISLOCA events within the capacity of the charging system are not significant contributors to the ISLOCA CDF. However, the U.S. EPR ISLOCA evaluation conservatively considers the possibility that multiple tubes could fail at an RCS heat exchanger interface, resulting in primary leakage in excess of the charging system capacity.

19-188

~~The ISLOCA systems and associated containment penetrations are reviewed based on the above criteria. ISLOCA preventive design features (i.e., in-series check valves, motor-operated valves, pipe strength, control room alarms and control room indications) are used to identify those RCS connections that are subject to further detailed evaluation. The systems requiring detailed quantitative modeling include:~~

Containment penetrations are reviewed to identify where an RCS connection could cause a significant ISLOCA outside containment. Penetrations are screened out if it is judged that they cannot result in an event challenging the safe shutdown of the plant. For instance, pathways are screened out if:

- The associated piping penetration diameter is 0.6 in. or less (see discussion above).
- The system does not have a direct connection to the RCS (e.g., sump system).
- The system is isolated from the RCS and is designed for RCS pressure.

Once this screen is performed, pathways are retained for further evaluation affecting three systems:

- Safety Injection System (LHSI/RHR, MHSI discharge lines, RHR suction line).
- CVCS System (charging line, letdown line).
- CCW System (high pressure cooler, RCP thermal barrier cooling coils).

For each of the pathways identified above, an ISLOCA frequency is calculated based on the frequency of the triggering event (e.g., valve rupture), and the failure probability of the isolation (manual and/or automatic). Pipe rupture probability for a low pressure system exposed to RCS pressure is assumed to be 1 (guaranteed failure).

The frequency of core damage for each postulated ISLOCA event is estimated as the product of two factors:

- The ISLOCA initiating event frequency for each ISLOCA pathway.
- The probability that the ISLOCA event cannot be successfully mitigated. ~~An ISLOCA event can be successfully mitigated if the pathway can be automatically or~~

19-188

~~manually isolated prior to the time at which RCS inventory is inadequate.~~
Additionally, for some For large ISLOCA events, (e.g., RHR suction line break), this probability is conservatively assumed to be 1 (guaranteed core damage). For smaller ISLOCAs, such as heat exchanger tube breaks, accident mitigation can be achieved by depressurizing the RCS and aligning RHR cooling.

Steam Generator Tube Rupture

SGTR initiating events are defined as failures of SG tubes resulting in primary coolant leakage into the secondary side of the SG. These events are similar to SLOCA events, except there are no containment indications of the event and that the leak can be terminated if the ruptured SG is isolated and RCS pressure is maintained at a pressure below the relief setpoints of the secondary valves on the ruptured SG. However, if the ruptured SG is not isolated, or if RCS pressure is not maintained below the MSSV/MSRT setpoint on the ruptured SG, RCS leakage could escape to the environment. The U.S. EPR SGTR mitigating strategy is based on having the MHSI shutoff head at a value below the lift setpoints on the secondary valves on the ruptured SG. The SGTR event is conservatively assumed to be a single double-ended tube rupture, although most historical SGTR events have been significantly less severe. The smaller leaks allow more time for operator response. Failure of more than one tube can be postulated. However, the analysis assumption that all SGTR initiators involve a double-ended break of a single tube is judged to result in a conservative estimate of the SGTR risk.

Induced Steam Generator Tube Rupture

Induced SGTRs are considered in the U.S. EPR as a separate initiating event. SGTRs can occur for initiating events that cause a large change in the pressure differential across the SG tubes, such as for main steam line breaks and main feed line breaks. The primary concern is with steam-line breaks outside of containment, as these events can result in a loss of RCS inventory outside containment if the RCS is not depressurized, whereas a break inside containment results in a loss of RCS inventory inside containment and behaves similarly to a LOCA event, with a much lower initiating event frequency. The induced SGTR initiating event frequency was estimated based on the NUREG/CR-6365 (Reference 17) methodology with consideration given to advances in materials technology (alloy 690), and consideration given to advances in degradation monitoring.

Secondary Line Break

Secondary line break initiating events include those secondary line breaks that are large enough to initiate secondary side isolation and safety injection actuation. The initiating events considered are discussed below:

- Steam line breaks can occur upstream or downstream of the MSIVs. Steam line breaks inside containment (SLBI) (i.e., breaks occurring upstream of the MSIVs)

Direct Current Electrical Distribution System

The direct current (DC) electrical distribution system PRA-credited function is to provide divisional DC electrical power to the frontline and support systems from the associated division’s DC battery. Each safety train division is equipped with a dedicated, Class 1E battery with redundant battery chargers. The divisional batteries are designed for a discharge of two hours based on the necessary loading of the batteries. The U.S. EPR also includes a separate non-class 1E uninterruptible power supply (UPS) system for severe accident management. This system consists of redundant batteries designed for twelve hour discharge.

Emergency Diesel Generators

The EDGs PRA-credited function is for each EDG to independently provide onsite AC electrical power to its associated electrical division should the normal offsite power source become unavailable. There are four 100 percent capacity EDGs. Each EDG is dedicated to an electrical division. The EDGs are located in two separate Emergency Power Generation Buildings (EPGB), which are spatially separated on the plant site. The EDGs are also physically separated within the EPGBs.

Station Blackout Diesel Generators

The SBO diesel generators PRA-credited function is for each SBO diesel generator to provide backup AC electrical power to its associated electrical division, independent and diverse from the divisional EDG. U.S. EPR has two SBO diesels generators to supply power to plant loads in the unlikely event of a LOOP with failure of all four EDGs (SBO-type event). The SBO diesels are associated with train Divisions 1 and 4 and are auto started and manually connected and loaded from the control room. The SBO diesels are independent and diverse of the EDGs based on consideration of

19-162

attributes (e.g., different ~~capacity rating, different manufacturer, different controls, batteries, different locations~~ model, control power, HVAC, engine cooling, fuel system, location). The SBO diesels are located in the Switchgear Building.

Essential Service Water System / Ultimate Heat Sink

The ESW system PRA-credited function is to remove reactor heat and heat generated by equipment and components during normal operating conditions, transients and accidents. ESW supplies water to the CCWS heat exchangers and consists of four independent trains. Each UHS train configuration consists of the divisional ESW pump, a two-cell mechanical draft cooling tower with basin and fans and associated instrumentation, and isolation valves. Train 4 basin and cooling fans support the dedicated cooling train to the SAHRS.

a high significance (a high FV) of the parameters used in the modeling of an RCP seal LOCA. It also shows that a CCF of stuck control rods has a RAW value larger than 420,000. This high importance could be attributed to an ATWS-related conservative assumption that for many high frequency events, which include a loss of MFW or a loss of condenser, a failure to scram is assumed to lead directly to core damage. LOOP-related basic events (a LOOP during 24 hours, or a consequential LOOP) also show a high significance (a high RAW). Preventive maintenance importance measures illustrate importance of the various safety trains. Based on the RAW values presented in Table 19.1-14, SAC Division 1 and Division 4 have the highest importance, which could be attributed to a general HVAC importance and to the fact that SAC Division 1 and Division 4, as air cooled, are independent from the CCW headers.

19.1.4.1.2.5 Assumptions

Assumptions in the PRA development are divided into two groups:

- Key assumptions in response to key sources of uncertainty in the knowledge
- Modeling assumptions made because of limitations in the PRA logic models or software

The most important assumptions from these two groups are listed below:

Key Assumptions:

19-162

- EDGs and SBO DGs are assigned to different common-cause groups. This assumption will be confirmed by assuring diversity between EDGs and SBO DGs (~~different vendors, different location, different cooling systems, different starting-systems, and different fuel supplies~~ model, control power, HVAC, engine cooling, fuel system, location).
- The HRA is performed under assumptions that the operating procedures and guidelines will be well written and complete; and so will operator training.
- Different operator actions HEPs are estimated for the SBO conditions (LOOP and all EDGs not available) versus non-SBO conditions (LOOP and at least one EDG available). It was assumed that operators will have more clear direction about the crosstie of buses and equipment, in clear SBO conditions, when no emergency power is available. This assumption will be evaluated when the operating procedures and guidelines are available.
- CVCS is not credited for an RCS injection function. CVCS is only credited for the RCP seal injection. It is assumed that the CVCS supply from the volume control tank will be available for majority of the events where CVCS is credited for the RCP seal injection, with an estimated probability of 0.1. This assumption will be evaluated when plant-specific information is available.
- RCP seal LOCA probability, given a total loss of seal cooling and the RCP trip, is assumed to be equal to 0.2.

Table 19.1-4—Summary of Initiating Events for the U.S. EPR PRA
Sheet 1 of 3

Event	Mean Frequency (/yr)	Distribution Type (Parameters)	Source for Frequency
Plant Transients			
GTR—general transient, including turbine or reactor trip that does not involve failure of systems that could be needed for core heat removal.	7.5E-01	Gamma (17.8, 23.7)	NUREG/CR-6928 (Reference 19)
LOC—loss of main condenser, including MSIV closure, loss of condenser circulating water, etc.	8.1E-02	Gamma (20, 247)	NUREG/CR-6928
LOMF—total loss of main feedwater	9.6E-02	Gamma (1.33, 13.8)	NUREG/CR-6928
Loss-of-Coolant Accidents (LOCA)			
SLOCA—small LOCA (0.6 to 3-in equivalent diameter)	1.4E-03	Gamma (1.4, 1014)	NUREG/CR-6928 and NUREG-1829, with addition of frequency for spurious opening of PSV failure of the PSVs to reseal (2E-04/yr)
MLOCA—medium LOCA (3 to 6-in equivalent diameter)	1.4E-05	Lognormal (EF = 16)	NUREG-1829 (Reference 44)
LLOCA—large LOCA (>6-in equivalent diameter)	1.3E-06	Gamma (0.42, 3.16E+5)	NUREG/CR-6928
SGTR			
SGTR	3.6E-03	Gamma (0.5, 14.1)	NUREG/CR-6928
IND SGTR—SGTR induced by a steam line break	1.2E-06	Lognormal (EF=32)	Calculated based on methodology from NUREG/CR-6365 (Reference 45)
Interfacing Systems LOCAs			
ISL-CCW RCPTB—ISLOCA, with leakage to CCW due to failure of the thermal barrier cooling coils for RCP seal cooling; frequency includes conditional failure of mitigation	4.2E-10 PE: 4.1E-10	Lognormal fit (EF = 55)	Lognormal fit to Design-specific fault-tree analysis
ISL-CVCS HPTR—ISLOCA due to rupture of tube in high pressure letdown cooler; frequency includes conditional failure of mitigation	1.5E-08 PE: 9.2E-10	Lognormal fit (EF = 370)	Lognormal fit to Design-specific fault-tree analysis

19-168

→ spurious opening of PSV failure of the PSVs to reseal (2E-04/yr)