

ArevaEPRDCPEm Resource

From: Pederson Ronda M (AREVA NP INC) [Ronda.Pederson@areva.com]
Sent: Tuesday, July 21, 2009 2:49 PM
To: Tesfaye, Getachew
Cc: BENNETT Kathy A (OFR) (AREVA NP INC); DELANO Karen V (AREVA NP INC); NOXON David B (AREVA NP INC)
Subject: Response to U.S. EPR Design Certification Application RAI No. 252, FSARCh. 19
Attachments: RAI 252 Response US EPR DC.pdf

Getachew,

Attached please find AREVA NP Inc.'s response to the subject request for additional information (RAI). The attached file, "RAI 252 Response US EPR DC.pdf" provides technically correct and complete responses to 2 of the 2 questions.

Appended to this file are affected pages of the U.S. EPR Final Safety Analysis Report in redline-strikeout format which support the response to RAI 252 Questions 19-314 and 19-315.

The following table indicates the respective pages in the response document, "RAI 252 Response US EPR DC.pdf," that contain AREVA NP's response to the subject questions.

Question #	Start Page	End Page
RAI 252 — 19-314	2	2
RAI 252 — 19-315	3	5

This concludes the formal AREVA NP response to RAI 252, and there are no questions from this RAI for which AREVA NP has not provided responses.

Sincerely,

Ronda Pederson

ronda.pederson@areva.com

Licensing Manager, U.S. EPR Design Certification

AREVA NP Inc.

An AREVA and Siemens company

3315 Old Forest Road

Lynchburg, VA 24506-0935

Phone: 434-832-3694

Cell: 434-841-8788

From: Tesfaye, Getachew [mailto:Getachew.Tesfaye@nrc.gov]
Sent: Monday, June 22, 2009 7:36 PM
To: ZZ-DL-A-USEPR-DL
Cc: Phan, Hanh; Clark, Theresa; Fuller, Edward; Mrowca, Lynn; Chowdhury, Prosanta; Colaccino, Joseph; ArevaEPRDCPEm Resource
Subject: U.S. EPR Design Certification Application RAI No. 252 (3058), FSARCh. 19

Attached please find the subject requests for additional information (RAI). A draft of the RAI was provided to you on May 18, 2009, and on June 22, 2009, you informed us that the RAI is clear and no further clarification is needed. As a result, no change is made to the draft RAI. The schedule we have established for review of your application assumes technically correct and complete responses within 30 days of receipt of RAIs. For any

RAIs that cannot be answered within 30 days, it is expected that a date for receipt of this information will be provided to the staff within the 30 day period so that the staff can assess how this information will impact the published schedule.

Thanks,
Getachew Tesfaye
Sr. Project Manager
NRO/DNRL/NARP
(301) 415-3361

Hearing Identifier: AREVA_EPR_DC_RAIs
Email Number: 677

Mail Envelope Properties (5CEC4184E98FFE49A383961FAD402D3101143915)

Subject: Response to U.S. EPR Design Certification Application RAI No. 252, FSARCh.
19
Sent Date: 7/21/2009 2:48:55 PM
Received Date: 7/21/2009 2:49:05 PM
From: Pederson Ronda M (AREVA NP INC)
Created By: Ronda.Pederson@areva.com

Recipients:

"BENNETT Kathy A (OFR) (AREVA NP INC)" <Kathy.Bennett@areva.com>
Tracking Status: None
"DELANO Karen V (AREVA NP INC)" <Karen.Delano@areva.com>
Tracking Status: None
"NOXON David B (AREVA NP INC)" <David.Noxon@areva.com>
Tracking Status: None
"Tesfaye, Getachew" <Getachew.Tesfaye@nrc.gov>
Tracking Status: None

Post Office: AUSLYNCMX02.adom.ad.corp

Files	Size	Date & Time
MESSAGE	2317	7/21/2009 2:49:05 PM
RAI 252 Response US EPR DC.pdf		144685

Options

Priority: Standard
Return Notification: No
Reply Requested: No
Sensitivity: Normal
Expiration Date:
Recipients Received:

Response to

Request for Additional Information No. 252

6/22/2009

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

**QUESTIONS for PRA Licensing, Operations Support and Maintenance Branch 1
(AP1000/EPR Projects) (SPLA)**

Question 19-314:

(Follow-up to Question 19.01-34, Item b) In the response to Question 19.01-34 of RAI 66, AREVA provided the requirements for transferring control of the plant to the remote shutdown station, such that:

- a) the transfer must be in a different fire area than the MCR and within close walking distance from the MCR, and
- b) the transfer must disable the MCR control and provide a seamless transfer to the RSS controls.

The response also stated that "COL item 19.1-9 listed in FSAR Table 1.8-2 is provided to confirm that assumptions used in the PRA remain valid for the as-to-be-operated plant."

Thus, please confirm that the above requirements are clearly documented in EPR DC FSAR and in Table 19.1-109 "U.S. EPR PRA General Assumptions."

Response to Question 19-314:

The remote shutdown station (RSS) capabilities are documented in U.S. EPR FSAR Tier 2, Sections 7.4.1.3.4 and 7.4.2.3.

The following items are considered U.S. EPR design features and will be added to U.S. EPR FSAR Tier 2, Table 19.1-102—U.S. EPR Design Features Contributing to Low Risk, Item 17:

"The following applies toward transferring control from the MCR to the RSS:

- a) The transfer must be in a different fire area than the MCR and within reasonable walking distance from the MCR.
- b) The transfer must disable the MCR control and provide transfer to the RSS controls without loss of control capability."

U.S. EPR FSAR Tier 2, Section 7.4.2.3 will be revised to consistently refer to RSS transfer switches located in a separate "fire area" instead of a separate "fire zone" than the MCR.

FSAR Impact:

U.S. EPR FSAR Tier 2, Table 19.1-102 and Section 7.4.2.3 will be revised as described in the response and indicated on the enclosed markup.

Question 19-315:

(Follow-up to Question 19.01-34, Item e) The credits taken for reducing HEP in the response to Question 19.01-34, Item e, assumes clear indications for abandonment of the MCR. However, the realistic cues for abandoning the MCR may be ambiguous rather than salient. For example, a burning smell without visible smoke or fire due to an overheated computer chip or control board may partially fail the MCR function that may lead to abandonment of the MCR. Since there is neither guidance nor procedure on MCR abandonment, taking credits of low complexity and good training on the scenarios may not be realistic. If HEP values are based on considering performance shaping factors of high stress, obvious diagnosis/nominal action complexity, and high in training as assumed in AREVA's response, the HEP total value could be:

- $HEP(\text{total}) = HEP(\text{diagnosis}) + HEP(\text{action})$
- $HEP(\text{diagnosis}) = 1.0E-2 * 2 * 0.1 * 0.5 = 1.0E-3$
- $HEP(\text{action}) = 1.0E-3 * 2 * 1.0 * 0.5 = 1.0E-3$
- $HEP(\text{Total}) = 2.0E-3$

The credits of obvious diagnosis, high in training, as well as extra time available can be taken if the cues for making decisions are salient and included in operator training. Please recalculate the HEP value to take into consideration the discussion above or justify that the calculated HEP value of $7E-5$ is reasonable.

Response to Question 19-315:

Cues; performance shaping factors (PSF); and consequences of failure, relative to the action of abandoning the main control room, are addressed below. This information justifies that the human error probability (HEP) value for main control room (MCR) evacuation used in the U.S. EPR FSAR probabilistic risk assessment (PRA) model is reasonable.

Action Cues: The design basis of the remote shutdown station (RSS) is to provide the capability for remote shutdown of the plant if the MCR becomes uninhabitable. The RSS is not intended to be a backup I&C system in case of MCR instrumentation and controls (I&C) failure. Therefore the MCR is not likely to be evacuated because there is a "burning smell," or "an overheated computer chip or control board" that may "partially fail the MCR function." The MCR I&C systems (process information and control system (PICS) and safety information and control system (SICS)) have sufficient redundancy and diversity to survive limited failures. Therefore the abandonment criteria for the MCR will be related to habitability, not I&C function, and the criteria will be unambiguous.

Action Complexity and Training PSF: Details of the specific RSS and transfer design, MCR abandonment procedures, and training will be developed later in the design process. Therefore, the selection of PSFs other than "nominal" for this action relied upon the assumptions addressed in the Response to RAI 66, Question 19.01-34. Complexity is assumed to be "obvious" for the diagnosis (and "nominal" for the action) because the cues for this action will not be ambiguous. Training is assumed to be "high" for the action (and "nominal" for the diagnosis) because it is reasonable to assume that the operators will be well trained for the MCR evacuation. Procedures that specifically deal with the decision to abandon the MCR and activate the RSS will be in place before the initial plant criticality.

Action Timing PSF: This PSF accounts for the main difference in the HEP numbers presented in the U.S.EPR FSAR PRA. The assumed action timing is a function of the relative timing between the MCR abandonment cue and the postulated initiating event caused by the fire. It is not possible to predict the relative timing of these two occurrences. The postulated initiating event (conservatively assumed in the PRA to be loss of balance of plant (LBOP)) may occur due to the impact that the MCR fire has upon non-safety-related systems, or it may occur as a consequence of the operators tripping the plant before exiting the MCR.

If the MCR evacuation cue occurs before the initiating event, then there is no urgency for the operator action until the initiating event occurs. On the other hand, if the initiating event occurs before the MCR evacuation cue, then the operators will continue actions to mitigate the initiating event from the MCR until it is no longer possible. Therefore, the human reliability analysis (HRA) model is based on the worst-case timing coincidence, which is that the initiating event and the MCR evacuation cue occur simultaneously. In addition, the overall time window for the MCR evacuation is also conservatively chosen to coincide with the timing of a worst-case operator mitigating action that might be required for a LBOP initiating event. As described in the Response to RAI 66, Question 19.01-34 item a, the 90 minute time window used to calculate this HEP is based on the operator action to restore core cooling via feed-and-bleed (F&B) following the postulated LBOP.

This time window is conservative for the MCR fire because it does not credit the emergency feedwater system (EFWS), which if available would extend the time window for RSS transfer. The realistic time window is much longer than the assumed 90 minutes because loss of the MCR I&C systems (PICS and/or SICS) does not prevent the automatic actuation of the EFWS by the safety-related protection system, whose automated functions are not dependent on PICS and SICS. The protection system is located in the Safeguards Buildings, with divisional independence and separation, and remains available during fires. There is no need to change the timing PSFs as assumed in the U.S. EPR FSAR PRA HEP calculations and presented in the Response to RAI 66, Question 19.01-34 (“expansive time” for diagnosis and “extra time” for action).

A sensitivity analysis is performed to quantitatively support the above discussion. Three different HEPs are used depending on the status of the EFWS, as follows:

- If no EFWS is available (failure of all four emergency feedwater (EFW) trains), the HEP of 2E-3 as suggested in the question is used as bounding.
- If at least one (but not all) EFW train is available, the EFWS train could supply the steam generators for at least six hours before an operator action is needed. During that time, the current PSF of “expansive time” for diagnosis and “extra time” for action would still apply and the HEP of 7E-5 is retained.
- If all EFW trains are available, then the PRA does not credit any operator actions in the 24 hours of mission time. During that time, it is extremely likely that control of the plant would be recovered.

This sensitivity case shows a core damage frequency (CDF) of 6.2E-9/year, which is less than the current CDF of 2.5E-8/year for that initiating event. Therefore, it is estimated that the treatment of this fire scenario is conservative and an update of the U.S. EPR FSAR is not warranted.

Based on the PRA assumption of a 15 minute median time to complete the action (MCR evacuation and RSS transfer), the following will be added to U.S. EPR FSAR Tier 2, Table 19.1-109, Item 74 to support this HEP:

"It is assumed that the time needed to transfer control from the MCR to the RSS will be approximately 15 minutes or less and that there will be a procedure for MCR evacuation, which will contain clear abandonment criteria and instructions for transfer of control to the RSS."

This HEP represents a risk-significant operator action (see U.S. EPR FSAR Tier 2, Tables 19.1-69 and 19.1-70) and will be tracked in accordance with the human reliability analysis (HRA) / human factors engineering (HFE) integration plan described in U.S. EPR FSAR Tier 2, Section 18.6. If needed, feedback from these activities and updates to the HRA will be performed based on the PRA maintenance and upgrade process described in U.S. EPR FSAR Tier 2, Section 19.1.2.4.

FSAR Impact:

U.S. EPR FSAR Tier 2, Table 19.1-109 will be revised as described in the response and indicated on the enclosed markup.

U.S. EPR Final Safety Analysis Report Markups

Table 19.1-102—U.S. EPR Design Features Contributing to Low Risk
Sheet 7 of 7

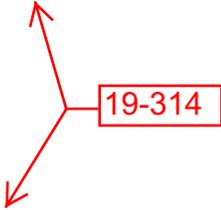
No	U.S. EPR Design Feature Description	Disposition
<p>17</p>	<p>The remote shutdown workstation is in a fire and flood area separate from the main control room.</p> <p>Although a main control room fire may defeat manual actuation of equipment from the main control room, it will not affect the automatic functioning of safe shutdown equipment via the PS or manual operation from the remote shutdown station. Sufficient instrumentation and control is provided at the remote shutdown station to bring the plant to safe shutdown conditions in case the control room must be evacuated. There are no differences between the main control room and remote shutdown workstation controls and monitoring that would be expected to affect safety system redundancy and reliability. <u>The following applies toward transferring control from the MCR to the RSS:</u></p> <ul style="list-style-type: none"> • <u>The transfer must be in a different fire area than the MCR and within reasonable walking distance from the MCR.</u> • <u>The transfer must disable the MCR control and provide transfer to the RSS controls without loss of control capability.</u> 	<p>Tier 2, Section 3.4.3.4; Tier 2, Section 9.5.1.2.1; Tier 2, Section 7.4.1.3; Tier 2, Section 7.4.2.3</p> <div style="text-align: center;">  <p>19-314</p> </div>
<p>18</p>	<p>MCR & RSS ventilation systems</p> <p>The main control room has its own ventilation system, and is pressurized. This prevents smoke, hot gases, or fire suppressants originating in areas outside the control room from entering the control room via the ventilation system. The ventilation system for the remote shutdown workstation is independent of the ventilation system for the main control room.</p>	<p>Tier 2, Section 6.4.2.4; Tier 2, Section 9.4.1.3</p>
<p>19</p>	<p>Seismic margins analysis</p> <p>The plant level HCLPF is ≥ 1.67 SSE, where the SSE is defined by the Certified Design Response Spectra (CSDRS), and there are no spatial seismic interaction issues. Differences between the as-built plant and the design used as the basis for the U.S. EPR FSAR seismic margins analysis will be reviewed.</p>	<p>COL Item 19.1-6; COL Item 19.1-9</p>
<p>20</p>	<p>Instrumentation through RPV top head</p> <p>The U.S. EPR location of the RPV instrumentation which is through RPV top head not lower head, reduces likelihood of LOCA during maintenance</p>	<p>Tier 2, Section 5.3.3.1.1</p>

Table 19.1-109—U.S. EPR PRA General Assumptions
Sheet 14 of 16

No.	Category ¹	PRA General Assumptions ²
73	Fire	The U.S. EPR RCPs will be fitted with an oil-collection system designed to prevent RCP oil leakage from reaching any ignition source. Because of this improved design, it is assumed that fire ignition due to RCP oil leakage reaching an ignition source does not occur.
74	Fire	<p>A fire in the MCR is assumed to disable the entirety of the MCR if it is not suppressed. This will happen if a fire affects either the functional capability of the MCR (destroying cables or workstations) or if it degrades the habitability to an extent where operators have to evacuate the control room. A corresponding operator action is associated with the entire process, including the decision to evacuate the MCR and the action of switching controls. It is assumed that once the operators resume control of the plant from the RSS, the status of the plant will be similar as that following a Loss of Balance of Plants (LBOP) since the fire in the MCR could result in a loss of control of secondary side balance of plant systems. Failure of the operators to transfer to the RSS is assumed to lead directly to core damage. The RSS is assumed to be available in all POS where fuel is loaded to the core. <u>It is assumed that the time needed to transfer control from the MCR to the RSS will be approximately 15 minutes or less and that there will be a procedure for MCR evacuation, which will contain clear abandonment criteria and instructions for transfer of control to the RSS.</u></p>
75	Fire	For the CSR and MCR, the generic room fire ignition frequency is modified by using the 0.5 correction factor to account for the fact that most of the cables routed through the CSR and MCR will be fiber optic cables that are not susceptible to ignition under any condition.
76	Fire	The consequences of the spurious opening of an MSRIV are dependent on the position of the MSIV, with higher consequences corresponding to an open MSIV. The MSIVs are designed to fail closed in the case that their associated SOVs are de-energized. However, hot shorts may still cause one or more MSIVs to remain open. It is conservatively assumed that if there is a fire in the valve room that causes a spurious opening of an MSRIV, it could affect MSIV on the same location, even though there is approximately 14 feet of spatial separation between the MSRIV and MSIV. Based on engineering judgment, it is assumed that a fire affecting an MSRIV would cause its associated MSIV to fail open with a probability of 0.5 and independently cause the other MSIV in the same Valve Room to fail open with a probability of 0.1. Since this modeling was finalized, fire barriers were added in each of the two main steam/main feedwater valve rooms to separate Division 1 from Division 2 and Division 3 from Division 4. This separation would prevent any fire impact on the second MSIV.

19-315



of the EBS is controlled by division 1 of the SAS and the other train is controlled by division 4 of the SAS. A single failure in the EBS system or in the SAS will not prevent the execution of safety functions of the EBS.

The RSS is located in separate physical locations other than the MCR. The RSS control transfer switches will disable MCR controls and enable control functions from the RSS. The transfer switches also provide isolation between the RSS and the MCR. Therefore, no single credible event will cause the MCR to be evacuated and cause the RSS to malfunction.

A failure within the safety-related I&C systems will not lead to design basis accident events even during maintenance or periodic testing.

7.4.2.2.4 Testing

Self and periodic testing of the safety-related I&C systems is implemented to detect failures that could prevent the execution of the safety-related functions.

Measures are taken to detect and identify failures during reactor operation in order to avoid long periods of operation with degraded safety-related I&C systems, structures, and components which might lead to a loss of function due to an accumulation of failures.

7.4.2.3 Remote Shutdown Capability

The RSS provides the capability to remotely shutdown the plant. The RSS transfer switches are located in a separate fire zone area than the MCR to allow transfer of control without entry into the MCR. Alarms in the MCR will alert operators that control is transferred to the RSS. Parameter indications common to both the MCR and RSS are maintained throughout the transfer of control.

19-314

The RSS contains controls and indications that will allow the operators to control and monitor the safe shutdown systems. Controls and indications of permissive signals are provided in the RSS. The capability to manually validate permissives allows the operator to enable or disable protective functions that may be necessary for proper shut down of the plant.

Administrative controls are provided to prevent unauthorized access to the RSS. The RSS transfer switches are key locked. Keys are maintained by appropriate plant personnel.

7.4.2.4 Loss of Plant Instrument Air Systems

The safety-related I&C necessary for safe shutdown are not reliant on instrument air. Any devices that use instrument air fail in a safe position upon loss of air. Section 9.3.1 describes the plant instrument air system.