Draft

Request for Additional Information No. 75 (570, 1131), Revision 0

9/9/2008

U. S. EPR Standard Design Certification
AREVA NP Inc.
Docket No. 52-020
SRP Section: 07.02 - Reactor Trip System
SRP Section: 07.08 - Diverse Instrumentation and Control Systems
Application Section: FSAR Ch 7

QUESTIONS

07.02-1

Provide sufficient information for the staff to conclude that the period testing, including self-testing, meets the requirements stated below. Specifically, address the following:

1. Description of all testing that is performed, including self-tests
2. How will the tests detect all detectable failures?
3. Why self-tests and other surveillance tests will not influence safety function and what are the mechanisms to ensure this? (Does the FMEA also show this and will it meet the single-failure criterion?)
4. Specific list of all self tests (i.e., watchdog timer, memory checks, communication checks, data integrity check, etc).
5. What is the safety classification of the self-test feature?
6. How is the execution of automatic tests confirmed during plant operation?
7. What are the provisions to periodically test and calibrate (if needed) the automatic test features?
8. What components cannot be tested with the reactor at power? What are the justifications for not testing them at power and when will they be tested?

IEEE STD 603-1991, Clause 5.7, states that "Capability for testing and calibration of safety system equipment shall be provided while retaining the capability of the safety systems to accomplish their safety functions. The capability for testing and calibration of safety system equipment shall be provided during power operation and shall duplicate, as closely as practicable, performance of the safety system." Acceptance criteria for this requirement is found in Regulatory Guides 1.22, 1.47, and 1.53.

FSAR 7.2.2.3.5 states that the “majority of the components required for RT can be tested with the reactor at power…During outages, extended computer self-testing is performed to verify functionality that cannot be tested with the reactor at power.” The staff needs additional information to determine that Clause 5.7 is adequately addressed in the U.S. EPR design.

07.02-2

Why are not all initiating events in the DC FSAR Tier 2, Table 15.0-1 not listed in Table 15.0-10, the latter listing initiating events and associated reactor trip functions? What

are the protective actions for initiating events listed in Table 15.0-1, but not in Table 15.0-10?

Clause 4.2 of IEEE Standard 603-1991 requires the safety functions and corresponding protective actions of the execute features for each design basis event.

DC FSAR, Tier 2, Section 7.2.2.1.1 states that Table 15.0-10 lists the correlation between each initiating event and corresponding RT function.

07.02-3

Is the system designed for manual or automatic transfer to the recirculation mode? If manual, describe timing margins for changeover from injection to recirculation mode.

Clause 4.5 of IEEE Standard 603-1991 describes the minimum criteria under which manual initiation and control of protective actions may be allowed. SRP BTP 7-6 provides specific guidance on determination if the timing margins for changeover from injection to recirculation mode are sufficient to allow manual initiation of the transition.

07.02-4

Identify all spatially dependent sensors or variables that are being monitored. What is the minimum number of spatially dependent sensors required to provide adequate protection and what is the basis for that number?

Clause 4.6 of IEEE Standard 603-1991 requires in part the identification of the minimum number and location of sensors for those variables in Clause 4.4 of IEEE Standard 603-1991 that have a spatial dependence. The applicant/licensee's analysis should demonstrate that the number and location of sensors are adequate. FSAR Tier 2, Section 7.2.2.1.5, states that “SPND are located systematically throughout the core to provide the spatially dependent neutron flux information.” DC FSAR, Tier 2, Section 7.2.2.1.5, states that “Provisions are made in the RT logic to accommodate any five failed SPNDs for the HLPD function, and any number of failed SPND on up to five fingers for the low DBNR.” What are the bases for accommodating any five failed SPNDs and any number of failed SPND on up to five fingers?

07.02-5

What functional degradation of the reactor trip system's performance occurs due to natural phenomena and unusual events? How will the reactor trip system retain necessary protective action when these events occur? What are the specific design features that address the natural phenomena?

Clause 4.8 of IEEE Standard 603 (1991) requires in part the identification of conditions having the potential for causing functional degradation of safety system performance, and for which provisions must be incorporated to retain necessary protective action. DC FSAR, Tier 2, Section 7.1.2.6.7 states that “safety systems are designed to perform their

required functions in the presence of natural phenomena and unusual events, which include seismic events, tornadoes and internal flooding.

07.02-6

Demonstrate how theprotection system meets the response times assumed in the accident analyses.

Clause 4.10 of IEEE Standard 603-1991 requires identification of the critical points in time or plant conditions for which the protective actions must be initiated. The RPS automatically initiates appropriate protective actions when a condition monitored by the system reaches a preset level. The critical points in time are determined by the RPS response time modeled in the accident analyses. The reactor trip system should be designed and tested to meet the response times assumed in the accident analyses. DC FSAR, Tier 2, Section7.2.2.1.6 states that “the plant conditions that define the proper completion of the reactor trip function are defined on an event-by-event basis in the Chapter 15 analyses.”

07.02-7

DC FSAR, Tier 2, Section7.1.2.6.10, does not explicitly state that safety systems meet Clause 4.11 of IEEE 603-1991. If safety systems do meet the requirement, provide information as to how compliance is achieved?

Clause 4.11 of IEEE Standard 603-1991 requires documentation of the equipment protective provisions that prevent the safety systems from accomplishing their safety function. DC FSAR, Tier 2, Section7.1.2.6.10, states that “I&C systems provide the capability to implement equipment protection of the safety process systems."

07.02-8

Does the U.S. EPR design meet Clause 4.12 of IEEE Std. 603-1991? The DC FSAR, Tier 2, Section 7.1.2.6.11 does not explicitly state that safety systems meet Clause 4.12.

07.02-9

FSAR 7.2.2.2 states that the terms detected and undetected do not correspond to the definition of a detectable failure in IEEE 603-1991. What is the rational for deviating from the standard?

IEEE 603 (1991) Clause 5.1 states in part that safety systems shall perform all safety functions required for a design basis event in the presence of: (1) any single detectable failure within the safety systems concurrent with all identifiable but non-detectable failures; (2) all failures caused by the single failure; and (3) all failures and spurious system actions that cause or are caused by the design basis event requiring the safety functions.

07.02-10

ITAAC were provided for physical and communications independence, but where is the ITAAC for electrical independence?

Clause 5.6 of IEEE Standard 603-1991 requires that redundant portions of a safety system provided for a safety function to be independent of and physically separated from each other to the degree necessary to retain the capability to accomplish the safety function during and following any design-basis event requiring that safety function. Three aspects of independence should be addressed in each case: Physical independence, Electrical independence, Communications independence. DC FSAR, Tier 1, Table 2.4.1-9, Protection System ITAAC, list the following relevant ITAAC: 2.2 Physical separation exists between the four divisions of the PS and 4.4 Communication independence is provided in the inter-division communication paths within the PS.

07.02-11

When will the Equipment Qualification Data Packages (EQDP) and Seismic Qualification Data Packages (SQDP) be available for staff to review?

FSAR 7.2.2.3.6 states that reactor trip function is implemented using the NRC approved TELEPERM XS digital platform. FSAR 7.1.2.6.15 states that safety systems shall meet the requirements of Clause 5.4 of IEEE 603-1998 and equipment used shall be qualified using appropriate method described in FSAR 3.11. FSAR 3.11.3 states that summaries and results of qualification tests for electrical equipment and components are documented in the EQDP, and summaries and results of seismic qualification tests for electrical and mechanical equipment and components in the harsh environment areas are documented in the SQDP.

07.02-12

Clarify the relationship between analytical limit and nominal setpoint, and how they align with the safety evaluation of the U.S. EPR Instrument Setpoint Methodology Topical Report (ANP-10275P).

Define Normal and Degraded Uncertainty terms used in Table 15.0-7 – Reactor Trip Setpoints and Delays Used in Accident Analysis. How are these terms related with that of RG 1.105, which endorses ISA-S67.04-1994 standard? This standard states that the uncertainty is generally identified within a probability and confidence level. What were the probability and confidence levels?

What are the bases for selection of nominal setpoints*?*

IEEE Std. 603-1991, Clause 4.4 requires, in part, the identification of the analytical limit associated with each variable. Review considerations in confirming that an adequate margin exists between analytical limits and setpoints. IEEE Std. 603-1991, Clause 6.8.1, states in part that the allowance for uncertainties between the process analytical limit

documented in Section 4.4 and the device setpoint shall be determined using a documented methodology.

FSAR 7.1.2.6.35 states that safety systems meet the requirements of Clause 6.8 of IEEE 603-1998, and that allowance for uncertainties between the process analytical limit and the setpoint used in the protective functions of the PS is determined using a documented methodology. FSAR Table 15.0-7, Note 1, states that "The value assumed in the accident analysis (i.e., the analytical limit) is the nominal setpoint (listed in this column) plus or minus the uncertainty (listed in the next column)."

07.02-13

How will plant staff verify that protective actions proceed to completion, and that the safety system returns to normal operation after an operator intervention?

Clause 5.2 of IEEE Standard 603 (Ref. 7.10-2) requires thesafety system design to provide features to ensure that system-level actions go to completion. Per SRP Appendix 7.1-C, the staff review of this item should include review of functional and logic diagrams, which are not available at this time, to ensure that "seal-in" features are provided to enable system level protective actions to go to completion. DC FSAR, Tier 2, Section 7.1.2.6.13, states that safety systems meet the requirements of Clause 5.2 of IEEE 603-1991, that when initiated by a safety system, protective actions proceed to completion, and the return to normal operation requires deliberate operator intervention.

07.02-14

Demonstrate the real-time performance of the Protection System.

Clause 5.5 of IEEE Standard 603-1991 requires that the safety system accomplish its safety functions under the full range of applicable conditions enumerated in the design basis. A special concern for digital computer-based systems is confirmation that system real-time performance is adequate to ensure completion of protective action within the critical points of time identified as required by Clause 4.10 of IEEE Standard 603-1991. SRP BTP 7-21 provides supplemental guidance on evaluating response time for digital computer-based systems, and discusses design constraints that allow greater confidence in the results analyses or prototype testing to determine real-time performance. DC FSAR, Tier 2, Section7.1.2.6.16, states that safety systems meet the requirements of Clause 5.5 of IEEE 603-1998 and the guidance of Clause 5.5 of IEEE 7-4.3.2-2003.

07.02-15

How and when will the following identifications be verified? Is there an ITAAC associated with the identification of safety system equipment?

Clause 5.11 of IEEE Std 603-1991 requires that (1) safety system equipment be distinctly identified in accordance with the requirements of IEEE Std 384 (Ref. 7.10- 44), (2) components or modules mounted in equipment or assemblies that are clearly identified as being in a single redundant portion of a safety system do not themselves required identification, (3) identification of safety system equipment be distinguishable from other purposes, (4) identification of safety system equipment not require frequent use of reference material, and (5) the associated documentation be distinctly identified.

DC FSAR, Tier 2, Section 7.1.2.6.22, states that safety systems meet the identification requirements of IEEE 603-1998 and the additional guidance of IEEE 7-4.3.2-2003. The applicant states that redundant divisions of each safety system are distinctively marked, versions of hardware are marked accordingly, and configuration management is used for maintaining identification of safety-related software.

07.02-16

What are the auxiliary features that are not required to be operable for the safety systems?

Clause 5.12 of IEEE Std 603-1991 states that (1) auxiliary supporting features shall meet all requirements of this standard, and (2) other auxiliary features that perform a function that is not required for the safety systems to accomplish their safety functions, or are part of the safety system by association, shall be designed to meet those criteria necessary to ensure that these components, equipment, and systems do not degrade the safety systems below an acceptable level. DC FSAR, Tier 2, Section 7.1.2.6.23, states that safety systems meet the requirements of Clause 5.12 of IEEE 603-1998 and that auxiliary supporting systems include EUPS, EPSS, and safety –related HVAC systems throughout the plant. Also, that other auxiliary features that are not required to be operable for the safety systems to perform their functions are designed to meet criteria that do not degrade the safety functionality of the safety systems below an acceptable level.

07.02-17

What are the effects of possible hardware and software failures? What design features have been incorporated to prevent or limit these effects of these failures?

Hardware failure conditions to be considered should include failures of portions of the computer itself and failures of portions of communication systems. Hard failures, transient failures, sustained failures, and partial failures should be considered. Software failure conditions to be considered should include, as appropriate, software common-cause failures, cascading failures, and undetected failures.

Clause 5.15 of IEEE 603-1991 requires that the degree of redundancy, diversity, testability, and quality provided in the safety system design is adequate to achieve functional reliability commensurate with the safety functions to be performed. For

computer systems, both hardware and software reliability should be analyzed. Standard Review Plan (SRP) Appendix 7.1-D describes the staff position on software reliability determination. SRP BTP 7-14 provides guidance for software development processes that are expected to produce reliable software.

DC FSAR, Tier 2, Section 7.1.2.6.26, states that safety systems meet the reliability requirements of IEEE 603-1998 and the additional guidance of IEEE 7-4.3.2-2003 to support overall plant availability. High reliability is provided through: highly redundant architecture, reliable equipment, independent subsystems, continuous online fault detection and accommodation abilities, high quality software design process, and strong operating experience of the TXS platform. However, the DC FSAR did not address hardware and software failures and how they are addressed.

07.02-18

What analyses have been performed to demonstrate that the performance requirements of the safety systems are met regarding setpoints, margins, errors, and response time? What design practices are implemented to avoid timing problems?

IEEE 603-1991, Clause 6.1, states in part that the safety system should, with precision and reliability, automatically initiate and execute protective action for the range of conditions and performance except as justified in Clause 4.5 of IEEE Std. 603-1991. The applicant/licensee's analysis should confirm that the safety system has been qualified to demonstrate that the performance requirements are met. The evaluation of the precision of the safety system should be addressed to the extent that setpoints, margins, errors, and response times are factored into the analysis. Standard Review Plan (SRP) and Branch Technical Position (BTP) 7-12 discuss considerations for the review of the process for establishing instrument setpoints. SRP BTP 7-21 discusses, for digital computer-based systems, that the evaluation should confirm that the functional requirements have been appropriately allocated into hardware and software requirements. The evaluation should also confirm that the system's real-time performance is deterministic and known.

FSAR 7.1.2.6.28 states that safety systems meet the requirements of Clauses 6.1 and 7.1 of IEEE 603-1998, and that PS is designed to automatically initiate reactor trip and actuate the ESF systems necessary to mitigate the effects of DBEs. However, it does not provide sufficient information to address setpoints, margins, errors, and response-time.

07.02-19

Regulatory Guide 1.62 suggests that operator should have easy access to the controls and be able take action in an expeditious manner. How were human factor considerations addressed?

IEEE 603 (1991), Clause 6.2 states in part the review of manual controls should include confirmation that the controls will be functional (e.g., power will be available and command equipment is appropriately qualified), accessible within the time constraints of

operator responses, and available during plant conditions under which manual actions may be necessary. Features for manual initiation of protective action should address the acceptance criteria in Regulatory Guide 1.62, “Manual Initiation of Protection Action.” DC FSAR, Tier 2, Section 7.1.2.6.29, states that safety systems meet the requirements of Clause 6.2 and 7.2 of IEEE 603-1998, and that manual actuation of protective actions is possible from the SICS.

07.02-20

What are the range, accuracy, resolution, response time, and sample rate for the instruments that produce the safety system inputs?

As stated in Clause 6.4 of IEEE Std. 603-1991, to the extent feasible and practical, sense and command feature inputs shall be derived from signals that are direct measures of the desired variables as specified in the design basis. Staff guidance in the Standard Review Plant states that a safety system that requires loss of flow protection would, for example, normally derive its signal from flow sensors. A design might use an indirect parameter such as a pressure signal or pump speed. However, the applicant/licensee should verify that any indirect parameter is a valid representation of the desired direct parameter for all events. For both direct and indirect parameters, the applicant/licensee should verify that the characteristics (e.g., range, accuracy, resolution, response time, sample rate) of the instruments that produce the safety system inputs are consistent with the analysis provided in Chapter 15 of the SAR.

DC FSAR, Tier 2, Section 7.1.2.6.31, states that safety systems meet the requirements of Clause 6.4 of IEEE 603-1998, and that signals used in the sense and command features are direct measures of the desired variable in the design basis. FSAR Table 7.2-1, "Reactor Trip Variables," list variables to be monitored and ranges.

07.02-21

Demonstrate how the Protection System (PS) addresses Clauses 6.6 and 7.4 of IEEE Std. 603-1991? What tests will be run to demonstrate compliance?

IEEE 603-1991, Clauses 6.6 and 7.4, state that whenever the applicable permissive conditions are not met, a safety system shall automatically prevent the activation of an operating bypass or initiate the appropriate safety function(s). If plant conditions change so that an activated operating bypass is no longer permissible, the safety system shall automatically accomplish one of the following actions:

(1) Remove the appropriate active operating bypass(es)
(2) Restore plant conditions so that permissive conditions once again exist
(3) Initiate the appropriate safety function(s)

SRP Appendix 7.1-C states that the requirement for automatic removal of operational bypasses means that the reactor operator shall have no role in such removal. The operator may take action to prevent the unnecessary initiation of a protective action.

DC FSAR, Tier 2, Section 7.1.2.6.33, states that safety systems meet the requirements of Clause 6.6 and 7.4 of IEEE 603-1998, and that operating bypasses are implemented using permissive signals from the PS. If the plant conditions associated with allowing operational bypasses are not met, the PS automatically prevents the activation of the operating bypass…If plant conditions change during activation of an operating bypass, and the operating bypass is no longer permissible, in general the PS automatically removes the appropriate active operating bypass.

07.02-22

Demonstrate through the design of the Protection System (PS) how Clause 6.7 of IEEE Std. 603-1991 is addressed? What tests will be run to demonstrate compliance?

IEEE 603-1991, Clause 6.7, states that capability of a safety system to accomplish its safety function shall be retained while sense and command features equipment is in maintenance bypass. During such operation, the sense and command features equipment shall continue to meet the requirements of 5.1 and 6.3.
DC FSAR, Tier 2, Section 7.1.2.6.34, states that safety systems meet the requirements of Clause 6.7 of IEEE 603 (1998), and that safety systems are designed to permit channel bypass for maintenance, testing, or repair. However, additional information is need for the staff to verify that the design meets Clause 6.7.

07.02-23

Where is in the U.S. EPR design certification application does it explicitly address Clause 7.3 of IEEE 603-1991?
DC FSAR, Tier 2, Section 7.1.2.6.13, has the word 7.3 in the subject header but there are no compliance or verification statements for Clause 7.3.

07.02-24

Where in the U.S. EPR design certification application does it explicitly address Clause 7.5 of IEEE 603-1991?
DC FSAR, Tier 2, Section 7.1.2.6.34, has the word 7.5 in the subject header but there are no compliance or verification statements for Clause 7.5.

07.02-25

What periodic tests are involved to make sure that the power systems function described below is as-designed? Describe load sequencer for emergency diesel generator (EDG).

IEEE 603-1991, Clause 8.1, states that those portions of the Class 1E power system that are required to provide the power to the many facets of the safety system are

governed by the criteria of this document and a portion of the safety system. Specific criteria unique to the Class 1E power systems are given in IEEE 308-1980.

DCFSAR, Tier 2, Section 7.1.2.6.36, states that safety systems meet the requirements of IEEE 603-1998, Clause 8.1, that safety systems are powered by the EUPS and EPSS - these systems provide reliable, Class 1E power that is backed by the EDGs. The EUPS provides uninterruptible power in case of an LOOP.

07.02-26

What tests are available to check themaintenance bypass capability described below? How will plant staff verify conformance to requirement?

IEEE 603-1991, Clause 8.3, states in part that the capability of the safety systems to accomplish their safety functions shall be retained while power sources are in maintenance bypass.

DC FSAR, Tier 2, Section 7.1.2.38, states that safety systems can perform their safety functions while power source are in maintenance bypass; details on the electrical power systems that fulfill this requirement are described in Chapter 8.

07.02-27

How will the self-diagnostic feature of TXS, as identified below, be verified to function as-designed?

Clause 5.10 of IEEE 603-1991 requires that the safety systems be designed to facilitate timely recognition, location, replacement, repair, and adjustment of malfunctioning equipment.

DC FSAR, Tier 2, Section 7.1.2.6.21, states that safety systems meet the requirements of Clause 5.10 of IEEE 603-1998, and that safety systems built upon the TXS platform contain self-diagnostic test features to detect both hardware and software faults and assist in diagnostic and repair activities.

07.02-28

DC FSAR, Tier 2, Section 7.1.2.6.19, references Section 7.2, 7.3, and 7.5 for further information on displays. Which specific Sub-sections in 7.2 are being referenced?

DC FSAR, Tier 2, Section 7.1.2.6.19, states that safety systems meet the requirements of Clause 5.8 of IEEE 603 (1998), that displays meet the requirements of IEEE 497 (2002), and to refer to Section 7.2, 7.3, and 7.5 for further information.

07.08-4

Demonstrate how the Process Information and Control System (PICS) will meet the requirements of 10 CFR 50.55a(a)1 and GDC 1, including its design, construction, installation, inspection, testing, operation, maintenance, and modifications. Discuss the quality assurance aspects associated with the PICS software development, hardware qualification, and system testing.

The PICS is credited as being a diverse system from the Protection System and provides controls for both safety-related and non-safety-related process systems. Section 7.8 of the Standard Review Plan identifies 10 CFR 50.55a(a)1 and GDC 1 as acceptance criteria for diverse instrumentation and control systems.

07.08-5

Explain the selection process and analysis that were used to select the functions that are automatically actuated by the Diverse Actuation System (DAS).

DC-FSAR Tier 1 Table 2.4.9-2 list functions that are automatically actuated by the DAS. However, this list is not a complete list when making a comparison to the digital protection system's (i.e., TXS, PS) automatic protection functions provided in DC-FSAR Tier 1 Table 2.4.1-3 and Table 2.4.1-4 (both sheets 1 and 2).

DC-FSAR Section 7.8.1.1.3 credits the DAS as a subsystem of the PAS that is used for execution of automatic functions to mitigate an anticipated transient without scram or software common-cause failure (CCF) of the safety I&C systems. DC-FSAR Section 7.8.2.2.7 states that the DAS is provided as a diverse backup in the event of a software CCF that disables both the reactor trip and engineered safety features actuation functions of the Protection System.

Branch Technical Position 7-19 (BTP 7-19) provides guidance for evaluation of diversity and defense-in-depth (D3) in digital computer-based instrumentation and control systems. The NRC has established a four-point position on D3. Point 3 of the four-point D3 position states:

"If a postulated common-cause failure could disable a safety function, a diverse means, with a documented basis that the diverse means is unlikely to be subject to the same common-cause failure, ***should be required to perform either the same function as the safety system function that is vulnerable to common-cause failure or a different function that provides adequate protection.*** The diverse or different function may be performed by a non-safety system if the system is of sufficient quality to perform the necessary function under the associated event conditions."

BTP 7-19 further provides acceptance criteria for plant response to a single, postulated CCF to be included within the D3 assessment submitted by the applicant/licensee and states that the D3 assessment should demonstrate compliance with the four-point position by confirming that anticipated operational occurrences and design basis accidents are mitigated in the presence of common-cause failure, by, among other things, showing that:

1. For each anticipated operational occurrence in the design basis occurring in conjunction with each single postulated common-cause failure, the plant response calculated using best-estimate (realistic assumptions) analyses should not result in radiation release exceeding 10 percent of the 10 CFR 100 guideline value or violation of the integrity of the primary coolant pressure boundary. The applicant/licensee should (1) demonstrate that sufficient diversity exists to achieve these goals, (2) identify the vulnerabilities discovered and the corrective actions taken, or (3) identify the vulnerabilities discovered and provide a documented basis that justifies taking no action.

2. For each postulated accident in the design basis occurring in conjunction with each single postulated common-cause failure, the plant response calculated using best-estimate (realistic assumptions) analyses should not result in radiation release exceeding the 10 CFR 100 guideline values, violation of the integrity of the primary coolant pressure boundary, or violation of the integrity of the containment (i.e., exceeding coolant system or containment design limits). The applicant/licensee should (1) demonstrate that sufficient diversity exists to achieve these goals, (2) identify the vulnerabilities discovered and the corrective actions taken, or (3) identify the vulnerabilities discovered and provide a documented basis that justifies taking no action.

The NRC staff has reviewed the applicant's D3 assessment, U.S. EPR Instrumentation and Control Diversity and Defense-in-Depth Methodology Topical Report, ANP-10284, Revision 0 [Adams Accession No. ML0717601881], and could not locate an analysis such as acceptance criteria items 1 and 2 above, which would demonstrate compliance with the NRC's four-point position on diversity. The staff could not locate the documented basis within the D3 assessment or the DC-FSAR which would demonstrate compliance with Point 3 of the NRC's four-point D3 position.

07.08-6

Describe the plant response using best-estimate analysis based on the Diverse Actuation System (DAS) setpoints and explain the process for selecting the DAS setpoints.

DC-FSAR Tier 2 Section 7.8.1.1.3 states that the DAS executes the automatic reactor trip and engineered safety feature actuation and that setpoints for these functions are set so that the Protection System will actuate prior to the DAS.

Branch Technical Position 7-19 (BTP 7-19) provides acceptance criteria for plant response to a single postulated common cause failure (CCF). This analysis should be included within the Defense-in-Depth and Diversity (D3) assessment submitted by the applicant/licensee. The D3 assessment should confirm that anticipated operational occurrences and design basis accidents are mitigated in the presence of a common-cause failure, by, among other things, showing that:

1. For each anticipated operational occurrence in the design basis occurring in conjunction with each single postulated common-cause failure, the plant response calculated using best-estimate (realistic assumptions) analyses should not result in radiation release exceeding 10 percent of the 10 CFR 100 guideline value or violation of the integrity of the primary coolant pressure boundary. The applicant/licensee should (1) demonstrate that sufficient diversity exists to achieve these goals, (2) identify the vulnerabilities discovered and the corrective actions taken, or (3) identify the vulnerabilities discovered and provide a documented basis that justifies taking no action.

2. For each postulated accident in the design basis occurring in conjunction with each single postulated common-cause failure, the plant response calculated using best-estimate (realistic assumptions) analyses should not result in radiation release exceeding the 10 CFR 100 guideline values, violation of the integrity of the primary coolant pressure boundary, or violation of the integrity of the containment (i.e., exceeding coolant system or containment design limits). The applicant/licensee should (1) demonstrate that sufficient diversity exists to achieve these goals, (2) identify the vulnerabilities discovered and the corrective actions taken, or (3) identify the vulnerabilities discovered and provide a documented basis that justifies taking no action.

The NRC staff has reviewed the applicant's D3 assessment, U.S. EPR Instrumentation and Control Diversity and Defense-in-Depth Methodology Topical Report, ANP-10284, Revision 0 [Adams Accession No. ML0717601881], and the DC-FSAR and could not locate an analysis of the plant response to a postulated common cause failure such as acceptance criteria items 1 and 2 above, which would demonstrate compliance with the NRC's four-point position on diversity. Specifically, the analysis should address the DAS setpoints and how they can meet the two items above and not interfere with the operation of the Protection System.