Request for Additional Information No. 57 (951,972), Revision 0

9/12/2008

U. S. EPR Standard Design Certification
AREVA NP Inc.
Docket No. 52-020
SRP Section: 07.07 - Control Systems
SRP Section: 07.08 - Diverse Instrumentation and Control Systems
Application Section: FSAR Ch 7
ICE1 Branch

QUESTIONS

07.07-1

Describe all signal and communication interchanges between the Reactor Control, Surveillance and Limitation (RCSL)system and the Protection System (PS) system (both unidirectional and bidirectional) providing schematics (with components labeled) and explanation of the type of isolation used. How will this isolation acceptance criteria in Regulatory Guide 1.75, IEEE 384-1992 and Standard Review Plan, Branch Technical Position 7-11?

10 CFR Part 50, Appendix A, General Design Criterion 24, "Separation of Protection and Control Systems," requires that the protection system be separated from control systems to the extent that failure of any single control system component or channel, or failure or removal from service of any single protection system component or channel which is common to the control and protection systems leaves intact a system satisfying all reliability, redundancy, and independence requirements of the protection system. Interconnection of the protection and control systems shall be limited so as to assure that safety is not significantly impaired.

One of the staff’s acceptance criteria is that isolation between a non-safety-related system and a safety related system conforms to the guidance of Regulatory Guide 1.75, "Criteria For Independence of Electrical safety Systems," which endorses IEEE Std. 384-1992, “Standard Criteria for Independence of Class 1E Equipment and Circuits”. Also address Branch Technical Position 7-11 with regards to qualified electrical isolation devices.

07.07-2

Are the rod position indicators that are discussed in Section 4.6.1 of the U.S. EPR DC-FSAR the same as the rod cluster control assembly (RCCA) lower end position sensors that are discussed in Section 7.2.1.3.6? If yes, what is the reason for using different terminology? If no, how are these two items/components different?

07.07-3

DC FSAR, Tier 2, Section 4.6.1, states that the safety-related analog measurement is addressed in Section 7.2. Where (section and page) exactly is the operation of the RCCA assemblies analog measurement discussed in detail in Section 7.2? Where are the schematics and the detailed functional diagrams for the analog measurement located? If they currently are not in the DC FSAR, please provide.

07.07-4

Please clarify where manual reactor trip buttons are to be used and where manual reactor trip switches will be located in the main control room. Please explain what type of manual reactor trip initiators will be placed on the SICS and what type will be used on the PICS.

Clause 6.2 of IEEE Std. 603-1991 requires means to be provided in the control room to implement manual initiation at the division level of the automatically initiated protective actions. In the U.S. EPR Digital Protection System Topical report, ANP-10281P, Revision 0, page 7-6, it states that, “There are four dedicated reactor trip buttons in the main control room, one for each division.” In the U.S. EPR Instrumentation and Control Diversity and Defense-in-Depth Methodology Topical Report, ANP-10284, Revision 0, page 3-6, it states that, “The hardwired controls on SICS to initiate reactor trip, as discussed in Section 2.1 of the report, are provided to address Point 4 of NUREG-0800, BTP-19. These controls consist of four switches, each assigned to an independent safety division.” Clarify the description of the mechanisms for performing a manual reactor trip, and their location(s).

07.07-5

DC FSAR, Tier 2, Section 7.1, page 7.1.1.4.5, states:

The RCSL consists of these functional units:

- Acquisition Units (AU).
- Control Units (CU).
- Drive Units (DU).
- MSIs.
- GWs.
- SUs.

10 CFR Part 50, Appendix A, General Design Criteria 13, requires, in part, that appropriate instrumentation and controls be provided to maintain variables and systems within prescribed operating ranges. What module in the RCSL performs input signal processing (i.e., calculations, setpoint comparisons, auctioneering)? Where is this explained in the DC FSAR? alternatively, please provide the information.

07.07-6

DC FSAR, Tier 2, Section 7.7.1.1, page 7.7-2, states: "The logic that generates the control current comes from the RCSL System." How does the RCSL [Reactor Control, Surveillance and Limitation] system perform logic processing? Provide detailed explanation and provide at a minimum a schematic of process components with associated signal inputs and outputs and a logic diagram.

10 CFR Part 50, Appendix A, General Design Criterion 10, requires in part, that the reactor core and associated coolant, control, and protection systems shall be designed with appropriate margin to assure that specified acceptable fuel design limits are not exceeded during any control of normal operation, including the effects of anticipated operational occurrences. The staff needs additional information on the RCSL system.

07.07-7

DC FSAR, Tier 2, Section 7.7.2.3.6, page 7.7-13, it states: "Four (i.e., one per PS division) RCCA drop detection logic signals are acquired in RCSL and voted one out of four." Explain and describe in detail how voting is accomplished in the RCSL. What is the design basis for voting “one out of four”? Provide schematic of process components with associated signal inputs and outputs.

10 CFR Part 50, Appendix A, General Design Criterion 13, requires, in part, appropriate controls to be provided to maintain variables that affect the fission process within prescribed operating ranges. The staff needs additional details regarding the RCCA drop detection logic to complete the review.

07.07-8

Explain the processes, procedures, and mechanisms in place to verify that the PICS is functioning correctly. Identify where such processes, procedures, and mechanisms are explained in the U.S. EPR DC-FSAR?

10 CFR Part 50, Appendix A, General Design Criteria 13 requires, in part, that instrumentation shall be provided to monitor variables and systems over their anticipated ranges for normal operation, for anticipated operational occurrences, and for accident conditions as appropriate to assure adequate safety, including those variables and systems that can affect the fission process, the integrity of the reactor core, the reactor coolant pressure boundary, and the containment and its associated systems. Appropriate controls shall be provided to maintain these variables and systems within prescribed operating ranges. U.S. EPR Digital Protection System Topical Report, ANP-10281P, Section 13.3, page 13-2, states that: "The PICS is the primary operator interface to the U.S. EPR I&C systems and is to be used in all plant conditions as long as it can be verified to be functioning correctly." The staff needs additional details regarding the capability to determine the functionality of PICS to complete the review.

07.07-9

The heading of Section 4.4 of Topical Report, EMF-2110(NP), Revision 1, “TELEPERM XS: A Digital Reactor Protection System," states “Single Wire Signal Transmission”. Is the heading “Single Wire Signal Transmission” synonymous with “Hardwired Signal Transmissions?” Does the term “Hardwired Signal Transmissions” mean the same thing as “Single Wire Signal Transmissions?”

07.07-10

Are all monitoring and service interfaces (MSIs) used in the U.S. EPR design classified as Class 1E? If not, state which ones are not Class 1E and the basis.

07.07-11

Provide a schematic that shows input signal connections and output signal connection to the device (i.e., APU module, Control module) that performs the signal selection algorithms. Additionally, describe in detail the signal selection algorithms in the Reactor Control, Surveillance and Limitation (RCSL) system.

10 CFR Part 50, Appendix A, General Design Criteria 13, requires, in part, that instrumentation shall be provided to monitor variables and systems over their anticipated ranges for normal operation, for anticipated operational occurrences, and for accident conditions as appropriate to assure adequate safety, including those variables and systems that can affect the fission process, the integrity of the reactor core, the reactor coolant pressure boundary, and the containment and its associated systems. Appropriate controls shall be provided to maintain these variables and systems within prescribed operating ranges.

DC FSAR, Tier 2, Section 7.7.2.10, states that the non-safety related Reactor Control, Surveillance and Limitation (RCSL) system uses signal selection algorithms to calculate a process representation value which is then used by the non-safety control system to take action. The calculated value reflects all the input signals and not a specific signal value. This technique provides fewer challenges to safety-related I&C systems due to non-safety control system failure. The staff requests additional information describing the signal selection algorithm and process in the RCSL to determine that appropriate controls are provided to maintain fission process variables within prescribed operating ranges.

07.07-12

Explain how the Reactor Control, Surveillance and Limitation (RCSL) system performs the processing (i.e., calculations, setpoint comparisons, auctioneering) of incoming sensor and detector signals. Provide a detailed explanation of how the signal selector algorithms work. Start from an input signal from the PS system and explain how the process representation value is calculated and how this value will eventually be used to initiate an operational and limitation function. If DC FSAR, Tier 2, Figure 7.7-1, "Average Coolant Temperature Control Logic," is to be referenced, provide a schematic that shows component or device that performs the control logic of Figure 7.7-1 and provide corresponding input signals, isolation devices used and output signals on schematic. The schematic should be of the type provided by Figure RAI 19-1, page 5, and Figure RAI 19-2, page 6, in “Response to Second Request for Additional information”, Attachment A, ANP-10284Q2P.

10 CFR Part 50, Appendix A, General Design Criteria (GDC) 13, requires, in part, that appropriate controls shall be provided to maintain these variables [fission process variables] and systems within prescribed operating ranges. GDC 24 requires, in part, that the protection system be separated from control systems to

the extent that failure of any single control system component or channel, or failure or removal from service of any single protection system component or channel, which is common to the control and protection systems leaves intact a system satisfying all reliability, redundancy, and independence requirements of the protection system.

DC FSAR, Tier 2, Section 7.7.2.10, states that the non-safety-related RCSL control system uses signal selection algorithms to calculate a process representation value which is then used by the non-safety control system to take action. The calculated value reflects all the input signals and not a specific signal value. This technique provides fewer challenges to safety-related I&C systems due to non-safety control system failure. The staff has insufficient information regarding the RCSL processing, including the signal selector algorithm.

07.07-13

Provide a list of non-safety control system failures, their effect on the plant, and the expected response of safety-related instrumentation and control systems.

10 CFR Part 50, Appendix A, General Design Criteria 13 requires, in part, that instrumentation shall be provided to monitor variables and systems over their anticipated ranges for normal operation, for anticipated operational occurrences, and for accident conditions as appropriate to assure adequate safety, including those variables and systems that can affect the fission process, the integrity of the reactor core, the reactor coolant pressure boundary, and the containment and its associated systems. Appropriate controls shall be provided to maintain these variables and systems within prescribed operating ranges.

DC FSAR, Tier 2, Section 7.7.2.10, states that the non-safety related RCSL control system uses signal selection algorithms to calculate a process representation value which is then used by the non-safety control system to take action. The calculated value reflects all the input signals and not a specific signal value. This technique provides fewer challenges to safety-related I&C systems due to non-safety control system failure. The staff requests additional information to understand the non-safety control system failure modes and their effects on the plant and safety systems.

07.07-14

Provide the basis that demonstrates how the signal selection algorithms provide fewer challenges to safety-related I&C systems due to non-safety control system failure.

10 CFR Part 50, Appendix A, General Design Criteria 13, requires, in part, that appropriate controls shall be provided to maintain these variables and systems [fission process variables and systems] within prescribed operating ranges.

DC FSAR, Tier 2, Section 7.7.2.10, states that the non-safetyrelated Reactor Control, Surveillance and Limitation (RCSL) control system uses signal selection algorithms to calculate a process representation value which is then used by the non-safety control system to take action. The calculated value reflects all the input signals and not a specific signal value. This technique provides fewer challenges to safety-related I&C systems due to non-safety control system failure.

07.07-15

DC FSAR, Tier 2, Section 4.6.2, states that Control Rod Drive Mechanisms (CRDMs) are equipped with a digital and analog position indication system. The same section also states that the analog position indication system is part of the Protection System. Describe the physical location of the analog position indication system and how it operates.

07.07-16

Provide the design basis and engineering judgment that would explain why the U.S. EPR incore and excore neutron instrumentation monitoring system does not need to meet the guidance of RG 1.151 and 1.105.

10 CFR Part 50, Appendix A, General Design Criteria 13 requires, in part, that instrumentation shall be provided to monitor variables and systems over their anticipated ranges for normal operation, for anticipated operational occurrences, and for accident conditions as appropriate to assure adequate safety, including those variables and systems that can affect the fission process, the integrity of the reactor core, the reactor coolant pressure boundary, and the containment and its associated systems. Appropriate controls shall be provided to maintain these variables and systems within prescribed operating ranges.

DC FSAR, Tier 2, Table 7.1-2, does not have the Regulatory Guide (RG) 1.151 and 1.105 checked as a system requirement for the incore or excore neutron instrumentation monitoring system. Standard Review Plan (SRP) Table 7-1 has both the RG 1.151 and 1.105 checked as an acceptance criteria for SRP Section 7.7 review items for conformance to GDC 13.

07.07-17

Explain how the Process Automation System performs the calculations, setpoint comparisons, generate actuation signal outputs (i.e. to open or close valve) and perform logic processing. Provide detailed explanation and provide schematic(s) of process components with associated signal inputs and outputs.

10 CFR Part 50, Appendix A, General Design Criteria 13 requires, in part, that instrumentation shall be provided to monitor variables and systems over their anticipated ranges for normal operation, for anticipated operational occurrences, and for accident conditions as appropriate to assure adequate safety, including those variables and systems that can affect the fission process, the integrity of the reactor core, the reactor coolant pressure boundary, and the containment and its associated systems. Appropriate controls shall be provided to maintain these variables and systems within prescribed operating ranges. The staff does not have sufficient information to determine adequacy of the PAS.

07.08-1

Provide the classification type (i.e., Class 1E, safety-related) and provide the test method and test results, in accordance with Standard Review Plan, Branch Technical Position (BTP) 7-11 and Regulatory Guide (RG) 1.75 for the electrical isolation device (shown as a box with parallel diagonal lines across the box at bottom of figure) for Figure RAI 19-2 on page 6 of the “Response to Second Request for Additional Information,” Attachment A, ANP-10284Q2P.

Clause 5.6.3 of IEEE Std. 603-1991, requires, in part, that the safety system design shall be such that credible failures in and consequential failures in and consequential actions by other systems shall not prevent the safety systems from meeting the requirements of this standard. One of the staff’s acceptance criteria for meeting the independence and separation requirements of IEEE Std. 603-1991, Clause 5.6.3, between safety systems and non-safety-related systems, is that the isolation of interconnections between the two systems meets the guidance of BTP 7-11 and RG 1.75. The staff could not locate schematics, type of test methods used, or test results that would show that the electrical isolation device used between the sensor, the Diverse Actuation System and the Protection System meet the independence criterion.

07.08-2

Address the periodic testing of the Diverse Actuation System (DAS) from end-to-end.

10 CFR 50.62(c) requires each pressurized water reactor to have equipment from sensor output to final actuation device, that is diverse from the reactor trip system. Generic Letter 85-06 provides guidance regarding the quality of such equipment. Specifically, Generic Letter 85-06, states in the enclosure titled “QA Guidance for Non-Safety-Related ATWS Equipment:”

> *Measures are to be established to test, as appropriate, non-safety-related ATWS equipment prior to installation and operation and periodically. Results of the tests should be evaluated to ensure that the test requirements have been satisfied.*

The staff was not able to locate information establishing the applicant’s commitment to periodically test the DAS to ensure availability.

07.08-3

Demonstrate quality assurance aspects of the Diverse Actuation System (DAS), including its design, construction, installation, inspection, testing, operation, maintenance, and modifications. Discuss the quality assurance aspects associated with the DAS software development, hardware qualification, and system testing. Identify where the DAS complies with acceptance criteria in Chapter 7 of the Standard Review Plan.

10 CFR 50.62(c) requires, in part, that each pressurized water reactor must have equipment from sensor output to final actuation device, that is diverse from the reactor trip system. Generic Letter 85-06 provides acceptance criteria for quality assurance for Anticipated Transient Without Scram systems. 10 CFR Part 50, Appendix A, General Design Criteria 22, requires, in part, that design techniques, such as functional diversity or diversity in component design and principles of operation, shall be used to the extent

practical to prevent loss of the protection function. The Staff Requirements Memorandum for SECY 93-087 provides guidance for diverse system to address common-cause failure of digital protection systems. Item II.Q.3 states that 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 staff was not able to locate where the applicant demonstrates that the DAS is of sufficient quality.