

## ArevaEPRDCPEm Resource

---

**From:** Tesfaye, Getachew  
**Sent:** Tuesday, May 25, 2010 8:07 PM  
**To:** Le, Hien; DeMarshall, Joseph; Kowal, Mark; Hearn, Peter; Colaccino, Joseph;  
ArevaEPRDCPEm Resource  
**Subject:** FW: Draft RAI 315 Supplement 1 for review  
**Attachments:** Batch 315 Supplement 1 DRAFT for NRC review-.pdf

---

**From:** BRYAN Martin (EXT) [mailto:Martin.Bryan.ext@areva.com]  
**Sent:** Tuesday, May 25, 2010 6:45 PM  
**To:** Tesfaye, Getachew  
**Cc:** RYAN Tom (AREVA NP INC); GARDNER George Darrell (AREVA NP INC); ROMINE Judy (AREVA NP INC)  
**Subject:** Draft RAI 315 Supplement 1 for review

Getachew,

Attached is a draft of RAI 315 Supplement 1 for your review. AREVA would like to interact with the NRC staff after they have had the opportunity to review in order to address any remaining questions.

Thanks,

Martin (Marty) C. Bryan  
U.S. EPR Design Certification Licensing Manager  
AREVA NP Inc.  
Tel: (434) 832-3016  
702 561-3528 cell  
[Martin.Bryan.ext@areva.com](mailto:Martin.Bryan.ext@areva.com)

**Hearing Identifier:** AREVA\_EPR\_DC\_RAIs  
**Email Number:** 1460

**Mail Envelope Properties** (0A64B42AAA8FD4418CE1EB5240A6FED1134504C9C7)

**Subject:** FW: Draft RAI 315 Supplement 1 for review  
**Sent Date:** 5/25/2010 8:06:33 PM  
**Received Date:** 5/25/2010 8:06:34 PM  
**From:** Tesfaye, Getachew

**Created By:** Getachew.Tesfaye@nrc.gov

**Recipients:**

"Le, Hien" <Hien.Le@nrc.gov>  
Tracking Status: None  
"DeMarshall, Joseph" <Joseph.DeMarshall@nrc.gov>  
Tracking Status: None  
"Kowal, Mark" <Mark.Kowal@nrc.gov>  
Tracking Status: None  
"Hearn, Peter" <Peter.Hearn@nrc.gov>  
Tracking Status: None  
"Colaccino, Joseph" <Joseph.Colaccino@nrc.gov>  
Tracking Status: None  
"ArevaEPRDCPEm Resource" <ArevaEPRDCPEm.Resource@nrc.gov>  
Tracking Status: None

**Post Office:** HQCLSTR02.nrc.gov

| <b>Files</b>                                     | <b>Size</b> | <b>Date &amp; Time</b> |
|--|-------------|------------------------|
| MESSAGE  | 735         | 5/25/2010 8:06:34 PM   |
| Batch 315 Supplement 1 DRAFT for NRC review-.pdf |             | 472763                 |

**Options**

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

**Response to**

**Request for Additional Information No. 315 (3878), Revision 0, Supplement 1**

**11/18/2009**

**U. S. EPR Standard Design Certification**

**AREVA NP Inc.**

**Docket No. 52-020**

**SRP Section: 16 - Technical Specifications**

**Application Section: TS 3.3**

**QUESTIONS for Technical Specification Branch (CTSB)**

**DRAFT**

**Question 16-318:****OPEN ITEM****Follow-up to RAI 103, Question 16-137.**

In RAI-SRP16-CTSB-103/137, the staff requested a technical justification regarding the omission of safety-related Reactor Trip (RT) signals in Table 3.3.1-2, Section A (Reactor Trip). FSAR Section 7.2.1.2 identifies the Safety Injection System (SIS) Actuation, Emergency Feedwater System (EFWS) Actuation, and the Manual RT signals from the Safety Information and Control System (SICS), as safety-related RT initiation signals. The applicant concludes that these RT initiation signals should not be included in Technical Specifications on the basis that 1) they are not credited in the EPR safety analysis as implied by their absence from Chapter 15 Tables 15.0-7 and 15.0-8, and 2) they do not satisfy Criterion 3 of 10 CFR 50.36 with regard to being part of the primary success path of a safety sequence analysis. NUREG-1431 includes both the Manual RT and the SIS Actuation initiation signals in comparable LCO 3.3.1, Reactor Trip System Instrumentation. The Manual RT initiation ensures that the control room operator has the capability to initiate a reactor trip at any time. This capability is critical whenever a parameter is rapidly trending toward its Trip Setpoint. Regarding the SIS Actuation, NUREG-1431 Bases B 3.3.1 specifically states that initiation of a reactor trip upon any signal that initiates a safety injection is a condition of acceptability for the LOCA. The EFWS Actuation is the primary success path which functions to mitigate the effects of a loss of Main Feedwater (MFW) event, providing a safety classified means to remove residual heat via the steam generators (SGs). FSAR Section 7.3.1.2.2 identifies a number of failure mechanisms that can result in a loss of MFW, including a Loss of Offsite Power, which is a highly credible event. In addition, it remains unclear how the applicant intends to ensure that surveillance testing requirements associated with the referenced safety-related trip signals will be met if they are not included in the Technical Specifications. The staff finds that the response does not provide the requisite technical justification to warrant exclusion of the safety-related RT initiation signals from Technical Specifications. This issue has been identified as an open item in the SER w/OI for Chapter 16 of the EPR FSAR

**Response to Question 16-318:**

This issue was further clarified on Page 16-20 of the NRC's March 10, 2010 Safety Evaluation, which states:

- In RAI 103, Question 16-137, the staff requested that the applicant provide a technical justification regarding the omission of safety-related RT signals in FSAR Tier 2, Table 3.3.1-2, Section A. FSAR Tier 2, Section 7.2.1.2, "Reactor Trip Functional Description," identifies the Safety Injection System (SIS) Actuation, Emergency Feedwater System (EFWS) Actuation, and the Manual RT signals from the Safety Information and Control System (SICS), as safety-related RT initiation signals. In a March 19, 2009, response to RAI 103, Question 16-137, the applicant concluded that these RT initiation signals should not be included in TS on the basis that (1) they are not credited in the U.S. EPR safety analysis as implied by their absence from FSAR Tier 2, Chapter 15, "Transient and Accident Analyses," FSAR Tier 2, Tables 15.0-7 and 15.0-8, and (2) they do not satisfy Criterion 3 of 10 CFR 50.36 with regard to being part of the primary success path of a safety-sequence analysis. NUREG-1431 includes both the Manual RT and the SIS Actuation initiation signals in comparable LCO 3.3.1, Reactor Trip System Instrumentation. The Manual RT

initiation ensures that the control room operator has the capability to initiate a reactor trip at any time. This capability is critical whenever a parameter is rapidly trending toward its Trip Setpoint. Regarding the SIS Actuation, NUREG-1431, Bases B 3.3.1 specifically states that initiation of a reactor trip upon any signal that initiates a safety injection is a condition of acceptability for the loss-of-coolant accident (LOCA). The EFWS Actuation is the primary success path, which functions to mitigate the effects of a loss of Main Feedwater (MFW) event, providing a safety classified means to remove residual heat via the steam generators. FSAR Tier 2, Section 7.3.1.2.2, "Emergency Feedwater System Actuation," identifies a number of failure mechanisms that can result in a loss of MFW, including a loss of offsite power, which is a highly credible event. In addition, it remains unclear how the applicant intends to ensure that surveillance testing requirements associated with the referenced safety-related trip signals will be met if they are not included in the TS. The staff determined that the response does not provide the requisite technical justification to warrant exclusion of the safety-related RT initiation signals from TS.

Due to similarities in the two NRC Questions, this response will address both 16-318 and 16-319. This response supersedes AREVA's previous responses to RAI 103, Questions 16-137 and 16-160.

#### BACKGROUND

As specified in NUREG-0800, *Standard Review Plan, Section 16.0, Technical Specifications*:

10 CFR 52.47(a)(11) and 52.79(a)(30) provides that a design certification (DC) applicant and an combined license (COL) applicant are to propose Technical Specifications (TS) prepared in accordance with 10 CFR 50.36 and 50.36a. COL applicants that reference a certified plant design should propose TS based on the TS approved during the design certification (DC) review. The certified generic TS serve as the standard TS for the certified NSSS design.

As previously discussed in the response to RAI 103, Question 16-137:

The required content of the Technical Specifications is specified in 10 CFR 50.36. The U.S. EPR Protection System and its reactor trip isolation signals satisfy Criterion 3 of 10 CFR 50.36:

"A structure, system, or component that is part of the primary success path and which functions or actuates to mitigate a design basis accident or transient that either assumes the failure of or presents a challenge to the integrity of a fission product barrier."

As discussed in the Final Policy Statement on Technical Specifications Improvements for Nuclear Power Plants (FR Doc. 93-17344):

"Discussion of Criterion 3: A third concept in the adequate protection of the public health and safety is that in the event that a postulated Design Basis Accident or Transient should occur, structures, systems, and components are available to function or to actuate in order to mitigate the consequence of the Design Basis Accident or Transient. Safety sequence analyses or their equivalent have been

performed in recent years and provide a method of presenting the plant response to an accident. These can be used to define the primary success paths.

A safety sequence analysis is a systematic examination of the actions required to mitigate the consequences of events considered in the plant's Design Basis Accident and Transient analyses, as presented in Chapters 6 and 15 of the plant's FSAR (or equivalent chapters). Such a safety sequence analysis considers all applicable events, whether explicitly or implicitly presented. The primary success path of a safety sequence analysis consists of the combination and sequences of equipment needed to operate (including consideration of the single failure criteria), so that the plant response to Design Basis Accidents and Transients limits the consequences of these events to within the appropriate acceptance criteria.

It is the intent of this criterion to capture into Technical Specifications only those structures, systems, and components that are part of the primary success path of a safety sequence analysis. Also captured by this criterion are those support and actuation systems that are necessary for items in the primary success path to successfully function. The primary success path for a particular mode of operation does not include backup and diverse equipment (e.g., rod withdrawal block which is a backup to the average power range monitor high flux trip in the startup mode, safety valves which are backup to low temperature overpressure relief valves during cold shutdown)."

#### BASIS FOR U.S EPR PROTECTION SYSTEM TECHNICAL SPECIFICATONS

In order to clarify the fundamental differences between the proposed U.S. EPR Protection System Technical Specifications and the Westinghouse Standard Technical Specifications for reactor trip and ESF functions, it should be noted that the proposed U.S. EPR Protection System Technical Specifications are component-based and address the components necessary for reactor trip and ESFAS functions. The Westinghouse Standard Technical Specifications are function-based and provide several LCOs for the reactor trip and ESF functions. This change in approach was necessary since:

1. In the Protection System, sensors and signal processors support multiple functions. Since failures in the plant would occur on a component basis, a component-based Technical Specification approach was determined to be advantageous since it specifies the required actions for the operators based on what component(s) have failed. Functional based Technical Specifications for the U.S. EPR Protection System would require additional operator analysis to determine what functions are affected by the failed component, which could delay implementation of the required actions. Delays would be especially important if the required action is to be taken immediately.
2. The Protection System for the U.S. EPR performs both the reactor trip and ESF functions. In many cases the same sensors and signal processors are utilized in both reactor trip and ESF functions. The Protection System Technical Specifications consist of one single Limiting Condition for Operation (LCO). Utilizing several LCOs, as is used in the Westinghouse Standard Technical Specifications, would result in needless duplications and could potentially result in conflicting requirements.

U.S. EPR FSAR Tier 2 Chapter 16 Limiting LCO 3.3.1 requires specific Protection System sensors, manual actuation switches, signal processors, and actuation devices to be operable. Thus, surveillance testing of these components is used in a series of sequential, overlapping or total divisional steps to ensure the operability of the Protection System, including the credited reactor trip and ESF functions that the system performs. The Protection System components that are required to be operable and the required surveillance testing for each component are specified in U.S. EPR FSAR Tier 2 Chapter 16, Technical Specifications, Table 3.3.1-1, *Protection System Sensors, Manual Actuation Switches, Signal Processors, and Actuation Devices*. The required number of components, required modes, and surveillance testing specified for each component envelopes the requirements for the credited reactor trip and ESF functions supported by each component. A summary of the generic strategy for periodic surveillance testing of the Protection System was provided in response to RAI 103, Question 16-193. In the Westinghouse Standard Technical Specification, required modes and surveillances are specified on a function by function basis. Both approaches ensure that reactor trip and ESF functions will maintain the Safety Limits during all design basis events and anticipated operational occurrences in the required modes.

However, as a result of the component-based approach taken for the U.S. EPR Protection System Technical Specifications, the listing of functions in U.S. EPR FSAR Tier 2 Chapter 16, Technical Specifications, Table 3.3.1-2, *Acquisition and Processing Unit Requirements Referenced from Table 3.3.1-1*, does not serve the same purpose as the listing of reactor trip and ESF functions in the function-based Westinghouse Standard Technical Specifications. In the Westinghouse Standard Technical Specifications, LCOs 3.3.1, "Reactor Trip System (RTS) Instrumentation," 3.3.2, "Engineered Safety Feature Actuation System (ESFAS) Instrumentation," 3.3.5, "Loss of Power (LOP) Diesel Generator (DG) Start Instrumentation," LCO 3.3.6, "Containment Purge and Exhaust Isolation Instrumentation," LCO 3.3.7, "Control Room Emergency Filtration System (CREFS) Actuation Instrumentation," 3.3.8, "Fuel Building Air Cleanup System (FBACS) Actuation Instrumentation," and 3.3.9, "Boron Dilution Protection System (BDPS)," require "instrumentation for each Function" to be operable and surveillances are specified on a function by function basis. As discussed above, the U.S. EPR Protection System Technical Specifications requires the specific Protection System sensors, manual actuation switches, signal processors, and actuation devices specified in Table 3.3.1-1 to be operable. Table 3.3.1-2 is referenced from Table 3.3.1-1 and is only entered when the number of operable Acquisition and Processing Units (APUs) drops below the minimum number required for functional capability. There were two purposes served by including the listing of reactor trip and ESF functions in Table 3.3.1-2 of the U.S. EPR Technical Specifications when they were originally developed:

- The primary purpose for Table 3.3.1-2 was to provide the location for setpoint values for the specific reactor trip and ESF functions. 10 CFR 50.36(d) states that the Technical Specifications will include items in the following categories: (1) Safety limits, limiting safety system settings, and limiting control settings. Regulatory Guide 1.105, *Setpoints for Safety-Related Instrumentation*, Revision 3, Regulatory Position C.3 states:

Section 4.3 of ISA-S67.04-1994 states that the limiting safety system setting (LSSS) may be maintained in technical specifications or appropriate plant procedures. However, 10 CFR 50.36 states that the technical specifications will include items in the categories of safety limits, limiting safety system settings,

and limiting control settings. Thus, the LSSS may not be maintained in plant procedures. Rather, the LSSS must be specified as a technical-specification-defined limit in order to satisfy the requirements of 10 CFR 50.36. The LSSS should be developed in accordance with the setpoint methodology set forth in the standard, **with the LSSS listed in the technical specifications.** (Emphasis added)

The U.S. EPR utilizes a digitally-based Protection System. In the U.S. EPR, setpoints are not physically adjusted parameters in hardwired components. Rather, the setpoints are values programmed into the software contained in the APU. Hence, the setpoints for each function performed by the APU are listed in the table that contains the required actions (Conditions) for the APUs. Thus, Table 3.3.1-2 satisfies the legal requirements for including setpoints in the Technical Specifications and would require the APU associated with the function to be declared inoperable if the setpoint for the function was determined to be incorrect or programmed into the APU incorrectly.

There are five APUs in each division of the Protection System (APUs A1, A2, A3, B1, and B2). Reactor trip and ESF functions are allocated amongst the five APUs as part of the detailed design process. The functions performed by each APU are the same for that APU in each division (i.e., APU A1 performs the same functions in each of the four divisions). Table 3.3.1-2 specifies that three divisions of APUs are required for the performance of each function. The structure of Table 3.3.1-2 implicitly allows a different APU to be inoperable in each division as long as three of the same APUs are operable (i.e., it is permissible to have APU A1 inoperable in Division 1, APU A2 inoperable in Division 2, and APU A3 inoperable in Division 3, since there are always three divisions of APUs operable for each function). Thus, inclusion of Table 3.3.1-2 provides flexibility in requiring three divisions of APUs be operable to support each function, while not requiring the functions to be performed by each APU to be specified at this time.

In practical terms, if the setpoints were relocated out of Table 3.3.1-2 (e.g., using a Setpoint Control Program type approach), Table 3.3.1-2 could be deleted and required actions for inoperable APUs could be specified in Table 3.3.1-1. This is the approach taken for Actuation Logic Units (ALUs) in Table 3.3.1-1. There would only be a loss in flexibility in that the failure of different APUs in different divisions (as described in the second bullet, above) would not be permitted without entering a Condition.

Additional discussions regarding the Reactor Trip on Safety Injection System (SIS) Actuation, Reactor Trip on Emergency Feedwater System (EFWS) Actuation, Manual Reactor Trip, and Emergency Feedwater System (EFWS) Isolation on High SG Level (Affected SGs) Engineered Safety Features Actuation System (ESFAS) functions discussed in the NRC's Questions are provided below:



## SPECIFIC FUNCTIONS DISCUSSED BY NRC

### **Reactor Trip on Safety Injection System (SIS) Actuation**

In the follow-up question, the NRC states that:

FSAR Section 7.2.1.2 identifies the Safety Injection System (SIS) Actuation as a safety-related Reactor Trip initiation signal. ...

NUREG-1431 includes both the Manual Reactor Trip and the SIS Actuation initiation signals in comparable LCO 3.3.1, Reactor Trip System Instrumentation. ... NUREG-1431 Bases B 3.3.1 specifically states that initiation of a reactor trip upon any signal that initiates a safety injection is a condition of acceptability for the LOCA. ...

In addition, it remains unclear how the applicant intends to ensure that surveillance testing requirements associated with the referenced safety-related trip signals will be met if they are not included in the Technical Specifications.

The Reactor Trip on SIS Actuation is a safety related design feature of the U.S. EPR. It is described in U.S. EPR FSAR Tier 2 Section 7.2.1.2.20 and is depicted in Figure 7.3-2. Section 7.2 reflects the design of the U.S. EPR Protection System. The Protection System design includes features that are not credited in the safety analysis. If the Reactor Trip on SIS Actuation function was deleted from the U.S. EPR design, there would be no impact to the safety analysis as summarized in Chapter 15 of the U.S. EPR FSAR. 10 CFR 50.36, Criterion 3, does not require safety related design features to be incorporated into the Technical Specifications unless the design features are credited in the safety analysis.

While AREVA has no direct knowledge of the proprietary safety analysis that supports the Westinghouse Standard Technical Specifications, AREVA assumes that the Westinghouse Standard Technical Specifications reflect the safety analysis Westinghouse used to support its design. The safety analysis used by AREVA for the U.S. EPR is summarized in U.S. EPR FSAR Tier 2 Chapter 15. Specifically, the analysis of Loss of Coolant Accidents (LOCAs) resulting from the spectrum of postulated piping breaks within the reactor coolant pressure boundary are summarized in U.S. EPR FSAR Tier 2 Section 15.6.5. The following reactor trip functions are credited to mitigate LOCAs in the U.S. EPR safety analysis:

- Low Pressurizer Pressure,
- Low Hot Leg Pressure, and
- High Containment pressure.

The Reactor Trip on SIS Actuation is not credited in the U.S. EPR safety analysis to mitigate the consequences of a LOCA. 10 CFR 50.36 requires an applicant's Technical Specifications to reflect its safety analysis. It does not require an applicant to incorporate functions in its Technical Specifications that another vendor assumed in their safety analysis. Incorporation of functions included by Westinghouse in their Standard Technical Specification into the U.S. EPR Technical Specifications is not supported by the requirements specified in 10 CFR 50.36 with regards to the content of U.S. EPR Technical Specifications.

With regards to surveillance testing, there are three Engineered Safety Features Actuation System Signals associated with Safety Injection System (SIS) actuation listed in the U.S. EPR Protection System Technical Specifications:

- SIS Actuation on Low Pressurizer Pressure,
- SIS Actuation on Low Delta Psat, and
- SIS Actuation on Low RCS Loop Level.

The sensors necessary to detect the conditions that necessitate an SIS actuation, the signal processors that generate the SIS actuation signal, and their surveillance requirements are listed in Table 3.3.1-1 of the Protection System Technical Specifications. Also included is a surveillance requirement to periodically verify the setpoints have been properly loaded into the signal processors. Similarly, the sensors, signal processors, and actuation devices necessary to perform reactor trip functions are also listed in Table 3.3.1-1 of the Protection System Technical Specifications. While the Reactor Trip on SIS Actuation function is not required to be included in the U.S. EPR Technical Specifications, the components necessary to perform this function and the verification of the actuation setpoints are already the subject of other surveillance requirements for other credited functions.

In addition, U.S. EPR FSAR Tier 2 Table 1.8-2 contains U.S. EPR Combined License Information Item 13.5-5, which requires a Combined License applicant that references the U.S. EPR design certification provide site-specific information for administrative, operating, emergency, maintenance, and other operating procedures. Information regarding testing procedures not required to be included in the Technical Specifications may be requested from the Combined License applicant.

### **Reactor Trip on Emergency Feedwater System (EFWS) Actuation**

The logic for not including the Reactor Trip on EFWS Actuation in the U.S. EPR Technical Specifications is generally the same as that for the Reactor Trip on SIS Actuation discussed above.

In the follow-up question, the NRC states that:

FSAR Section 7.2.1.2 identifies the EFWS Actuation as a safety-related Reactor Trip initiation signal. ...

The EFWS Actuation is the primary success path which functions to mitigate the effects of a loss of Main Feedwater (MFW) event, providing a safety classified means to remove residual heat via the steam generators (SGs). FSAR Section 7.3.1.2.2 identifies a number of failure mechanisms that can result in a loss of MFW, including a Loss of Offsite Power, which is a highly credible event. ...

In addition, it remains unclear how the applicant intends to ensure that surveillance testing requirements associated with the referenced safety-related trip signals will be met if they are not included in the Technical Specifications.

First, it should be noted that the Reactor Trip on EFWS Actuation (First NRC excerpt, above) is not the function that initiates EFW in the event of a Loss of Normal Feedwater Flow event (Second NRC excerpt, above). Reactor trip functions for the U.S. EPR insert the Rod Cluster Control Assemblies (RCCAs) into the reactor core. ESF functions are used to initiate Emergency Core Cooling Systems. There are two credited ESF functions that actuate EFW:

- EFWS Actuation on Low-Low SG Level (Affected SG), and
- EFWS Actuation on Loss of Offsite Power and SIS Actuation (All SGs).

The Reactor Trip on EFWS Actuation is a safety related design feature of the U.S. EPR. It is described in U.S. EPR FSAR Tier 2 Section 7.2.1.2.21 and is depicted in Figure 7.3-3. As discussed in the NRC's Final Policy Statement on Technical Specifications Improvements for Nuclear Power Plants, 10 CFR 50.36, Criterion 3, does not require safety related design features to be incorporated into the Technical Specifications unless the features are credited in the safety analysis.

Section 7.2 reflects the Protection System design. The Protection System design includes features that are not credited in the safety analysis. The safety analysis used by AREVA for the U.S. EPR is summarized in U.S. EPR FSAR Tier 2 Chapter 15. Specifically, the loss of normal Feedwater flow is addressed in Section 15.2.7 and Feedwater piping breaks inside and outside containment are addressed in Section 15.2.8.

The following reactor trip functions are credited to mitigate the loss of normal Feedwater flow in the U.S. EPR safety analysis:

- Low Steam Generator Level, and
- Low DNBR

The following reactor trip functions are credited to mitigate the entire spectrum of Feedwater piping breaks inside and outside containment in the U.S. EPR safety analysis:

- Steam Generator Pressure Drop,
- Low Steam Generator Pressure,
- Low Steam Generator Level,
- High Containment Pressure, and
- Low DNBR.

The Reactor Trip on EFWS Actuation is not credited in the U.S. EPR safety analysis to mitigate the consequences of a LOCA or any other design basis event or abnormal operational occurrence. 10 CFR 50.36 requires an applicants Technical Specifications to reflect its safety analysis. The implication by the NRC that AREVA needs to incorporate into its Technical Specifications functions that are not credited in their safety analysis is not supported by the requirements specified in 10 CFR 50.36.

With regards to surveillance testing, the sensors credited with detecting the conditions that necessitate a reactor trip to mitigate the loss of normal Feedwater flow or Feedwater piping breaks inside and outside containment, the signal processors that generate the reactor trip signal, the reactor trip actuation devices, and their surveillance requirements are listed in Table 3.3.1-1 of the Protection System Technical Specifications. Also included is a surveillance

requirement to periodically verify the reactor trip setpoints have been properly loaded into the signal processors. Also listed in Table 3.3.1-1 are the sensors, signal processors, and actuation devices credited in the safety analysis for initiating EFWS Actuation on Low-Low SG Level (Affected SG) and EFWS Actuation on Loss of Offsite Power and SIS Actuation (All SGs) ESFAS functions. While the Reactor Trip on EFWS Actuation function is not required to be included in the U.S. EPR Technical Specifications, the components necessary to perform this function and the verification of the actuation setpoints are already the subject of other surveillance requirements for other credited functions.

In addition, U.S. EPR FSAR Tier 2 Table 1.8-2 contains U.S. EPR Combined License Information Item 13.5-5, which requires a Combined License applicant that references the U.S. EPR design certification provide site-specific information for administrative, operating, emergency, maintenance, and other operating procedures. Information regarding testing procedures not included in the Technical Specifications may be requested from the Combined License applicant.

### **Manual Reactor Trip**

The context of the original Question 16-137 was in regard to the manual reactor trip signal not being listed as a separate function in Table 3.3.1-2.

In the follow-up question, the NRC states that:

FSAR Section 7.2.1.2 identifies the manual reactor trip signal from the Safety Information and Control System (SICS) as a safety-related reactor trip initiation signal.  
...

The Manual RT initiation ensures that the control room operator has the capability to initiate a reactor trip at any time. This capability is critical whenever a parameter is rapidly trending toward its Trip Setpoint.

In addition, it remains unclear how the applicant intends to ensure that surveillance testing requirements associated with the referenced safety-related trip signals will be met if they are not included in the Technical Specifications.

The manual reactor trip is a safety related design feature of the U.S. EPR and is described in U.S. EPR FSAR Tier 2 Section 7.2.1.2.22 and depicted in Figure 7.2-3. As shown in Figure 7.2-3, the manual reactor trip is initiated by a switch in the Main Control Room which goes directly to the Reactor Trip Breakers. The manual reactor trip actuation switches and their surveillance requirements are listed in Table 3.3.1-1 of the Protection System Technical Specifications. Similarly, the actuation devices necessary to perform reactor trip functions are also listed in Table 3.3.1-1 of the Protection System Technical Specifications. The surveillances on the manual reactor trip actuation switches and the Reactor Trip Breakers ensure that a manual reactor trip will occur when initiated.

The manual reactor trip switches do not provide a signal to the APUs and there is no software "function" for the manual reactor trip loaded in the APUs. The list of functions in Table 3.3.1-2 only contains the credited reactor trip and ESF software functions performed by the APUs. Since the U.S. EPR Protection System Technical Specifications are component based, the

format does not readily allow the listing of a function in Table 3.3.1-2 that is not performed by the APUs.

### **EFWS Isolation on High SG Level (Affected SGs) ESFAS Signal**

The logic for not including the automatic EFWS Isolation on High SG Level (Affected SG) ESFAS function in Table 3.3.1-2 of the U.S. EPR Technical Specifications is generally the same as that for the Reactor Trip on SIS Actuation and Reactor Trip on EFWS Actuation signals discussed above.

Both the automatic and manual EFWS Isolation on High SG Level (Affected SG) ESFAS signals are safety related design features of the U.S. EPR. They are described in U.S. EPR FSAR Tier 2 Section 7.3.1.2.3 and are depicted in Figures 7.3-5 through 7.3-7. Section 7.3 reflects the design of the U.S. EPR Protection System. The Protection System design includes features that are not credited in the safety analysis. If the automatic EFWS Isolation on High SG Level (Affected SG) ESFAS function was deleted from the U.S. EPR design, there would be no impact to the credited safety analysis path summarized in Chapter 15 of the U.S. EPR FSAR. 10 CFR 50.36, Criterion 3, does not require safety related design features to be incorporated into the Technical Specifications unless the design features are credited in the safety analysis.

In the follow-up question, the NRC states that:

If the EFWS system is actuated to mitigate the effects of a loss of Main Feedwater (MFW) event, then isolation of the EFWS system is considered the primary success path for mitigating a SGTR.

First, it should be noted that in both U.S. EPR LCO 3.3.1, "Protection System" and Westinghouse Standard Technical Specification LCO 3.3.2, "Engineered Safety Feature Actuation System (ESFAS) Instrumentation," the instrumentation that initiates the ESFAS signal is within the scope of the "Instrumentation" LCO. The system that actually performs the ESFAS function is governed by other LCOs outside the "Instrumentation" section of the Technical Specifications.

The safety analysis for the U.S. EPR Steam Generator Tube Rupture (SGTR) event is summarized in U.S. EPR FSAR Tier 2 Section 15.6.3. There are two scenarios discussed:

- Scenario 1 - Charging Pumps are not operating, and
- Scenario 2 - Charging Pumps are operating.

For the first scenario, the FSAR states:

If not already initiated automatically by the combination of high activity or high Steam Generator (SG) level in combination with a partial cooldown, the operator isolates the affected SG. To isolate the SG, **the operator closes** its main steam isolation valve (MSIV), resets its Main Steam Relief Train (MSRT) setpoint high, and closes its Main Feedwater (MFW) and **Emergency Feedwater System (EFWS) isolation valves**. This action terminates the radiological release from the affected SG. (Emphasis added)

For the second scenario, the FSAR states:

The **operator** institutes the following SGTR mitigation procedure: ...

- **Close the MFW and EFWS isolation valves** in the affected SG. (Emphasis added)

Therefore, the EFWS Isolation function is not credited with automatically mitigating the effects of a SGTR. Rather, manual operator action to isolate the EFWS is the primary success path credited in Chapter 15 for mitigating a SGTR. Please note that in RAI 285, Question 07.03-27, AREVA was requested to clarify its technical position concerning manual initiation of a steam generator isolation due to a steam generator tube rupture event.

With regards to surveillance testing, the manual actuation switches used for SG Isolation are specified in Table 3.3.1-1 of the Protection System Technical Specifications. The surveillance requirements specified therein and in Limiting Condition for Operation 3.7.5, "Emergency Feedwater System," are sufficient to ensure the ability of the operator to isolate the EFWS. As shown on Figures 7.3-5 through 7.3-7, the manual isolation signal is not routed through the APU. There is no software "function" for the manual EFWS isolation loaded in the APUs. As previously discussed, the list of functions in Table 3.3.1-2 **only applies to the reactor trip and ESF software functions performed by the APUs**. Since the U.S. EPR Protection System Technical Specifications are component based, the format does not readily allow the listing of a function in Table 3.3.1-2 that is not performed by the APUs.

While the automatic EFWS Isolation on High SG Level (Affected SG) ESFAS function is not required to be included in the U.S. EPR Technical Specifications, the components necessary to perform this function (i.e., Steam Generator Level (Wide Range) sensors, APUs, ALUs, and the Hot Leg Temperature (Wide Range) sensors that provide input to associated Permissive P13) are listed in Table 3.3.1-1 of the Protection System Technical Specifications and are already the subject of other surveillance requirements for other credited functions.

In addition, U.S. EPR FSAR Tier 2 Table 1.8-2 contains U.S. EPR Combined License Information Item 13.5-5, which requires a Combined License applicant that references the U.S. EPR design certification provide site-specific information for administrative, operating, emergency, maintenance, and other operating procedures. Information regarding testing procedures not included in the Technical Specifications may be requested from the Combined License applicant.

## SUMMARY

In summary, the Reactor Trip on SIS Actuation and Reactor Trip on EFWS Actuation functions are not credited in the safety analysis and are not required by 10 CFR 50.36, Criterion 3, to be included in the U.S. EPR Technical Specifications. The components that perform these functions are already demonstrated operable by surveillances specified in the Protection System Technical Specifications for other credited reactor trip and ESFAS functions.

The switches that initiate the manual reactor trip and EFWS isolation functions are demonstrated operable by surveillances specified in the component based Protection System Technical Specifications. The component based format utilized for the Protection System Technical Specifications does not allow a manual reactor trip function to be listed, since it is not a software function performed by the APUs.

**FSAR Impact:**

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

DRAFT

**Question 16-319:****OPEN ITEM****Follow-up to RAI 103, Question 16-160.**

In RAI-SRP16-CTSB-103/160, the staff requested an explanation regarding the mode applicability for Hot Leg Temperature Wide Range (WR) instrumentation with respect to ESFAS Function B.6.c, Emergency Feedwater System (EFWS) Isolation on High SG Level (Affected SGs). Although this issue is identified and addressed under RAI-SRP16-CTSB-103/144, the staff questions the applicant's removal of the EFWS Isolation on High SG Level function from Technical Specifications as indicated in the response to Question 16-160 on page 30 of 63. The applicant concludes that ESFAS Function B.6.c should not be included in Technical Specifications on the basis that 1) the function is no longer credited in U.S. EPR FSAR Tier 2, Table 15.0-8 and 2) Manual operator action is assumed to mitigate a SG tube rupture (SGTR) event with no automatic actions. The EFWS Isolation function automatically mitigates the effects of a SGTR. The EFWS is isolated at a high level setpoint to avoid an uncontrolled SG level increase, subsequent SG overfill, and potential radioactive water discharge via the main steam relief train. If the EFWS system is actuated to mitigate the effects of a loss of Main Feedwater (MFW) event, then isolation of the EFWS system is considered the primary success path for mitigating a SGTR. In addition, the applicant has not demonstrated that the surveillance testing requirements associated with the EFWS Isolation function are met if they are not included in the Technical Specifications. Exclusion from Table 15.0-8 and reliance upon manual operator action to avoid an uncontrolled SG level increase and potential radioactive discharge, do not necessarily warrant exclusion of the EFWS Isolation function from the Technical Specifications. This issue has been identified as an open item in the SER w/OI for Chapter 16 of the EPR FSAR.

**Response to Question 16-319:**

This issue was further clarified on Page 16-20 of the NRC's March 10, 2010 Safety Evaluation, which states:

- In RAI 103, Question 16-160, the staff requested that the applicant provide an explanation regarding the mode applicability for Hot Leg Temperature Wide Range instrumentation with respect to ESFAS Function B.6.c, "Emergency Feedwater System Isolation on High-SG Level (Affected SGs)." Although this issue is identified and addressed under RAI 103, Question 16-144, the staff questions the applicant's removal of the EFWS Isolation on High-SG Level function from Technical Specifications as indicated in the response to RAI 103, Question 16-160 on Page 30 of 63. In a June 30, 2009, response to RAI 103, Question 16-160, the applicant concluded that ESFAS Function B.6.c should not be included in TS on the basis that (1) the function is no longer credited in FSAR Tier 2, Table 15.0-8, "Engineered Safety Features Functions Used in the Accident Analysis," and (2) Manual operator action is assumed to mitigate a steam generator tube rupture (SGTR) event with no automatic actions. The EFWS Isolation function automatically mitigates the effects of a SGTR. The EFWS is isolated at a high-level setpoint to avoid an uncontrolled SG level increase, subsequent SG overfill, and potential radioactive water discharge via the main steam relief train. If the EFWS system is actuated to mitigate the effects of a loss of Main Feedwater event, then isolation of the EFWS system is considered



the primary success path for mitigating a SGTR. In addition, it remains unclear how the applicant intends to ensure that surveillance testing requirements associated with the EFWS Isolation function will be met if they are not included in the TS. Exclusion from FSAR Tier 2, Table 15.0-8 and reliance upon manual operator action to avoid an uncontrolled SG level increase and potential radioactive discharge do not necessarily warrant exclusion of the EFWS Isolation function from the Technical Specifications.

Refer to the response to Question 16-318.

**FSAR Impact:**

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

DRAFT

**Question 16-320:****OPEN ITEM****Follow-up to RAI 110, Question 16-215.**

In RAI-SRP16-CTSB-110/215, the staff requested the information necessary to ensure that EPR Bases B 3.3.3, Remote Shutdown System (RSS), includes all of the functions, control circuits, transfer switches and instrumentation necessary to meet the requirements of GDC 19, Control Room. The response states that the applicant has revised its design and regulatory compliance approach with regards to the Remote Shutdown System and its associated Technical Specifications. Instead of specifying the required functions in U.S. EPR FSAR Tier 2, Chapter 16, Technical Specification Bases Section 3.3.3, the Bases is being revised to state that the displays and controls at the RSS are functionally the same as the displays and controls normally used by the operator to achieve and maintain Mode 3 from the main control room. Given the revised specification, the applicant has not identified the actions that would be taken if a single sensor associated with one of the RSS functions became inoperable. The entire Remote Shutdown Station apparently defaults to an inoperable status since the specification as written, removes all references to "required Functions" in the LCO. The intent is not clearly understood. The staff was unable to make a conclusive determination that the applicant's revised design and regulatory compliance approach meets the requirements of GDC 19, on the basis of the information provided. This issue has been identified as an open item in the SER w/OI for Chapter 16 of the EPR FSAR.

**Response to Question 16-320:**

Additionally, this issue was further clarified on Page 16-39 of the NRC's March 10, 2010 Safety Evaluation, which states:

The applicant also maintains that Channel Checks are no longer necessary on the basis of its June 30, 2009, response to RAI 110, Question 16-215, which is used to support the claim that there are no separate and unique analog instruments located at the "Remote Shutdown Station," which require a surveillance. In a June 30, 2009, response to RAI 110, Question 16-215, the applicant proposes to revise its design and regulatory approach with regards to the Remote Shutdown System and its associated TS. Instead of specifying the required Remote Shutdown System functions in TS Bases B 3.3.3, the Bases will be revised to state that the displays and controls at the "Remote Shutdown Station" are functionally the same as the displays and controls normally used by the operator to achieve and maintain Mode 3 from the main control room.

In general, fire protection Technical Specifications, including the requirements for the Remote Shutdown Station (RSS) were retrofitted into existing plants' licensing basis as part of the review and approval of fire protection plans necessary to implement the requirements of 10 CFR 50.48. The supporting fire protection safe shutdown analyses were developed, which allowed the definition of the specific functions and equipment necessary to be included with the RSS.

The underlying Westinghouse plant design, which includes the RSS equipment, that formed the basis for LCO 3.3.4, "Remote Shutdown System," in the Standard Technical Specifications for Westinghouse Plants (NUREG-1431) is fundamentally different than the design of the next generation plants, including the RSS equipment, that utilize a highly integrated control room

concept. These fundamental differences, along with status of design necessary to support a Design Certification, has necessitated a refinement in the approach taken for RSS Technical Specifications. A refined approach was previously proposed for the AP1000 Technical Specifications for the Remote Shutdown Workstation (LCO 3.3.4), which were approved as documented in NUREG-1793, "Final Safety Evaluation Report Related to Certification of the AP1000 Standard Design."

Specifically, in the current operating plants, the RSS includes hard-wired instrumentation and controls. Since the instrumentation and controls are hard-wired, failures in the wiring could result in an inoperable sensor, display, or control, which could render a required RSS function inoperable, while the function from the Main Control Room (MCR) would still be operable. Thus, the Technical Specifications for currently operating plants require periodic surveillance testing to demonstrate, on a function by function basis, the operability of both the instrumentation and controls necessary to take the plant to a safe shutdown state from the RSS.

The U.S. EPR RSS reflects the use of a highly integrated control room. The RSS contains Human Machine Interface (HMI) workstations necessary to bring the plant to, and maintain it in, a safe shutdown state. As shown on U.S. EPR FSAR Tier 2 Figure 7.1-2, "U.S. EPR I&C Architecture," the Plant Information Control System (PICS) portion of the U.S. EPR RSS consists of an operators' computer terminal that gathers data for display and communicates equipment control commands through the plant data network. This is the same method used by the operators' computer terminal in the control room for data display and equipment control command communication. Thus, from a broad perspective, demonstrating the operability of the U.S. EPR RSS PICS communication with the plant data network, provides the assurance that the information and control capabilities present in the MCR can be replicated by the RSS.

While the detailed U.S. EPR fire protection safe shutdown analysis is not required to be and has not been finalized, the displays and controls in the RSS to allow the monitoring and control of the following safe shutdown functions in all four divisions during a postulated fire in the MCR or during an event that could cause the MCR to become uninhabitable, coupled with a single failure. As stated in U.S. EPR FSAR Tier 2 Section 7.4.1.3.4, "Remote Shutdown Station," the PICS in the RSS, will include the monitoring and control functions necessary for:

- Reactivity control,
- Reactor coolant makeup,
- Reactor coolant system pressure control,
- Decay heat removal, and
- Control and monitoring of safety support systems for the above functions, as well as service water, component cooling water, and onsite power including the emergency diesel generators.

The RSS Technical Specification, as implied by title of Section 3.3, "Instrumentation," addresses the display and control aspect of these safe shutdown functions. The operability of the systems that perform these functions is governed, as required, by other Technical Specification sections and Limiting Condition for Operations (LCOs).

In addition, the U.S. EPR Technical Specifications also have a relevant unique aspect which provides NRC with added assurance that the instrumentation required to perform safe shutdown functions will be operable when required. As stated in the Westinghouse Standard Technical

Specifications, the Remote Shutdown System LCO provides the operability requirements of the instrumentation and controls necessary to place and maintain the unit in Mode 3 from a location other than the control room. As stated in the Westinghouse Standard Technical Specifications Bases for LCO 3.3.4:

"A Function of a Remote Shutdown System is OPERABLE if all instrument and control channels needed to support the Remote Shutdown System Function are OPERABLE. In some cases, Table B 3.3.4-1 may indicate that the required information or control capability is available from several alternate sources. In these cases, the Function is OPERABLE as long as one channel of any of the alternate information or control sources is OPERABLE. ...

For channels that fulfill GDC 19 requirements, the number of OPERABLE channels required depends upon the unit licensing basis as described in the NRC unit specific Safety Evaluation Report (SER). Generally, two divisions are required OPERABLE. However, only one channel per a given Function is required if the unit has justified such a design, and NRC's SER accepted the justification."

In the Westinghouse Standard Technical Specifications, the systems that perform the reactor trip and Engineered Safety Features functions are addressed at a functional level. Due to the sharing of components, these systems are addressed at the component level in the U.S. EPR Protection System Technical Specifications. As a result, the specific instrumentation that can be utilized to support the RSS safe shutdown functions may already be explicitly addressed by the requirements of the Protection System or other Technical Specifications. Many of these EPR Technical Specifications are equivalent or more restrictive, in terms of the required number of divisions and required actions, than the Westinghouse Standard Technical Specification requirements for the corresponding RSS functions. A review of the above safe shutdown functions, supporting instrumentation, and existing Technical Specification requirements are presented in Table 16-320-1.

Thus, it is not necessary for the U.S. EPR RSS Technical Specifications to identify and demonstrate on a function-by-function basis that each individual safe shutdown function is operable. Rather, the underlying purpose of the LCO, which is to provide the requirements for the operability of the instrumentation and controls necessary to place and maintain the plant in MODE 3 from a location other than the control room, can be accomplished by:

- Demonstrating that each required transfer switch is capable of performing its function,
- Verifying that each RSS division communicates both indications and control commands, and
- Verifying the operability of the RSS hardware and software.

The removal of references to "required Functions" in the LCO is consistent with the wording of the AP1000 Technical Specifications for the Remote Shutdown Workstation (LCO 3.3.4), which were approved as documented in NUREG-1793. In order to improve fidelity with the NRC approved precedent and more explicitly reflect the specific testing necessary to demonstrate the

operability of the U.S. EPR RSS, additional surveillance requirements and their associated Bases changes will be added to U.S. EPR FSAR Tier 2 Chapter 16, "Technical Specifications," LCO 3.3.3, "Remote Shutdown Station."

Revision 2 of U.S. EPR FSAR and the response to RAI 383 will provide clarification regarding the crediting of the Safety Information and Control System (SICS) and descriptions of the Minimum Inventory.

**FSAR Impact:**

The changes to U.S. EPR FSAR Tier 2 Chapter 16 Technical Specifications and Technical Specification Bases will be made as discussed in the above response.

DRAFT

**TABLE 16-320-1**  
**COMPARISON OF SUPPORTING INSTRUMENTATION FOR SAFE SHUTDOWN FUNCTIONS**  
**VERSUS EXISTING TECHNICAL SPECIFICATION REQUIREMENTS**

| SAFE SHUTDOWN FUNCTION<br>SUPPORTING INSTRUMENTATION | EXISTING TECHNICAL SPECIFICATION REQUIREMENTS<br>FOR OPERABILITY IN MODES 1, 2 AND 3  |
|--|---|
| <b>Reactivity Control</b>                            |   |
| – Reactor Trip Signal                                | Signal generated by the Protection System. Operability governed by LCO 3.3.1 in Modes 1 and 2 and in Mode 3 with the RCSL System capable of withdrawing a RCCA or one or more RCCAs not fully inserted.   |
| – Safety Injection Signal                            | Signal generated by the Protection System. Operability governed by LCO 3.3.1 in Modes 1, 2 and 3.   |
| – Neutron Flux                                       |   |
| ○ Self-Powered Neutron Detectors                     | Operability required by LCO 3.3.1, Table 3.3.1-1 in Mode 1 with RTP greater than or equal to 10% RTP. With less than 67 of 72 detectors operable, power must be reduced to less than 10% RTP in six hours.  |
| ○ Power Range Monitors                               | Operability required by LCO 3.3.1, Table 3.3.1-1 in Modes 1 and 2 and in Mode 3 with the RCSL System capable of withdrawing a RCCA or one or more RCCAs not fully inserted. With less than three divisions operable (with two detectors in each division), the plant must be in Mode 3 in six hours and the reactor trip breakers opened. |
| ○ Intermediate Range Monitors                        | Operability required by LCO 3.3.1, Table 3.3.1-1 in Modes 1 and 2 and in Mode 3 with the RCSL System capable of withdrawing a RCCA or one or more RCCAs not fully inserted. With less than three divisions operable, the plant must be in Mode 3 in six hours and the reactor trip breakers opened.                                       |
| ○ Source Range Monitors                              | Operability of two divisions required by LCO 3.3.2. Required actions are to restore one required division to operable status within 30 days, have one required division operable within 7 days, or the plant must be in Mode 3 in six hours and Mode 4 in 12 hours.   |

**SAFE SHUTDOWN FUNCTION  
SUPPORTING INSTRUMENTATION****EXISTING TECHNICAL SPECIFICATION REQUIREMENTS  
FOR OPERABILITY IN MODES 1, 2 AND 3**

|  |   |
|--|---|
| – Cold Leg Temperature (Narrow Range)    | Operability required by LCO 3.3.1, Table 3.3.1-1 in Mode 1 with RTP greater than or equal to 10% RTP. With less than three divisions operable, power must be reduced to less than 10% RTP in six hours.   |
| – Cold Leg Temperature (Wide Range)      | Operability required by LCO 3.3.1, Table 3.3.1-1 in Mode 1, in Mode 2 with flux greater than or equal to 10 E-5% RTP, and in Modes 3 when one or more RCSs are in operation. With less than three divisions operable, the plant must be in Mode 3 in six hours and Mode 5 in 36 hours.                  |
| – Hot Leg Temperature (Narrow Range)     | Operability required by LCO 3.3.1, Table 3.3.1-1 in Mode 1 and in Mode 2 with flux greater than or equal to 10 E-5% RTP. With less than three divisions operable (with three sensors in each division), the plant must be in Mode 3 in six hours.   |
| – Hot Leg Temperature (Wide Range)       | Operability required by LCO 3.3.1, Table 3.3.1-1 in Modes 1, 2 and 3. With less than three divisions operable, the plant must be in Mode 3 in six hours and Mode 5 in 36 hours.   |
| – RCCA Analog Position Indication        | Operability required by LCO 3.1.7 in Modes 1 and 2. The indicators must be restored to operable status within 24 hours such that a maximum of one in the associated bank is inoperable or the plant must be in Mode 3 in 6 hours.   |
| – RCCA Bottom Position Indication        | Operability required by LCO 3.3.1, Table 3.3.1-1 in Mode 3 with one or more RCPs in operation. If an RCCA Analog Position Indicator is inoperable, the plant suspend operations involving positive reactivity additions that could result in a loss of required Shutdown Margin or boron concentration. |
| – RCCA Bottom Position Indication        | Operability required by LCO 3.1.7 in Modes 1 and 2. If a Digital RCCA Position Indicator is inoperable, it has to be restored to operable status or all Analog RCCA Position Indicators verified operable every 8 hours, or reactor power must be reduced to less than 50% RTP in 6 hours.              |
| – CVCS Charging Line Boron Concentration | Operability required by LCO 3.3.1, Table 3.3.1-1 in Modes 1, 2 and 3. With less than three divisions operable, the plant must be in Mode 3 in six hours and Mode 5 in 36 hours.   |

**SAFE SHUTDOWN FUNCTION  
SUPPORTING INSTRUMENTATION****EXISTING TECHNICAL SPECIFICATION REQUIREMENTS  
FOR OPERABILITY IN MODES 1, 2 AND 3****Heat Transfer (RCS Pressure and  
Temperature) Control**

- Cold Leg Temperature (Narrow Range) Operability required by LCO 3.3.1, Table 3.3.1-1 in Mode 1 with RTP greater than or equal to 10% RTP. With less than three divisions operable, power must be reduced to less than 10% RTP in six hours.
- Cold Leg Temperature (Wide Range) Operability required by LCO 3.3.1, Table 3.3.1-1 in Mode 1, in Mode 2 with flux greater than or equal to 10 E-5% RTP, and in Modes 3 when one or more RCSs are in operation. With less than three divisions operable, the plant must be in Mode 3 in six hours and Mode 5 in 36 hours.
- Hot Leg Temperature (Narrow Range) Operability required by LCO 3.3.1, Table 3.3.1-1 in Mode 1 and in Mode 2 with flux greater than or equal to 10 E-5% RTP. With less than three divisions operable (with three sensors in each division), the plant must be in Mode 3 in six hours.
- Hot Leg Temperature (Wide Range) Operability required by LCO 3.3.1, Table 3.3.1-1 in Modes 1, 2 and 3. With less than three divisions operable, the plant must be in Mode 3 in six hours and Mode 5 in 36 hours.
- RCS (Hot Leg) Pressure (Wide Range) Operability required by LCO 3.3.1, Table 3.3.1-1 in Modes 1, 2 and 3. With less than three divisions operable, the plant must be in Mode 3 in six hours and Mode 5 in 36 hours.
- Subcooling Margin (Delta Tsat)
  - Hot Leg Pressure (Wide Range) Operability of two divisions required by LCO 3.3.2. Required actions are to restore one required division to operable status within 30 days, have one required division operable within 7 days, or the plant must be in Mode 3 in six hours and Mode 4 in 12 hours.
  - Incore Thermocouples Operability required by LCO 3.3.1, Table 3.3.1-1 in Modes 1, 2 and 3. With less than three divisions operable, the plant must be in Mode 3 in six hours and Mode 5 in 36 hours.
  - Incore Thermocouples Operability of two divisions required by LCO 3.3.2. Required actions are to restore one required division to operable status within 30 days, have one required division operable within 7 days, or initiate action in accordance with Specification 5.6.5.



**SAFE SHUTDOWN FUNCTION****SUPPORTING INSTRUMENTATION****EXISTING TECHNICAL SPECIFICATION REQUIREMENTS  
FOR OPERABILITY IN MODES 1, 2 AND 3**

|  |   |
|--|---|
| ○ Hot Leg Temperature (Wide Range)     | Operability required by LCO 3.3.1, Table 3.3.1-1 in Modes 1, 2 and 3. With less than three divisions operable, the plant must be in Mode 3 in six hours and Mode 5 in 36 hours.   |
| – Pressurizer Level                    | Operability required by LCO 3.3.1, Table 3.3.1-1 in Modes 1, 2 and 3. With less than three divisions operable, the plant must be in Mode 3 in six hours and Mode 5 in 36 hours.   |
| – Steam Generator Level (Narrow Range) | Operability required by LCO 3.3.1, Table 3.3.1-1 in Modes 1 and 2 and in Mode 3, except when all Man Feedwater full load and low load lines are isolated. With less than three divisions operable, the plant must be in Mode 3 in six hours and Mode 4 in 12 hours. |
| – Steam Generator Level (Wide Range)   | Operability required by LCO 3.3.1, Table 3.3.1-1 in Modes 1, 2 and 3. With less than three divisions operable, the plant must be in Mode 3 in six hours and Mode 4 in 12 hours.   |
| – Steam Generator Pressure             | Operability required by LCO 3.3.1, Table 3.3.1-1 in Modes 1, 2 and 3. With less than three divisions operable, the plant must be in Mode 3 in six hours and Mode 5 in 36 hours.   |
| <b>RCS Inventory Control</b>           |   |
| – Pressurizer Level                    | Operability required by LCO 3.3.1, Table 3.3.1-1 in Modes 1, 2 and 3. With less than three divisions operable, the plant must be in Mode 3 in six hours and Mode 5 in 36 hours.   |
| – RCS (Hot Leg) Pressure (Wide Range)  | Operability required by LCO 3.3.1, Table 3.3.1-1 in Modes 1, 2 and 3. With less than three divisions operable, the plant must be in Mode 3 in six hours and Mode 5 in 36 hours.   |
| – Core Outlet Temperature              | Operability of two divisions required by LCO 3.3.2. Required actions are to restore one required division to operable status within 30 days, have one required division operable within 7 days, or initiate action in accordance with Specification 5.6.5.          |

**SAFE SHUTDOWN FUNCTION  
SUPPORTING INSTRUMENTATION****EXISTING TECHNICAL SPECIFICATION REQUIREMENTS  
FOR OPERABILITY IN MODES 1, 2 AND 3**

- |   |  |
|---|--|
| <ul style="list-style-type: none"> <li>- Subcooling Margin (Delta Tsat)           <ul style="list-style-type: none"> <li>o Hot Leg Pressure (Wide Range)</li> <li>o Incore Thermocouples</li> <li>o Hot Leg Temperature (Wide Range)</li> </ul> </li> <li>- Safety Injection System Operation           <ul style="list-style-type: none"> <li>o IRWST Level</li> <li>o LHSI Flow</li> <li>o MHSI Flow</li> </ul> </li> <li>- CVCS Operation           <ul style="list-style-type: none"> <li>o CVCS Charging Line Flow</li> <li>o Volume Control Tank Level</li> <li>o Auxiliary Spray Flow</li> <li>o Letdown Flow</li> </ul> </li> </ul> | <p>Operability required by LCO 3.3.1, Table 3.3.1-1 in Modes 1, 2 and 3. With less than three divisions operable, the plant must be in Mode 3 in six hours and Mode 5 in 36 hours.</p> <p>Operability of two divisions required by LCO 3.3.2. Required actions are to restore one required division to operable status within 30 days, have one required division operable within 7 days, or initiate action in accordance with Specification 5.6.5.</p> <p>Operability required by LCO 3.3.1, Table 3.3.1-1 in Modes 1, 2 and 3. With less than three divisions operable, the plant must be in Mode 3 in six hours and Mode 5 in 36 hours.</p> <p>IRWST level is used to verify IRWST volume every 7 days while in Modes 1, 2, and 3 per Surveillance Requirement 3.5.4.2. If IRWST volume cannot be verified or restored to within limits in 8 hours, the plant must be in Mode 3 in six hours and Mode 5 in 36 hours.</p> <p>Operability of two divisions required by LCO 3.3.2. Required actions are to restore one required division to operable status within 30 days, have one required division operable within 7 days, or initiate action in accordance with Specification 5.6.5.</p> <p>Operability of two divisions required by LCO 3.3.2. Required actions are to restore one required division to operable status within 30 days, have one required division operable within 7 days, or initiate action in accordance with Specification 5.6.5.</p> <p>Operability required by LCO 3.3.1, Table 3.3.1-1 in Modes 1 and 2 and in Mode 3 with one or more RCPs in operation. With less than three divisions operable, the plant must be in Mode 3 in six hours and Mode 5 in 36 hours.</p> <p><i>Not included in the U.S. EPR Technical Specifications.</i></p> <p><i>Not included in the U.S. EPR Technical Specifications.</i></p> <p><i>Not included in the U.S. EPR Technical Specifications.</i></p> |
|---|--|

**SAFE SHUTDOWN FUNCTION  
SUPPORTING INSTRUMENTATION****EXISTING TECHNICAL SPECIFICATION REQUIREMENTS  
FOR OPERABILITY IN MODES 1, 2 AND 3****Steam Generator Integrity Control**

- Steam Generator Level (Narrow Range)
- Steam Generator Level (Wide Range)
- Steam Generator Pressure
- Steam Generator Blowdown Activity
- Main Steam Line Activity
- Feedwater Flow

Operability required by LCO 3.3.1, Table 3.3.1-1 in Modes 1 and 2 and in Mode 3, except when all Man Feedwater full load and low load lines are isolated. With less than three divisions operable, the plant must be in Mode 3 in six hours and Mode 4 in 12 hours.

Operability required by LCO 3.3.1, Table 3.3.1-1 in Modes 1, 2 and 3. With less than three divisions operable, the plant must be in Mode 3 in six hours and Mode 4 in 12 hours.

Operability required by LCO 3.3.1, Table 3.3.1-1 in Modes 1, 2 and 3. With less than three divisions operable, the plant must be in Mode 3 in six hours and Mode 5 in 36 hours.

*Not included in the U.S. EPR Technical Specifications.*

Operability of two divisions required by LCO 3.3.2. Required actions are to restore one required division to operable status within 30 days, have one required division operable within 7 days, or the plant must be in Mode 3 in six hours and Mode 4 in 12 hours.

Operability of two divisions required by LCO 3.3.2. Required actions are to restore one required division to operable status within 30 days, have one required division operable within 7 days, or the plant must be in Mode 3 in six hours and Mode 4 in 12 hours.

**Steam Generator Inventory Control**

- Steam Generator Level (Narrow Range)
- Steam Generator Level (Wide Range)

Operability required by LCO 3.3.1, Table 3.3.1-1 in Modes 1 and 2 and in Mode 3, except when all Man Feedwater full load and low load lines are isolated. With less than three divisions operable, the plant must be in Mode 3 in six hours and Mode 4 in 12 hours.

Operability required by LCO 3.3.1, Table 3.3.1-1 in Modes 1, 2 and 3. With less than three divisions operable, the plant must be in Mode 3 in six hours and Mode 4 in 12 hours.

**SAFE SHUTDOWN FUNCTION  
SUPPORTING INSTRUMENTATION****EXISTING TECHNICAL SPECIFICATION REQUIREMENTS  
FOR OPERABILITY IN MODES 1, 2 AND 3**

|   |   |
|---|---|
| – Steam Generator Pressure                                | Operability required by LCO 3.3.1, Table 3.3.1-1 in Modes 1, 2 and 3. With less than three divisions operable, the plant must be in Mode 3 in six hours and Mode 5 in 36 hours.   |
| – Feedwater Flow  | Operability of two divisions required by LCO 3.3.2. Required actions are to restore one required division to operable status within 30 days, have one required division operable within 7 days, or the plant must be in Mode 3 in six hours and Mode 4 in 12 hours.   |
| <b>Containment Integrity</b>                              |   |
| – Containment Equipment Compartment Pressure              | Operability required by LCO 3.3.1, Table 3.3.1-1 in Modes 1 and 2 and in Mode 3 with the RCSL System capable of withdrawing a RCCA or one or more RCCAs not fully inserted. With less than three divisions operable (with two detectors in each division), the plant must be in Mode 3 in six hours and the reactor trip breakers opened. |
| – Containment Service Compartment Pressure (Narrow Range) | Operability required by LCO 3.3.1, Table 3.3.1-1 in Modes 1 and 2 and in Mode 3 with the RCSL System capable of withdrawing a RCCA or one or more RCCAs not fully inserted. With less than three divisions operable (with two detectors in each division), the plant must be in Mode 3 in six hours and the reactor trip breakers opened. |
| – Containment Service Compartment Pressure (Wide Range)   | Operability required by LCO 3.3.1, Table 3.3.1-1 in Modes 1, 2, and 3. With less than three divisions operable, the plant must be in Mode 3 in six hours and Mode 5 in 36 hours.  |
| – Containment Sump (Level or Discharge Flow)              | Operability required by LCO 3.4.14 in Modes 1, 2, and 3. With less than one monitor operable, the monitor must be restored to operable status in 30 days or the plant must be in Mode 3 in six hours and Mode 5 in 36 hours.  |
| – Containment Air Cooler Condensate Flow Rate             | Operability required by LCO 3.4.14 in Modes 1, 2, and 3. With less than one monitor operable, grab samples must be analyzed once per 24 hours or the plant must be in Mode 3 in six hours and Mode 5 in 36 hours.   |

**SAFE SHUTDOWN FUNCTION  
SUPPORTING INSTRUMENTATION**

**EXISTING TECHNICAL SPECIFICATION REQUIREMENTS  
FOR OPERABILITY IN MODES 1, 2 AND 3**

- Containment Atmosphere Radioactivity (Particulate) Monitor
  
- Radiation Monitor - Containment High Range

Operability required by LCO 3.4.14 in Modes 1, 2, and 3. With less than one monitor operable, grab samples must be analyzed or perform an RCS water inventory balance once per 24 hours and the monitor must be restored to operable status or verify the containment air cooler condensate flow rate monitor is operable in 30 days or the plant must be in Mode 3 in six hours and Mode 5 in 36 hours.

Operability required by LCO 3.4.14 in Modes 1, 2, and 3. With less than one monitor operable, the monitor must be restored to operable status or verify the containment air cooler condensate flow rate monitor is operable in 30 days or the plant must be in Mode 3 in six hours and Mode 5 in 36 hours.

DRAFT

**Question 16-321:****OPEN ITEM****Follow-up to RAI 110, Question 16-222.**

In RAI-SRP16-CTSB-110/222, the staff requested an explanation regarding the Bases statement on page B 3.3.1-9 of Rev. 0, which reads "The implementation of manual system level actuation of ESF functions and the priority between the automatic functions of the PS and the manual system level initiation is determined on a case-by-case basis." The response states that because the possibility exists for contradictory protective orders (one automatic, one manual) to be given to a function simultaneously, priority must be established between the two functions. Although the response discusses compliance with requirements for manual initiation identified in IEEE std 603-1998, it does not adequately address the staff's question regarding the operator's ability to effectively implement manual protective actions in all cases. The applicant has deleted the statement on the basis that it is not necessary to the Technical Specification Bases discussion and could be confusing. This issue is identified as an open item in the SER w/OI for Chapter 16 of the EPR FSAR.

**Response to Question 16-321:**

The U.S. EPR Instrumentation and Control (I&C) architecture implements several interrelated design principles such as defense-in-depth, diversity, redundancy, independence and priority to optimize plant safety. These principles are applied so that the impact of failures is minimized and the required safety functions are executed when required.

As discussed in U.S. EPR FSAR Tier 2 Section 7.1.1.6.5, "Priority," the U.S. EPR I&C design allows for multiple I&C systems to send requests to a given actuator. To make certain that each individual actuator executes the proper action for the given plant condition, priority management rules are provided. The four primary functional categories provide the basis for priority management of the U.S. EPR I&C architecture. The order of priority for automatic functions is listed from highest to lowest:

- Safety-related I&C functions (safety-related)
  - Actuation functions
  - Control functions
- Risk reduction I&C functions (non-safety-related)
- Limitation I&C functions (non-safety-related)
- Operational I&C functions (non-safety-related)
  - Equipment protection functions
  - Automatic control
  - Manual control

The Priority and Actuator Control System manages priority for safety-related components. For non-safety-related components, priority is managed in the application software of the Level 1 I&C systems.

The I&C systems design is integrated with the human factors engineering (HFE) principles addressed in U.S. EPR FSAR Tier 2 Chapter 18, "Human Factors Engineering," for improved human reliability and overall plant safety.

The relative priority between manual and automatic functions is not addressed by or in the requirements, guidance, or content of 10 CFR 50.36, "Technical Specifications," Standard Review Plan Chapter 16, "Technical Specifications," the NRC Policy Statement on Technical Specification Improvements for Nuclear Power Plants, or the NRC's Standard Technical Specifications. Therefore, AREVA believes that this I&C design issue is already addressed as part of the review of U.S. EPR FSAR Tier 2 Chapter 7, "Instrumentation and Controls."

**FSAR Impact:**

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

DRAFT

# U.S. EPR Final Safety Analysis Report Markups

DRAFT



3.3 INSTRUMENTATION

3.3.3 Remote Shutdown ~~System~~ Station (RSS)

16-320

LCO 3.3.3 The RSS Functions shall be OPERABLE.

APPLICABILITY: MODES 1, 2, and 3.

ACTIONS

NOTE

~~Separate Condition entry is allowed for each Function.~~

| CONDITION   | REQUIRED ACTION   | COMPLETION TIME |
|---|---|-----------------|
| A. <del>One or more required Functions</del> <u>RSS</u> inoperable. | A.1 Restore <del>required Functions</del> to OPERABLE status. | 30 days         |
| B. Required Action and associated Completion Time not met.          | B.1 Be in MODE 3.   | 6 hours         |
|   | <u>AND</u><br>B.2 Be in MODE 4.                               | 12 hours        |

SURVEILLANCE REQUIREMENTS

| SURVEILLANCE  | FREQUENCY |
|---|-----------|
| SR 3.3.3.1 Verify each required control circuit and transfer switch is capable of performing the intended function. | 24 months |

SURVEILLANCE REQUIREMENTS (continued)

| SURVEILLANCE          |   | FREQUENCY            |
|-----------------------|---|----------------------|
| SR 3.3.3.2            | <p>-----NOTE-----<br/>Neutron detectors are excluded from the CALIBRATION.<br/>-----</p> <p>Perform CALIBRATION for each required instrument division.</p>  | 24 months            |
| <del>SR 3.3.3.3</del> | <del>Perform SENSOR OPERATIONAL TEST of each required Safety Information and Control System division performing the Remote Shutdown System functions.</del> | <del>24 months</del> |
| <u>SR 3.3.3.3</u>     | <u>Verify that the RSS communicates controls and indications with each division of the Plant Information Control System.</u>                                | <u>24 months</u>     |
| <u>SR 3.3.3.4</u>     | <u>Verify the OPERABILITY of the RSS hardware and software.</u>   | <u>24 months</u>     |

16-320

BASES

---

ACTIONS

A.1

Condition A addresses the situation where ~~one or more functions of the~~ RSS ~~are~~ is inoperable. This includes the control and transfer switches ~~for any required Function.~~

The Required Action is to restore the ~~divisions~~ RSS to OPERABLE status within 30 days. The Completion Time is based on operating experience and the low probability of an event that would require evacuation of the control room.

B.1 and B.2

If the Required Action and associated Completion Time of Condition A are not met, the plant must be brought to a MODE in which the LCO does not apply. To achieve this status, the plant must be brought to at least MODE 3 within 6 hours and to MODE 4 within 12 hours. The allowed Completion Times are reasonable, based on operating experience, to reach the required MODE from full power conditions in an orderly manner and without challenging plant systems.

SURVEILLANCE  
REQUIREMENTS

SR 3.3.3.1

SR 3.3.3.1 verifies that each required RSS transfer switch and control circuit performs its intended function. This verification is performed from the reactor shutdown panel and locally, as appropriate. Operation of the equipment from the remote shutdown panel is not necessary. ~~Displays in the MCR and RSS contain real-time plant data prior to, during, and after control transfer from one station to the other.~~ The RSS data is populated from the same information busses that supply data to the MCR. During the time control is transferred from the MCR to the RSS or vice versa, the operator will have seamless transfer of control and data will not be interrupted. The operators will have an indication via the control system that RSS control has been established. This will ensure that if the control room becomes inaccessible, the plant can be brought to and maintained in MODE 3 from the reactor shutdown panel and the local control stations. The 24 month Frequency is based on the need to perform this Surveillance under the conditions that apply during a plant outage and the potential for an unplanned transient if the Surveillance were performed with the reactor at power. Operating experience demonstrates that RSS control usually passes the Surveillance when performed at a Frequency of once every 24 months.

16-320

## BASES

## SURVEILLANCE REQUIREMENTS (continued)

SR 3.3.3.2

A CALIBRATION of each required instrument display function on the RSS every 24 months ensures that each instrument division is reading accurately and within tolerance. A CALIBRATION is a complete check of the instrument division, including the sensor. The test verifies that the division responds to the measured parameter within the necessary range and accuracy. CALIBRATION leaves the division adjusted to account for instrument drift to ensure that the division remains operational between successive tests.

SR 3.3.3.3

This Surveillance verifies that the RSS communicates controls and indications with each division of the Plant Information and Control System (PICS). The operator can select the controls and indications available through each PICS division. The Frequency is based on the known reliability of the Functions and the redundancy available, and has been shown to be acceptable through operating experience.

SR 3.3.3.4

16-320 →

SR 3.3.3.4 verifies the OPERABILITY of the RSS hardware and software by performing diagnostics to show that operator displays are capable of being called up and displayed to an operator at the RSS. The RSS has video display units which can be used by the operator. The operator can display information on the video display units in the same manner in which the information is displayed in the control room. The operator normally selects an appropriate set of displays based on the particular operational goals being controlled by the operator at the time. The Frequency of 24 months is based on the use of the data display capability in the control room as part of the normal unit operation and the availability of multiple video display units at the RSS. The Frequency of 24 months is based upon operating experience and consistency with control room hardware and software.

SR 3.3.3.3

~~A SOT on each division performing the RSS functions is performed every 24 months to ensure the entire division will perform its intended function when needed. A SOT shall be the injection of a simulated or actual signal into the division as close to the sensor as practicable to verify OPERABILITY of all devices in the division required for division OPERABILITY. The SOT shall include adjustments, as necessary, of the required alarm, interlock, and trip setpoints required for division~~