

ArevaEPRDCPEm Resource

From: Tesfaye, Getachew
Sent: Friday, May 28, 2010 5:46 PM
To: Cheung, Calvin; Mott, Kenneth; Zhang, Deanna; Spaulding, Deirdre; Jackson, Terry; Canova, Michael; Colaccino, Joseph; ArevaEPRDCPEm Resource
Subject: FW: DRAFT Response RAI 286
Attachments: RAI 286 Supplement 7 (Draft) Response US EPR DC.pdf

From: BRYAN Martin (EXT) [mailto:Martin.Bryan.ext@areva.com]
Sent: Friday, May 28, 2010 4:09 PM
To: Tesfaye, Getachew
Cc: GARDNER George Darrell (AREVA NP INC); PANNELL George L (AREVA NP INC); ROMINE Judy (AREVA NP INC)
Subject: DRAFT Response RAI 286

Getachew,

Earlier today I provided a revised date to complete the response for RAI 286 (June 30, 2010). Attached is the draft response for the staff review. Please let me know if there are questions or we need an interaction to discuss.

Thanks,

Martin (Marty) C. Bryan
U.S. EPR Design Certification Licensing Manager
AREVA NP Inc.
Tel: (434) 832-3016
702 561-3528 cell
Martin.Bryan.ext@areva.com

Hearing Identifier: AREVA_EPR_DC_RAIs
Email Number: 1482

Mail Envelope Properties (0A64B42AAA8FD4418CE1EB5240A6FED1134504C9E0)

Subject: FW: DRAFT Response RAI 286
Sent Date: 5/28/2010 5:45:47 PM
Received Date: 5/28/2010 5:45:48 PM
From: Tesfaye, Getachew

Created By: Getachew.Tesfaye@nrc.gov

Recipients:

"Cheung, Calvin" <Calvin.Cheung@nrc.gov>
Tracking Status: None
"Mott, Kenneth" <Kenneth.Mott@nrc.gov>
Tracking Status: None
"Zhang, Deanna" <Deanna.Zhang@nrc.gov>
Tracking Status: None
"Spaulding, Deirdre" <Deirdre.Spaulding@nrc.gov>
Tracking Status: None
"Jackson, Terry" <Terry.Jackson@nrc.gov>
Tracking Status: None
"Canova, Michael" <Michael.Canova@nrc.gov>
Tracking Status: None
"Colaccino, Joseph" <Joseph.Colaccino@nrc.gov>
Tracking Status: None
"ArevaEPRDCPEm Resource" <ArevaEPRDCPEm.Resource@nrc.gov>
Tracking Status: None

Post Office: HQCLSTR02.nrc.gov

Files	Size	Date & Time
MESSAGE	754	5/28/2010 5:45:48 PM
RAI 286 Supplement 7 (Draft) Response US EPR DC.pdf		363337

Options

Priority: Standard
Return Notification: No
Reply Requested: No
Sensitivity: Normal
Expiration Date:
Recipients Received:

Response to

**Request for Additional Information No. 286, Supplement 7 (3567, 3561, 3562,
3563), Revision 1**

10/14/2009

U. S. EPR Standard Design Certification

AREVA NP Inc.

Docket No. 52-020

SRP Section: 07.06 - Interlock Systems Important to Safety

SRP Section: 07.07 - Control Systems

SRP Section: 07.08 - Diverse Instrumentation and Control Systems

SRP Section: 07.09 - Data Communication Systems

Application Section: FSAR Ch. 7

QUESTIONS for Instrumentation, Controls and Electrical Engineering 1

(AP1000/EPR Projects) (ICE1)

Question 07.08-9:

Follow-up to RAI Question No. 07.08-4

Further justify why the Process Information and Control System (PICS) does not need to meet 10 CFR Part 50, Appendix A, General Design Criteria (GDC) 1.

GDC 1 requires, in part, that structures, systems and components important to safety shall be design, fabricated, erected, and tested to quality standards commensurate with the importance of the safety functions to be performed. The staff identified throughout Chapter 7 of the U.S. EPR DC-FSAR that PICS is the system that the operators will normally use to monitor and control plant safety systems during all conditions of plant operation, "including normal operation, anticipated operational occurrences, postulated accidents, and beyond design basis events. Additionally, PICS provides functions that address the requirements of GDC 13 and 19 (e.g., post-accident monitoring), as well as diverse actuation functions provided there is a software common-cause failure. As such, the staff sees that PICS is an important to safety system and is required to meet GDC1. The staff requests that information be provided as to the quality standards that PICS will designed and tested. As one example, if PICS is credited for diverse actuation, AREVA NP should address the applicability of Generic Letter 85-06 and its enclosure as one potential standard/guidance. AREVA NP should also describe compliance to GDC 1 for systems that support PICS and enable its proper operation, such as the plant data network.

Response to Question 07.08-9:

As stated in the Response to RAI 75, Supplement 4, Question 07.08-04, the PICS is designed in accordance with a quality assurance program (QAP) that satisfies GL 85-06. U.S. EPR FSAR Tier 2, Section 7.1 will be revised to clarify this commitment to GL 85-06 for the PICS.

The PICS is the primary operator interface used in the plant conditions for the duration of its availability. This approach allows the operator to use the same human machine interface (HMI) interface to operate the plant equipment required to complete a task, regardless of the safety-related classification of individual functions performed or equipment operated. This method benefits plant safety because the probability for human errors resulting from continuous transitions between different operator interfaces is minimized. The PICS is not credited to perform any safety-related functions in the U.S. EPR FSAR Tier 2, Chapter 15 safety analysis for the U.S. EPR. Manual indications and controls needed to bring the plant to a safe shutdown following an event are available on the safety-related safety information and control system (SICS) if the PICS is not available.

Given AREVA NP's design approach for the PICS and understanding of the importance of the PICS system to overall plant operation, application of the additional quality requirements described in this response is appropriate and sufficient for this non-safety-related system.

Topical Report ANP-10266A describes the QAP for the U.S. EPR. Topical Report ANP-10266A, Addendum A defines the QAP for the non-safety-related U.S. EPR systems. This addendum addresses the eighteen topics contained in the enclosure to GL 85-06. The PICS, the plant data network, and the other non-safety-related instrumentation and controls (I&C) systems are designed under a QAP that satisfies GL 85-06.

In addition to the measures outlined in GL 85-06 and Topical Report ANP-10266A, Addendum A, other quality requirements are applied to the design of the PICS. These additional requirements reflect the importance of the PICS as the primary operator interface:

- The design of the PICS is accomplished through a phased approach, including the following (or equivalent) phases:
 - System requirements phase.
 - System design phase.
 - Software/hardware requirements phase.
 - Software/hardware design phase.
 - Software/hardware implementation phase.
 - Software/hardware validation phase.
 - System integration phase.
 - System validation phase.
- A criticality analysis is performed for the PICS software in accordance with accepted industrial practice.
- Verification and validation (V&V) of the PICS software is performed according to a V&V plan that is consistent with accepted industrial practice.
- The PICS requirements are documented in a traceable form that is under configuration management.
- The PICS design is validated through acceptance tests in the system validation (or equivalent) phase.

U.S. EPR FSAR Tier 2, Section 7.1 will be revised to reflect these requirements.

U.S. EPR FSAR Tier 1, Section 2.4.10 will be revised to include the PICS design phases.

In addition to quality assurance measures taken during the design of the PICS, AREVA NP recognizes how verifying correct functioning of the PICS on a periodic basis during plant operation is important to system quality. The Response to RAI 285, Supplement 3, Question 07.04-13 and its associated U.S. EPR FSAR markups describe the means for verifying correct functioning of the PICS during plant operation.

As described in the Response to RAI 56, Supplement 1, Question 07.09-30, the PICS employs redundancy for fault tolerance and is designed to industrial EMI/RFI standards.

FSAR Impact:

U.S. EPR FSAR Tier 1, Section 2.4.10 and U.S. EPR FSAR Tier 2, Section 7.1 will be revised as described in the response and indicated on the enclosed markup.

U.S. EPR Final Safety Analysis Report Markups

Draft

2.4.10 Process Information and Control System

1.0 Description

The process information and control system (PICS) is a digital human machine interface (HMI). It provides monitoring and control of plant systems. The PICS is non-~~safety~~ safety-related and is provided in both the main control room (MCR) and the remote shutdown station (RSS).

2.0 I&C Design Features

2.1 The system hardware and software in the PICS is diverse from the safety-related system hardware and software in the Safety Information and Control System (SICS).

2.2 The PICS system design is accomplished through a phased approach which includes the following (or equivalent) phases:

1. System Requirements Phase.
2. System Design Phase.
3. Software/Hardware Requirements Phase.
4. Software/Hardware Design Phase.
5. Software/Hardware Implementation Phase.
6. Software/Hardware Validation Phase.
7. System Integration Phase.
8. System Validation Phase.

~~2.2 Deleted.~~

↑
07.08-9

2.3 Deleted.

2.4 Electrical isolation is provided on PICS connections between the RSS and the MCR ~~for the PICS.~~

2.5 The capability to transfer control of the PICS from the MCR to the RSS exists in a fire area separate from the MCR and allows transfer of control without entry into the MCR.

3.0 System Inspections, Tests, Analyses, and Acceptance Criteria

Table 2.4.10-~~1~~2 lists the PICS ITAAC.

**Table 2.4.10-1—Process Information and Control System
ITAAC (3 Sheets)**

	Commitment Wording	Inspections, Tests, Analyses	Acceptance Criteria
2.1	The system hardware and software in the PICS is diverse from the safety-related system hardware and software in the SICS.	An analysis will be performed to demonstrate that the system hardware and software in the PICS is diverse from the safety-related system hardware and software in the SICS.	A report exists and concludes that the system hardware and software in the PICS is diverse from the safety-related system hardware and software in the SICS.
2.2	<p><u>The PICS system design is accomplished through a phased approach which includes the following (or equivalent) phases:</u></p> <ol style="list-style-type: none"> <u>1) System Requirements Phase.</u> <u>2) System Design Phase.</u> <u>3) Software/Hardware Requirements Phase.</u> <u>4) Software/Hardware Design Phase.</u> <u>5) Software/Hardware Implementation Phase.</u> <u>6) Software/Hardware Validation Phase.</u> <u>7) System Integration Phase.</u> <u>8) System Validation Phase.</u> Deleted. 	<p><u>a. Analyses will be performed to verify that the outputs for the PICS system requirements phase conform to the requirements of that phase.</u> {}DAC{} Deleted.</p> <p><u>b. Analyses will be performed to verify that the outputs for the PICS system design phase conform to the requirements of that phase.</u> {}DAC{} Deleted.</p> <p><u>c. Analyses will be performed to verify that the outputs for the PICS software/hardware requirements phase conform to the requirements of that phase.</u> {}DAC{} Deleted.</p> <p><u>d. Analyses will be performed to verify that the outputs for the PICS software/hardware design phase conform to the requirements of that phase.</u> {}DAC{} Deleted.</p> <p><u>e. Analyses will be performed to verify that the outputs for the PICS software/hardware implementation phase conform to the requirements of that phase.</u> {}DAC{} Deleted.</p>	<p><u>a. A report exists and concludes that the outputs for the PICS system requirements phase conform to the requirements of that phase.</u> {}DAC{} Deleted.</p> <p><u>b. A report exists and concludes that the outputs for the PICS system design phase conform to the requirements of that phase.</u> {}DAC{} Deleted.</p> <p><u>c. A report exists and concludes that the outputs for the PICS software/hardware requirements phase conform to the requirements of that phase.</u> {}DAC{} Deleted.</p> <p><u>d. A report exists and concludes that the outputs for the PICS software/hardware design phase conform to the requirements of that phase.</u> {}DAC{} Deleted.</p> <p><u>e. A report exists and concludes that the outputs for the PICS software/hardware implementation phase conform to the requirements of that phase.</u> {}DAC{} Deleted.</p>

↑
07.08-9

Table 2.4.10-1—Process Information and Control System
ITAAC (3 Sheets)

	Commitment Wording	Inspections, Tests, Analyses	Acceptance Criteria
		<p><u>f. Analyses will be performed to verify that the outputs for the PICS software/hardware validation phase conform to the requirements of that phase.</u></p> <p><u>g. Analyses will be performed to verify that the outputs for the PICS system integration phase conform to the requirements of that phase.</u></p> <p><u>h. Analyses will be performed to verify that the outputs for the PICS system validation phase conform to the requirements of that phase.</u></p>	<p><u>f. A report exists and concludes that the outputs for the PICS software/hardware validation phase conform to the requirements of that phase.</u></p> <p><u>g. A report exists and concludes that the outputs for the PICS system integration phase conform to the requirements of that phase.</u></p> <p><u>h. A report exists and concludes that the outputs for the PICS system validation phase conform to the requirements of that phase.</u></p>
2.3	Deleted.	Deleted.	Deleted.
2.4	<p>Electrical Isolation-isolation is provided <u>on PICS connections</u> between the RSS and the MCR for the PICS.</p>	<p><u>a. Analyses will be performed to determine the test specification for electrical isolation devices on connections between the RSS and the MCR for the PICS.</u></p> <p><u>b. Type tests, analyses, or a combination of type tests and analyses will be performed on the electrical isolation devices between the RSS and the MCR for the PICS.</u></p>	<p><u>a. A test plan exists that provides the test specification for determining whether a device is capable of preventing the propagation of credible electrical faults on connections between the RSS and the MCR for the PICS.</u></p> <p><u>b. A report exists and concludes that the isolation devices used between the RSS and the MCR for the PICS prevent the propagation of credible electrical faults.</u></p>

07.08-9

This section describes the PICS with regards to I&C design. Details such as screen displays, levels of automation, and panel layout are designed using the HFE principles described in Chapter 18.

Classification

The PICS is classified as non-safety-related, augmented quality. ← 07.08-9

Functions

The PICS performs these functions:

- Monitoring and control of process systems during normal operation, including startup, power, and shutdown operation.
- Monitor the status of the automatic reactor trip and ESF systems during abnormal events, including anticipated operational occurrences (AOO) ~~and~~, postulated accidents, and special events.
- Manual reset of automatic reactor trip and ESF actuation functions.
- Non-credited means to monitor and control systems required to achieve and maintain safe shutdown.
- Manual component level control of safety-related process systems via the process automation system (PAS) and priority and actuator control system (PACS) ~~diverse from the TXS-based safety systems~~.
- Manual actuation of critical safety functions via the DAS or PAS.
- Primary SPDS functions.
- Display of Type A-E PAM variables.
- Monitoring and control of systems required to mitigate severe accidents.
- Display bypassed and inoperable status of safety systems.
- Alarm management.
- Data archival.
- Interface to external I&C computers.
- Interface to external computers via a unidirectional firewall.

Architecture

Figure 7.1-5—Process Information and Control System Architecture provides a functional representation of the PICS.

of large panels that display an overview of plant and system status. Equipment such as network switches and electrical and fiber optic cable are provided to support data communications.

The plant annunciator is integrated into the PICS operating and monitoring system. Special screens display and organize alarms and warnings based on their status and relative level of importance. An alarm hierarchy with a color coding system is used to immediately alert the operator of the importance of the alarm based on the relevance to plant safety.

The PICS is used to control both safety-related and non-safety-related process systems. The PICS implements these measures to preclude spurious actuation of plant equipment:

- Operation of plant equipment is performed using a two-step process. A single mouse click on a component is followed by a verification step requiring a second single mouse click, so a single inadvertent action by the operator does not result in a command signal.
- Touch screen displays are not used.

Qualification Requirements

In the unlikely event of a software common cause failure of the PS, the PICS equipment must function properly under conditions during and following design basis events. The PICS equipment is located in Safeguard Buildings that provide a mild environment during and following design basis events. Equipment selected for use in the PICS will be rated by the manufacturer (or otherwise reasonably expected) to operate under the mild environmental conditions expected to exist at its location during the events that the equipment is expected to be used. ~~There are no qualification requirements for the PICS equipment.~~

07.08-9 →

Quality Requirements

In its role as the primary operator interface, and as a system relied on to mitigate the effects of CCF of the PS, the PICS is required to be of sufficient quality to perform its functions in a reliable manner. The PICS is designed using a robust engineering process with appropriate reviews, verifications, tests, and approvals. Sufficient quality is achieved in the design of the PICS through the following measures:

- The PICS is designed, fabricated, erected, and tested under the quality assurance program described in Topical Report ANP-1066A, Addendum A (Reference 45). This quality assurance program is consistent with the guidance of Generic Letter 85-06 (Reference 46).
- The design of the PICS is accomplished through a phased approach, including the following (or equivalent) phases:

07.08-9 →

- System requirements phase.
- System design phase.
- Software/hardware requirements phase.
- Software/hardware design phase.
- Software/hardware implementation phase.
- Software/hardware validation phase.
- System integration phase.
- System validation phase.
- A criticality analysis is performed for the PICS software in accordance with accepted industrial practice.
- Verification and validation (V&V) of the PICS software is performed according to a V&V plan that is consistent with accepted industrial practice.
- PICS requirements are documented in a traceable form that is under configuration management.
- The PICS design is validated through acceptance test in the system validation (or equivalent) phase. ~~There are no quality requirements for the PICS equipment.~~

Diversity Requirements

The PICS is credited by the defense-in-depth and diversity analysis described in ~~Section 7.8.2~~ Section 7.8. ~~These diversity requirements are established~~ Diversity requirements for the PICS are identified in Reference 8:

- ~~The system hardware in the PICS is diverse from the TXS system hardware.~~
- ~~The system software in the PICS is diverse from the TXS system software.~~
- The PICS displays are diverse from the SICS displays (QDS).

Data Communications

The PUs transmit data to and receive data from the Level 1 I&C systems via the plant data network. The PUs, operator workstations, POP, and XUs exchange data via the terminal data network. These networks implement periodic communications and message validation for robust data communications. Remote access of the PICS is not possible.

7.1.1.4.7

Diverse Actuation System (DAS)

The DAS is the non-safety-related I&C system that provides diverse actuation of protective functions in the unlikely event of an ATWS or a software common cause failure of the PS.

Classification

The DAS is classified as non-safety related, augmented quality. ← 07.08-9

Functions

The DAS performs automatic risk-reduction functions, including:

- Mitigation of ATWS and PS software common cause failure.
- Manual, system-level actuation of critical safety functions.
- Mitigation of SBO.
- Mitigation of other risk significant events.

Architecture

Figure 7.1-13 – Diverse Actuation System Architecture provides a functional representation of the DAS.

The DAS is organized into four redundant divisions located in separate Safeguards Buildings. Each division of the DAS contains a diverse actuation unit (DAU). Hardwired signals are acquired from the PS, as described in Section 7.1.1.6.4, and compared to a setpoint. Fiber optic data connections are provided to share trip requests, and two-out-of-four voting is done in each DAU. Outputs are sent to the PACS via hardwired connections.

The DAUs interface with the PICS via the plant data network to display information.

Equipment

The DAS is implemented with an industrial digital I&C platform.

The DAS generally consists of subracks, I/O modules, function processors, communication modules, and link modules. Fiber optic and copper cable is used for the various data and hardwired connections. Specialized components may be used.

Qualification Requirements

In the unlikely event of a software common cause failure of the PS, the DAS equipment must function properly under conditions during and following design basis

events. The DAS equipment is located in Safeguard Buildings that provide a mild environment during and following design basis events. Equipment selected for use in the DAS shall be rated by the manufacturer (or otherwise reasonably expected) to operate under the mild environmental conditions expected to exist at its location during the events for which the equipment is expected to respond.

07.08-9

Quality Requirements

As a system relied on to mitigate the effects of CCF of the PS, the DAS is required to be of sufficient quality to perform its functions in a reliable manner. The DAS is therefore designed using a robust engineering process with appropriate reviews, verification, tests, and approvals. Sufficient quality is achieved in the design of the DAS through the following measures:

07.08-9 →

- The DAS is designed, fabricated, erected, and tested under the quality assurance program described in Topical Report ANP-1066A, Addendum A (Reference 45). This quality assurance program is consistent with the guidance of Generic Letter 85-06 (Reference 46).
- The design of the DAS is accomplished through a phased approach including the following (or equivalent) phases:
 - System requirements phase.
 - System design phase.
 - Software/hardware requirements phase.
 - Software/hardware design phase.
 - Software/hardware implementation phase.
 - Software/hardware validation phase.
 - System integration phase.
 - System validation phase.
- A criticality analysis is performed for the DAS software in accordance with accepted industrial practice.
- Verification and validation (V&V) of the DAS software is performed according to a V&V plan that is consistent with accepted industrial practice.
- DAS requirements are documented in a traceable form that is under configuration management.
- The DAS design is validated through acceptance test in the system validation (or equivalent) phase.

07.08-9 →

07.08-9 →

45. [ANP-10266A, Revision 1, "AREVA NP Inc. Quality Assurance Plan \(QAP\) for Design Certification of the U.S. EPR Topical Report."](#) AREVA NP Inc., April 2007.
46. [Generic Letter 85-06, "Quality Assurance Guidance for ATWS Equipment that is Not Safety-Related,"](#) U.S. Nuclear Regulatory Commission, April 16, 1985.

Draft