

**Response to**

**Request for Additional Information No. 61 (970,977), Revision 0**

**9/12/2008**

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

**AREVA NP Inc.**

**Docket No. 52-020**

**SRP Section: 07.04 - Safe Shutdown Systems**

**SRP Section: 07.05 - Information Systems Important to Safety**

**Application Section: FSAR Ch 7**

**ICE1 Branch**

**Question 07.04-1:**

Do the safe shutdown functions of the controls and systems listed in DC FSAR, section 7.4.1.2.1 through 7.4.1.2.13 involve features or operating modes that are unique to their safe shutdown functions and if so how do you demonstrate compliance to 10 CFR 50.55a(h) criteria listed in NUREG-0800, SRP Section 7.4?

DC FSAR, Tier 2 Section 7.4.1.1 states, "Engineered safety features (ESF) are used to achieve and maintain safe shutdown. The actuation of the ESF is performed by the protection system (PS). The I&C that perform ESF actuation are described in Section 7.3. The safety automation system (SAS) automatically controls the safety-related systems once those systems are actuated by the PS. The SAS provides manual and grouped commands execution initiated from either the safety information and control system (SICS) or the process information and control system (PICS)."

It is unclear whether these 'manual and grouped commands' executed from the SICS or PICS are unique to safe shutdown functions or used in a way not fully detailed in Sections 7.2 and 7.3 of the DC FSAR.

**Response to Question 07.04-1:**

A response to this question will be provided by December 4, 2008.

**Question 07.04-2:**

Demonstrate how the safe shutdown system design meets the requirements of 10 CFR 50.34(f)(2)(xx), "Power for Pressurizer Level Indication and Controls for Pressurizer Relief and Block Valves," or equivalent TMI action plan requirements imposed by Generic Letters.

DC FSAR, Tier 2 Section 7.4.2 does not address this requirement as required by NURG-0800, SRP Section 7.4.

**Response to Question 07.04-2:**

U.S. EPR FSAR Tier 2, Section 7.5.2.1.1 addresses 10 CFR 50.34(f)(2)(xx) in regards to power to pressurizer (PZR) level indication with the following:

"Each of the four PZR level sensors generates a signal that is received in one of the four divisions of the PS. The PZR level sensors are powered from the Class 1E bus of the PS division in which the sensor signal is received. PZR level indication is provided by PICS and backed by the safety related SICS.

Each division of the PS and the SICS is supplied by an independent Class 1E, uninterruptible electrical bus. These busses are backed by the emergency diesel generator to cope with loss of offsite power. Inside a division, the PS cabinets are supplied by the two redundant, uninterruptible 24 Vdc feeds. To cope with loss of onsite and offsite power, the feeds to the PS cabinets are supplied with two-hour batteries."

The function of the PZR relief and block valves referred to in 10 CFR 50.34(f)(2)(xx) is provided in the U.S. EPR by the PZR safety relief valves (PSRV).. U.S. EPR FSAR Tier 2, Section 7.1.2.1.11 addresses 10 CFR 50.34(f)(2)(xx) on the power to the controls of the PSRVs with the following:

"The pilot valves for the pressurizer safety relief valves (PSRV) are controlled by the PS and the PACS as described in 7.3.1.2.13. The PS and PACS are powered by the EUPS as described in Section 7.1.1.4.1 and Section 7.1.1.4.3. The PSRVs are described in Section 5.2. The EUPS is described in Section 8.3."

**FSAR Impact:**

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

**Question 07.04-3:**

Provide information to demonstrate how the safe shutdown I&C design meets 10 CFR 50, Appendix A GDC 2 & 4 in accordance with the acceptance criteria of Section 7.4 of NUREG-0800.

DC FSAR, Tier 2 Section 7.4. Section 7.4.1.1, 'I&C Systems Associated with Safe Shutdown,' identifies the following as systems used for safe shutdown; protection system (PS), safety automation system (SAS), safety information and control system (SICS), process information and control system (PICS) and the process automation system (PAS). DC FSAR, Section 7.4.2.1, 'Conformance to General Design Criteria' identifies conformance to GDC 2 and 4. DC FSAR, Section 7.1 Table 7.1-2 lists GDC 2 and 4 as not applicable to PAS and PICS.

**Response to Question 07.04-3:**

The safety-related systems that meet GDC 2 and GDC 4 are the PS, SAS, SICS, and the priority and actuator control system (PACS) as identified in U.S. EPR FSAR Tier 2, Table 7.1-2—I&C System Requirements Matrix. PAS and PICS are non-safety-related instrumentation and controls (I&C) systems and are not required to perform safety-related functions. PICS and PAS are not credited in the safe shutdown scenario using only safety-related equipment in accordance with BTP 5-4. However, PAS and PICS are used in the safe shutdown scenarios where non-safety-related equipment is allowed by regulations. Post-fire safe shutdown in accordance with RG 1.189 and safe shutdown during and following a station blackout (SBO) are the scenarios where non-safety-related equipment is used.

The PACS will be added to the I&C systems associated with safe shutdown. The following paragraph will be added in U.S. EPR FSAR Tier 2, Section 7.4.1.1:

“A priority and actuator control system (PACS) module is assigned to safety-related components associated with safe shutdown. The functions performed by PACS modules are described in Section 7.1.1.4.3.”

**FSAR Impact:**

U.S. EPR FSAR Tier 2, Section 7.4.1.1 will be revised as described in the response and indicated on the enclosed markup.

**Question 07.04-4:**

Demonstrate how the remote shutdown station design provides the capability for (1) prompt, hot shutdown of the reactor, including necessary I&C to maintain the unit in a safe condition during hot shutdown, and (2) with a potential capability for subsequent cold shutdown of the reactor through the use of suitable procedures, meeting the requirements of GDC 19. DCD FSAR, Section 7.4.1.3.4 references a “safe shutdown state.”

**Response to Question 07.04-4:**

The human factors engineering (HFE) program described in U.S. EPR FSAR Tier 2, Chapter 18 applies to the design of the remote shutdown station (RSS). The RSS design will include the design of the human system interface (HSI), which will be implemented on the process information and control system (PICS) and the safety information and control system (SICS). The HFE program provides a design process that will determine the proper HSI in the RSS necessary to bring the reactor to safe shutdown. U.S. EPR FSAR Tier 1, Table 3.4-1—Human Factors Engineering Inspections, Tests, Analyses, and Acceptance Criteria provides inspection, tests, analysis, and acceptance criteria (ITTAC) for designing the HSI in the RSS and verifying that the final design allows operator actions necessary to achieve safe shutdown.

Safe shutdown is defined in the response to RAI 61 Question 07.04-5.

**FSAR Impact:**

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

**Question 07.04-5:**

DC FSAR, Section 7.4 states the definition of safe shutdown (is) different depending on the scenario. Define safe shutdown for each of the given three scenarios provided in Section 7.4 in accordance with GDC 19. Also, identify the equipment and process of achieving safe shutdown for the three scenarios.

**Response to Question 07.04-5:**

A response to this question will be provided by December 4, 2008.

**Question 07.04-6:**

Is the equipment in the remote shutdown station designed to the same standards as the corresponding equipment in the main control room to meet our guidance given in SRP Section 7.4? If not, to what standards is the remote shutdown equipment designed to?

**Response to Question 07.04-6:**

The equipment in the remote shutdown station (RSS) is designed to the same standards as the corresponding equipment in the main control room (MCR).

**FSAR Impact:**

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

**Question 07.04-7:**

Provide information to demonstrate how the safe shutdown I&C design meets 10 CFR 50, Appendix A, GDC 34, 35 and 38 in accordance with the acceptance criteria of Section 7.4 of NUREG-0800.

DC FSAR, Tier 2, Section 7.4.2.1, "Conformance to General Design Criteria," identifies conformance to GDC 34. However, DC FSAR, Tier 2, Table 7.1-2, lists GDC 34, 35, and 38 as not applicable to PAS and PICS.

**Response to Question 07.04-7:**

10 CFR 50, Appendix A, GDC 34 requires a system to remove residual heat. The residual heat removal system (RHRS) along with auxiliary supporting systems for safe shutdown such as the component cooling water system (CCWS) and the essential service water system (ESWS) are controlled by the safety automation system (SAS). In the event of loss of coolant accident (LOCA), the protection system (PS) provides initiation signals to the components of the RHRS, such as the low head medium injection pumps. The priority and actuator control system (PACS) system contains PACS modules that are assigned to each safety-related actuator. The PACS modules perform prioritization of instrumentation and controls (I&C) signals sent from the Level I I&C systems to the actuators of components used for residual heat removal (RHR).

10 CFR 50, Appendix A, GDC 35 requires a system to provide abundant emergency core cooling. The safety injection system (SIS), using the medium head safety injection pumps, provides the means for abundant emergency core cooling in the event of LOCA. The PS provides automatic initiation signals to start the SIS as described in U.S. EPR FSAR Tier 2, Section 7.3.1.2.1. The SAS provides controls to the auxiliary supporting systems necessary for emergency core cooling. The PACS modules perform prioritization of I&C signals sent from the Level I I&C systems to the actuators of components used for emergency core cooling.

10 CFR 50, Appendix A, GDC 38 requires a system to remove heat from the reactor containment. The SIS performs containment heat removal in the event of LOCA. The PS provides the automatic initiation signals to start the SIS as described in U.S. EPR FSAR Tier 2, Section 7.3.1.2.1. The SAS provides the control of the auxiliary supporting systems necessary for containment heat removal. The PACS modules perform prioritization of the I&C signals sent from the Level I I&C systems to the actuators of components used for containment heat removal.

As stated in U.S. EPR FSAR Tier 2, Section 7.4.1.1, the SAS provides manual and grouped commands execution initiated from either the safety information and control system (SICS) or the process information and control system (PICS). This is designed to provide control of the safety-related systems that are needed to reach safe shut down of the plant. PICS provides a non-credited means to monitor and control systems required for safe shutdown. The process automation system (PAS) implements non-safety related or non-credited control functions. PICS and PAS are not credited for meeting GDC 34, 35, and 38.

The PACS will be added to the I&C systems associated with safe shutdown. The following paragraph will be added in U.S. EPR FSAR Tier 2, Section 7.4.1.1:

“A priority and actuator control system (PACS) module is assigned to safety-related components associated with safe shutdown. The functions performed by PACS modules are described in Section 7.1.1.4.3.”

**FSAR Impact:**

U.S. EPR FSAR Tier 2, Section 7.4.1.1 will be revised as described in the response and indicated on the enclosed markup.

**Question 07.04-8:**

DC FSAR, Tier 2, Section 7.4.1.3, lists the main feedwater system and the chemical and volume control system as additional systems to the ESF systems listed in Section 7.4.1.2 for post-fire safe shutdown. Is the fuel pool cooling system described in Section 7.4.1.3.3 to be included as a post-fire safe shutdown system?

**Response to Question 07.04-8:**

The fuel pool cooling system (FPCS) described in U.S. EPR FSAR Tier 2, Section 7.4.1.3.3 is included as a post-fire safe shutdown system.

**FSAR Impact:**

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

**Question 07.04-9:**

Which is the credited system for safe shutdown PICS/PAS or SICS/SAS? What are the differences in the two, in particular their capabilities and qualification, and how will that affect performing safe shutdown from either system. Demonstrate how the credited system meets the requirements for safe shutdown and how it addresses the NRC's acceptance criteria. If PICS/PAS are not credited for safe shutdown, but used as the primary system for safe shutdown actions, demonstrate how operators will be alerted to various hardware and software failures within PICS/PAS in order to use SICS/SAS.

DC FSAR, Tier 2, Section 7.4.1.1, 'I&C Systems Associated with Safe Shutdown,' identifies the following as systems used for safe shutdown; protection system (PS), safety automation system (SAS), safety information and control system (SICS), process information and control system (PICS) and the process automation system (PAS).

**Response to Question 07.04-9:**

A response to this question will be provided by December 4, 2008.

**Question 07.05-1:**

Provide information to demonstrate how the design addresses 10 CFR 50.55a(h) in accordance with the acceptance criteria of Section 7.5 of NUREG-0800. For accident monitoring instrumentation isolated from the protection system, the applicable requirements of 10 CFR 50.55a (h) for IEEE Std. 603-1991 are Clause 5.6.3, "Independence between Safety Systems and Other Systems," and Clause 6.3, "Interaction between the Sense and Command Features and Other Systems."

DC-FSAR Sections 7.1 and 7.5.1.2, specify the use of the non-safety-related process information and control system (PICS) as the primary component of the accident monitoring system. DC-FSAR Table 7.1-2 identifies that 10 CFR 50.55a (h) is not applicable to PICS because it is non-safety-related.

**Response to Question 07.05-1:**

A response to this question will be provided by December 4, 2008.

**Question 07.05-2:**

Address the compliance to 10 CFR 50.34(f)(2)(xii), regarding auxiliary feedwater system flow indication for the accident monitoring instrumentation in accordance with the acceptance criteria of Section 7.5 of NUREG-0800.

Section 7.5.2.1.1 of the DC-FSAR indicates compliance. This section states, "Emergency feedwater flow to each steam generator (SG) is provided in the main control room." Which system does this requirement apply to (PICS or SICS)? Table 7.1-2 of the DC-FSAR indicates that the regulation does not apply to the process information and control system (PICS) the primary component of the accident monitoring system and is applicable to SICS.

**Response to Question 07.05-2:**

Because the safety information and control system (SICS) is the credited safety-related human system interface (HSI), compliance to 10 CFR 50.34(f)(2)(xii) to provide auxiliary feedwater system (emergency feedwater) flow indication in the main control room (MCR) applies to the SICS.

**FSAR Impact:**

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

**Question 07.05-3:**

Provide a complete list of post accident monitoring instrumentation with PAM variable type and ITAAC to verify variables meet the guidance of Regulatory Guide (RG) 1.97.

RG 1.97 and IEEE Std. 497-2002 require seismic qualification for Type A, B, C and D variables. Section 7.5.2.2.1 of the DC-FSAR describes a methodology for selecting the final list of accident monitoring variables in accordance with RG 1.97 instead of defining the variables. The staff requires this issue to be resolved in order to conclude that 10 CFR 50, Appendix A, GDC 2 requirements have been met.

**Response to Question 07.05-3:**

A response to this question will be provided by December 4, 2008.

**Question 07.05-4:**

Provide a complete list of post accident monitoring (PAM) instrumentation with PAM variable type and ITAAC to verify variables meet the guidance of Regulatory Guide 1.97.

Revision 4 of Regulatory Guide 1.97, accident monitoring equipment identified as Type A, B, or C in accordance with that guide should be environmentally qualified as required by 10 CFR 50.49. Type D variables should be environmentally qualified for the particular accident's postulated environment at the installed location in accordance with the plant's licensing basis. The staff requires this issue to be resolved in order to conclude that 10 CFR 50, Appendix A, GDC 4 requirements have been met.

**Response to Question 07.05-4:**

A response to this question will be provided by December 4, 2008.

**Question 07.05-5:**

Provide a complete list of post accident monitoring instrumentation with PAM variable type and ITAAC to verify variables in accordance with Revision 4 of Regulatory Guide 1.97, accident monitoring equipment and IEEE 497 Section 5, performance criteria.

Section 7.5.2.2.1 of the DC-FSAR describes a methodology for selecting the final list of accident monitoring variables instead of defining the variables.

**Response to Question 07.05-5:**

A response to this question will be provided by December 4, 2008.

**Question 07.05-6:**

Provide information to demonstrate how the design meets 10 CFR 50, Appendix A, General Design Criterion (GDC) 24, Separation of protection and control systems in accordance with the acceptance criteria of Section 7.5 of NUREG-0800 and IEEE 497-2002.

DC-FSAR Sections 7.1, 7.5.1.1, 7.5.1.2, 7.5.1.3 and 7.5.1.4 specify the use of the non-safety-related process information and control system (PICS) as the primary component of the accident monitoring system, bypass and inoperable status indication, annunciator system and the SPDS, ERF and ERDS information systems. DC-FSAR Table 7.1-2 identifies 10 CFR 50, Appendix A, GDC 24 as not applicable to PICS because it is non-safety-related. However, DC-FSAR Section 7.1.1.3.2 states that the PICS is used to control both safety-related and non-safety related process systems. The interface between non-safety-related and safety-related requires that independence and separation be addressed.

**Response to Question 07.05-6:**

A response to this question will be provided by December 4, 2008.

**Question 07.05-7:**

Which system PICS or SICS is the credited system for accident monitoring instrumentation?

DC FSAR, Tier 2 Sections 7.1 and 7.5.1.2, specify the use of the non-safety-related process information and control system (PICS) as the primary component of the accident monitoring system. The primary operator interface in the MCR for displaying all PAM variables is the non-safety-related PICS. If the PICS is not available, the safety-related SICS is used.

**Response to Question 07.05-7:**

The PICS is the primary component of the accident monitoring system. Because the PICS is not credited for performance of safety-related functions, the safety information and control system (SICS) is credited to provide control capabilities of safety-related accident monitoring variables. The SICS is a backup human machine interface (HMI) system to the PICS.

Upon completion of the emergency operating procedures (EOP), the post-accident monitoring (PAM) variables will be defined. Once the variables are defined, they will be allocated to either the PICS, the SICS, or both, depending on the performance, design, qualification, and display criteria in IEEE 497-2002 with the modifications specified in RG 1.97 and in accordance with BTP 7-10. Both the PICS and the SICS are used to meet accident monitoring instrumentation requirements.

**FSAR Impact:**

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

**Question 07.05-8:**

Which system PICS or SICS is the credited system for annunciator system? What are the limited backup annunciation functions of SICS?

DC-FSAR Sections 7.1 and 7.5.1.1, specify the use of the non-safety-related process information and control system (PICS) as the primary annunciator system. The safety information and control system (SICS) provides some limited backup annunciation functions if PICS is unavailable.

**Response to Question 07.05-8:**

The U.S. EPR has an alarm management system that is integrated with the PICS. It performs the alarming functions that are traditionally implemented on a conventional annunciator window system in current plants. If an annunciator is required to prompt the operator to perform a credited manual action, the annunciator will be implemented on the SICS. The U.S. EPR will provide a minimum inventory of fixed alarms, displays, and controls as documented in the U.S. EPR FSAR Tier 1, Section 3.4 and U.S. EPR FSAR Tier 2, Section 18.7. A minimum inventory is listed in U.S. EPR FSAR Tier 2, Table 18.7-1—Minimum Inventory of Main Control Room Fixed Alarms, Displays, and Controls.

The control and display human system interface (HSI) functions credited in the safety analyses of design basis events are represented. Credited functions are backed up on the SICS; however, they do not represent the complete inventory. Additional alarm functions on the SICS will be added to meet the functions defined in U.S. EPR FSAR Tier 2, Section 7.1.1.3.1.

**FSAR Impact:**

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

# U.S. EPR Final Safety Analysis Report Markups

In certain scenarios, non-safety-related systems perform shutdown functions. These functions are initiated in the process automation system (PAS). The priority and actuator control system (PACS) module is assigned to safety-related components associated with safe shutdown. The functions performed by PACS modules are described in Section 7.1.1.4.3.

The human machine interface (HMI) is the PICS. In case of unavailability of the PICS, functions needed to achieve and maintain a safe shutdown condition can be controlled through the SICS. Monitoring and control of the safety-related systems are both available in the main control room (MCR) and the remote shutdown station (RSS).

#### 7.4.1.2 Safe Shutdown Using Safety-Related Systems and Equipment

The plant is designed so that it can be taken from normal operating conditions to cold shutdown using only safety-related systems. The safety-related systems and equipment, that with proper alignment are capable of achieving a safe shutdown of the plant, are described in Section 7.4.1.2.1 through Section 7.4.1.2.13. These systems satisfy GDC 1, GDC 2, GDC 3, and GDC 4.

The systems and equipment described in Section 7.4.1.2.1 through Section 7.4.1.2.13 are capable of bringing the plant to a cold shutdown condition, with only offsite or onsite power available along with the most limiting single failure. The entire shutdown procedure is completed from the MCR.

##### 7.4.1.2.1 Emergency Feedwater System

The emergency feedwater system (EFWS) provides a safety-related means of supplying feedwater to the steam generators (SG) for decay heat removal. This system is capable of maintaining hot standby and facilitating a plant cooldown. The I&C associated with the EFWS, are described in Section 10.4.9.

##### 7.4.1.2.2 Main Steam Supply System

The main steam supply system (MSSS) contains the main steam relief train (MSRT). The MSRT provides secondary side pressure control capability. The MSRT valves are located outside of containment upstream of the main steam isolation valves (MSIV). These valves are used to remove decay heat via the SGs in the event the condenser is unavailable (including loss of power), and to dissipate the heat to atmosphere. The MSRT may be used to cool and depressurize the reactor coolant system (RCS) to conditions necessary to initiate residual heat removal. The MSSS contains the MSIVs and associated bypass valves that are necessary to isolate the secondary plant and to allow decay heat removal by the MSRT. The I&C associated with the MSSS are described in Section 10.3.