Response to

Request for Additional Information No. 110 (1295, 1331), Revision 0

10/28/2008

U. S. EPR Standard Design Certification
AREVA NP Inc.
Docket No. 52-020
SRP Section: 16 - Technical Specifications
Application Section: FSAR Ch. 16

QUESTIONS for Technical Specification Branch (CTSB)

Question 16-210:

Resolve the apparent deviation from the definition and scope provided in 10 CFR 50.36 for limiting safety system settings (LSSS), as described in the BACKGROUND portion of B 3.3.1. Revise the text accordingly.

On page B 3.3.1-4, third full paragraph, it was proposed that: "Meeting the acceptable dose limit for an accident category is considered having acceptable consequences for that event. However, these values and their associated LTSPs are not considered to be LSSS as defined in 10 CFR 50.36." Contrary to this statement, 10 CFR 50.36 defines LSSS as settings for automatic protective devices related to those variables having significant safety functions. This would include settings for protective devices needed for initiation of engineered safety features to mitigate design basis accidents such that 10 CFR 100 limits are not exceeded.

Response to Question 16-210:

The approach utilized to address setpoints for the U.S. EPR Technical Specifications was to follow the ongoing NRC/industry setpoint developments. The related Technical Specification Task Force (TSTF) Traveler (TSTF-493) was originally submitted to NRC on January 27, 2006. The approach and wording of the Bases utilized in the development of the U.S. EPR Technical Specifications was based on Revision 2 of TSTF-493. AREVA NP is not aware of a more suitable industry guidance document, approved NRC policy, or precedent on which to base an update to its approach.

It is noted that for this citation, the recommended NUREG-1431 wording in the TSTF section for RTS Instrumentation is different than the wording for engineered safety feature actuation system (ESFAS) instrumentation. However, since both sets of wording state that these types of value as specified in the Technical Specifications, are not considered to be Limited Safety System Settings (LSSSs), no changes will be made.

FSAR Impact:

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

Question 16-211:

Provide a cross-reference between the EPR TS Section 3.3 and the NUREG-1431 TS Section 3.3 showing how the nine original subsections of NUREG-1431 have been addressed by the three subsections of the EPR application.

NUREG-1431, Standard Technical Specifications for Westinghouse Plants, TS Section 3.3, Instrumentation, has the following nine subsections:

Reactor Trip System
Engineered Safety Feature Actuation System
Post Accident Monitoring Instrumentation
Remote Shutdown System
Loss of Power Diesel Generator Start Instrumentation
Containment Purge and Exhaust Isolation Instrumentation
Control Room Emergency Filtration System Actuation Instrumentation
Fuel Building Air Cleanup System Actuation Instrumentation
Boron Dilution Protection System

The corresponding TS Section 3.3 in the EPR Design Certification (DC) application addresses only the following three subsections:

Protection System
Post Accident Monitoring Instrumentation
Remote Shutdown System

This is required to ensure that the necessary specifications for Instrumentation and Controls have been addressed.

Response to Question 16-211:

As discussed in U.S. EPR FSAR Tier 2, Chapter 16, Technical Specification (TS) Bases 3.3.1 "Protection System (PS)", the PS initiates a reactor trip to protect against violating the core specified acceptable fuel design limits and breaching the reactor coolant pressure boundary during anticipated operational occurrences (AOO). The PS also initiates the Engineered Safety Features (ESF) actuations that are used to mitigate accidents. The ESF actuates necessary safety systems, based upon the values of selected unit parameters, to protect against violating core design limits, maintain the reactor coolant system pressure boundary, and mitigate the consequences of accidents that could result in potential exposures comparable to the guidelines set forth in 10 CFR 100 during AOO and provides an acceptable consequences during accidents. As such, the NUREG-1431, Standard Technical Specifications for Westinghouse Plants, Sections "Reactor Trip System" and " Engineered Safety Feature Actuation System (ESFAS)" were combined in the U.S. EPR Technical Specifications and are addressed in U.S. EPR FSAR Tier 2, Chapter 16, Technical Specification 3.3.1 "Protection System (PS)".

The NUREG-1431, Standard Technical Specifications for Westinghouse Plants, Section for "Post Accident Monitoring Instrumentation" corresponds to U.S. EPR FSAR Tier 2, Chapter 16, Technical Specification 3.3.2, "Post Accident Monitoring (PAM) Instrumentation".

The NUREG-1431, Standard Technical Specifications for Westinghouse Plants, Section for "Remote Shutdown System" corresponds to U.S. EPR FSAR Tier 2, Chapter 16, Technical Specification 3.3.3, "Remote Shutdown System (RSS)".

The NUREG-1431, Standard Technical Specifications for Westinghouse Plants, requirements for "Loss of Power Diesel Generator Start Instrumentation" have been incorporated into U.S. EPR FSAR Tier 2, Chapter 16, Technical Specification 3.3.1 "Protection System (PS)". The functions are explicitly cited in TS Table 3.3.1-2.

The NUREG-1431, Standard Technical Specifications for Westinghouse Plants, requirements for "Control Room Emergency Filtration System Actuation Instrumentation" have been incorporated into U.S. EPR FSAR Tier 2, Chapter 16, Technical Specification 3.3.1 "Protection System (PS)". The functions are explicitly cited in TS Table 3.3.1-2 as Control Room Heating, Ventilation, and Air Conditioning Reconfiguration to Recirculation Mode on High Intake Activity.

The NUREG-1431, Standard Technical Specifications for Westinghouse Plants, requirements for "Boron Dilution Protection System" have been incorporated into U.S. EPR FSAR Tier 2, Chapter 16, Technical Specification 3.3.1 "Protection System (PS)". The functions are explicitly cited in TS Table 3.3.1-2 as the Chemical and Volume Control System (CVCS) Anti-Dilution Mitigation functions.

There are no corresponding functions in the U.S. EPR design for "Containment Purge and Exhaust Isolation Instrumentation" or "Fuel Building Air Cleanup System Actuation Instrumentation". There are no corresponding ESF as described in U.S. EPR FSAR Tier 2, Chapter 7 or credited in U.S. EPR FSAR Tier 2, Chapter 15.

FSAR Impact:

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

Question 16-212:

Provide a summary of the analysis or identify the summary of the anaylsis in the EPR FSAR.

In the EPR FSAR add a summary of the analysis (if needed) and identify in the EPR Bases, Section B 3.3.2 where the summary of the analysis can be found in the EPR FSAR to ensure that the EPR GTS, Table 3.3.2-1, Post Accident Monitoring Instrumentation includes the entire population of instruments required by GDC 13, 19 and 64 and the guidance included in IEEE 497-2002 and Regulatory Guide 1.97. that established the required instrumentation for post accident monitoring.

This additional information is needed to ensure the accuracy and completeness of the EPR GTS, Bases and FSAR.

Response to Question 16-212:

A response to this question will be provided by March 19, 2009.

Question 16-213:

Provide additional information needed to clarify information in the EPR Bases, Section B 3.3.2, regarding secondary loop cooling.

The EPR Bases, Section B 3.3.2, LCO Section (pg B 3.3.2-3 and 4), Item 1, Cold Leg Temperature (Wide Range) states that "the key variables for monitoring core cooling are Hot Leg Temperature, Core Exit Temperature, and Steam Generator Pressure. Cold Leg Temperature provides backup temperature monitoring to Hot Leg Temperature and Core Exit Temperature when forced or verified natural circulation exists. Cold Leg Temperature is used with Hot Leg Temperature and Core Exit Temperature to verify natural circulation. Cold Leg Temperature is compared to the saturation temperature for steam generator pressure (Tsat) to determine primary to secondary loop coupling. Item 9, Hot Leg Temperature (Wide Range) states that "Hot Leg Temperature is required to monitor core cooling, to verify natural circulation, and to verify primary to secondary loop coupling along with steam generator pressure. Hot Leg temperature and RCS pressure are used to determine loop subcooling margin if the calculation is not available." Provide addition information to the EPR Bases, Section B 3.3.2, needed to clarify how Hot Leg Temperature can be used to confirm secondary loop cooling without Cold Leg Temperature.

This additional information is needed to ensure the accuracy and completeness of the EPR Bases.

Response to Question 16-213:

A response to this question will be provided by March 19, 2009.

Question 16-214:

Provide additional information to clarify the EPR Bases, Section B 3.3.2, Action Section reference to D.1 and D.2 in the EPR GTS, Table 3.3.2-1.

EPR Bases, Section B 3.3.2, Action Section reference to D.1 and D.2 states that "if the Required Action and associated Completion Time of Condition C are not met and Table 3.3.2-1 directs entry into Condition E, 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 plant conditions from full power conditions in an orderly manner and without challenging plant systems. However, the EPR GTS, LCO 3.3.2, Action D.1 and D.2 do not reference Table 3.3.2-1. Clarification is needed to explain these inconsistencies between the EPR GTS and EPR Bases.

The additional information is needed to ensure accuracy and completeness of the EPT GTS and Bases.

Response to Question 16-214:

U.S. EPR FSAR Tier 2, Chapter 16, Technical Specification Section 3.3.2 "PAM Instrumentation" Bases will be clarified to remove reference to Table 3.3.2-1.

FSAR Impact:

U.S. EPR FSAR Tier 2, Chapter 16, Technical Specification Section 3.3.2 Bases will be revised as described in the response and indicated on the enclosed markup.

Question 16-215:

Provide an EPR FSAR summary of the analysis or identify the EPR FSAR summary of the anaylsis in the EPR Bases.

In the EPR FSAR add a summary of the analysis (if not already documented) and identify in the EPR Bases, Section B 3.3.3 where the summary of the analysis can be found in the EPR FSAR. Insure the summary of analysis includes the required functions, required control circuits, required transfer switches and required instruments required by GDCs 1, 2, 3, 4 and 19 and the guidance contained in RG 1.155 and 1.189 that established the required instrumentation for the Remote Shutdown System.

This additional information is needed to ensure the accuracy and completeness of the EPR GTS, Bases and FSAR.

Response to Question 16-215:

A response to this question will be provided by March 19, 2009.

Question 16-216:

Provide additional information needed to clarify the completion of a reactor trip and confirm the reactor trip from the remote shutdown station (RSS) in the EPR Bases, Section B3.3.3.

The EPR Bases, Section B 3.3.3, Applicable Safety Analyses Section, state that the RSS provides the control room operator with sufficient instrumentation and controls to place and maintain the unit in a safe shutdown condition, however, the Bases does not provide any information on the achievment of a safe shutdown condition or maintaining the safe shutdown condition from the RSS.

This additional information is needed to ensure the accuracy and completeness of the EPR GTS and Bases.

Response to Question 16-216:

The Applicable Safety Analyses Section for U.S. EPR FSAR Tier 2, Chapter 16, Technical Specification Bases 3.3.3 "Remote Shutdown System (RSS)" contains the same information and level of detail provided in the Applicable Safety Analyses Section in the Standard Technical Specifications for Westinghouse Plants NUREG-1431, Bases 3.3.4 "Remote Shutdown System".

FSAR Impact:

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

Question 16-217:

LCO 3.3.1, Protection System

Confirm that the reactor trip and ESF actuation functions credited in the accident analysis are specifically identified by FSAR Table 7.2-1, "Reactor Trip Variables," and Table 7.3-1, ESF Actuation Variables, and identify any exceptions or additions relative to these tables, based on the FSAR Chapter 15 accident analysis. Revise the text accordingly, to provide a more explicit description of credited functions and supporting references.

On page B 3.3.1-11, the proposed Applicable Safety Analyses section provides a general reference to FSAR Sections 7.2 and 7.3 for the bases of functions not credited in the accident analysis and the bases for exclusion from the Technical Specifications. However, these references were not sufficiently explicit to provide traceability to the accident analysis with respect to credited functions and associated instrumentation.

Response to Question 16-217:

A response to this question will be provided by June 30, 2009.

Question 16-218:

LCO 3.3.1, Protection System

Resolve the inconsistency between TS Table 3.3.1-1, "Protection System Sensors, Manual Action Switches, Signal Processors, and Actuation Devices," and the TS Bases (page B3.3.1-15 and Table B 3.3.1-1) as well as with FSAR Table 7.2-1 and FSAR Figure 7.2-5, with respect to rod cluster control assembly (RCCA) position, which was not included in Table 3.3.1-1 as a reactor protection sensor.

Table B 3.3.1-1, "Protection System Functional Dependencies," FSAR Table 7.2-1, "Reactor Trip Variables," and FSAR Figure 7.2-5, "Low DNBR," identify RCCA position as a monitored variable used as an input for the low DNBR protective function. However, RCCA position was not included as a sensor in TS Table 3.3.1-1. Resolution is required to demonstrate consistency of the proposed Technical Specification with the reactor protection design and licensing basis.

Response to Question 16-218:

The requirements for RCCA Position Indication are included in U.S. EPR FSAR Tier 2, Chapter 16, Technical Specification LCO 3.1.7, "Rod Control Cluster Assembly (RCCA) Position Indication". To avoid duplication, the potential for different requirements, and to minimize the potential for operator error, the requirements for RCCA position indication are contained in only one location.

FSAR Impact:

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

Question 16-219:

Confirm, in the Background portion of B 3.3.1, that the acceptable limits during accidents are such that the offsite dose shall be maintained within an acceptable fraction of [emphasis added] 10 CFR 100 limits, based on the probability of occurrence of the specific accident category. Revise the text accordingly, or justify the deviation.

The proposed wording on page B 3.3.1-4, third full paragraph, does not identify the need for margins to 10 CFR 100 limits, based on probability of occurrence of the specific accident. This appears to deviate from the Bases in NUREG-1431 (WOG STS p. B 3.3.1-3), which includes this provision.

Response to Question 16-219:

The Bases will be clarified to reflect the need to limit doses to within an acceptable fraction of 10 CFR 100 limits.

FSAR Impact:

U.S. EPR FSAR Tier 2, Chapter 16, Technical Specification Section 3.3.1 Bases will be revised as described in the response and indicated on the enclosed markup.

Question 16-220:

Clarify what is meant by "associated instrumentation" in the Background portion of B 3.3.1, where it is stated that one type of module is "sensors, which include associated instrumentation." Describe the hardware and software boundaries for this type of module. Revise the text accordingly.

The reference to sensors and associated instrumentation appears on pp. B 3.3.1-4 and B 3.3.1-5. It was not evident what hardware or software would be included in this description. For example, state if this includes analog filters and analog-to-digital converters, or if these components are included in the remote acquisition units (RAUs) and / or the acquisition and processing units (APUs). Because the term "sensors" is used throughout the TS for LCOs and surveillance requirements, it is necessary to define the term actually included in this terminology.

Response to Question 16-220:

The Protection System architecture is described in ANP-10281P, “U.S. EPR Digital Protection System Topical Report,” which is cited as Reference 1 in this Bases section. The Bases will be revised to delete the reference to associated instrumentation and to replace it with the term "signal conditioning" to be more closely in alignment with the Topical Report.

The Standard Technical Specifications for Westinghouse Plants (NUREG-1431) does not define each component of the Reactor Trip System Instrumentation in the Reactor Trip System Instrumentation Section (B 3.3.1); nor does it define each component of the Engineered Safety Feature Actuation System in the Engineered Safety Feature Actuation System Instrumentation Section (B 3.3.2).

The U.S. EPR Technical Specification Bases for the Protection System contains a greater level of detail than the corresponding Standard Technical Specifications and the details of the Protection System architecture are more appropriately contained in the Topical Report and design documents.

FSAR Impact:

U.S. EPR FSAR Tier 2, Chapter 16, Technical Specification Section 3.3.1 Bases will be revised as described in the response and indicated on the enclosed markup.

Question 16-221:

Clarify the basis for processing data from "three or four" redundant divisions of APU outputs in the voter computers (ALUs). Confirm that this simply means that there are some protection functions implemented with three divisions rather than four, or provide an alternate explanation. Revise the text accordingly.

The conditions under which the ALUs would only process data from three divisions, rather than four, was not clear from the text on page B 3.3.1-7, fourth paragraph. As worded, it might suggest that one division could be ignored (vs. determined to have invalid data) and excluded from all processing. Or the description could imply that there are some protection functions implemented with three divisions rather than four, which is the case for a few components in Table 3.3.1-1.

Response to Question 16-221:

The acquisition and processing units (APU) are the data-processing computers. As shown in TS Table 3.3.1-1, and discussed in the Bases, the Protection System contains four divisions of APU. TS Table 3.3.1-2 shows that only three divisions are required for functional capability. In the Bases, the following is states:

> "Three of the four divisions are necessary to meet the redundancy and testability of GDC 21 in 10 CFR 50, Appendix A (Ref. 3). The fourth division provides additional flexibility by allowing one division to be removed from service for maintenance or testing while still maintaining a minimum two-out-of-three logic."

In the context of the cited sentence and as noted in the NRC Question, the reference to three or four is subject to interpretation and does not add to the discussion. Therefore, the reference to "three or four" will be deleted.

FSAR Impact:

U.S. EPR FSAR Tier 2, Chapter 16, Technical Specification Section 3.3.1 Bases will be revised as described in the response and indicated on the enclosed markup.

Question 16-222:

Explain what is meant by the statement on page B 3.3.1-9, "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." Describe the complience with requirements for manual initiation identified in IEEE Std 603-1998. Revise the text accordingly.

IEEE Std 603-1998, "IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations," Section 6.2, "Manual control," requires in part that "Means shall be provided in the control room to implement manual initiation at the division level of the automatically initiated protective actions." This is a fundamental functional and design requirement, which contains no consideration of priorities between automatic functions and manual system level initiation as suggested by the proposed Bases.

Response to Question 16-222:

A response to this question will be provided by March 31, 2009.

Question 16-223:

Describe the bases for LCOs and surveillance testing of the hardwired "AND" logic for reactor trip functions, and the hardwired "OR" logic for ESF actuation functions. Identify the specific LCO conditions and surveillance(s) that are credited for the instrumentation supporting these functions. Modify the text and Table 3.3.1-1, "Protection System Sensors, Manual Actuation Switches, Signal Processors, and Actuation Devices," as necessary to provide or clarify this information.

FSAR Figure 7.2-1, "Typical RT Actuation," and Figure 7.3-1, "Typical ESF Actuation," identify hardwired logic downstream of the ALUs. FSAR 7.2.2.2, Failure Modes and Effects Analysis, notes that failures in the hardwired output logic are generally not detected automatically by the PS. This implies that the hardwired "AND" logic for reactor trip, the hardwired "OR" logic for ESF actuation functions, and other downstream logic require periodic surveillance. The specific LCO conditions and surveillances applicable to this instrumentation were not evident from the Bases or from Table 3.3.1-1.

Response to Question 16-223:

A response to this question will be provided by March 31, 2009.

Question 16-224:

The following are editorial and typographical errors discovered in the text of EPR GTS Section 3.3.

#1 On page B 3.3.1-6, second full paragraph, should be "Allowable Value,"not "Allowable Values."

#2 On page B 3.3.1-6, third full paragraph, should be "process transmitter," not "processing transmitter."

#3 On page B 3.3.1-9, last paragraph, should be "CRDM."

Response to Question 16-224:

The cited editorial and typographical errors will be corrected in U.S. EPR FSAR Tier 2, Chapter 16, Technical Specification Section 3.3.1 "Protection System (PS)" Bases.

FSAR Impact:

U.S. EPR FSAR Tier 2, Chapter 16, Technical Specification Section 3.3.1 Bases will be revised as described in the response and indicated on the enclosed markup.

Question 16-225:

Delete the sentence, "Non-credited functions are purely equipment protective, and their use minimizes the potential for equipment damage."

The foregoing statement appears on page B 3.3.1-11. It is incorrect, because functions not credited in the accident analysis may also include, for example, anticipatory trips, control system functions, and other functions not considered equipment protective.

Response to Question 16-225:

The referenced sentence in U.S. EPR FSAR Tier 2, Chapter 16, Technical Specification Section 3.3.1 "Protection System (PS)" Bases will be deleted.

FSAR Impact:

U.S. EPR FSAR Tier 2, Chapter 16, Technical Specification Section 3.3.1 Bases will be revised as described in the response and indicated on the enclosed markup.

Question 16-226:

Confirm that in Modes 4 and 5, the protection system sensors, manual actuation switches, and specified actuation devices that support reactor trips are not required to be Operable, only if all rods are fully inserted, and only if the rod control system is placed in a configuration whereby inadvertent control rod withdrawal is precluded. Revise the text accordingly, to clarify the basis for not requiring that this instrumentation and devices be operable in Modes 4 & 5.

Page B 3.3.1-12 includes a statement that this instrumentation and devices are not required to be operable in Modes 4 & 5, and that the reactor is protected in these Modes by ensuring adequate shutdown margin. The statement needs to be clarified to confirm that the proposed basis is not less restrictive than similar bases in NUREG 1431 (WOG STS).

Response to Question 16-226:

A response to this question will be provided by June 30, 2009.

Question 16-227:

Correct as necessary the inequality signs associated with the limiting trip setpoints identified in Table 3.3.1-2.

In a few cases, the inequality sign associated with the proposed limiting trip setpoint (LTSP) was reversed. For example: the LTSP for reactor trip function 17, low steam generator level, is shown as ≤ 20% narrow range, rather than ≥ 20% narrow range; the LTSP for reactor trip function 19 (high containment pressure) does not include an inequality sign.

Response to Question 16-227:

A response to this question will be provided by March 31, 2009.

Question 16-228:

Revise the Bases description of the low saturation margin reactor trip, to more closely reflect the accident analysis basis.

The Bases described for the low saturation margin trip (p. B 3.3.1-17, reactor trip no. 5) is presented as identical to the high core power level trip, but there is a significant difference. Per FSAR 7.2.1.2.4, "Reactor Trip on High Core Power Level or Low Saturation Margin," the high core power trip function calculates core thermal power from an enthalpy balance, using thermal hydraulic conditions. If saturation were to occur in a hot leg, this calculation would be invalid. This is a basis for the additional low saturation margin trip.

Response to Question 16-228:

A response to this question will be provided by March 31, 2009..

Question 16-229:

Clarify the means by which the emergency diesel generator start signals (LOOP and degraded voltage) are implemented in the protection system, and justify or otherwise explain the "NA" (not applicable) designation for minimum required divisions for functional capability, as presented in Table 3.3.1-2, "Acquisition and Processing Unit Requirements Referenced from Table 3.3.1-1." Revise the Technical Specifications and Bases accordingly.

Acquisition and processing functions, however implemented, would be required for emergency diesel generator (EDG) start signals and logic. In addition, Table 3.3.1-1 contradicts the Bases (p. 3.3.1-44, function 10, Emergency Diesel Generator), which states the following:

"The automatic EDG Start on Degraded Grid Voltage requires four divisions of the following processors to be OPERABLE in MODES 1, 2, 3, and 4 or when the associated EDG is required to be OPERABLE in accordance with
LCO 3.8.2, "AC Sources - Shutdown":

a. 6.9 kV voltage sensors,
b. APUs, and
c. ALUs

The Bases contains a similar statement (p. 3.3.1-44) for starting an EDG on a loss of offsite power (LOOP) condition.

The foregoing suggests that APUs and ALUs are involved in the processing of 6.9 kV bus voltage sensors, which appears contrary to the "NA" assignment in Table 3.3.1-2

Response to Question 16-229:

Refer to the response to RAI 103, Question 16-135.

FSAR Impact:

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

Question 16-230:

Confirm that the continuous self-monitoring functions referenced in SR 3.3.1.7 will be verified during periodic functional tests, and that execution of the automatic tests will be confirmed during plant operation. Revise the Bases and Technical Specifications accordingly.

The Bases for SR 3.3.1.7 identified Extended Self Tests performed at computer startup each cycle. This section also referenced (B 3.3.1 Reference 8) a general summary of features for continuous self-monitoring of the protection system. SR 3.3.1.7 was not applied to these self-monitoring features, nor was any other Surveillance Requirement evident for this purpose. If credit is taken for these features (for example, to perform channel checks or functional tests), then a means is required to confirm that these self-test features remain functional.

Response to Question 16-230:

The self-monitoring functions (i.e., cyclic self-monitoring task) verify the operability of TXS hardware by continuously testing the function computer. The cyclic self-monitoring task performed by the TXS protective systems is described in Reference 1 and has been reviewed and accepted by the NRC as described in Reference 2. The cyclic self-monitoring task is implemented as a continuous test process in each function computer to provide the earliest possible detection of hardware faults. The cyclic self-monitoring task checks the functions of the computer and the connected components, which are tested during operation without impeding the safety tasks. It operates as an independent task with lowest priority and can be interrupted by programs with a higher priority. The time remaining between the end of processing of the functional tasks and the beginning of the next cycle is used for the processing of cyclic self-monitoring task. Because a complete self-test procedure requires more than a single computer cycle, the cyclic self-monitoring task is divided into smaller tasks that are not interrupted. The small size makes sure that the deterministic cyclic operation of the system is not influenced by the cyclic self-monitoring task. A complete pass of these tests can last a few minutes. The cyclic self-monitoring task also includes a cyclic redundancy check to verify the software has not been degraded. If the cyclic self-monitoring task is not completed within one hour, an error message is generated.

Periodic surveillance testing is normally required to check for degradation in systems and components that are not continuously in operation (i.e., inoperability would not be readily apparent). As discussed previously, the cyclic self-monitoring task is in continuous operation and will alarm if not successful. The cyclic self-monitoring task is performed by software. The adequacy of the software and its proper functioning does not have to be periodically verified by surveillance testing. The adequacy of the Protection System software is based on the software development methodology, verification and validation (V&V) of the software, and the ability of the Protection System to continuously verify that the software has not been degraded. The extended self test (TS Surveillance Requirement 3.3.17) includes a basic hardware test and a cyclic redundancy check to verify the software has not been degraded (Reference 3).

References:

1. EMF-2110(NP)(A), Revision 1, “TELEPERM XS: A Digital Reactor Protection System,” Siemens Power Corporation, July 2000.

2. Letter dated Mar 5, 2000, from Stuart A. Richards, NRC, to Jim Mallay, Siemens Power Corporation, "Acceptance for Referencing of Licensing Topical Report EMF-2110(NP), Revision 1, "TELEPERM XS: A Digital Reactor Protection System" (TAC No. MA1983)."

3. EMF-2341(P), Revision 1, "Generic Strategy for Periodic Surveillance Testing of TELEPERM XS Systems in U.S. Nuclear Generating Stations," March 2000.

FSAR Impact:

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

Question 16-231:

Provide the basis for the six hour delay permitted for entry into associated Conditions and Required Actions, when a sensor, manual actuation switch, signal processor, or actuation device is placed in an inoperable status solely for performance of required Surveillances.

Note 2 of the Surveillance Requirements stipulates that "when a sensor, manual actuation switch, signal processor, or actuation device is placed in an inoperable status solely for performance of required Surveillances, entry into associated Conditions and Required Actions may be delayed for up to 6 hours provided the associated Trip/Actuation Function maintains functional capability."
The basis for Note 2 was not provided in the Bases for 3.3.1.

Response to Question 16-231:

The basis for the Note will be provided in U.S. EPR FSAR Tier 2, Chapter 16, Technical Specification Bases 3.3.1 "Protection System (PS)".

FSAR Impact:

U.S. EPR FSAR Tier 2, Chapter 16, Technical Specification Section 3.3.1 Bases will be revised as described in the response and indicated on the enclosed markup.

Question 16-232:

Revise the Bases to reference the versions or revisions of topical reports for which the Staff has issued an SER accepting the report.

The following references cited in the Bases for 3.3.1 were not versions accepted by the Staff via an SER:

a. Reference 4: ANP-10287, Incore Trip Setpoint and Transient Methodology for U.S. EPR, November 2007.

b. Reference 7: ANP-10271P, Revision 0, US EPR Nuclear Incore Instrumentation Systems Report, December 2006.

c. Reference 8: EMF-2341(P), Revision 1, Generic Strategy for Periodic Surveillance Testing of TELEPERM XS System in U.S. Nuclear Generating Stations, March 2000.

Response to Question 16-232:

ANP-10287, “Incore Trip Setpoint and Transient Methodology for U.S. EPR,” November 2007, is under NRC review.

With regards to the reference to ANP-10271P, “U.S. EPR Nuclear Incore Instrumentation Systems Report,” December 2006, the reference will be revised to cite a more recent Topical Report: ANP-10282P, "POWERTRAX/E Online Core Monitoring Software for the U.S. EPR Technical Report," November 2007 and is under NRC review.

EMF-2341(P), Revision 1, Generic Strategy for Periodic Surveillance Testing of TELEPERM XS System in U.S. Nuclear Generating Stations, was referenced by NRC in the May 5, 2000 Safety Evaluation for Licensing Topical Report EMF-2110(NP), Revision 1, rather than separately approved.

In addition, on the same page in the U.S. EPR FSAR Tier 2, Chapter 16, Technical Specification Section 3.3.1 "Protection System (PS)" Bases, the reference to ANP-10275P, "U.S. EPR Instrument Setpoint Methodology Topical Report,” will be updated to reflect the NRC approved version.

FSAR Impact:

U.S. EPR FSAR Tier 2, Chapter 16, Technical Specification Section 3.3.1 Bases will be revised as described in the response and indicated on the enclosed markup.

Question 16-233:

Provide a specific reference to the source document supporting the assertion that, single failures upstream of the ALU layer that could result in an invalid signal being used in the reactor trip actuation are marked as faulted by modifying the vote in the ALU layer, and that for the reactor trip functions, the vote is always modified toward actuation.

The foregoing assertion appears on page B 3.3.1-8, last paragraph. The supporting design and licensing basis was not evident in FSAR Chapter 7.

Response to Question 16-233:

Supporting information for the cited statement can be found in Section 7.3 of ANP-10281P, "U.S. EPR Digital Protection System Topical Report," March 2007, which is referenced in U.S. EPR FSAR Tier 2, Section 7.1, "Instrumentation and Controls - Introduction".

FSAR Impact:

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

Question 16-234:

The EPR Bases, Section 3.3.2, SR 3.3.2.2 states that "the SOTshall include adjustments, as necessary, of the required alarm, interlock, and trip setpoints required for division OPERABILITY such that the setpoints are within the necessary range and accuracy." Additional information is needed to explain the intent of this statement because the PAM system contains monitoring instrumentation, not alarms, interlocks or trips.

This additional information is need to ensure the accuracy and completeness of the EPR Bases.

Response to Question 16-234:

References to the Sensor Operational Test will be deleted in U.S. EPR FSAR Tier 2, Chapter 16, Technical Specification 3.3.2, "PAM Instrumentation" and U.S. EPR FSAR Tier 2, Chapter 16, Technical Specification Bases 3.3.2, "PAM Instrumentation".

FSAR Impact:

U.S. EPR FSAR Tier 2, Chapter 16, Technical Specification Section 3.3.2 and Bases will be revised as described in the response and indicated on the enclosed markup.

Question 16-235:

The EPR Bases, Section 3.3.3, Applicability Section states that "this LCO is not applicable in MODE 4, 5, or 6. In these MODES, the unit is already subcritical and in the condition of reduced RCS energy. Under these conditions, considerable time is available to restore necessary instrument control Functions if control room instruments or control become unavailable." The Westinghouse STS states that "in MODES 4, 5,and 6, unit conditions are such that the likelihood of an event that would require PAM instrumentation is low, therefore, the PAM instrumentation is not required to be OPERABLE in these MODEs." Provide a technical justification for the STS Bases statement not applying to the EPR design or revise the EPR Bases to reflect the wording in the STS.

This technical justification is need to ensure the accuracy and completeness of the EPR Bases and for consistency with amongst the GTS, STS, and PTS.

Response to Question 16-235:

A comparison between the wording of comparable sections in the U.S. EPR FSAR Tier 2, Chapter 16 Technical Specifications and NUREG-1431 is presented below, with the differences are highlighted:

U.S. EPR TECHNICAL SPECIFICATIONS BASES SECTION 3.3.2, PAM INSTRUMENATION – APPLICABILITY	NUREG-1431 BASES SECTION 3.3.3, PAM INSTRUMENTATION – APPLICABILITY
The PAM instrumentation LCO is applicable in MODES 1, 2, and 3. These variables are related to the diagnosis and preplanned actions required to mitigate postulated accidents. The applicable postulated accidents are assumed to occur in MODES 1, 2, and 3. In MODES 4, 5, and 6, plant conditions are such that the likelihood of an event occurring that would require PAM instrumentation is low; therefore, PAM instrumentation is not required to be OPERABLE in these MODES.	The PAM instrumentation LCO is applicable in MODES 1, 2, and 3. These variables are related to the diagnosis and pre-planned actions required to mitigate DBAs. The applicable DBAs are assumed to occur in MODES 1, 2, and 3. In MODES 4, 5, and 6, unit conditions are such that the likelihood of an event that would require PAM instrumentation is low; therefore, the PAM instrumentation is not required to be OPERABLE in these MODES.

U.S. EPR TECHNICAL SPECIFICATIONS BASES SECTION 3.3.3, REMOTE SHUTDOWN SYSTEM (RSS) - APPLICABILITY	NUREG-1431 BASES SECTION 3.3.4, REMOTE SHUTDOWN SYSTEM - APPLICABILITY
The RSS LCO is applicable in MODES 1, 2, and 3. This is required so that the unit can be placed and maintained in MODE 3 for an extended period of time from a location other than the control room.	The Remote Shutdown System LCO is applicable in MODES 1, 2, and 3. This is required so that the unit can be placed and maintained in MODE 3 for an extended period of time from a location other than the control room.
This LCO is not applicable in MODE 4, 5, or 6. In these MODES, the unit is already subcritical and in the condition of reduced RCS energy. Under these conditions, considerable time is available to restore necessary instrument control Functions if control room instruments or control become unavailable.	This LCO is not applicable in MODE 4, 5, or 6. In these MODES, the facility is already subcritical and in a condition of reduced RCS energy. Under these conditions, considerable time is available to restore necessary instrument control functions if control room instruments or controls become unavailable.

The applicability requirements between the comparable sections are the same.

FSAR Impact:

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

Question 16-236:

Confirm EPR EDG fuel oil capacity.

Confirm that 1350 gallons fuel oil tank capacity is sufficient for one EDG in each train to carry the alternate feed and operating loads for an entire division. The EPR GTS, SR 3.8.1.4, requires a minimum of 1350 gallons in each EDG day tank. This is required to ensure adequate fuel oil will be available.

Technical justification is needed to ensure the accuracy and completeness of the EPR GTS.

Response to Question 16-236:

A response to this question will be provided by March 31, 2009..

Question 16-237:

Provide additional information to confirm that the EPR EDG voltage acceptance criteria will result in acceptable voltage for all safety-related loads.

Surveillance Requirement 3.8.1.2 provided non-bracketed acceptance criteria for EDG steady state voltage and frequency indicating those values were applicable for all EPR sites. The BASES refers to American National Standards Institute Standard ANSI 84.1, Electric Power Systems and Equipment - Voltage Ratings (60 Hz), as the reference for the acceptance for the permissible tolerances for voltage. ANSI C84.1 references National Electrical Manufacturers Association standard, NEMA MG-1, Motors and Generators. NEMA MG-1 provides minimum operating parameters specifically for motors and generators. NEMA MG-1 states that the acceptable voltage range is nominal voltage +/- 10% and the acceptable frequency range is 60 Hertz +/- 5%. However, NEMA MG-1 does not recognize using both extremes of voltage and frequency simultaneously. NEMA MG-1 does permit variations in both voltage and frequency if the total variation does not exceed a total of +/- 10 %. The applicant proposes to limit voltage to +5/- 10 % and limit frequency to +/- 2 %. This could result in a total negative variation of -12 % which is outside the total range permitted by NEMA MG-1. This is required to ensure that the safety related loads connected to the EDG will not require derating.

This technical justification is needed to ensure the accurace and completeness of the EPR GTS.

Response to Question 16-237:

A response to this question will be provided by June 30, 2009.

Question 16-238:

Provide a technical justification to explain the differences between the EPR GTS, EDG rating and the applicable STS.

The EPR GTS, SR 3.8.1.10 requires that the momentary voltage developed by the EDG following a full load rejection does not exceed 8280 V, which is 20% greater than rated voltage. The Westinghouse STS, SR 3.8.1.10 requires that the momentary voltage developed by the EDG following a full load rejection does not exceed 5000 V, which is 10% greater than rated voltage. Provide a technical justification for the higher (20%) voltage allowed for the EPR EDGS.

This technical justification is needed to ensure the accurace and completeness of the EPR GTS.

Response to Question 16-238:

The voltage limit provided in the U.S. EPR FSAR Tier 2, Chapter 16, Technical Specification Surveillance Requirement 3.8.1.10 of 8280 V is 20 percent greater than the emergency diesel generator (EDG) rated voltage of 6900 V. The transient voltage rise is consistent with the voltage limit provided in the Standard Technical Specifications for Westinghouse Plants (NUREG-1431) Surveillance Requirement 3.8.1.10 of 5000 V, which is 20 percent greater than the EDG rated voltage of 4160 V. Therefore, the limit of 20 percent for a transient voltage rise is not greater than the transient voltage rise limit provided in NUREG-1431 and is consistent with the guidance provided in NEMA MG 1-2006 (NEMA MG 1-2006, “NEMA Standards Publication MG 1-2006 Motors and Generators,” National Electrical Manufacturers Association, 2006) for definite purpose synchronous generators.

FSAR Impact:

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

Question 16-239:

Provide additional information to verify the differences between the EPR GTS and the applicable STS.

Confirm that the EPR, EDG design supplied to EPR plants do not have an engine mounted fuel oil tank. If there is an engine mounted tank, an EPR GTS, Section 3.8 will require a SR to check and remove water from the EDG engine mounted fuel oil tank.

This additional information is needed to ensure the accuracy and completeness of the EPR GTS.

Response to Question 16-239:

The diesel generator fuel oil storage and transfer system (DGFOSTS) is described in U.S. EPR FSAR Tier 2, Section 9.5.4, "Diesel Generator Fuel Oil Storage and Transfer System". The major components are described in Subsection 9.5.4.2.2, "Component Description". Each emergency diesel generator (EDG) has a separate, independent fuel oil storage and transfer system, as shown in U.S. EPR FSAR Tier 2, Figure 9.5.4-1, "Emergency Diesel Generator Fuel Oil Storage and Transfer System". The information included in the U.S. EPR FSAR includes a storage tank, electrically driven transfer pumps, day tank, fuel delivery pump, piping, strainers, filters, and monitoring systems up to, but not including, that portion of the engine-mounted equipment supplied by the diesel vendor with the diesel generator unit. There is no engine mounted fuel oil tank in the current design.

FSAR Impact:

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

Question 16-240:

Provide additional information to justify differences between the EPR GTS, Sections 5.2.2.d and 5.2.2.f and the applicable STS.

Confirm that the responsibilities and organizational title change to "Senior Operator and the Operator" in the EPR GTS, Sections 5.1, 5.2, and 5.3 have not changed the structure of command from the previous NRC designations of Senior Reactor Operator and Reactor Operator.

This additional information is needed to ensure the accuracy and completeness of the EPR GTS.

Response to Question 16-240:

The terms "Senior Operator" and "Operator" are used in the U.S. EPR GTS to conform to the terminology used by the NRC in RG 1.8, “Qualification and Training of Personnel for Nuclear Power Plants,” and RG 1.114, “Guidance to Operators at the Controls and to Senior Operators in the Control Room of a Nuclear Power Unit” and in 10 CFR 50.54 and 10 CFR 55. The change in terminology to conform to NRC regulations and regulatory guides does not convey any change in roles, responsibility, or organizational structure.

FSAR Impact:

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

Question 16-241:

Provide rationale for omitting COLR limitations on the combination of THERMAL POWER, Reactor Coolant System (RCS) highest loop average temperature and pressurizer pressure from the EPR GTS, Section 2.1.1.

The EPR GTS, Section 2.1.1, Reactor Core SLs, COLR limitations on the combination of THERMAL POWER, Reactor Coolant System (RCS) highest loop average temperature and pressurizer pressure are not delineated in the technical specification. (Note: The EPR Bases, Section B 2.1.1 also discusses COLR requirements.)

This additional information is needed to ensure the accuracy and completeness of the EPR GTS and Bases.

Response to Question 16-241:

A response to this question will be provided by March 31, 2009.

Question 16-242:

Provide the additional information or changes to the EPR GTS, LCO 3.0.6 to make it consistent with the applicable STS.

The EPR Bases, LCO 3.0.6 first sentence of the first paragraph currently states that " LCO 3.0.6 establishes an exception to LCO 3.0.2 for support systems that have an LCO specified in the Technical Specifications (TS)." This sentence should read: "LCO 3.0.6 establishes an exception to LCO 3.0.2 for support systems that have a support system LCO specified in the Technical Specifications (TS)" to remain consistent with the applicable Bases for Westinghouse STS.

The EPR Bases, LCO 3.0.6 fourth paragraph has been edited to insert a new paragraph opening between the second and third sentences. The inserted paragraph should be added after the original fourth paragraph so that the intended meaning behind the fourth paragraph in the applicable bases of the Westinghouse STS remains intact.

Provide a technical justification for not including the Westinghouse STS Bases three Loss of Safety Function conditions a, b, & c and the respective three examples provided in NUREG-1431, Bases document (pg B3.0-8) in the EPR Bases.

Provide a technical justification for not including the Westinghouse STS Bases Figure B 3.0-1, Configuration of Trains and Systems, provided in NUREG-1431, Bases document (pg B3.0-9) in the EPR Bases.

This additional information, technical justifications, and revision are needed to ensure the accuracy and completeness of the EPR Bases and consistency amongst the GTS, STS, and PTS.

Response to Question 16-242:

The U.S. EPR FSAR Tier 2, Chapter 16, Technical Specification LCO 3.0.6 Bases will be revised to conform to the Westinghouse STS.

The two train examples have limited applicability to the U.S. EPR since the safety systems such as emergency core cooling system (ECCS), Emergency Feedwater (EFW), emergency power, Component Cooling Water (CCW), and Essential Service Water (ESW) are four train systems.

FSAR Impact:

U.S. EPR FSAR Tier 2, Chapter 16, Technical Specification LCO 3.0.6 Bases will be revised as described in the response and indicated on the enclosed markup.

U.S. EPR Final Safety Analysis Report Markups

BASES

LCO 3.0.6

16-242

LCO 3.0.6 establishes an exception to LCO 3.0.2 for supported systems that have ~~an~~ a support system LCO specified in the Technical Specifications (TS). This exception is provided because LCO 3.0.2 would require that the Conditions and Required Actions of the associated inoperable supported system LCO be entered solely due to the inoperability of the support system. This exception is justified because the actions that are required to ensure the unit is maintained in a safe condition are specified in the support system LCO's Required Actions. These Required Actions may include entering the supported system's Conditions and Required Actions or may specify other Required Actions.

When a support system is inoperable and there is an LCO specified for it in the TS, the supported system(s) are required to be declared inoperable if determined to be inoperable as a result of the support system inoperability. However, it is not necessary to enter into the supported systems' Conditions and Required Actions unless directed to do so by the support system's Required Actions. The potential confusion and inconsistency of requirements related to the entry into multiple support and supported systems' LCOs' Conditions and Required Actions are eliminated by providing all the actions that are necessary to ensure the unit is maintained in a safe condition in the support system's Required Actions.

However, there are instances where a support system's Required Action may either direct a supported system to be declared inoperable or direct entry into Conditions and Required Actions for the supported system. This may occur immediately or after some specified delay to perform some other Required Action. Regardless of whether it is immediate or after some delay, when a support system's Required Action directs a supported system to be declared inoperable or directs entry into Conditions and Required Actions for a supported system, the applicable Conditions and Required Actions shall be entered in accordance with LCO 3.0.2.

Format per 16-242

Specification 5.5.14, "Safety Function Determination Program (SFDP)," ensures loss of safety function is detected and appropriate actions are taken. Upon entry into LCO 3.0.6, an evaluation shall be made to determine if loss of safety function exists. Additionally, other limitations, remedial actions, or compensatory actions may be identified as a result of the support system inoperability and corresponding exception to entering supported system Conditions and Required Actions. The SFDP implements the requirements of LCO 3.0.6.

Cross train checks to identify a loss of safety function for those support systems that support multiple and redundant safety systems are required.

SURVEILLANCE REQUIREMENTS

----------NOTE----------
This SR applies to each PAM instrumentation Function.

SURVEILLANCE		FREQUENCY
SR 3.3.2.1	Perform CALIBRATION	24 months
~~SR 3.3.2.2~~	~~Perform SENSOR OPERATIONAL TEST of the Safety Information and Control System division performing the PAM functions listed in Table 3.3.2-1.~~	~~24 months~~

16-234

BASES

BACKGROUND (continued)

OPERATIONAL TEST (SOT). As such, the Allowable Value differs from the LTSP by an amount greater than or equal to the expected instrument channel uncertainties, such as drift, during the surveillance interval. In this manner, the actual setting of the device will ensure that an SL is not exceeded at any given point of time as long as the device has not drifted beyond that expected during the surveillance interval. Note that, although the channel is OPERABLE under these circumstances, the setpoint must be left adjusted to a value within the as-left tolerance, and confirmed to be operating within the statistical allowances of the uncertainty terms assigned (as-found). If the actual setting of the device is found to be non-conservative with respect to the Allowable Value, the device would be considered inoperable from a Technical Specification perspective. This requires corrective action including those actions required by 10 CFR 50.36 when automatic protective devices do not function as required.

During AOOs, which are those events expected to occur one or more times during the plant life, the acceptable limits are:

- The departure from nucleate boiling ratio (DNBR) shall be maintained above the SL value to prevent departure from nucleate boiling (DNB),
- Fuel centerline melting shall not occur; and
- The RCS pressure SL of 2803 psia shall not be exceeded.

Maintaining the parameters within the above values ensures that the offsite dose will be within the 10 CFR 100 (Ref. 2) criteria during AOOs.

Accidents are events that are analyzed even though they are not expected to occur during the plant life. The acceptable limit during accidents is that the offsite dose shall be maintained within an acceptable fraction of 10 CFR 100 limits. Meeting the acceptable dose limit for an accident category is considered having acceptable consequences for that event. However, these values and their associated LTSPs are not considered to be LSSS as defined in 10 CFR 50.36.

16-219

The PS is segmented into four interconnected modules and associated LCOs for the reactor trips and ESF functions. These modules are:

- Sensors, which include the associated ~~instrumentation~~signal conditioning;
- Manual actuation switches;

16-220

BASES

BACKGROUND (continued)

- Signal Processors, which include:
  - Remote Acquisition Units (RAUs), which acquire the signals from the Self-Powered Neutron Detectors (SPND) and distribute these signals;
  - Acquisition and Processing Units (APUs), which perform calculations and make setpoint comparisons; and
  - Actuation Logic Units (ALUs), which perform voting of the processing results from the redundant APUs in the different divisions and to issue actuation orders based on the voting results; and
- Actuation Devices, which includes the reactor trip breakers and contactors and the Priority and ~~Actuation~~ Actuator~~and~~ Control Systems (PACS) control modules for the Reactor Coolant Pump (RCP) bus and trip breakers.

The PS is a digital, integrated reactor protection system and engineered safety features actuation system. Individual sensors, signal processors, or the ALUs that provide the actuation signal voting function, can be associated with multiple reactor trip, ESF functions, and Permissives.

16-220

Sensors

Measurement channels, consisting of field transmitters or process sensors and associated ~~instrumentation~~signal conditioning, provide a measurable electronic signal based upon the physical characteristics of the parameter being measured.

The Power Density Detector System, which uses SPND and RAUs, provides the in-core monitoring function. The Power Range, Intermediate Range, and Source Range monitors provide the ex-core monitoring functions.

The instrument setpoint methodologies used for the US EPR were submitted to NRC in References 1 and 4. The majority of PS trips or protection functions are based on single channel inputs; therefore, the uncertainties identified in Section 3.1 of Reference 1 are applicable for the trip. Reference 4 addresses the protection system trips or protection functions that are based on multiple inputs. The uncertainty calculations for the SPNDs, incore instrumentation, high linear power density, high

BASES

BACKGROUND (continued)

core power level, low saturation margin, anti-dilution, and DNBR use the statistical methodology described in Reference 4. As described therein, the LTSP is the LSSS since all known errors are appropriately combined in the total loop uncertainty calculation.

LTSPs in accordance with the Allowable Value will ensure that SLs of Chapter 2.0, "Safety Limits (SLs)," are not violated during AOOs, and the consequences of postulated accidents will be acceptable, providing the plant is operated from within the LCOs at the onset of the AOO or postulated accident and the equipment functions as designed.

16-224

Note that the Allowable Value~~s~~ is the least conservative value of the as-found setpoint that a Trip/Actuation Function can have during a periodic CALIBRATION or SOT, such that a Trip/Actuation Function is OPERABLE if the as-found setpoint is conservative with respect to the Allowable Value.

Functional testing of the entire PS, from sensor input through the opening of individual sets of Reactor Trip Circuit Breakers (RTCB) or contactors, is performed each refueling cycle. Process~~ing~~ transmitter CALIBRATION is also normally performed on a refueling basis.

16-224

Trip Setpoints that directly protect against violating the reactor core or RCS pressure boundary Safety Limits during AOOs are SL-LSSS. Permissive setpoints allow bypass of trips when they are not required by the Safety Analysis. These permissives and interlocks ensure that the starting conditions are consistent with the safety analysis, before preventative or mitigating actions occur. Because these permissives or interlocks are only one of multiple conservative starting assumptions for the accident analysis, they are generally considered as nominal values without regard to measurement accuracy, (i.e. the value indicated is sufficiently close to the necessary value to ensure proper operation of the safety systems to turn the AOO). Therefore permissives and interlocks are not considered to be SL-LSSS.

Manual Actuation Switches

Manual controls necessary to perform the manual operator actions credited in the safety analysis are included within the scope of the Technical Specifications. Manual actuation switches are provided to initiate the reactor trip function from the main control room (MCR) and the remote shutdown station (RSS). The ability to manually initiate ESF systems is provided in the MCR. Manual actuation of ESF systems initiates all actions performed by the corresponding automatic actuation including starting auxiliary or supporting systems and performing required sequencing functions.

BASES

BACKGROUND (continued)

Signal Processors

The PS is a distributed, redundant computer system. It consists of four independent redundant data-processing automatic paths (divisions), each with layers of operation and running asynchronous with respect to each other. In addition to the computers associated with the automatic paths, there are two redundant message and service interface computers to interface with each division.

The measurement channels or signal acquisition layer (which includes the RAUs) in each division acquires analog and binary input signals from sensors in the plant (such as for temperature, pressure, and level measurements). Each signal acquisition computer distributes its acquired and preprocessed input signals to the PS logic and controls, which includes the data processing computers (APUs).

The data-processing computers (APUs) perform signal processing for plant protective functions such as signal online validation, limit value monitoring and closed-loop control calculations. Each PS division contains four ALUs, two assigned to each subsystem. Two ALUs of the same subsystem within a division are redundant and perform the same processing using the same inputs. The outputs of two redundant ALUs are combined in a hardwired "functional AND" logic for reactor trip functions and in a hardwired OR logic for ESF functions. This avoids both unavailability of ESF functions and spurious reactor trips. The data processing computers then send their outputs to two independent voter computer units (ALUs) in each division.

16-221

In the voter computers, the outputs of the data-processing computers of redundant ~~(three or four)~~ divisions are processed together. A voter computer controls a set of actuators. Each voter receives the actuation signal from each of the redundant data-processing computers. The voter's task is to compare this redundant information and compute a validated (voted) actuating signal, which is used for actuating the end devices.

When a signal processor is placed in lockout, network outputs are marked as invalid and are disregarded in downstream processing. For example, a two out of four voting function that receives one faulty input votes two out of three on the remaining non-faulty inputs. Hardwired outputs (i.e., ALU outputs) are forced to a no output state, resulting in a "reactor trip output" and no ESF actuation. No manual actions, beyond placing the signal processor in lockout, are required for the downstream processing to properly accommodate the signal processor in a lockout condition.

BASES

BACKGROUND (continued)

Actuation Devices

16-224

Reactor Trip Actuation Devices

The reactor trip actuation is performed by interrupting electrical power to the Control Rod Drive Mechanisms (~~CRMD~~CRDM). Electrical power to the CRDM is delivered by the Control Rod Drive Power Supply System (CRDPSS). The CRDPSS consists of 220 V DC distribution boards which are fed from the Uninterruptible Power Supply System.

The power supply of the CDRM can be switched off via the following features:

- Four main trip breakers distributed in two electrical divisions. Two breakers are located in Division 2, two others in Division 3. The main trip breakers can be opened by two coils: one with a de-energized logic using an under voltage coil and the other with an energized logic using a shunt trip coil.

- There are 23 sets of four trip contactors, each set capable of removing power to four CRDM power supplies. Eleven sets of contactors are located in physical division one and twelve sets are located in physical division four. Each division of the PS is assigned to one contactor in each of the 23 sets. Each set of four contactors is arranged to require two out of four PS reactor trip orders to drop the rods assigned to the contactor set.

- The electronics of the RodPilot can switch-off the power supply of four CRDMs. Two groups of four commands can actuate this electronic module, one with low active and one with high active logic. The electronics of the RodPilot is a non-safety device of the reactor trip but is the fastest switching device and allows the contactors and the trip breaker to open without stress.

- The under voltage coil of the main trip breakers is actuated by the automatic reactor trip signals of the PS and the manual trip from the SICS panel. The shunt coil of the main trip breakers is actuated by the automatic reactor trip signal from the SAS and the manual trip signal from the RSS. The shunt coil of the trip breakers receives two different signals from SAS and RSS combined in an "OR" logic performed at the level of trip breakers.

BASES

APPLICABLE SAFETY ANALYSES, LCO, and APPLICABILITY (continued)

16-225

included in the Technical Specifications are credited as part of the primary success path in the accident analysis. ~~Non-credited functions are purely equipment protective, and their use minimizes the potential for equipment damage.~~ Non-credited functions are not included in the Technical Specifications. Refer to FSAR Sections 7.2 and 7.3.

The LCO requires the PS sensors, manual actuation switches, signal processors, and specified actuation devices to be OPERABLE. The LCO ensures that each of the following requirements is met:

- A reactor trip or ESF function will be initiated when necessary; and
- Sufficient redundancy is maintained to permit a component to be out of service for testing or maintenance.

Failure of any sensors, signal processors, or actuation device reduces redundancy or renders the affected division(s) inoperable.

Trip Setpoints that directly protect against violating the reactor core or RCS pressure boundary SLs during AOOs are SL-LSSS. Permissive and interlock setpoints allow bypass of trips when they are not required by the Safety Analysis. These permissives and interlocks ensure that the starting conditions are consistent with the safety analysis, before preventative or mitigating actions occur. Because these permissives or interlocks are only one of multiple conservative starting assumptions for the accident analysis, they are generally considered as nominal values without regard to measurement accuracy, (i.e. the value indicated is sufficiently close to the necessary value to ensure proper operation of the safety systems to turn the AOO). Therefore permissives and interlocks are not considered to be SL-LSSS. Each LTSP specified is more conservative than the analytical limit assumed in the safety analysis in order to account for instrument uncertainties appropriate to the trip Function. The methodologies for considering uncertainties are defined in References 1 and 4.

The PS sensors, manual actuation switches, signal processors, and specified actuation devices satisfy Criterion 3 of 10 CFR 50.36(~~d~~c)(2)(ii) .

The PS sensors, manual actuation switches, signal processors, and specified actuation devices that support ~~reactor trips~~ESFs are required to be OPERABLE in MODES 1, 2 and/or 3 because the reactor is or can be made critical in these MODES. The automatic reactor trip functions are designed to take the reactor subcritical, which maintains the SLs during AOOs and assists the ESF in providing acceptable consequences during accidents. The PS sensors, manual actuation switches, signal processors, and specified actuation devices that support automatic reactor trip functions are not required to be OPERABLE in MODES 4 and

BASES

SURVEILLANCE REQUIREMENTS (continued)

sufficient margin to the SL and/or Analytical Limit is maintained. If the as-left instrument setting cannot be returned to a setting within the as-left tolerance, then the Trip/Actuation Function shall be declared inoperable. The second Note also requires that the LTSP and the methodologies for calculating the as-left and the as-found tolerances be in a document controlled under 10 CFR 50.59.

The digital PS provides continual online automatic monitoring of each of the input signal in each division, perform software limit checking (signal online validation) against required acceptance criteria, and provide hardware functional validation so that a division check is continuously being performed. If any PS input signal is identified to be in a failure status, this condition is alarmed in the Control Room. As such, a periodic "channel check" is no longer necessary.

16-231

The Surveillances are modified by a Note to indicate that when a sensor, manual actuation switch, signal processor, or actuation device is placed in an inoperable status solely for performance of required Surveillances, entry into associated Conditions and Required Actions may be delayed for up to 6 hours provided the associated Trip/Actuation Function maintains functional capability. Upon completion of the Surveillance, or expiration of the 6 hour allowance, the sensor, manual actuation switch, signal processor, or actuation device must be returned to OPERABLE status or the applicable Condition entered and Required Actions taken. This Note is based on the overall system reliability and an assumption of the average time required to perform a Surveillance. The 6 hour testing allowance does not significantly reduce the probability that the PS will actuate when required.

SR 3.3.1.1

SR ~~3.3.1.2~~3.3.1.1 compares the calorimetric heat balance calculation to the power range division output every 24 hours. If the calorimetric heat balance calculation results exceed the power range division output by more than 2% RTP, the power range division is not declared inoperable, but must be adjusted. The power range division output shall be adjusted consistent with the calorimetric heat balance calculation results if the calorimetric calculation exceed the power range division output by more than + 2% RTP. If the power range division output cannot be properly adjusted, the division ~~I~~is declared inoperable.

If the calorimetric is performed at part power (< 70% RTP), adjusting the power range division indication in the increasing power direction will assure a reactor trip below the safety analysis limit (< 11% RTP). Making no adjustment to the power range division in the decreasing power

BASES

SURVEILLANCE REQUIREMENTS (continued)

signal. Excluding the detectors is acceptable because the principles of detector operation ensure a virtually instantaneous response.

REFERENCES

1. ANP-10275P-A, ~~Revision 0,~~ "U.S. EPR Instrument Setpoint Methodology Topical Report," ~~March 2007~~February 2008.

2. 10 CFR 100.

3. 10 CFR 50, Appendix A, GDC 21.

4. ANP-10287P, "Incore Trip Setpoint and Transient Methodology for U.S. EPR Topical Report," November 2007.

5. FSAR Chapter 15.

6. 10 CFR 50.49.

7. ANP-~~10271P~~10282P, ~~Revision 0, US EPR Nuclear Incore Instrumentation Systems Report, December 2006.~~ "POWERTRAX/E Online Core Monitoring Software for the U.S. EPR Technical Report," November 2007.

8. EMF-2341(P), Revision 1, "Generic Strategy for Periodic Surveillance Testing of TELEPERM XS Systems in U.S. Nuclear Generating Stations," March 2000.

16-232

16-232

16-232

BASES

ACTIONS (continued)

D.1 and D.2

16-214

If the Required Action and associated Completion Time of Condition C are not met ~~and Table 3.3.2-1 directs entry into Condition E~~, 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 plant conditions from full power conditions in an orderly manner and without challenging plant systems.

SURVEILLANCE REQUIREMENTS

A Note at the beginning of the SR Table specifies that the following SR applies to each PAM instrumentation Function found in Table 3.3.2-1.

SR 3.3.2.1

A CALIBRATION is performed every 24 months or approximately every refueling. CALIBRATION is a complete check of the instrument division including the sensor. The Surveillance verifies the function responds to the measured parameter within the necessary range and accuracy. ~~A Note allows exclusion of the neutron detectors from the CALIBRATION. The requirements for CALIBRATION of neutron detectors is Specified in Specification 3.3.1," Protection System and Safety Automation System".~~

The Frequency is based upon operating experience and consistency with the typical industry refueling cycle and is justified by the assumption of a 24 month CALIBRATION interval for the determination of the magnitude of equipment drift.

16-234

~~SR 3.3.2.2~~

~~A SOT on each Safety Information and Control System performing the PAM functions listed in Table 3.3.2-1 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 OPERABILITY such that the setpoints are within the necessary range and accuracy. The SOT may be performed by means of any series of sequential, overlapping, or total steps.~~