## ArevaEPRDCPEm Resource

**From:** WILLIFORD Dennis (AREVA) [Dennis.Williford@areva.com]
**Sent:** Monday, September 24, 2012 2:52 PM
**To:** Tesfaye, Getachew
**Cc:** BENNETT Kathy (AREVA); DELANO Karen (AREVA); LEIGHLITER John (AREVA); ROMINE Judy (AREVA); RYAN Tom (AREVA)
**Subject:** Response to U.S. EPR Design Certification Application RAI No. 555 (6611), FSAR Ch. 7
**Attachments:** RAI 555 Response US EPR DC.pdf

Getachew,

Attached please find AREVA NP Inc.'s response to the subject request for additional information (RAI). The attached file, "RAI 555 Response US EPR DC.pdf," provides a schedule since a technically correct and complete response to the three questions cannot be provided at this time.

The following table indicates the respective pages in the response document, "RAI 553 Response US EPR DC.pdf," that contain AREVA NP's response to the subject questions.

| Question # | Start Page | End Page |
|---|---|---|
| RAI 555 — 07.01-53 | 2 | 3 |
| RAI 555 — 07.01-54 | 4 | 6 |
| RAI 555 — 07.01-55 | 7 | 9 |

The schedule for technically correct and complete responses to Questions 07.01-54 and 07.01-55 is provided below. A preliminary schedule for the response to Question 07.01-53 is also provided below. The schedule for the response to Question 07.01-53 is being reevaluated and a new supplement with a revised schedule will be transmitted by November 15, 2012.

| Question # | Response Date |
|---|---|
| RAI 555 — 07.01-53 | **November 15, 2012** |
| RAI 555 — 07.01-54 | **February 21, 2013** |
| RAI 555 — 07.01-55 | **February 21, 2013** |

Sincerely,

***Dennis Williford, P.E.***
***U.S. EPR Design Certification Licensing Manager***
**AREVA NP Inc.**
7207 IBM Drive, Mail Code CLT 2B
Charlotte, NC 28262
Phone: 704-805-2223
Email: Dennis.Williford@areva.com

**From:** Tesfaye, Getachew [mailto:Getachew.Tesfaye@nrc.gov]
**Sent:** Friday, August 24, 2012 3:01 PM

**To:** ZZ-DL-A-USEPR-DL
**Cc:** Morton, Wendell; Zhang, Deanna; Spaulding, Deirdre; Mott, Kenneth; Truong, Tung; Zhao, Jack; Mills, Daniel; Jackson, Terry; Canova, Michael; Segala, John; ArevaEPRDCPEm Resource
**Subject:** U.S. EPR Design Certification Application RAI No. 555 (6611), FSAR Ch. 7

Attached please find the subject request for additional information (RAI). A draft of the RAI was provided to you on August 15, 2012, and on August 24, 2012, you informed us that the RAI is clear and no further clarification is needed. As a result, no change is made to the draft RAI. The schedule we have established for review of your application assumes technically correct and complete responses within 30 days of receipt of RAIs. For any RAIs that cannot be answered within 30 days, it is expected that a date for receipt of this information will be provided to the staff within the 30 day period so that the staff can assess how this information will impact the published schedule.

Thanks,
Getachew Tesfaye
Sr. Project Manager
NRO/DNRL/LB1
(301) 415-3361

**Hearing Identifier:** AREVA_EPR_DC_RAIs
**Email Number:** 4050

**Mail Envelope Properties** (2FBE1051AEB2E748A0F98DF9EEE5A5D4E30CEC)

**Subject:** Response to U.S. EPR Design Certification Application RAI No. 555 (6611), FSAR Ch. 7
**Sent Date:** 9/24/2012 2:52:24 PM
**Received Date:** 9/24/2012 2:52:28 PM
**From:** WILLIFORD Dennis (AREVA)

**Created By:** Dennis.Williford@areva.com

**Recipients:**
"BENNETT Kathy (AREVA)" <Kathy.Bennett@areva.com>
Tracking Status: None
"DELANO Karen (AREVA)" <Karen.Delano@areva.com>
Tracking Status: None
"LEIGHLITER John (AREVA)" <John.Leighliter@areva.com>
Tracking Status: None
"ROMINE Judy (AREVA)" <Judy.Romine@areva.com>
Tracking Status: None
"RYAN Tom (AREVA)" <Tom.Ryan@areva.com>
Tracking Status: None
"Tesfaye, Getachew" <Getachew.Tesfaye@nrc.gov>
Tracking Status: None

**Post Office:** auscharmx02.adom.ad.corp

| **Files** | **Size** | **Date & Time** |
|---|---|---|
| MESSAGE | 2690 | 9/24/2012 2:52:28 PM |
| RAI 555 Response US EPR DC.pdf | 83206 | |

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

**Response to**

**Request for Additional Information 555 (6611), Revision 0**

**8/24/2012**

**U. S. EPR Standard Design Certification**
**AREVA NP Inc.**
**Docket No. 52-020**
**Review Section: 07.01-A Appendix - Acceptance Criteria and Guidelines for Instrumentation and Control Systems Important to Safety**
**Application Section: 7.1**

**Question 07.01-53:**

**Open Item**

**Follow up to RAI 505, Question 07.01-48**

The staff requests the applicant provide additional information on how the U.S. EPR Design takes into account and bounds the effects of potential failure(s) of the Process Automation System (PAS) and Process Information and Control Systems (PICS) on safety-related components and systems. This question is a follow-on question based on technical information presented to the staff within the applicant's response to RAI 505, Question 07.01-48.

IEEE Std. 603-1991, Clause 5.6.3.1(2), “Isolation”, as endorsed by 10 CFR 50.55a(h),states in part, that no credible failure on the non-safety side of an isolation device shall prevent any portion of a safety system from meeting its minimum performance requirements during and following any design basis event requiring that safety function. According to U.S. EPR FSAR, Tier 2, Section 7.1, Revision 3, PAS and PICS are non-safety related systems. The PAS provides controls for both safety-related and non-safety-related equipment. The Process Information and Control System (PICS), by means of computer network connections through PAS, can provide manual, component-level and grouped control of safety-related equipment, according to FSAR Tier 2, Table 7.1-3, Sheet 1 of 2. Therefore, failures of PAS and PICS can directly affect safety-related components. U.S. EPR FSAR, Tier 2, Section 15.0.0.3.8 discusses single failures that have been incorporated into the Accident Analysis. Table 15.0-11 provides a listing of the most limiting single failure for each design basis event in the Accident Analysis. Based upon the above information and the information contained in the FSAR, it appears that PAS could fail in such a way that its failure could:

1. Potentially cause a system perturbation for which the Protection System (PS) and other safety systems may have to mitigate.

2. Potentially inhibit the ability of the PS and other safety systems to meet their performance requiremetns, such as those required by Clause 4 of IEEE Std. 603-1991 (Design Bases). In particular, Sub-clause 4.10 establishes the requirement for response times of the safety system. A failure(s) of PAS calls into question whether the stated response times in FSAR Table 15.0-8 for the Engineered Safety Features Acutation System (ESFAS) are adequate to protect the plant and ensure design basis limits are not exceeded in the presence of a failure of PAS or a failure of PAS concurrent with a design basis event.Potentially inhibit the ability of the PS and other safety systems to meet their performance requirements, such as those required by Clause 4 of IEEE Std. 603-1991 (Design Bases). In particular, Sub-clause 4.10 establishes the requirement for response times of the safety system. A failure of PAS calls into question whether the stated response times in FSAR Table 15.0-8 for the Engineered Safety Features Actuation System (ESFAS) are adequate to protect the plant and ensure design basis limits are not exceeded in the presence of a failure of PAS or a failure of PAS concurrent with a design basis event.

3. Exceed the bounds of the analyzed events documented in FSAR Table 15.0-11. For example, if a failure of PAS or PICS occurs, the failure could happen in such a way that it affects all four divisions of a safety-related component and not just a single division as captured in Table 15.0-11.

As identified in Clause 5.6.3.1(2) of IEEE Std. 603-1991 above, credible failures of non-safety systems must not prevent any portion of a safety system from meeting its minimum performance requirements. The staff considers a software failure of the non-safety related PAS and PICS to be a credible failure that could potentially impact multiple safety divisions. For example, in FSAR Section 15.1.4.1, the applicant postulates, the inadvertent opening of a single Main Steam Relief Train Isolation Valve (MSRIV), concurrent with a single failure of the associated MSRCV failing open. This AOO only pertains to a single affected Steam Generator (SG). The applicant considers the single failure of the MSRCV as the most severe single failure. The analysis in FSAR Section 15.1.4.1 does not appear to be comprehensive for the full scope of possible PAS failures considering that a software error in PAS could potentially cause the inadvertent opening of a MSRIV concurrent with a failure of the MSRCV in all four SGs at the same time. It is not clear from the analysis that the plant would be adequately protected from this type of failure, or why a PAS failure of this type and magnitude is not credible. The staff has similar concerns with the other non-safety-related control system failures in the safety analysis as well.

The staff cannot determine through a review of available design documentation that a failure of PAS would not adversely impact the performance of safety-related components and safety systems such as PS or the Safety Automation System (SAS). Based upon teleconferences with the applicant and the applicant's response to RAI 505, Question 07.01-46, it is clear that the applicant has considered the effects of a PAS/PICS failure on safety-related components and/or trains of components. With Revision 3 of the FSAR, the applicant introduced the Operational I&C Disable Switch (OICS). The OICS is located on the Safety Information and Control System (SICS). The design function of the OICS is to ensure that, when the OICS is enabled, manual commands from the SICS are not overridden by automatic commands from PAS by disabling automatic commands from PAS at the priority module. In subsequent teleconferences with the applicant, the staff learned that the additional design function of the OICS is to preclude any negative system effects as a result of PAS/PICS failures. The OICS addresses PAS failures from a controls standpoint, but the applicant doesn't appear to fully evaluate the full scope of PAS failures and how they would impact the accident analysis; particularly with regards to safety I&C system performance.

The staff requests the applicant to address the following questions:

a. Demonstrate how the plant would be adequately protected from each PAS failure, including software and hardware failures that could prevent or delay the safety function in multiple safety divisions. Are the safety functions and their corresponding response times in FSAR Table 15.0-8 sufficient to protect the plant if a PICS/PAS failure occurs, and is the PS capable of mitigating a Design Basis Event (DBE) concurrent with a PICS/PAS failure?
b. If the applicant does not consider certain failures of PICS/PAS to be credible, provide justification on why those specific failures are not credible.

**Response to Question 07.01-53:**

A response to this question will be provided by November 15, 2012.

**Question 07.01-54:**

**Open Item**

**Follow up to RAI 505, Question 07.01-46**

The staff requests the applicant to provide an analysis of the priority logic scheme for the U.S. EPR instrumentation and control (I&C) systems in order to verify the absence of potential conflicts between various I&C systems such as PS, SICS, SAS, PAS, and DAS that have the capability to control safety-related plant equipment. The staff is interested in how the priority logic scheme in conjunction with the duration and timing of activation/de-activation signals from I&C systems (that in some cases operate independently) would not prevent the safety function from continuing to completion during various operating scenarios. This RAI was created as a follow-up question to new design information provide to the staff within the applicant's response to RAI 505, Question 07.01-46 as well as other new design information provided to the staff in Phase 4 of the U.S. EPR design certification review.

IEEE Std. 603, Clause 5.2, "Completion of Protective Action". Clause 5.2 states, in part, that the safety systems shall be designed so that, once initiated automatically or manually, the intended sequence of protective actions of the execute features shall continue until completion. Technical Report ANP-10310P, "Methodology for 100% Combinatorial Testing of the U.S. EPR Priority Module Technical Report" Revision 1, defines a latched actuation signal as a priority module input that functions as follows. Following an actuation input signal transition from a valid logic "1" to a valid logic "0", the logic "1" continues to be used in processing (i.e., it is latched). When a different (pre-designated) actuation input signal (e.g., an actuation signal in counter-direction) transitions from a valid logic "0" value to a valid logic "1", the latched value returns to a logic "0" for use in processing. Technical Report ANP-10310P also defines a non-latched actuation signal as a priority module input whose logic value present as a valid input is the value used in processing. Section 5.2 of Technical Report ANP-10309P, "U.S. EPR Protection System Technical Report", Revision 4, states that, "The ALU also contains the logic used to latch and either manually or automatically un-latch actuation outputs." Section 8.1, "ENGINEERED SAFETY FEATURES ACTUATION" of Technical Report ANP-10309P, states, in part, that one of the activities performed in the ALU layer is signal latching. This section goes on to state that, "the actuation signal is latched via set-reset function block in the ALU to confirm completion of the function." The following are observations regarding the two technical reports:

1. Technical Report ANP-10309P does not clearly define the terms "latch" and "unlatch" with regards to system. Specifically, this section does not state whether the ALU is the only device in the U.S. EPR design that has the capability to latch or unlatch an output signal. In other words it is not known whether SAS, DAS, PAS, or SICS can also latch or unlatch a signal at the PACS module. Also, the definition of latched and unlatched does not appear to take into account the safety classification of the signal's originating system. Therefore, it is unknown if a system such as PAS or DAS can unlatch or latch a signal from a safety-related system.
2. It is not clear how a latched actuation signal adequately confirms completion of the function, as opposed to using feedback or checkback signals from the PACS modules that would demonstrate component operation has been completed.

3. Section 8.1 of Technical Report ANP-10309P also does not provide details on how an ALU can “manually” unlatch a signal, nor does it state the conditions, reasoning, and criteria that would make it acceptable to automatically unlatch an actuation output.
4. From the definitions in Technical Report ANP-10310P of latched and unlatched signals, there’s no clear delineation of how signal priority can be achieved. In terms of latched signals, there does not seem to be a limitation placed on what I&C system can initiate a logic transition, or ‘unlatch’ an actuation signal. The only criteria necessary is that an actuation signal in a counter direction be present. Overall, it is not clear whether these definitions are generically applicable to all interfacing I&C systems.
5. It is not clear how the definitions in Technical Report ANP-10310P correspond to how these signals are used in PS operation in Technical Report ANP-10309P.

Additional examples that demonstrate the need to clarify the priority logic scheme include the following. Section 7.3.1.2.2 of U.S. EPR FSAR Tier 2, Section 7.3.1.2.2, Revision 3, “Emergency Feedwater System Actuation [EFW]”, states that, “When EFW actuation occurs due to LOOP and SIS actuation, the PS sends a pulse of limited duration to start the actuation. The duration of the pulse is long enough for the intended actions of the execute features to go to completion.” The description of this signal described for EFW completion of action in Section 7.3.1.2.2 does not appear to be consistent with how Technical Report ANP-10309P describes how a latched signal is used to determined completion of the function. Furthermore, the staff is not clear as to how the EFW system will respond if a non-PS I&C system sends a signal to start or stop outside the PS pulse of limited duration. In U.S. EPR FSAR, Tier 2, Section 7.1.1.6.5, “Priority”, the applicant provides an outline of how signals from various safety and non-safety related systems are prioritized at the PACS module. This section states, in part, that the U.S. EPR I&C design allows for multiple systems to send request to a given actuator, in case of competing signals. However, the staff requires more clarification on how the priority logic interprets non-competing signals from different I&C systems, both safety and non-safety related. For example, based on the OICS, the staff understands that, under normal operating conditions PAS automatic signals have higher priority at PACS modules than SICS manual signals. This section does not explicitly state that the PACS module maintains or somehow retains the priority of signals it receives. The section also does not state how the prioritization is performed nor does the section provide any detail on how latched, unlatched, delayed, limited duration, or any other types of signals are used at the PACS modules in order to ensure priority. In terms of signals that have an associated time delay or duration, this section does not state how safety functions that utilize those types of signals have ensured priority and do not lose priority if the signal expires. Finally, it is not clear how safety functions that require sequencing of actions could not be interrupted. For instance, if a loss-of-offsite power event requires load shedding and re-sequencing of loads to the safety-related electrical bus, could systems such as DAS and PAS potentially impact the sequencing of equipment since they operate independent of the PS?

The staff request the applicant to address the following items in order to clarify the prioritization scheme for the U.S. EPR:

a. Provide an analysis that demonstrates the capability of the prioritization scheme to adequately address potential operating scenarios for each safety-related plant component that can be operated by multiple I&C systems. Identify the priority

scheme for each plant component and describe how the scheme can address potential operating scenarios such as concurrent and conflicting signals, non-concurrent signals (signals received at different times), and signals received during a coordinated sequence of actions.

b. Clarify the definition of the terms “latched” and “unlatched” in the U.S. EPR Design. In addition:

   b-1. Identify what devices in each I&C system latches and unlatches signals to the PACS modules and describe the reason for the latching/unlatching and how this is performed.

   b-2. Clarify how the priority scheme of the PACS module prevents a system of lower priority from latching or latching a signal from a system of a higher priority. For example, based upon the current definitions of latched and unlatched signals in Technical Report ANP-10310P, how is the DAS prevented from latching or unlatching a signal from the PS for a given actuator?

   b-3. Based upon the above reference to Technical Report ANP-10309P, Section 8.1, clarify how a latched signal for the ESF function confirms a completion of protective function.

   b-4. Clarify how check-back signals, as documented in Technical Report ANP-10310P, Section 2.0, are utilized by each I&C safety system for which they apply to.

   b-5 Clarify how an ALU can “manually” unlatch a signal. Also provide the criteria for when an ALU would automatically latch or unlatch a signal.

c. Identify all safety functions that utilize pulse signals of limited duration. Provide a technical basis on why those functions use limited duration signals as opposed to a latched signal and justify why the use of limited duration signals is an acceptable means to verify completion of protective action.

d. Document all the specific system functions and applications for which delayed actuation signals are used. Provide a technical basis for why they are used in each instance. In addition:

   d-1. Are there differences in the amount of delay for various delayed actuation signals? If so, why and provide clarifying details.

   d-2. Is the PS, SAS, etc. responsible for attaching a time delay for these signals or are these signals all have a pre-defined time delay?

   d-3. How would a failure of this type of signal manifest itself? Provide details on how would its failure affect system functions or performance?

e. Is signal latching/unlatching for safety systems verified through periodic maintenance? If so, how is this done?

**Response to Question 07.01-54:**

A response to this question will be provided by February 21, 2013.

**Question 07.01-55:**

**Open Item**

**Follow up to RAI 505, Question 07.01-46**

The staff requests the applicant provide additional design information on the Operational I&C Disable Switches (OICS) including: (1) Identification of all operational situations for which the OICS would be used; (2) Clarification of the operational effects of the OICS on all affected I&C systems; and (3) Identification of the consequences of OICS to provide its safety function, including the impact on the plant and the ability of operators to fulfill credited actions and/or mitigate anticipated operational occurrences and postulated accidents. This RAI is a follow-on to RAI 505, 07.01-46.

IEEE Std. 603-1991, Clause 5.2, states in part, that the safety systems shall be designed so that, once initiated automatically or manually, the intended sequence of protective actions of the execute features shall continue until completion. Clause 6.2.1 states, in part, that 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. The applicant introduced the OICS in Revision 3 of the U.S. EPR FSAR, Section 7.1.1.6.5. The staff, upon reviewing the new design information, issued RAI 505, Question 07.01-46 to request clarification on the design functionality, implementation and other general questions. The applicant's response to RAI 505, 07.01-46 (Supplement 18) did not adequately address all of the staff's concerns regarding this newly submitted design attribute.

According to U.S. EPR FSAR, Tier 2, Section 7.1.1.6.5, Revision 3, the applicant states the following regarding OICS:

"During normal operation, the operational I&C disable switch on the SICS is set so that the PAS can send commands to the PACS. In this configuration, automatic commands from the PAS override manual commands from the SICS because of the nature of the manual control logic in the PACS. If the operational I&C disable switch is set to DISABLE by the operator, the PAS input will be disabled (i.e., the input signals from the PAS to the communications module will be blocked from being sent to the priority module), providing the priority of the SICS manual commands. The operational I&C disable switch disables PAS inputs, all other PACS inputs remain operational."

The applicant's revised interim Revision 4 FSAR section markup, submitted as part of its response to RAI 505, Question 07.01-46, states,

"The SICS manual component level commands are momentary signals that are removed once the actuator has reached its final limit position. Once the SICS component level command signal is removed, the PAS has the ability to manipulate the actuator. This may be undesirable to the operator controlling the device. Therefore, four safety-related Operational I&C Disable switches are implemented to prevent PAS from manipulating the actuator. During normal operation, the Operational I&C Disable switches on the SICS are set so that the PAS can send commands to the PACS. If at least two of the four switches (2 out of 4 voting) are set to DISABLE by the operator, the PAS input is blocked by the PAC modules. This blocking function

is implemented within the PACS. The Operational I&C Disable switches block PAS inputs. The other PACS inputs remain operational."

In Revision 3 of FSAR Section 7.1.1.6.5, the applicant states that the automatic Process Automation System (PAS) commands normally override any SICS commands because of the nature of manual control logic at the Priority and Actuator Control System (PACS). This appears to be a design inconsistency in terms of the priority logic at the PACS module if a non-safety related system can override the commands of any safety-related I&C system (unless state-based priority logic is employed). In addition, when the OICS are enabled, the applicant states that PAS input will be disabled or blocked. The addition of the OICS is an indication that the applicant considers a failure of the non-safety related PAS to potentially impact safety functions. The staff could not determine, through a review of available documentation how the applicant addressed ta failure of the OICS.

The staff requests the applicant address the following questions:

a. Identify all operational situations for which the OICS would be used, including failures of PAS, AOOs, PAs, etc. Also clarify whether the SICS is, under normal conditions, at a higher priority than the PAS.
b. Identify the consequences of failure of OICS to provide their safety function on the plant and the ability of operators to fulfill credited actions and/or mitigate anticipated operational occurrences (AOOs) and postulated accidents (PAs).
c. Is the functionality provided by the OICS, considering it is safety-related, documented in Chapter 15? Per the definition of a safety function in IEEE Std. 603-1991, it appears the OICS functionality would be essential to help maintain plant parameters within acceptable limits established for a design basis event.
d. The applicant states, in part, that enabling 2oo4 OICS will, "….block PAS inputs, all other PACS inputs remain operational":

    d-1. Does this mean that all PAS inputs to all PACS communication modules will be blocked? If so, how does this affect the overall operations of PAS and other systems that are affected by PAS functionality?

    d-2. Does enabling the switches cause a complete loss of manual component or manual grouped control functionality on PICS?

    d-3. Does the PACS perform the blocking of PAS inputs? If so, describe in details how this blocking takes place on the PACS when a 2oo4 vote is received.

    d-4. In terms of the 2oo4 voting logic in the OICS: (i) Does this take place within the PS? (ii) Is this hardwired logic? (iii) Does the applicant have a figure that demonstrates this voting configuration for the staff's review?

e. Is OICS functionality required at the RSS? If not, provides details on why its functionality is not necessary at the RSS.
f. U.S. EPR FSAR markup, Page 7.1-51, states "The SICS manual component level commands are momentary signals that are removed once the actuators has reached its final limit position." Explain why the SICS manual controls are momentary signals and why the priority logic is not (or cannot be) implemented in

a way that ensures SICS commands always have priority over PAS in all operational situations for a given actuator.

g. Is OICS functionality verified through periodic surveillance testing?

**Response to Question 07.01-55:**

A response to this question will be provided by February 21, 2013.