# Response to Request for Additional Information – ANP-10284

## "U.S. EPR Instrumentation and Control

## Diversity and Defense-In-Depth Methodology

## Topical Report" (TAC No. MD5884)

**NRC Comment**

By letter to the U.S. Nuclear Regulatory Commission (NRC) dated June 20, 2007 (Agencywide Documents Access and Management System (ADAMS Accession Number ML071760187), AREVA NP, Inc. submitted for NRC staff review, ANP-10284, Revision 0, "U.S. EPR Instrumentation and Control Diversity and Defense-in-Depth Methodology Topical Report." By letter dated August 20, 2007 (ADAMS Accession Number ML072150532), the NRC staff accepted this topical report for review. The NRC staff is reviewing AREVA's submittal and has determined that the following additional information is required in order to complete the review.

***RAI 1***: *Provide the diversity and defense-in-depth (D3) analysis that is described in the methodology topical report (TR).*

*ANP-10284, Section 1.1 states, "AREVA NP requests the approval of the following items in this report:..The adequacy of the proposed design features to mitigate the consequences of a postulated CCF [common cause failure] in the safety I&C [Instrumentation and Control] systems."*

*However, NUREG-0800, "Standard Review Plan," Branch Technical Position (BTP) 7-19, "Guidance for Evaluation of Diversity and Defense-Indepth in Digital Computer-Based Instrumentation and Controls System," states, "...the NRC has established the following …position on D3...*

*Point 1. The applicant/licensee should assess the D3 of the proposed I&C system to demonstrate that vulnerabilities to common-cause failures have been adequately addressed.*

*Point 2. In performing the assessment, the vendor or applicant/licensee should analyze each postulated common-cause failure for each event that is evaluated in the accident analysis section of the safety analysis report (SAR) using best-estimate or SAR Chapter 15 analysis methods. The vendor or applicant/licensee should demonstrate adequate diversity within the design for each of these events." ….*

*Therefore BTP 7-19 states that the adequacy of proposed design features to mitigate the consequences of postulated CCF should be based on an assessment that has been performed.*

*In order to evaluate the proposed design features, an assessment or a justification, as to how the alternative proposed (i.e., the methodology for performing the assessment) provides an acceptable method of complying with the rules or regulations, is needed.*

**Response 1:**

ANP-10284 describes the methodology to be followed for evaluating the adequacy of the U.S. EPR I&C design with respect to defense-in-depth and diversity (D3). The design features that are described in Section 3.2 are included in the report to provide the NRC staff greater understanding of the I&C architecture and the design features that are provided for defense-in-depth and diversity. These are the architecture and design features that will be assessed during the D3 analysis.

AREVA NP is not requesting approval of these design features, solely as described in this document, to meet the requirements of BTP-19. The analysis that demonstrates an acceptable design with respect to BTP-19 is summarized in Section 7.8 of the U.S. EPR FSAR and will be finalized following the methodology described in ANP-10284.

A conservative design approach (duplication of several protective functions in a diverse system) has been taken by AREVA NP which allows the majority of the analysis to be un-complicated in nature. The acceptability of the D3 features included in the U.S. EPR design will be demonstrated on a best estimate basis consistent with existing Chapter 15 design basis analyses methods.

To clarify what is requested for approval, AREVA NP proposes to modify Section 1.1 and Section 5.0 of ANP-10284 (see Attachment 1) to the following:

"AREVA NP requests the approval of the following items in this report:

- The U.S. EPR defense-in-depth concept.
- The methodology used to evaluate the adequacy of the I&C design with respect to D3."

Essentially, AREVA NP is requesting approval of 1.) a methodology for performing a plant-specific D3 analysis and, 2.) the D3 concepts incorporated

into the I&C architecture that constitute the basis of the design features to be evaluated during the analysis.

This approach is consistent with the D3 approach approved by the NRC for TXS upgrades to existing plants. Siemens Report EMF-2267(P), "Siemens Power Corporation Methodology Report for Diversity and Defense-in-Depth" was submitted to the NRC to describe D3 concepts and a methodology to be followed in performing plant-specific D3 analyses for system upgrades using TXS technology.

The SER for Siemens Report EMF-2110(NP), which approved the TXS platform for use in safety related nuclear applications, states:

> "On the basis of its review, the staff found that Siemens' diversity and defense-in-depth assessment methodology as described in EMF-2267(P) is consistent with the staff position stated in SRP BTP HICB-19 and is, therefore, acceptable. Applications following this methodology for a plant-specific diversity and defense-in-depth assessment should be found acceptable in this area. The actual review and verification of the major differences between the TXS and TXP was outside the scope of staff review. This is a plant-specific action item."

AREVA NP believes that ANP-10284 contains sufficient information to support a similar finding.

***RAI 2**: Provide a description of how adequate quality is achieved for the diverse actuation system (DAS).*

*One of the requirements that is addressed by BTP 7-19 is 10 CFR 50.62, "Requirements for reduction of risk from anticipated transients without scram (ATWS) events for light-water-cooled nuclear power plants." Section 50.62(c)(1) states, "...This equipment must be designed to perform its function in a reliable manner..."*

*AREVA has stated that the DAS will be used to address ATWS requirements. (ANP-10284, Section 4.2, states, "...ATWS evaluations to determine required functionality of the DAS for ATWS mitigation.")*

*Provide a description of the DAS that describes how it is designed to perform its function in a reliable manner (see Generic Letter 85-06, "QA Guidance for ATWS Equipment that is not Safety Related," and NUREG-0800, Chapter 7, "Instrumentation and Controls – Overview of Review Process," Section 7.8, "Diverse Instrumentation and Control System").*

**Response 2:**

The DAS, because it is used for ATWS mitigation, is subject to the quality requirements of 10 CFR 50.62 and GL 85-06. Quality requirements for the DAS are described in Section 7.1.1.4.6 of the U.S. EPR FSAR. Because AREVA NP has committed to meet the ATWS quality requirements for the DAS, the DAS will be implemented in a manner consistent with NRC guidance for systems credited in mitigating beyond design basis events.

The response to RAI 1 clarifies the items for which approval is requested. The request for approval of "the adequacy of the proposed design features to mitigate the consequences of a postulated CCF in the safety I&C systems" has been withdrawn (see Attachment 1 proposed changes). Therefore, compliance of the DAS with requirements for quality does not need to be addressed in the context of ANP-10284. This information should not be required to conclude that the defense-in-depth concept and method of assessment are acceptable.

***RAI 3**:* *Provide a description of how the DAS performs its function independent (from sensor output to the final actuation device) from the protection system (PS).*

*One of the requirements that is addressed by BTP 7-19 is 10 CFR 50.62. Section 50.62 (c)(1) states, "...This equipment must... be independent (from sensor output to the final actuation device) from the existing reactor trip system."*

*AREVA has stated that the DAS will be used to address ATWS requirements. (ANP-10284, Section 4.2: "... ATWS evaluations to determine required functionality of the DAS for ATWS mitigation.")*

*AREVA has not provided a description of the DAS that describes how it performs its function independent (from sensor output to the final actuation device) from the PS.*

*ANP-10284, Section 2, states, "The I&C architecture for the U.S. EPR is depicted in Figure 2-1. The I&C architecture is arranged into three levels—Level 2 (Supervisory Control), Level 1 (System Level Automation), and Level 0 (Process Interface). In general, functions (both automatic and manual) are allocated to the various Level 1 systems depending on the safety classification of the function, and what the function is designed for (e.g., rod control, initiation of safety injection). Interfaces are provided within the Level 2 I&C systems for manual functions."*

*ANP-10284, Section 2.5, states, "In general, the lines of defense apply to the architecture level 1 automation systems."*

*The assessment methodology proposed by AREVA does not seem address the regulatory basis, since Level 0 (Process Interface) is excluded from the analysis.*

**Response 3:**

NRC has no specific rules or guidance documents that specify independence or diversity requirements for sensors (Level 0) used for the PS and DAS.

10 CFR 50.62(c)(1) requires that:

"Each pressurized water reactor must have equipment from sensor output to final actuation device, that is diverse from the reactor trip system, to automatically initiate the auxiliary (or emergency) feedwater system and initiate a turbine trip under conditions indicative of an ATWS. This equipment must be designed to perform its function in a reliable manner and be independent (from sensor output to the final actuation device) from the existing reactor trip system."

No additional regulations are imposed for new plants. Instead, 10 CFR 52.47(a)(15) simply requires:

"Information demonstrating how the applicant will comply with requirements for reduction of risk from anticipated transients without scram events in § 50.62;"

The NRC guidance document applicable to DAS is Standard Review Plan Section (SRP) 7.8, "Diverse Instrumentation and Control Systems," Revision 5, issued in March 2007. The review procedure outlined on pages 7 and 8 states that "Sensors need not be of a diverse design or manufacturer".

Therefore the DAS, as proposed, complies with 10CFR50.62, 10CFR52.47(a)(15), and conforms with the guidance of SRP 7.8.

***RAI 4**: Please demonstrate that the DAS will be sufficiently reliable to perform its diverse backup function for the Protection System (PS).*

*The DAS subsystem serves as a diverse backup to the PS. The description of the DAS however does not allow for an evaluation of DAS reliability. In view of the fact that simple systems are generally more reliable than complex*

*systems (i.e. complex systems have a greater likelihood of failures and software errors), simple digital systems have been identified to be acceptable. The proposed DAS will be expected to perform this function reliably.*

*It is understood that the D3 report is not intended to include a description of the DAS, but rather to identify those D3 related design constraints on the DAS that are required to support the D3 analysis.*

**Response 4:**

The design and implementation of the DAS is subject to augmented quality requirements as described in Sections 7.1 and 7.8 of the U.S. EPR FSAR. The DAS is implemented in four redundant divisions to support the U.S. EPR overall concept for reliability. To minimize the complexity of the system, automatic functionality is only included in the DAS if it is deemed necessary according to the proposed D3 analysis methodology. These are the attributes of the DAS that allow the system to function in a reliable manner.

The text of RAI 4 seems to imply that in order to be considered reliable a digital system must be considered “simple”. AREVA NP does not agree with this implication.

AREVA NP has not specified that the DAS be limited to simple digital equipment. In addition, NRC has no specific rules or guidance documents that specify that systems used for diverse instrumentation and controls be limited to simple digital equipment.

The NRC staff stated in SECY-93-087 on page 56 that:

> “The intent is to permit the use of diverse digital equipment that is not affected by the identified common-mode failures and to reduce complexity in the design. The staff will not require only analog equipment and will consider allowing simple digital equipment.”

The NRC staff proposed four staff positions on page 57 and added additional clarifying discussion on page 58 to address diversity and defense-in-depth.

The Commission approved, in part, and disapproved, in part, the staff's diversity and defense-in-depth recommendations in the Staff Requirements Memorandum for SECY-93-87 dated July 21, 1993. In particular, the Commission only approved a revised version of the four positions. The Commission specifically eliminated the clarifying notes and stated that it “approves only that such prescriptiveness be considered as general guidance, the practicality of which should be determined on a case-by-case basis.”

The NRC guidance document applicable to DAS is SRP Section 7.8, "Diverse Instrumentation and Control Systems," Revision 5, issued in March 2007. The applicable acceptance criteria listed in the document states:

1. For plants with a digital RTS or ESFAS, the NRC position on D3 should be especially noted. This position is contained in Item II.Q, "Defense Against Common-Mode Failures in Digital Instrument and Control Systems," of the Staff Requirements Memorandum on SECY-93-087, "Policy, Technical, and Licensing Issues Pertaining to Evolutionary and Advanced Light-Water Reactor (ALWR) Designs." SRM requirements applicable to diverse I&C functions are as follows:

   "If a postulated common-mode failure could disable a safety function, then a diverse means, with a documented basis that the diverse means is unlikely to be subject to the same common-mode failure [as the safety system], shall be required to perform either the same function [as the safety system function that is vulnerable to common mode 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 functions under the associated event conditions."

   "A set of displays and controls located in the main control room shall be provided for manual system-level actuation of critical safety functions and monitoring of parameters that support the safety functions. The displays and controls shall be independent and diverse from the safety computer system[s] …"

The SRP 7.8 acceptance criteria allow diverse non-safety digital equipment without any limitation that the equipment be considered simple.

Additional NRC guidance for DAS is provided in Branch Technical Position (BTP) 7-19, "Guidance for Evaluation of Diversity and Defense-In-Depth in Digital Computer-Based Instrumentation and Control Systems," Revision 5, issued in March 2007.

Point 3 of the BTP 7-19 guidance 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.

The guidance also notes that:

> 10 CFR 50.62 requires that the ATWS mitigation system be composed of equipment that is diverse from the RTS. If "sufficient" difference in manufacturer cannot be demonstrated, a case-by-case assessment of the mitigation system designs should be conducted. This analysis should include differences such as manufacturing division (within a corporate entity), software (including implementation language), equipment (including central processing unit architecture), function, people (design and verification/validation team), and initiating events.

The BTP 7-19 guidance allows diverse non-safety digital equipment without any limitation that the equipment be considered simple.

BTP 7-19 does suggest simplicity (full testability) of digital equipment that is used at the point of connection between diverse manual controls and the safety equipment downstream of that safety equipment susceptible to software CCF. Consistent with this guidance, the point of connection used in the U.S. EPR design is the PACS system which utilizes the fully testable AV42 module.

***RAI 5:*** *Describe how the proposed design features or assessment methodology addresses sensor independence between the echelons of defense. BTP 7-19 identifies NUREG/CR-6303, "Method for Performing Defense-in-Depth and Diversity Analyses of the Reactor Protection System" as relevant regulatory guidance, and acceptance criteria, for addressing the regulatory requirements addressed by BTP 7-19. NUREG/CR-6303, Section 2.2, states, "All four echelons depend upon sensors to determine when to perform their functions, and a serious safety concern is to ensure that no more than one echelon is disabled by a common sensor failure or its direct consequences" (see also quotation from NUREG-0493, "A Defense-in-Depth and Diversity Assessment of the RESAR-414 Integrated Protection System," in RAI No. 8).*

*ANP-10284, Section 3.2.1.4, states, "The PAS provides diverse processing of sensor information because the PAS obtains sensor information independently of the PS and SAS [Safety Actuation System] software." This implies that the same sensors are used by both safety and non-safety systems (see also Figure 3-5).*

*AREVA has proposed to define different echelons of defense than those defined in NUREG/CR-6303. In addition, the analysis methodology proposed does not seem to address sensor independence (see also quotations from Section 2 and 2.5 in RAI No. 3 above). Therefore, the D3 TR does not appear to address the concern of sensor independence.*

*Note: NUREG-0800, Chapter 7, Section 7.5, "Information Systems Important to Safety," contains guidance for meeting regulatory requirements. The acceptance criteria contained in NUREG-0800, Section 7.5 include Regulatory Guide 1.97, Revision 4, which endorses the Institute of Electrical and Electronics Engineers (IEEE) STD 497-2002, "IEEE Standard Criteria for Accident Monitoring Instrumentation for Nuclear Power Generating Stations – Description." IEEE 497-2002, Clause 6.2, "Common Cause Failure," contains additional guidance for "instrumentation using microprocessor based sensors, data acquisition, or display equipment." For example:*

- *"Common cause failures for the instrumentation channels shall be addressed at the variable level."*
- *"System interaction between accident monitoring microprocessor-based instrumentation systems and other systems that may be served by the data acquisition and display system shall be considered as part of the common cause failure evaluation."*

**Response 5:**

In the U.S. EPR design, sensors are shared between safety and non-safety systems. This implementation of shared sensors complies with the IEEE 603 independence requirements.

In the text of RAI 5 the staff quotes from NUREG/CR-6303, "…and a serious safety concern is to ensure that no more than one echelon is disabled by a common sensor failure or its direct consequences."

In the U.S. EPR design, this concern is satisfied through redundancy of sensors and signal selection techniques employed in both the safety and non-safety-related systems.

For example, the protection system (PS) and the DAS may utilize a common level measurement. There are four redundant, independent level sensors. Each of the redundant sensors is acquired by one division of the PS and one division of the DAS. Class 1E isolation is employed on the measurement, between the two systems. A common sensor failure leaves three redundant, operable sensors for each of the two systems. Signal selection or voting is used in each system to accommodate the failed sensor, and neither echelon

of defense is disabled by this common sensor failure. This technique is also used in other control systems to preclude an inadvertent control action that might use the same measurement as a protective action.

In the U.S. EPR design, independence is maintained between the main line of defense and the risk reduction line of defense regardless of whether sensors are shared between the two. Additionally, neither line of defense is disabled by a common sensor failure or its direct consequences.

***RAI 6**: Describe how the proposed design features or assessment methodology addresses display independence.*

*BTP 7-19 states, "This BTP has the objective of confirming that vulnerabilities to common-cause failures have been addressed in accordance with the guidance of the SRM on SECY-93-087, specifically: ... Verify that the displays and manual controls for critical safety functions initiated by operator action are diverse from computer systems used in the automatic portion of the protection systems."*

*AREVA has proposed to define different echelons of defense than those defined in BTP 7-19. In addition, the analysis methodology proposed does not seem to address display independence (see quotations from Section 2 and 2.5 in RAI No. 3 above).*

**Response 6:**

RAI 6 requests information related to independence of displays. The passage quoted in RAI 6 from BTP 7-19 addresses diversity of displays. These are two separate issues that must be addressed individually.

The safety-related displays used in the U.S. EPR design (part of SICS) are subject to the independence requirements of IEEE 603. Independence is maintained between redundant portions of the SICS, and independence is maintained between the safety-related portions of the SICS and all non-safety related systems. Independence of display systems is not a subject of topical report ANP-10284, and should not be required for approval of the report. Compliance of I&C safety systems with the requirements of IEEE 603 is addressed in Section 7.1 of the U.S. EPR FSAR.

The description of indications and alarms provided in Section 3.2.1.4 of ANP-10284 describes the implementation of diverse display systems.

The analysis methodology proposed by AREVA NP also addresses diversity of displays.

As part of step 2 of the proposed methodology, additional functionality is identified that is required to mitigate an event in the presence of a safety system CCF. Then, as stated in Section 4.2 of the report:

> "For any additional functionality, a judgment will be made as to whether it can be performed manually or automatically. Operator action will be allowed to be used if it is judged to be feasible by the participants given the event description and assumed CCF."

Step 3 of the proposed methodology then describes how the inventory of diverse controls and indications are assigned to the display systems. Diverse controls are provided either through hardwired controls on the SICS or through digital controls on the PICS. Diverse indications are provided on the PICS as described in Section 4.3.3.

Section 4.6, "Platform Diversity Analysis" of ANP-10284 describes step 6 of the analysis methodology. This section states:

> "An analysis will be performed to demonstrate that the digital platform implemented for the PAS and PICS is diverse from TXS. This analysis will be performed using the diversity principles discussed in NUREG/CR-6303 as a guide…"

The methodology proposed in ANP-10284 identifies the need for diverse displays and controls. The report also describes the methods used to determine the inventory of such displays and controls, and to demonstrate that the platform on which they are implemented is diverse from the automatic portions of the safety systems.

**RAI 7**: *Describe how the proposed design features or assessment methodology addresses IEEE STD 603-1991, "IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations –Description," manual control independence requirements.*

*IEEE 603, Section 6.2.1 states, "Means shall be provided in the control room to implement manual initiation at the division level of the automatically initiated protective actions. The means provided shall minimize the number of discrete operator manipulations and shall depend on the operation of a minimum of equipment consistent with the constraints of 5.6.1."*

*ANP-10284, Section 2.1, states, "For the initiation of critical safety functions at the system level (e.g., reactor trip, safety injection), conventional means*

*(i.e., buttons, switches) are provided on the SICS [Safety Instrumentation and Control System]. These signals bypass the TXS computers and are hardwired directly to actuation devices (e.g., reactor trip devices or priority actuation and control (PAC) modules)."*

*ANP-10284, Section 4.3.1, states, "The inventory of hardwired controls on SICS is developed using the following requirements:*

- *System-level manual actuation for critical safety functions, which include: reactor shutdown, core inventory control, decay heat removal, containment isolation and containment integrity.*

- *System level manual actuation of those safety functions that were credited for manual operator action in Step 2."*

*It is not clear that "the automatically initiated protective actions" of IEEE 603 are a subset of "critical safety functions" as described in the D3 TR. If these are in fact two names for the same set of controls, then why use two different names?*

*AREVA uses different terms than those used in IEEE 603. In addition, the analysis methodology proposed by AREVA, does not seem to address assessment of IEEE 603 manual control independence (see quotations from Section 2 and 2.5 in RAI No. 3 above).*

**Response 7:**

As described in the response to RAI 16 for ANP-10281P (PS topical report), it is the AREVA NP position that IEEE 603-1998 does not require manual initiation of protective actions at the system level to be independent of the automatically initiated protective functions.

The system level manual initiations of the automatically initiated protective actions are described in the PS topical report. These are the manual functions intended to satisfy Clause 6.2.1 of IEEE 603-1998. Specifically, the responses to RAIs 16 and 18 for the PS topical report clarify the implementation of these initiations. These RAI responses clarify that AREVA NP intends to utilize the computers of the PS for a significant portion of the system level initiation functions required by IEEE 603. The RAI responses also clarify that only manual system level initiations that are implemented to bypass the computers of the PS can be credited in a D3 analysis.

Compliance to IEEE 603 requirements for independence is not a subject of ANP-10284 (D3 topical report) and should not be required for approval of the

report. Compliance of I&C safety systems with the requirements of IEEE 603 is addressed in Section 7.1 of the U.S. EPR FSAR.

Recent regulatory developments in the area of defense-in-depth and diversity (e.g., interim staff guidance, statements made by the staff in the transcript of the September 13, 2007 ACRS Digital I&C System Subcommittee meeting) have indicated that component level controls implemented through a diverse, non-safety-related system are adequate to satisfy BTP 7-19 position 4. Therefore, modifications are required to Section 2.1, Section 4.3.1, and other sections of the D3 topical report to clarify the implementation of system level manual initiation functionality and certain portions of the D3 analysis methodology. These proposed modifications are detailed in Attachment 1.

***RAI 8**: Describe how the proposed methodology addresses the assessment of the separation of protection and control systems.*

*One of the requirements that is addressed by BTP 7-19 is 10 CFR Part 50, "Domestic Licensing of Production and Utilization Facilities," Appendix A, "General Design Criteria for Nuclear Power Plants," which states, "Criterion 24--Separation of protection and control systems. ... Interconnection of the protection and control systems shall be limited so as to assure that safety is not significantly impaired."*

*NUREG-0493 (first complete paragraph at the top of page 4-12) documents that a plant, has in the past, been accepted to "... be control from the same measurements with which it is protected ... " based on a " ...demonstration of insignificant impairment to safety."*

*ANP-10284, Section 4.3.2, states, "Safety-related plant equipment will have the capability of being controlled manually at the component level from the PICS via the PAS and PACS. This will fulfill the requirement of performing manual functions that don't require system level manual actuation."*

*The description of the proposed design features does not address the regulatory requirement for separation of protection and control systems. In addition, the analysis methodology does not seem to address the demonstration of insignificant impairment to safety (nor assessment of the separation of protection and control systems) (see also RAI 5).*

**Response 8:**

The proposed methodology is based on the premise that adequate separation exists between protection and control systems through compliance with IEEE 603, and does not need to be re-established through a D3 analysis.

Through compliance with IEEE 603 (and thus GDC 24), the interconnections between protection and control systems are limited to assure that safety is not significantly impaired. Additionally, control systems are designed with features that minimize and limit challenges to the protection system due to control system failures. Worst-case credible failures of the plant control systems are postulated in the analysis of operational transients and accidents.

Compliance of I&C safety systems with the General Design Criteria and the requirements of IEEE 603 is addressed in Section 7.1 of the U.S. EPR FSAR.

***RAI 9***: *Provide additional documentation to support the assumption that the AV42 is not susceptible to CCF.*

*NUREG-0800, Chapter 7, Table 7.1 identifies "SRM to SECY-93-087 II.Q" as acceptance criteria for D3 assessments.*

*SECY-93-087, Enclosure 1, Page 54 states, "... digital I&C systems share more data transmission functions and shares more process equipment than their analog counter parts. Redundant trains of digital I&C systems may share databases (software) and process equipment (hardware). Therefore, a hardware design error, software design error, or software programming error may result in a common-mode or common-cause failure of redundant equipment."*

*It is now possible to design hardware by using software design methodologies (i.e., programmed in C, C++, or VHDL). Therefore, hardware that is designed by using software methodologies could be considered susceptible to CCF. The AV42 uses a programmable logic device (PLD) and, therefore, could be considered susceptible to common mode failures.*

*ANP-10284, Section 3.1.1.2, states, "Based on the design features and testing described above the AV42 is not susceptible to a CCF." However insufficient information has been provided to allow the NRC to reach this conclusion independently. The proposed methodology does not include any validation of this assumption.*

*A description of the PACS has not been submitted, but it is understood that the PACS will consist primarily of AV42 modules. Note: ANP-10284, Section 3.0 states, "... the main line of defense consists of the automatic safety functions performed by ... PACS, and therefore these are the systems of interest when considering CCFs."*

**Response 9:**

A topical report for the AV42 (PACS) module (ANP-10273) was submitted to the NRC for review on November 28, 2006. AREVA has responded to RAIs related to the AV42 topical report review.

A meeting/audit with the NRC staff and contract reviewer was conducted on September 26-27, 2007. The issues raised in D3 topical report RAI 9 were addressed at this meeting, and the full testability of the AV42 module was explained in detail. Responses to the RAIs that resulted from the initial AV42 topical review plus those generated by the ORNL contract reviewer (59 total) have been submitted to the NRC.

In Section 5 of the DI&C-ISG-02 guidance on diversity and defense-in-depth issues (rev. 1), it is stated that full testability is a design attribute that is sufficient to eliminate consideration of CCF.

The responses to AV42 topical report RAIs 1, 29, 38, and 56 are particularly relevant to the issue of non-susceptibility of the AV42 to CCF. AREVA NP believes that these issues are sufficiently addressed in the context of the AV42 topical report and subsequent review.

***RAI 10***: *Are all of the engineered safety feature (ESF) functions as described in IEEE STD 603-1991, implemented in four systems: 1) PS, 2) SAS, 3) SICS, and 4) PACS? Are there any other safety systems that implement ESF functions?*

*ANP-10284, Section 3.2.1.2, states, "The PS is the primary means of performing ESF actuations." Does this PS function fulfill the requirements of IEEE 603, Section 6.1?*

*ANP-10284, Section 3.2.1.4, states, "The SAS is the primary means of performing ESF control functions." Does the SAS address IEEE 603, Section 6.2.2?*

*ANP-10284, Section 3.2.1.2, states, "... manual means of actuating an ESF system is provided on the SICS in the MCR." Does this SICS function fulfill the requirements of IEEE 603, Section 6.2.1?*

**Response 10:**

Automatic initiation of ESF systems for event mitigation is performed by the PS in conjunction with the PACS. System level initiation of ESF functions is performed from the SICS and processed through the PS and/or PACS.

Subsequent automatic control of ESF systems is performed by the SAS in conjunction with the PACS. Manual control of ESF systems is available from the SICS, and processed by the SAS and/or PACS.

No safety related I&C systems, other than the four described above, are used to implement ESF functions.

Compliance of the I&C safety systems to the requirements of IEEE 603-1998 is addressed in Section 7.1 of the U.S. EPR FSAR.

***RAI 11**: Provide an explanation of how the D3 TR lines of defense are comparable to those of NUREG/CR-6303, since the lines have different scopes.*

*The scope of the AREVA lines of defense do not seem to include the sensors, displays or controls associated with the I&C systems (see quotes from Section 2 and 2.4. in RAI No. 3). In addition, Section 3.0 states, "... the main line of defense consists of the automatic safety functions performed by the PS, SAS, and PACS, and therefore these are the systems of interest when considering CCFs." The displays and controls are in the SICS or PICS and are therefore, not in the scope to the D3 TR.*

*ANP-10284, Section 2.5: "The U.S. EPR lines of defense are compared to these four echelons of defense discussed in NUREG/CR-6303 in Table 2-2."*

*The scope of the lines of defense in NUREG/CR-6303 is clarified by the definitions for those systems in NUREG-0493 and IEEE STD 603-1991.*

- *NUREG-0493, Section 1.2.2.1: "The scram system consists of sensors, signal processors, logic, and actuation initiation devices necessary to affect the reactor trip or scram, including essential auxiliary systems. This echelon of defense performs a safety function. The scram system is also known as the reactor trip system."*
- *NUREG-0493, Section 1.2.2.2: "The ESF system consists of sensors, signal processors, logic, and actuation initiation devices necessary to affect engineered safety features (for example, auxiliary feedwater, containment isolation, emergency core cooling, emergency power), including essential auxiliary systems. This echelon of defense performs a safety function."*

- *NUREG-0493, Section 1.2.2.3: "The control system consists of all instrumentation and control equipment not included in the scram or ESF actuation systems, including automatic and manual process controls, presentation of information to the operator (plant monitoring system), and plant computer(s) that are not part of the scram or ESF actuation systems. This echelon of defense does not perform a safety function, but is nevertheless important to the defense-in-depth principle."*
- *IEEE 603: See Figure 1 & 3*

*These lines of defense explicitly include sensors, displays and controls.*

**Response 11:**

Section 2.5 of the D3 topical report provides a comparison of the U.S. EPR I&C lines of defense and the NUREG/CR-6303 echelons of defense.

It is not appropriate to use definitions of echelons of defense contained in NUREG-0493 to define the echelons described in NUREG/CR-6303. The two documents do not describe the same number of echelons, and the definition for the control echelon in 0493 includes items that are part of a completely separate echelon in 6303 (i.e., monitoring and indication). Additionally, NUREG-0493 is not listed as relevant guidance in BTP 7-19, while NUREG/CR-6303 is cited as relevant.

Likewise, it is not appropriate to use the IEEE 603 definition of the scope of IEEE 603 coverage (Figure 1), or the IEEE 603 definition of elements of a safety system (Figure 3), to somehow define the echelons of defense for a complete I&C architecture. For example, Figure 3 of IEEE 603 combines the RTS and ESF systems into the same operational element, while NUREG/CR-6303 defines these as two separate echelons of defense. Additionally, IEEE 603 does not address the elements of non-safety-related systems, which comprise major portions of the echelons of defense as described in NUREG/CR-6303.

Sensors are required for the I&C systems in all of the lines of defense to perform their functions. Likewise, displays and manual controls play a role in the functionality of each system in each line of defense. Sensors, displays and manual controls are not in and of themselves lines of defense in the U.S. EPR design. Instead, they operate to support all lines of defense.

***RAI 12**: Figure 2-2 does not include the PACS as part of the main line of defense. However, ANP-10284, Section 3.0, states, "... the main line of defense*

*consists of the automatic safety functions performed by the PS, SAS, and PACS..." Please clarify (see also related RAI No. 15).*

**Response 12:**

The PACS is not included in Figure 2-2 because it participates in the functionality of all of the lines of defense. The statement: "…the main line of defense consists of the automatic safety functions performed by the PS, SAS, and PACS…" is accurate.

While the PACS processes actuation orders from the PS and SAS, it is not subject to the postulated CCF that disables these safety systems (see response to RAI 9). Because the PACS is common to multiple lines of defense, and it is not subject to the postulated CCF, it does not need to be assigned to a specific line of defense for the purpose of performing a D3 analysis.

***RAI 13**: Provide a description of why the PAS should be considered to be simple digital equipment.*

*BTP 7-19 identifies the SRM on SECY-93-087 as relevant regulatory guidance for addressing the regulatory requirements addressed by BTP 7-19. The SRM on SECY-93-087 approved the staff position in SECY-93-087 with minor changes.*

*SECY-93-087 states (Enclosure 1, bottom of page 56): "The staff has concluded that analyses that demonstrate adequate rather than equivalent, defense against the postulated common-mode failures would be allowed in the diversity assessment required of the applicant. ... The staff will not require only analog equipment and will consider allowing simple digital equipment."*

*AREVA has stated that the PAS will be used to address CCF. (ANP-10284, Section 3.2.1.3 states, "The SAS is the primary means of performing ESF control functions. Assuming a postulated CCF renders the SAS inoperable, the PAS is available as a diverse means of executing ESF control functions." ANP-10284, Section 3.2.1.4, states, "The PAS provides diverse processing of sensor information because the PAS obtains sensor information independently of the PS and SAS software.")*

*AREVA has not provided a description of the PAS that describes why it should be considered to be simple digital equipment. The methodology described does not include an assessment of the simplicity of the PAS (see also related RAI No. 4).*

**Response 13:**

The response to RAI 4 describes why the DAS is not required to be "simple" digital equipment. The same logic is used by AREVA NP to determine that the PAS is not required to be "simple" digital equipment (the DAS is a sub-system of the PAS).

***RAI 14**: Do SICS displays address the requirements of IEEE STD 603-1991, Sections 5.8.1 and 5.8.4?*

*ANP-10284, Section 3.2.1.4, states, "... including type A, B and C post accident monitoring variables as defined in Regulatory Guide 1.97 ... The PS and SAS are the credited means of processing these variables, and the SICS is the credited means for display."*

**Response 14:**

The SICS displays meet the requirements of IEEE 603-1998 Clauses 5.8.1 and 5.8.4.

Compliance with these clauses of IEEE 603 is not a subject of ANP-10284, and should not be required for approval of the report. Compliance of the I&C safety systems to the requirements of IEEE 603-1998 is addressed in Section 7.1 of the U.S. EPR FSAR.

***RAI 15**: List all safety systems that will be analyzed.*

*ANP-10284, Section 2.4, states, "In general, the lines of defense apply to the architecture level 1 automation systems." However, ANP-10284, Section 4.1, states, "An analysis of the safety I&C systems will be performed to determine their susceptibility to a CCF." Therefore, without an explicit list of the systems that will be analyzed in ANP-10284, Section 4.1, it is not clear if the PACS and SICS will be included in the D3 analysis (see also related RAI No. 12).*

**Response 15:**

Section 4.1 of the D3 topical report states the following assumptions that are used when performing the analysis:

"A CCF of the TXS platform is postulated (conservative assumption). This postulated CCF is such that the TXS based I&C systems do not perform their functions when required."

"The AV42 is not affected by a CCF of the TXS process computers. It is not considered to be susceptible to a software CCF."

Table 2-1 in the D3 topical report lists the I&C systems and their associated platforms. According to the assumptions defined in Section 4.1, all TXS computer-based systems (PS, SAS, QDS as part of SICS)) are assumed to fail to actuate when required due to a TXS platform software CCF.

***RAI 16**: How will the analysis methodology described in the D3 TR differ from the methodology in NUREG/CR-6303.*

*ANP-10284, Section 4.1, states, "This analysis addresses Point 1 of NUREG-0800, BTP 7-19, and will be performed using NUREG/CR-6303 as a model." How is "using NUREG/CR-6303 as a model" different from following the methodology described in NUREG/CR-6303?*

**Response 16:**

The statement in Section 4.1: "this analysis addresses Point 1 of NUREG-0800, BTP 7-19, and will be performed using NUREG/CR-6303 as a model" incorrectly implies that only step 1 (Susceptibility Analysis of Safety I&C Systems to CCF) is performed using NUREG/CR-6303 as a model.

The intent of AREVA NP is to demonstrate that the entire Diversity and Defense-in-Depth methodology presented in Section 4 of the D3 topical report is consistent with NUREG/CR-6303 and will be used for the analysis.

The statement quoted above will be modified, as proposed in Attachment 1, to clarify this issue.

***RAI 17**: Describe why a postulated failure of the TXS platform is more conservative than outputs assumed to fail in a manner that is credible but that produces the most detrimental consequences.*

*NUREG/CR-6303, Section 3.5, "Guideline 5 - Method of Evaluation" states, "Block output signals must be assumed to fail in a manner that is credible but that produces the most detrimental consequences when analyses in accordance with Guideline 9."*

*ANP-10284, Section 4.1, states, "The following assumptions are to be used when performing this analysis: ... A CCF of the TXS platform is postulated (conservative assumption). This postulated CCF is such that the TXS based I&C systems do not perform their functions when required."*

**Response 17:**

The Staff Position in the current Interim Staff Guidance in the area of defense-in-depth and diversity issues (DI&C-ISG-02) states in Section 4:

"In general, spurious trips and actuations are of a lesser safety concern than failures to trip or actuate. There may be plant and safety system challenges and stresses; however, these challenges are not as significant as failures to respond to abnormal operating occurrences and design basis events. For these reasons, spurious trips or actuations of safety-related digital protection systems resulting from CCFs do not need to be addressed beyond what is already set forth in plant design basis evaluations."

AREVA NP agrees with this staff position and asserts that a simultaneous and complete failure of all TXS computer systems to perform their safety function concurrent with an event requiring protective action is in fact the failure that produces the most detrimental consequences. This approach is consistent with the failure assumptions documented in Siemens Report EMF-2267(P), and approved by the NRC as described in the response to RAI 1.

Additionally, the guidance in NUREG/CR-6303 would have the applicant divide the safety systems into smaller "blocks" and assume the CCF of all identical blocks. This approach would allow credit to be taken for other non-identical "blocks" within the safety systems to mitigate any concurrent event. Therefore, an assumed total failure of all TXS systems to perform their safety function is more conservative than the approach described in NUREG/CR-6303.

**Attachment 1: Proposed modifications to ANP-10284**

***Affected Section:*** 1.1 and 5.0

***Affected Text:***

AREVA NP requests the approval of the following items in this report:

- The U.S. EPR defense-in-depth concept.
- The adequacy of the proposed design features to mitigate the consequences of a postulated CCF in the safety systems.
- The methodology used to evaluate the adequacy of the I&C design with respect to D3.

***Replace Affected Text With:***

AREVA NP requests the approval of the following items in this report:

- The U.S. EPR defense-in-depth concept.
- The methodology used to evaluate the adequacy of the I&C design with respect to D3.

***Affected Section:*** 2.1

***Affected Text:***

For the initiation of critical safety functions at the system level (e.g., reactor trip, safety injection), conventional means (i.e., buttons, switches) are provided on the SICS. These signals bypass the TXS computers and are hardwired directly to actuation devices (e.g., reactor trip devices or priority actuation and control (PAC) modules).

***Replace Affected Text With:***

For the initiation of protective actions at the system level (e.g., reactor trip, safety injection), conventional means (i.e., buttons, switches) are provided on the SICS. For ESF system initiations, these signals are either acquired by TXS computers and combined with the automatic actuation logic, or are hardwired directly to PACS modules. For RT initiation, the signals are hardwired directly to the reactor trip devices to bypass the TXS computers.

***Affected Section:*** 2.4

***Affected Text:***

In general, the lines of defense apply to the architecture level 1 automation systems. The PACS is used to prioritize actuation requests from the various I&C systems.

***Replace Affected Text With:***

In general, the lines of defense apply to the architecture level 1 automation systems. The PACS prioritizes actuation requests from I&C systems within each of the lines of defense and therefore does not belong to any single line of defense. The prioritization of actuation requests incorporates the D3 concepts and is described in Section 7.1 of the U.S. EPR Final Safety Analysis Report (FSAR).

***Affected Section:*** 3.2.1.2

***Affected Text:***

If an ESF actuation is required to be automatic, it is performed by the DAS, a subsystem of the PAS. If automatic actuation is not required, manual means of actuating an ESF system is provided on the SICS in the MCR. These means are provided to address Point 4 of NUREG-0800, BTP 7-19. These are hardwired controls that are assigned to the independent safety divisions. The controls are diverse because a software failure of the safety systems will not affect the operation of the hardwired controls. This diversity is shown in Figure 3-3.

In addition, diverse actuation of ESF systems at the component level is provided from PICS via PAS.

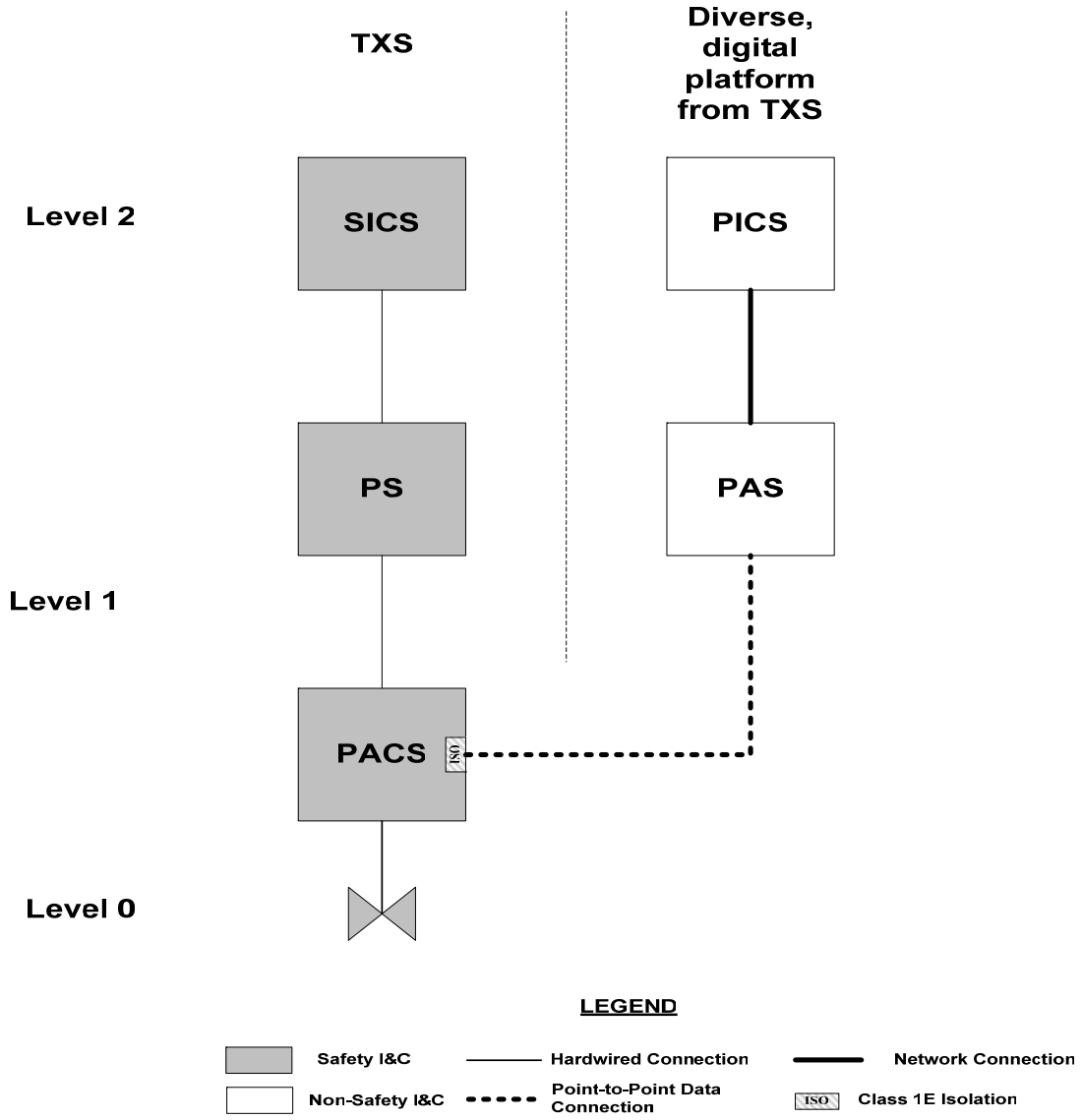
***Replace Affected Text With:***

If an ESF actuation is required to be automatic, it is performed by the DAS, a subsystem of the PAS. If automatic actuation is not required, manual means of actuating an ESF system are provided at the component level from the PICS via the PAS. The controls are diverse because a software failure of the safety systems will not affect the operation of the PICS or PAS.

***Affected Figure:*** Figure 3-3 "Diversity for Actuation of ESF Systems"

***Replace Affected Figure With:***

**Figure 3-3 – Diversity for Actuation and Control of ESF Systems**



***Affected Section:*** 3.2.1.3

***Affected Text:***

The controls provided in PAS address the guidance of Section 7.3 of NUREG-0800 on diversity of ESF controls. This diversity is shown in Figure 3-4.

***Replace Affected Text With:***

The controls provided in PAS address the guidance of Section 7.3 of NUREG-0800 on diversity of ESF controls. This diversity is shown in Figure 3-3.

***Affected Figure:*** Figure 3-4

***Replace Affected Figure With:***

Figure 3-4 is removed from the report.

***Affected Section:*** 3.2.1.4

***Affected Text:***

The PICS, which is used during all plant conditions, as long as it is available, provides a diverse display. This diversity is shown in Figure 3-5.

***Replace Affected Text With:***

The PICS, which is used during all plant conditions, as long as it is available, provides a diverse display. This diversity is shown in Figure 3-4.

***Affected Section:*** Title of Figure 3-5

***Affected Text:***

Figure 3-5 – Diversity of Indications and Alarms

***Replace Affected Text With:***

Figure 3-4 – Diversity of Indications and Alarms

***Affected Section:*** 4.0

***Affected Text:***

The methodology addresses the guidance in NUREG-0800, BTP 7-19.

***Replace Affected Text With:***

The methodology addresses the guidance in NUREG-0800, BTP 7-19, and is consistent with the methodology outlined in NUREG/CR-6303.

***Affected Section:*** 4.1

***Affected Text:***

This analysis addresses Point 1 of NUREG-0800, BTP 7-19, and will be performed using NUREG/CR-6303 as a model. The following assumptions are to be used when performing this analysis:

***Replace Affected Text With:***

This analysis addresses Point 1 of NUREG-0800, BTP 7-19. The following assumptions are to be used when performing this analysis:

***Affected Section:*** 4.3.1

***Affected Text:***

**4.3.1 Hardwired Controls on SICS**

The inventory of hardwired controls on SICS is developed using the following requirements:

- System-level manual actuation for critical safety functions, which include: reactor shutdown, core inventory control, decay heat removal, containment isolation and containment integrity.
- System-level manual actuation of those safety functions that were credited for manual operator action in Step 2.

***Replace Affected Text With:***

**4.3.1 Controls on SICS**

Safety related controls are provided on the SICS. However, these controls are not credited for providing diverse manual initiation of ESF systems in case of a software CCF of the safety systems. Hardwired controls provided on SICS for reactor trip are credited in the D3 analysis.

***Affected Section:*** 4.3.2

***Affected Text:***

Safety-related plant equipment will have the capability of being controlled manually at the component level from the PICS via the PAS and PACS. This will fulfill the requirement of performing manual functions that don't require system level manual actuation.

***Replace Affected Text With:***

Safety-related plant equipment will have the capability of being controlled manually at the component level from the PICS via the PAS and PACS. The functions that were credited for manual operator action in Step 2 are performed via these PICS controls.