

Response to

Request for Additional Information No. 53 (1006), Revision 0

8/22/2008

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: 19.0

SPLA Branch

Question 19-193:

Table 19.1-3 of the Final Safety Analysis Report (FSAR) indicates that very small loss-of-coolant accidents (LOCA) are not modeled because it is assumed that normal charging will maintain the reactor coolant system (RCS) inventory. However, this assumption is not included in the list of assumptions and insights in Table 19.1-102. Additionally, the components associated with charging injection may be inappropriately excluded from probabilistic risk assessment (PRA) input to other programs. Provide additional qualitative justification for the exclusion of very small LOCAs, discuss the impact of the exclusion on input to other programs such as the reliability assurance program (RAP), and add assumptions and insights to the FSAR as appropriate.

Response to Question 19-193:

As stated in the question, very small loss-of-coolant accidents (LOCA) are not modeled in the U.S. EPR PRA because they would not exceed capacity of the charging system (CVCS) to maintain the reactor coolant system (RCS) inventory. An additional failure of the charging system needs to occur to cause an initiator. The plant response and mitigating requirements would be similar to the response to a small LOCA. An estimated frequency for this initiator is as follows:

$$\text{(Very small LOCA frequency} \times \text{(CVCS failure probability))} = 1.5\text{E-}3/\text{yr} \times 2\text{E-}3 = 3\text{E-}6/\text{yr}$$

This frequency is not significant (0.2%) when compared to the U.S. EPR small LOCA frequency of $1.4\text{E-}03/\text{yr}$.

The CVCS system is included in the PRA, not as a part of safety injection, but as a part of seal injection. Importance measures associated with the CVCS system (common cause failures of both CVCS pumps to run) are as follows:

$$\text{(CVCS Pumps Common Cause FTR) importance measures: FV} = 1.6\text{E-}06; \text{RAW} = 1.2$$

Considering CVCS failure as a part of the above initiator would not impact the risk-significance of the charging system. Small loss-of-coolant accident (SLOCA) initiating event contributes 0.09 to the total CDF. As shown above, 0.002 of SLOCA is due to a CVCS failure. This gives the CVCS an estimated F-V of 0.0002, well below the significance criteria of 0.005.

Based on the low significance of very small LOCAs and related CVCS failures, assumptions associated with these items will not be added to U.S. EPR FSAR Tier 2, Table 19-102.

FSAR Impact:

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

Question 19-194:

Justify the exclusion of vessel rupture as an initiating event in the U.S. EPR PRA. Discuss the impact of the exclusion on the U.S. EPR risk profile and on input to other programs such as the reliability assurance program (RAP), and add assumptions and insights to the FSAR as appropriate.

Response to Question 19-194:

The vessel rupture is excluded as an initiating event in the U.S. EPR PRA, because no associated frequency information is available for the advanced light water reactor (ALWR). The vessel rupture frequency used in the current generation of the nuclear plants is $1E-7/yr$. This is an estimate based on engineering judgment, and was not considered an important contributor to the total core damage frequency (CDF). However, the same value could be a major contributor to the advanced light water reactor (ALWR) CDF.

If considered in the U.S. EPR CDF, at this failure frequency, the vessel rupture initiator would increase the total internal events CDF ($2.9E-7/yr$) approximately 1.4 times (40%), or total CDF ($5.3E-7/yr$) approximately 1.2 times (20%). This event would dominate the risk results and could lead to non-conservative importance measures, as illustrated below.

For example, assuming that the new CDF is 1.4 times larger than the base case CDF:

$$CDF_1 = 1.4 * CDF_0,$$

would result in the new FV values of:

$$FV_1 = FV_0 * CDF_0 / CDF_1 = FV_0 / 1.4.$$

Based on the above equation, the components with the current $FV < 0.007$, may not be identified as important in the equipment importance ranking.

Similarly, the impact on the RAW would be as shown below:

$$RAW_1 = (RAW_0 + (CDF_1 - CDF_0)) * CDF_0 / CDF_1 = (RAW_0 + 0.4) / 1.4$$

Based on the above equation, the components with the current $RAW < 2.4$, may not be identified as important in the equipment importance ranking.

An exclusion of the vessel rupture as an initiating event creates more conservative importance measures because the results are not masked by this contributor. Until a more realistic frequency estimate is available for the vessel rupture event, this event will not be included as a U.S. EPR initiating event.

FSAR Impact:

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

Question 19-195:

(Follow-up to Question 19-66) The response to Question 19-66 discusses conservatism in the steam line break inside containment (SLBI) initiating event frequencies as a justification for not modeling feedwater line breaks inside containment (FLBI). However, SLBI represents an overcooling event and FLBI represents an overheating event. Discuss how the PRA model addresses the different mitigating strategies and consequences (e.g., possible lifting and sticking of pressurizer safety relief valves (PSRV)) of the two events.

Response to Question 19-195:

A response to this question will be provided by November 14, 2008.

Question 19-196:

To the discussion of system modeling in section 19.1.4.1.1.3 of the FSAR, add a description of the screening process used to exclude failure events or failure modes from the PRA model based on low probability or other considerations. Such screening is addressed by supporting requirement SY-A14 of the ASME PRA standard (RA-Sb-2005), as endorsed by the U.S. Nuclear Regulatory Commission (NRC) staff in Regulatory Guide (RG) 1.200.

Response to Question 19-196:

The ASME PRA Standard supporting requirement SY-A14 was used as guidance on screening failure events and failure modes from the PRA. This discussion will be added to FSAR Section 19.1.4.1.1.3.

FSAR Impact:

U.S. EPR FSAR Tier 2, Section 19.1.4.1.1.3 will be revised to include the discussion as described in the response and as indicated in the enclosed markup.

Question 19-197:

(Follow-up to Questions 19-70 and 19-5) The cutsets provided in Table 19.1-7 of the FSAR show the initiating event as one element of the cutset rather than including the individual failures that cause the initiating event. Clarify whether the initiating event fault trees are linked to the mitigating system fault trees during quantification, or whether the initiating event frequencies are assessed separately. In addition:

- a) How do the cutset examination and sensitivity study presented in response to Question 19-70 address combinations of human errors among initiating events and mitigating systems?
- b) How do the correlation classes presented in response to Question 19-5 address combinations of similar components among initiating events and mitigating systems?

Response to Question 19-197:

The initiating event fault trees are not linked to the mitigating system fault trees, because the Risk Spectrum[®] software does not allow inclusion of the same basic event with two different mission times. The initiating event frequencies are calculated separately, and entered as values/distributions into the PRA model.

- a) There is a very limited number of human actions in the initiating event (IE) fault trees: none in LOMFW, loss of balance of plant (LBOP), loss of single bus, or any of the LOCCW initiating events. The only human actions in the IE fault trees are human actions to isolate intersystem loss-of-coolant accident (ISLOCA) events. Dependency between those actions and the following operator action to depressurize reactor coolant system (RCS) and start residual heat removal (RHR) are explicitly considered in the simple ISLOCA event trees, as discussed in the responses to RAI 7, Question 19-61. No operator action, other than the action to depressurize and start RHR, shows in the ISLOCA accident sequence. Each of the ISLOCA isolation human errors would occur either as a single action or jointly with this dependent action. Therefore, the separation of models will not have an impact on the sensitivity study presented in the response to RAI 7, Question 19-70.
- b) Because the initiating event fault trees are not linked to the mitigating system fault trees, the correlation between the similar components, IEs and mitigating systems is not addressed in the uncertainty analysis. Omission of these correlations should not have a significant impact on the overall uncertainty results, because of the following:
 - Correlation between component cooling water/essential service water (CCW/ESW) pumps would be applied to loss of component cooling water (LOCCW) initiating events when only a partial loss of CCW/ESW occurs. However, all LOCCW IEs are small contributors to the total CDF (3.1 %). The most important CCW/ESW initiators are: LOCCW-CH1L, a leak in the CCW common header (1.5% of the total CDF), and LOCCW-ALL, a loss of all CCW/ESW trains (0.7% of the total CDF). For both of these initiators, correlations between common header relief valves or CCW/ESW pumps are limited to the initiating event fault trees.

- Correlation among different valves in the current PRA model is very conservative. For example, all motor operated valves (MOV) are included in the same correlation group. The addition of a few valves from the initiating events is not likely to significantly affect the results.

FSAR Impact:

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

Question 19-198:

(Follow-up to Question 19-126) The response to Question 19-126 states that the importance measures provided in Chapter 19 of the FSAR are grouped where appropriate, and that “the presented importance measures are always the highest of any component in the group.” Does this statement apply only to the risk achievement worth (RAW) importance measures? That is, does a group’s Fussell-Vesely (FV) importance measure represent the sum of the group’s FV measures, as was made clear for multiple failure modes of a single component?

Response to Question 19-198:

The importance measures are grouped based on the following:

- Symmetrical components among multiple trains (for example, one of four emergency diesel generators, or one of two emergency feedwater (EFW) pumps for Trains 2 and 3) are grouped for both RAW & FV importance measures, because they are expected to have similar RAW and FV values (they have the same failure rates). In this case, “train” refers not to a physical train (pumps, valves, etc.) but to a specific division (emergency diesel generator (EDG) divisions 1, 2, 3, and 4). In this case, the largest FV for the grouped components was provided.
- Different components in the same physical train (pumps, valves, etc.) are grouped only for RAW importance measures, because they are expected to have the same RAW values (the impact of their failures is the same).

The FV values were not summed for these groups. The FV values are summed only for multiple failure modes of the same component, as discussed in the response to RAI 5, Question 17.04-1.

FSAR Impact:

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

Question 19-199:

(Follow-up to Question 19-127) Question 19-127 asked for the maintenance assumptions for all equipment modeled in the PRA, but the response appears to be limited to “mechanical equipment.” Clarify whether any components modeled in the PRA (e.g., batteries, inverters, buses) that may not be considered “mechanical equipment” have different maintenance assumptions from those stated. If so, these assumptions should be clearly stated in the appropriate location in the FSAR.

Response to Question 19-199:

In the U.S. EPR PRA model, maintenance unavailability is included for stand-by equipment. For electrical components, maintenance unavailability was included for Emergency Diesel Generators and SBO Diesel Generators. Preventive maintenance on the buses, batteries and inverters is not likely at-power because of the short allowed outage time (AOT) in Tech Specs. A corrective maintenance also was not modeled for this equipment because frequency of the maintenance is expected to be very low (equipment is very reliable) and maintenance duration is expected to be very short (short AOTs in technical specifications: two hours for batteries, eight hours for buses, 24 hours for inverters). Omission of these corrective maintenance unavailabilities in the U.S. EPR PRA model is not expected to have a significant impact on the overall risk results.

FSAR Impact:

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

Question 19-200:

(Follow-up to Questions 19-133 and 19-143) Additional information is needed on the operator action timing assumptions in the U.S. EPR PRA. Specifically:

- a) The response to Question 19-143 states that operator isolation of residual heat removal system (RHRS) flow diversions is not credited if less than 25 minutes is available. The response to Question 19-133 appears to credit human action in cases where 16, 27, or 28 minutes are available, but not when 15 minutes are available. Clarify the apparent discrepancy between these two approaches.
- b) Page 19.1-42 of the FSAR indicates that the PRA is “not limited to the design philosophy expectation” that operator actions are not required within the first 30 minutes for control room actions or the first 60 minutes for local actions. So that the staff can understand the impact of this approach on the PRA, provide the results of a sensitivity study with no credit for operator actions with less than 30 or 60 minutes available, respectively.
- c) Provide additional detail about the “engineering judgment” used to estimate a median time for diagnosis and the adjustment of action times “for actions that entail multiple steps or complexity,” both of which are mentioned on page 19.1-43 of the FSAR.

Response to Question 19-200:

- a) In the response to RAI 14, Question 19-133 (Table 19-133-1) the time to boil associated with plant operating state (POS) CAu is shown as 16 minutes. The time to boil in U.S. EPR FSAR Tier 2, Table 19-133-1 for POS CAu should have been reported as 45 minutes.

The 16 minute value was from an initial screening calculation that assumed worst case conditions across the POS. Conservatively, as for all “RHR re-starting” human actions, the starting level was assumed to be mid-loop. In this POS, the reactor coolant pumps (RCP) were assumed to be running. However, these conditions will not exist at this POS. The RCPs are used to heatup the reactor coolant system (RCS) for startup; however, the RCPs will not be started until there is a level in the pressurizer. Therefore the initial condition of RCPs running at mid-loop is not valid. For the initial condition of RCPs running and pressurizer level on-scale, the time to boil is also much longer (45 minutes used).

The other cases cited in the question regarding 27 and 28 minutes are not applicable. There is no operator action associated with the 28 minute case—all residual heat removal (RHR) trains are assumed failed—and both cases have operator action times greater than 25 minutes.

Therefore, the responses to RAI 14, Question 19-133 and 19-143 are consistent with respect to not crediting the RHR system operator actions if less than 25 minutes was available.

- b) Table 19-200-1 lists the operator actions that were credited in less than 30 minutes for main control room (MCR) actions. There are no local actions in the PRA that have been credited in less than 60 minutes. This includes all of the operator actions in the Level 1, Level 2, and low-power shutdown (LPSD) PRAs.

Table 19-200-1—MCR Operator Actions Credited in less than 30 Minutes

| Operator Action ID | Description | Time Available (minutes) |
|-------------------------|--|--------------------------|
| Level 1 at Power | | |
| OPF-RCP-SI | Trip RCPs on loss of seal injection | <15 |
| OPF-DWS/FST | Start DWS pump for FST makeup for SSS | <30 |
| OPF-RT | Trip Reactor Manually | <5 |
| Level 1 Shutdown | | |
| OPF_RHR_DD | Start RHR in DD | <30 |
| OPE-FB-CAD (C2) | Initiate feed and bleed (F&B) after LOCA in CAD | <30 |
| OPE-FB-CAU (C2) | Initiate feed and bleed (F&B) after LOCA in CAU | <30 |
| OPF-ISOIRWSTFD-E | Isolation of flow RHR diversion path (JNG_0AA001) in POS E | <30 |
| OPF-ISORHRBRK | Isolation of RHR pipe break | <30 |
| Level 2 | | |
| None | N/A | N/A |

Table 19-200-2 shows the sensitivity of core damage frequency (CDF) if no credit is given for these operator actions.

Table 19-200-2—Sensitivity Case Results for No Operator Action Credit in less than 30 Minutes

| Risk Measure | Base Case | Sensitivity Case | Change in CDF |
|---|-----------|------------------|---------------|
| Total CDF at power (internal events, fire, and flood; per year) | 5.3E-07 | 5.9E-07 | +12% |
| Total CDF for LPSD (per year) | 5.8E-08 | 7.7E-08 | +34% |

- c) Engineering judgment was used to estimate the times needed for diagnosis and action, which are compared to the available time, for the various human error probabilities (HEP). As described in the response to RAI 7, Question 19-72, the process for developing the human reliability analysis (HRA) involved conferring with team members in the disciplines of human factors engineering (HFE), operations, thermal hydraulic analysis, and design.

The SPAR-H HRA methodology was chosen for the U.S. EPR because it is a conservative methodology and because it is an appropriate methodology for a design that lacks detail with respect to emergency procedure guidelines (EPG) and human machine interface (HMI) designs. The SPAR-H results are dependent upon the relative ratio of time available to time needed. They are not particularly sensitive to small perturbations of the absolute timing.

The engineering judgments were made in the context of the expected cues and their timing, the expected emergency procedure guideline (EPG) threshold criteria for the action, and the team members' experience with symptom-oriented procedures. Representative modular accident analysis program (MAAP) runs were used to provide an approximate indication of the chronology of the event and the associated symptoms. The engineering judgment considered, in light of the chronology and complexity of the event, whether the cues presented unambiguous direction relative to the expected EPG criteria, or were likely to involve corroboration by secondary symptoms. The engineering judgment also considered whether navigation of several emergency operating procedure (EOP) steps is expected before reaching the desired action, as opposed to triggering of an immediate rule-based response.

Typical diagnostic times are five to twenty minutes. An example of a diagnostic time that is shorter than five minutes is for manual reactor trip (which is performed immediately upon entry into EOPs). An example of a diagnostic time longer than 20 minutes is for starting backup heating, ventilation and air conditioning (HVAC), which conservatively assumes that

the operator delays diagnosis until room heat-up symptoms corroborate the system failure cues.

For most action times, five minutes was allowed for simple executions performed from the MCR (such as opening valves). More time was allowed for a multi-step process such as initiating steam generator (SG) isolation and cooldown for steam generator tube rupture (SGTR) mitigation (15 minutes).

Since the timing estimates are based on engineering judgment, the HFE/HRA integration plan, discussed in response to RAI 7, Question 19-72 and in U.S. EPR FSAR Tier 2, Section 18.6, is relied upon for refinement of the HRA as the HMI design and the related EPG mature. Risk-significant human actions are addressed during HFE activities throughout detailed design. As described in U.S. EPR FSAR Tier 2, Section 18.10, the HFE verification and validation (V&V) activities will validate the important HRA assumptions such as timing when the EPG, HMI design, and simulator are further developed. Incorporation of feedback from these activities and updates to the HRA are performed in accordance with the HFE/HRA integration plan described in U.S. EPR FSAR Tier 2, Section 18.6, and the PRA maintenance and upgrade process described in U.S. EPR FSAR Tier 2, Section 19.1.2.4.

FSAR Impact:

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

Question 19-201:

(Follow-up to Question 19-139) The response to Question 19-139 did not discuss how doors or removable barriers between fire areas will be controlled during shutdown. Address this aspect of the question, and provide a sensitivity study in which fire areas separated by a door or removable barrier are considered as a single fire area.

Response to Question 19-201:

Administrative controls will define the control of fire barriers during shutdown. As requested, a sensitivity study is provided to evaluate the impact of considering fire areas separated by a door as a single fire area. These are the fire areas shown in response to RAI 14, Question 19-139, Table 19-139-1. The door in Safeguard Building 1 (or 4) that links PFA-SAB-MECH and PFA-SAB14-AC is not considered a likely fire propagation path. This door separates a cable shaft from an access room in the mechanical area where no significant amount of combustible should be present. An unlikely fire in that access room would have to propagate via the cable shaft up 3 floors to reach the switchgear room, or release enough heat via this shaft to damage the switchgears. Therefore it is reasonable to assume that the separation between these two fire areas is very unlikely to be compromised and that these two fire areas should not be merged.

The sensitivity study is run by merging the following fire areas:

Table 19-201-1—Merging of Fire Areas

| Safeguard Building 1 or 4 | | Safeguard Building 2 or 3 | |
|---------------------------|------------------------|---------------------------|------------------------|
| <i>Base case PFAs</i> | <i>Sensitivity PFA</i> | <i>Base case PFA</i> | <i>Sensitivity PFA</i> |
| PFA-SAB14-AC | PFA-SB14 | PFA-SAB23-AC | PFA-SAB23-ELEC |
| PFA-SAB14-DC | | | |
| PFA-BATT | | PFA-SAB23-DC | |

Two fire areas are merged into a single one as follows:

- The fire ignition frequency of the resulting fire area is the sum of the initial fire ignition frequencies.
- The associated fire scenario is assumed to fail all equipment failed by each of the initial fire scenarios.

The resulting Fire CDF for this sensitivity case is 2.2E-07/yr. This represents a 4.6E-08/yr (26%) increase compared to the base fire CDF for one full reactor-year. The corresponding

increase in the total CDF is 9%. Considering that the fire barriers could only be jeopardized during shutdown, this increase has to be multiplied by the assumed fraction of the year the plant is shutdown (0.05) and is considered not to be significant (<1%).

FSAR Impact:

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

Question 19-202:

Provide additional information on the emergency feedwater system (EFWS) success criteria in the at-power internal events PRA. Specifically:

- a) How many trains of the emergency feedwater system (EFWS) are required for success in various scenarios in the at-power internal events PRA? Provide a summary of the calculations that support these success criteria.
- b) Discuss whether the water in EFWS pools is expected to be exhausted in any scenario, and how the refill operation is modeled in the PRA.
- c) If EFWS success depends on tripping the reactor coolant pumps (RCP), clarify which scenarios require an RCP trip, discuss how the operator action to trip the RCPs is modeled in the PRA, and document any related assumptions.

Response to Question 19-202:

a) For all applicable event sequences, a single EFWS train is sufficient for decay heat removal when steam relief is provided via one or more MSRVs. A single MSRv is sufficient, independent of whether or not RCPs are running, provided that the operating MSRv is connected to at least one SG that is being supplied with EFWS flow (for events where MSIVs are closed, both feed and steam relief must be from the same SG).

If there are no available MSRVs, and steam relief is provided by the MSSVs, then two EFW trains are required for decay heat removal for cases where RCPs are running. One EFW train is sufficient in this case for events where RCPs are tripped.

For LOCA events, RCP pumps will trip, but independently of the RCP status, the success criterion for partial cooldown is single EFWS train via one or more MSRVs. The success criteria for fast cooldown is two EFWS trains via corresponding MSRVs; that could be conservative as discussed in the response to RAI 7, Question 19-60.

The mission success criteria for EFW are based on a variety of MAAP runs encompassing the spectrum of initiating events. The MAAP analysis and benchmarking against S-RELAP5 is described in FSAR Section 19.1.4.1.1.7. The EFWS design capability assumed in MAAP was verified against EFWS hydraulics analysis, which examined the flow rate provided by the EFWS trains for various scenarios including MSRv and MSSV steam relief.

b) There is sufficient inventory in the EFWS pools to allow cooldown to RHR with all RCPs running (additional heat load from RCPs) as well as with all RCPs tripped. The minimum EFWS Storage Pool inventory required for decay heat removal and cooldown to RHR entry conditions for bounding design basis events is protected by Technical Specifications. The availability of makeup water for the EFWS storage pools is not required for EFWS success. The initial available volume of water in the EFW storage pools is over 412,000 gallons. Makeup may be helpful to operational availability by extending the time that the plant can stay at hot standby before commencing cooldown (for example while attempting to restore MFW). However, if makeup is unavailable, then plant operations will begin a cooldown to RHR if EFWS pool inventory drops below the minimum Technical Specification limit. Therefore, makeup to the EFWS storage pools is not explicitly modeled in the PRA, except for the cases where there is a

specific pipe break or a leak in an EFW pool. In these cases, the human action to isolate the break also implicitly includes action to make up to the EFW pools

c) As discussed above, EFWS success does not depend on tripping of the RCPs. Therefore, operator action to trip the RCPs is only modeled for the cases where RCP seal cooling is lost, in the RCP seal LOCA analysis.

FSAR Impact:

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

Question 19-203:

Page 19.1-19 of the FSAR indicates that, as part of the initiating events assessment, a failure modes and effects (FMEA) approach was taken to identify system failures that could affect plant operation. Did this evaluation include (a) spurious actuation of automatic signals and (b) human errors (such as during maintenance)? If so, provide the results of the analysis and discuss how they were incorporated in the PRA. If not, justify the exclusion or amend the PRA and FSAR to include these initiating events.

Response to Question 19-203:

- a) The initiating events assessment includes consideration of spurious actuation of automatic signals. The impact of a spurious actuation is captured within the various initiating events analyzed.

For example, the following spurious operations were considered and implicitly included in the PRA as part of other initiating events.

- IE GT - Spurious actuation of the Reactor Protection System and spurious operation of the Emergency Boration System.
- IE MSSV - Spurious operation (opening) of a secondary steam relief valve.
- IE ISL-CVCS REDS - Spurious opening of the chemical and volume control system (CVCS) reducing station.

Spurious operation of Main Head Safety Injection and Low Head Safety Injection—a spurious safety injection system (SIS) signal—are screened as initiating events because the pumps shutoff head is lower than the Reactor Coolant System (RCS) normal operating pressure and spurious operation is not likely to cause an initiating event.

- b) Human errors during maintenance will be considered after the maintenance procedures and insights from maintenance practice are available.

FSAR Impact:

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

Question 19-204:

Please describe how dependencies between automatic and manual actions (e.g., following a signal failure) have been addressed in the U.S. EPR PRA.

Response to Question 19-204:

Dependencies between automatic and manual actions are not explicitly considered in the U.S. EPR PRA. The PRA credited few manual recovery actions that occur after failure of automatic protective system actions or signals. The human reliability analysis (HRA) contains only a few operator actions of this type. For example, in the at-power PRA:

- There are manual actions to trip reactor coolant pumps (RCP) after either a loss of thermal barrier cooling or after a loss of bearing cooling. These are backups to non-safety-related automatic signals.
- There is a manual reactor trip credited in the PRA. This action is included not because it is a backup to automatic reactor trip, but because it is a rote action taken upon any entry into emergency operating procedures (EOP).
- Manual containment isolation is credited in the Level 2 PRA as a backup to the automatic containment isolation signal.

For these operator actions, the performance shaping factors (PSF) in the SPAR-H human reliability model were assigned 2x or 5x multipliers for stress, in order to account for the operator's expectation of automatic plant response and/or the stress associated with failure of the automatic plant response.

A different approach is taken in the low power shutdown (LPSD) PRA. There are operator actions in the LPSD PRA that are backups to automatic signals. The automated signals associated with these actions are primarily provided by the non-safety-related (NSR) process automation system (PAS). The HRA model used for LPSD is simplified, in that all of the PSFs except those related to timing are assumed to be nominal. As explained in the response to RAI 2, Question 19-18, the "nominal" PSF is recommended for use in SPAR-H when insufficient information is available to determine otherwise. As described in the response to RAI 7 Question 19-72, the HRA will be refined as the human machine interface (HMI), I&C design, and operating guidelines develop during detailed design. COL item 19.1-9 listed in U.S. EPR FSAR Tier 2, Table 1.8-2 is provided to confirm that assumptions used in the PRA remain valid for the as-to-be-operated plant.

FSAR Impact:

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

Question 19-205:

Please discuss how dependencies between pre-initiator human errors have been addressed in the U.S. EPR PRA.

Response to Question 19-205:

Dependencies between pre-initiator human errors were not considered in the U.S. EPR PRA. Such dependencies are a function of test and maintenance procedures.

FSAR Impact:

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

Question 19-206:

(Follow-up to Question 19-56) The response to Question 19-56 indicates that the standstill seal system (SSSS) failure probability of $1.0E-3$ is based on engineering judgment. The SSSS design information provided in the FSAR is not sufficient to determine whether this failure probability is appropriate. Provide the following additional information on the SSSS:

- a) Discussion of the required support systems (e.g., nitrogen supply, power).
- b) Simplified piping and instrumentation diagram (P&ID) that shows the components (e.g, valves, accumulators) needed for system function.
- c) Actuation logic for the SSSS and instrumentation and control (I&C) platform used, with supporting diagrams as appropriate (note that if this actuation signal fits into any of the categories described in Chapter 7 of the FSAR, the FSAR should be revised to include it).

Response to Question 19-206:

- a) Once the reactor coolant pump (RCP) is tripped and comes to a complete stop, the SSSS is actuated. The SSSS requires pressurized nitrogen to physically move the seal into the closed position and electricity to operate the valves which direct the flow of nitrogen and maintain pressure in the system. An accumulator and check valve provides adequate nitrogen pressure to actuate the seal, regardless of the status of the central gas distribution system. All valves required for SSSS actuation, including the RCP seal leak-off lines, are powered from an uninterruptible power supply and the station blackout (SBO) diesel generators. Refer to U.S. EPR FSAR Tier 2, Section 5.4.1.2.1 for further description of the SSSS.
- b) Refer to U.S. EPR FSAR Tier 2, Figure 5.1-4 (Sheet 4) for a P&ID of the SSSS showing components needed for system function.
- c) Actuation of the SSSS is not a safety-related function. It is a function supplied to reduce risk, and the actuation logic is therefore processed by the Process Automation System (PAS), which is described in the U.S. EPR FSAR Tier 2, Section 7.1.1.4.6. The SSSS can also be manually operated from process information and control system (PICS) if the RCP has been tripped and after sufficient delay for coast-down. Automatic actuation, by the PAS, of the SSSS sequence, including RCP trip, is caused by detection of a total loss of seal cooling and by detection of a failed seal number 1 and seal number 2.

The simultaneous loss of the thermal barrier cooling and seal number 1 injection is detected by:

| | | |
|---|-----|----------------------------------|
| High RCP cavity temperature on both of the number 1 seal monitors | | |
| OR | | |
| Low seal water injection flow | AND | High thermal barrier temperature |
| | | OR |
| | | Low thermal barrier flow |

A simultaneous failure of RCP seal number 1 and seal number 2 is detected by:

| |
|--|
| High seal leakage flow rate from seal number 2 for greater than 2 seconds |
| AND |
| The associated seal number 1 leak-off isolation valve is closed (another function closes this isolation valve upon detection of high seal leak-off flow) |

The SSSS actuation sequence for the above conditions proceeds as follows:

- The RCP will trip
- When current transformers indicate no current to the RCP for greater than 15 minutes (allows for RCP coast-down), the SSSS will be actuated for the affected RCP as follows:
 - The associated SSSS atmospheric vent valve will be closed.
 - The associated SSSS nitrogen supply valve will be opened, and the mechanical seal will engage.
 - The seal number 3 leak-off isolation valve will be closed.
 - The seal number 2 leak-off isolation valve will be closed.
 - The seal number 1 leak-off isolation valve will be closed.

Note that the valves and the associated support systems for the SSSS are modeled in the fault trees explicitly. The 1.0E-3 failure probability includes only failure of the actual mechanical seal itself.

FSAR Impact:

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

Question 19-207:

(Follow-up to Question 19-36) The response to Question 19-36 states that “simultaneous loss of AC/DC divisions is very unlikely without a significant spatial impact which is analyzed for the internal hazards.” Provide a quantitative justification for this statement, including a discussion of common-cause failure (CCF) of the electrical buses, considering both active and passive components. Also, discuss how bus failures resulting in fire or explosion can affect other electrical buses in the same fire area.

Response to Question 19-207:

Electrical buses are considered passive components and as such are not considered for common cause failures in the U.S. EPR PRA, as stated in the assumptions in U.S. EPR FSAR Tier 2, Section 19.1.4.1.1.4. Moreover, AC and DC buses are of different type, size, and are located in different rooms. Simultaneous failure due to the loss of a common support system (e.g., HVAC) is explicitly modeled in the PRA.

A bus failure resulting in a fire or an explosion is considered in the fire PRA. Bus failures are included in the generic fire ignition frequencies that are used for the switchgear room fire areas. For each ignition source, the corresponding fire scenario considers that all buses are disabled by the fire.

FSAR Impact:

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

Question 19-208:

After a loss of main feedwater, the startup and shutdown feedwater system (SSS) is credited as a mitigating system. Given that certain failures could disable both main feedwater and the SSS, discuss how dependencies between the two systems are modeled in the U.S. EPR PRA.

Response to Question 19-208:

Dependencies between the main feedwater and the startup and shutdown systems are modeled in the U.S. EPR PRA by including an additional common failure basic event in the SSS fault tree that only shows after a loss of main feedwater (LOMFW) initiating event (CCF-LOMFW/SSS unavailability of 0.2). The value for this basic event is estimated by merging the main feedwater and the startup and shutdown system fault trees. Dependencies between the two systems are based on the common parts of the injection lines. The SSS pump train, that dominates the SSS system unavailability, is independent from the main feedwater (MFW) pumps.

FSAR Impact:

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

Question 19-209:

(Follow-up to Question 19-58) The response to Question 19-58 presents the differences between the various loss of component cooling water system (CCWS) and essential service water system (ESWS) initiating events. However, the success criteria and event tree provided in Appendix 19A of the FSAR treats loss of CCWS or ESWS as a single initiating event. So that the staff can clearly understand the impact of these initiators, amend Appendix 19A to specify the success criteria for each sub-initiator (e.g., in some cases, only two trains may be available; in others, the function may be guaranteed to fail). A single event tree is appropriate if the success criteria tables make clear which top events are applicable for each sub-initiator.

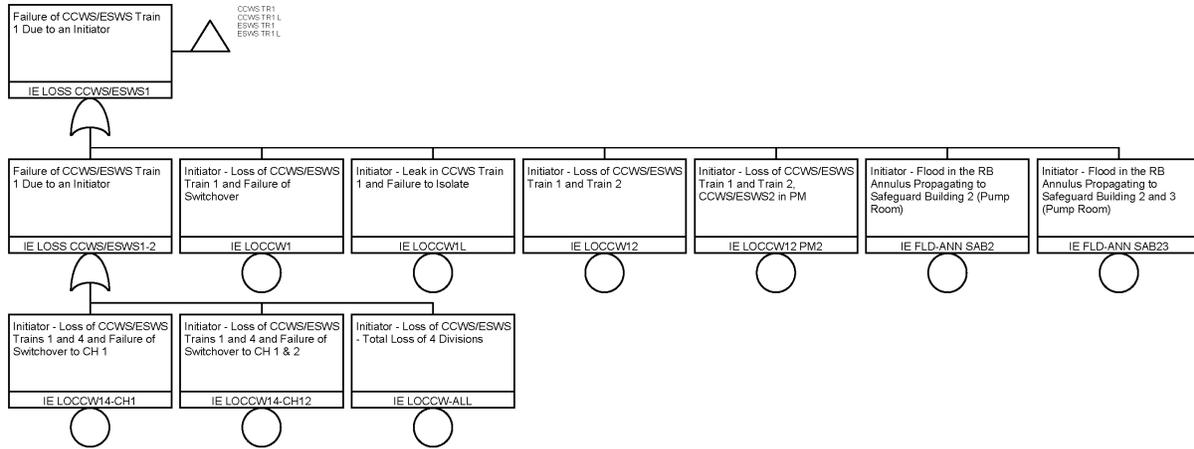
Response to Question 19-209:

For each loss of component cooling water/essential service water (LOCCW/ESW) initiating event, the corresponding support system trains (CCW, ESW) are disabled directly in the fault trees. Since the support systems are not shown directly in the event trees, the same event tree (LOCCW) is used to propagate these events, even for the LOCCW-ALL initiator for which two of the functional events would be a direct failure (MHSI and MHSI 01). Disabling corresponding trains for specific initiating events (IE), as performed in the RiskSpectrum[®], is illustrated in Figure 19-209-1. Figure 19-209-1 illustrates that CCW Train 1 is disabled for IEs LOCCW1, LOCCW1L, LOCCW12, LOCCW12PM, LOCCW14-CH1, LOCCW14-CH12, LOCCW-ALL, and other initiators unrelated to CCS/ESW losses. ESW Train 1 is disabled for the same initiators. This feature of RiskSpectrum[®] allows for a straightforward modeling of the initiating event impact, and simplifies event tree modeling. It is not necessary to include the success criteria for the LOCCW initiating events to Appendix 19A, since the specific impacts of these initiators are defined in their description. These impacts are also defined in the response to RAI 7, Question 19-58 (a).

FSAR Impact:

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

Figure 19-209-1 – Illustration of Disabling Corresponding Trains for Specific Initiating Events



Question 19-211:

Table 19.1-88 of the FSAR indicates that a generic small LOCA frequency was used to develop the shutdown LOCA initiating event frequency. Provide the source and value of this generic small LOCA frequency. Discuss how this frequency was combined with flow diversions and fault tree analysis to develop the initiating event frequencies presented in Table 19.1-90 of the FSAR.

Response to Question 19-211:

The generic small LOCA frequency used to support U.S. EPR FSAR Tier 2, Table 19.1-88, and Table 19.1-90 is a combination of:

- 5.77E-04 per year. This is the SLOCA frequency from Table 8-1 of NUREG/CR-6928 and includes breaks between 0.5 and 2 inches.
- 6.04E-04 per year. This is the LOCA frequency from Table 1 and Figure 1 of NUREG-1829 and includes breaks from 1.625 and 3 inches.

The sum of these is about 1.2E-03 per year and it is considered the generic small LOCA frequency in the U.S. EPR PRA.

The method to combine this frequency with flow diversions and fault tree analysis to develop the values presented in U.S. EPR FSAR Tier 2, Table 19.1-90 is as follows. The generic small LOCA frequency of 1.2E-03 per year was divided by 365 to get a frequency of 3.3E-06 per 24 hours. For each plant operating state (POS), this value was entered into a fault tree under an "OR" gate along with gates and events to represent residual heat removal (RHR) flow diversions through the RHR flow diversion paths identified. This process produced one fault tree (with many subtrees) for each POS. The calculated fault tree unavailability (for 24 hour mission time) is combined with the expected number of days in each POS per year to produce the initiating event frequency for this POS per year.

FSAR Impact:

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

Question 19-212:

(Follow-up to Question 19-143) The response to Question 19-143 lists several valves that, if opened, would allow draining of the RCS to the in-containment refueling water storage tank (IRWST). Discuss how inadvertent opening of these valves by the operators is modeled in the PRA. If such errors are not included in the PRA, justify their exclusion. Describe how the U.S. EPR human factors program (including procedures and training) accounts for the risk associated with inadvertently opening these valves.

Response to Question 19-212:

The valves which can be inadvertently opened by an operator to cause the RCS to drain to the IRWST are the SIS suction MOV and the LHSI mini flow motor operated check valves as defined below for Train 1 (Division 1):

- JNG10AA001 LHSI suction motor operated valve (MOV) from in-containment refueling water storage tank (IRWST).
- JNG10AA003 LHSI radial mini flow motor operated check valve.
- JNG10AA004 LHSI tangential mini flow motor operated check valve.

Spurious operation of these valves is included in the PRA model; inadvertent opening of these valves by the operators is not.

The LHSI suction valve from the IRWST and the mini flow line motor operated check valves are closed under a grouped command associated with RHR train connection and initiation. The operators will have no need to operate these valves in the operating RHR trains. Doing so would be classified as an aggravated error of commission.

As stated in the response to RAI 19-203, human error during maintenance will be considered after the maintenance procedures and insights from maintenance practice are available for review.

The response to RAI 7, Question 19-72 describes the process that is being used to ensure that important human actions, or important assumptions related to the human actions, will be reflected in the human factors program.

FSAR Impact:

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

U.S. EPR Final Safety Analysis Report Markups

detailed fault trees. The level of detail to which the fault trees were developed is consistent with that for comparable analyses for operating nuclear power plants. In some cases, specific design details are not available at the design certification stage. In these cases, if development of the fault trees was affected (e.g., if bounding assumptions had to be made), the treatment is documented in a detailed report.

The fault trees are integrated in two ways:

- Top events for system failures that include a core damage sequence are combined under AND logic, to perform the linking necessary for the quantification process.
- Connections to support systems are modeled in the fault trees, such that common dependencies among the various systems credited in the accident sequence analysis are accounted for in the quantification.

The systems for which detailed fault trees were developed are summarized in Table 19.1-5—Systems Analyzed in U.S. EPR PRA.

A brief description of the major U.S. EPR frontline systems and support systems that are modeled in the PRA is provided below. The differences between the design of the digital I&C systems for the U.S. EPR and that of the I&C systems for currently operating plants are generally greater than they are for other systems. Therefore, a more detailed discussion of the design of the digital I&C system, and the manner in which it is treated in the U.S. EPR PRA, is provided in a separate section that follows. A discussion of system dependencies and their modeling is also provided.

19-196

Failure events and failure modes were screened from the PRA where they met the criteria described in supporting requirement SY-A14 of the 2005 ASME PRA Standard. Contributors to the unreliability or unavailability may be excluded if:

- The total failure probability of the failure mode results in the same effect on system operation and is at least two orders of magnitude lower than the highest failure probability of other components in the same train that have the same effect on system operation.
- The contribution of the failure mode to the failure rate or probability is less than one percent of the total failure rate for the component and the effect on system operation is the same.

Modeling of Inventory Control Systems

Medium Head Safety Injection System

The MHSI PRA-credited function is to provide RCS inventory make-up to ensure adequate core heat transfer for events that result in a loss of RCS inventory. The MHSI consists of four 100-percent capacity, independent trains that are physically separated and protected within their respective Safeguard Buildings (SB). MHSI takes suction