ArevaEPRDCPEm Resource

From: Miernicki, Michael
Sent: Tuesday, October 22, 2013 2:40 PM
To: ArevaEPRDCPEm Resource
Subject: FW: US EPR DC DRAFT RAI 609, Chapter 7, Section: 07.01 - Instrumentation and Controls
Attachments: DRAFT RAI 609_ICE_7223.docx

Michael J. Miernicki
Sr. Project Manager
NRC/NRO/DNRL/LB1
301-415-2304

From: Miernicki, Michael
Sent: Tuesday, October 22, 2013 2:39 PM
To: "usepr@areva.com' (usepr@areva.com)'
Cc: Jackson, Terry; Morton, Wendell; Zhang, Deanna; Segala, John; Mitra, Sikhindra
Subject: RE: US EPR DC DRAFT RAI 609, Chapter 7, Section: 07.01 - Instrumentation and Controls

Attached please find Draft RAI No. 609 regarding your application for standard design certification of the U.S. EPR. If you have any questions or need clarification regarding this Draft RAI, please let me know as soon as possible, I will have our technical Staff available to discuss them with you.

Please also review the Draft RAI to ensure that we have not inadvertently included proprietary information. If there is any proprietary information, please let me know within the next ten days. If I do not hear from you within the next ten days, I will assume there are none and will make the Draft RAI publicly available.

Thank You,

Mike

Michael J. Miernicki
Sr. Project Manager
NRC/NRO/DNRL/LB1
301-415-2304

Hearing Identifier: AREVA_EPR_DC_RAIs
Email Number: 4702

Mail Envelope Properties (9C2386A0C0BC584684916F7A0482B6CAEAF42FC313)

Subject: FW: US EPR DC DRAFT RAI 609, Chapter 7, Section: 07.01 - Instrumentation and Controls
Sent Date: 10/22/2013 2:40:10 PM
Received Date: 10/22/2013 2:40:13 PM
From: Miernicki, Michael

Created By: Michael.Miernicki@nrc.gov

Recipients:
"ArevaEPRDCPEm Resource" <ArevaEPRDCPEm.Resource@nrc.gov>
Tracking Status: None

Post Office: HQCLSTR02.nrc.gov

Files	**Size**	**Date & Time**
MESSAGE	1164	10/22/2013 2:40:13 PM
DRAFT RAI 609_ICE_7223.docx	52090	

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

DRAFT
Request for Additional Information 609

Issue Date: 10/22/2013
Application Title: U. S. EPR Standard Design Certification - Docket Number 52-020
Operating Company: AREVA NP Inc.
Docket No. 52-020
Review Section: 07.01 - Instrumentation and Controls - Introduction
Application Section: 07.01

QUESTIONS

07.01-64

Provide a definition for the term "computerized" in the US-EPR FSAR, Tier 2 Chapter 7.

10 CFR 52.47(a)(2), “Contents of applications; technical information”, states, in part, with regard to systems, structures and components (SSCs) that the description shall be sufficient to permit understanding of the system designs. Tier 2 Section 7.1.1.4.8 states that “The [Signal Conditioning and Distribution System] (SCDS) is composed of non-computerized signal conditioning modules and signal distribution modules that are part of the TXS platform.” The FSAR does not provide a definition for the term "computerized." In addition, Section 7.1.1.6.6 states that the SCDS do not contain running software and therefore software common cause failure does not apply to the SCDS. However, this section does not provide a description of what is meant by "running software." Provide a definition for the term "computerized," and clarify what is meant by running software and whether the SCDS contains programmable technology. If the SCDS does contain programmable technology, how are software common-cause failures mitigated.

07.01-65

Provide clarification and corrections to US EPR Tier 2 FSAR Figure 7.3-35 and FSAR Sections 7.3, 7.6 and 9.2.2.

In accordance with 10 CFR50 Appendix A and GDC 44, cooling water must have the capability to transfer heat from systems, structures, systems, and components (SSCs) important to safety to an ultimate heat sink during both normal and accident conditions, with suitable redundancy, assuming a single active component failure coincident with either the loss of offsite power or loss of onsite power. Based on the staff's review of US-EPR FSAR Revision 5, the following questions are needed related to the component cooling water system (CCWS) and SSCs important to safety. FSAR discrepancies were noted when reviewing Tier 2 Sections 9.2.2 (CCWS); 7.3.1, “Engineered Safety Features Systems;” and 7.6, “Interlock Systems Important to Safety”.

FSAR Tier 2 Section 9.2.2.2, “Component Description,” states:

The non-safety load isolation valves are also fast-acting, hydraulically-operated valves. Each hydraulically-operated valve has multiple solenoid-operated pilot valves and hydraulic fluid pumps. Pilot valves and hydraulic fluid pumps are powered from different Class 1E divisions to provide redundancy.

FSAR Tier 2 Section 9.2.2.6.1.1, “CCWS Automatic I&C Safety-Related Functions,” states:

If the surge tank level continues to decrease to less than the MIN3 setpoint, the common headers are isolated by closure of the switchover valves (KAA10/20/30/40 AA006/010/032/033) and the switchover sequence is prohibited. If the surge tank level continues to decrease to less than MIN4 set-point, the associated CCWS train pump is tripped and the common-user-sets switchover sequence function is unlocked to allow supplying of the common users by the opposite train capable of supplying the common header. The demineralized water distribution system (DWDS) supply isolation valve (KAA10/20/30/40 AA027) is also closed in order to avoid demineralized water (DW) water supply to a train with a leak. The surge tank level is detected by two redundant analog level measurements. The functional logic is shown on Figure 7.3-35.

Questions:

1. Figure 7.3-35 does not accurately describe I&C logic to close hydraulic valve 50AA004 on low surge tank level. The valve (50AA004) is missing from this figure.
2. Figure 7.3-35 does not shown how the I&C logic opens pilot valves (B, C, D) for all the trains; that is, the figure is drawn to only show Division 1 and the staff is unable to understand the I&C interactions with Divisions 2, 3 and 4.
3. FSAR Section 9.2.2.6.1.1 does not accurately describe all the valves that are closed due to CCWS emergency leak detection.
4. FSAR Section 9.2.2, Section 7.3, Section 7.6, and Figure 7.3-35 does not clearly described how hydraulic switchover valves AA032/033 only require 2 pilot valves to meet single failure criteria and hydraulic valves switchover valves AA006/010 required 4 pilot valves.
5. Figure 7.3-35 Trains 1, 2, 3, and 4 “boxes” lack details of the associated I&C logic and the staff needs additional details to fully understand the I&C interactions between valves and train pilot valves.

07.01-66

Provide clarification and corrections to US EPR Tier 2 FSAR Figure 7.3-36 and FSAR Sections 7.3, 7.6 and 9.2.2.

In accordance with 10 CFR50 Appendix A and GDC 44, cooling water must have the capability to transfer heat from systems, structures, systems, and components (SSCs) important to safety to an ultimate heat sink during both normal and accident conditions, with suitable redundancy, assuming a single active component failure coincident with either the loss of offsite power or loss of onsite power.

Based on the staff's review of US-EPR FSAR Revision 5, the following questions are needed related to the component cooling water system (CCWS) and SSCs important to safety. FSAR discrepancies were noted when reviewing Tier 2 Sections 9.2.2 (CCWS); 7.3.1, “Engineered Safety Features Systems;” and 7.6, “Interlock Systems Important to Safety”.

FSAR Tier 2 Section 9.2.2.6.1.1, “CCWS Automatic I&C Safety-Related Functions,” states:

> In the event of a switchover valve seat leakage or failure, and depending upon the difference in pressure between the two CCWS trains, a water transfer could occur. If the water transfer leads to a MAX2 surge tank level in one of the two associated trains and a MIN3 surge tank level on the other, the common users are automatically isolated from the safety trains. This action allows both trains to perform their main safety related function. The function logic is shown on Figure 7.3-36.

Questions:

1. FSAR Section 9.2.2, Section 7.3, Section 7.6, and Figure 7.3-36 does not clearly describe how hydraulic switchover valves AA032/33 only required 2 pilot valves to meet single failure criteria while hydraulic valves switchover valves AA006/010 required 4 pilot valves.
2. Figure 7.3-36 does not show how the I&C logic opens pilot valves (C, D) for all the trains; that is, the figure is drawn to only show Divisions 1 and 2 and the staff is unable to understand the I&C interactions with Divisions 3 and 4.
3. Figure 7.3-36 Trains 1, 2, 3, and 4 “boxes” lack details of the associated I&C logic and the staff needs additional details to fully understand the I&C interactions between valves and train pilot valves.

07.01-67

Provide clarification and corrections to US EPR Tier 2 FSAR Figures 7.6-1 and 7.3-33 and FSAR Section 7.3.1.

In accordance with 10 CFR50 Appendix A and GDC 44, cooling water must have the capability to transfer heat from systems, structures, systems, and components (SSCs) important to safety to an ultimate heat sink during both normal and accident conditions, with suitable redundancy, assuming a single active component failure coincident with either the loss of offsite power or loss of onsite power.

Based on the staff's review of US-EPR FSAR Revision 5, the following questions are needed related to the component cooling water system (CCWS) and SSCs important to safety. FSAR discrepancies were noted when reviewing Tier 2 Sections 9.2.2 (CCWS); 7.3.1, “Engineered Safety Features Systems;” and 7.6, “Interlock Systems Important to Safety”.

FSAR Tier 2 Section 9.2.2.6.1.1, “CCWS Automatic I&C Safety-Related Functions,” states:

> Train separation of redundant CCWS divisions confirms that a fault affects no more than one train via a switchover valve interlock. To prohibit more than one train from being connected to a common header, the following groupings of valves cannot be simultaneously opened:
>
> ● Common 1.a – KAA10AA032/033 with KAA20AA032/033.
> ● Common 2.a – KAA30AA032/033 with KAA40AA032/033.
> ● Common 1.b – KAA10AA006/010 and KAA20AA006/010.
> ● Common 2.b – KAA30AA006/010 and KAA40AA006/010.
>
> The functional logic is shown on Figure 7.6-1.
>
> Train automatic backup switchover consists of:
> ● Close switchover valves (KAA10/20/30/40 AA006/010) on the initial train and open LHSI heat exchanger isolation valve (KAA12/22/32/42 AA005).
> ● Open common 1.b (2.b) switchover valves (KAA10/20/30/40 AA006/010) on the on-coming train.
> ● Start CCWS pump (KAA10/20/30/40 AP001) on the on-coming train. The on-coming train common 1.a (2.a) sub-header switchover valve may then be manually opened. The functional logic is shown on Figure 7.3-33.

Questions:

1. Trains 1, 2, 3, and 4 “boxes” on Figure 7.6-1 lack details of the associated I&C logic and the staff needs additional details to fully understand the I&C interactions between valves and train pilot valves. Specifically, the “boxes” for the trains do not have any pilot valve numbers.

2. Division 3 and 4 are not shown on Figure 7.6-1. The staff needs Divisions 3 and 4 described to fully understand the I&C interactions between valves and train pilot valves.

3. The dark division vertical lines on Figures 7.3-33 and 7.6-1 are incorrectly drawn and should be corrected.

4. FSAR Section 7.3.1.4.1 text does not clearly describe other automatic functions (such as CCWS pumps, UHS fans, and LHSI and ESWS valve opening) which are shown in Figure 7.3-33.

07.01-68

Provide clarification and corrections to US EPR Tier 2 FSAR Figures 7.6-2 and 7.6-12.

In accordance with 10 CFR50 Appendix A and GDC 44, cooling water must have the capability to transfer heat from systems, structures, systems, and components (SSCs) important to safety to an ultimate heat sink during both normal and accident conditions, with suitable redundancy, assuming a single active component failure coincident with either the loss of offsite power or loss of onsite power.

Based on the staff's review of US-EPR FSAR Revision 5, the following questions are needed related to the component cooling water system (CCWS) and SSCs important to safety. FSAR discrepancies were noted when reviewing Tier 2 Sections 9.2.2 (CCWS); 7.3.1, “Engineered Safety Features Systems;” and 7.6, “Interlock Systems Important to Safety”.

FSAR Tier 2 Section 9.2.2.6.1.1, “CCWS Automatic I&C Safety-Related Functions,” states:

> Either the common 1.b or 2.b headers can provide cooling to the RCP thermal barriers. To maintain strict train separation of the redundant CCWS division supplying either common header and to confirm that a fault affects no more than one train, the CIVs (KAB30 AA049/050/051/052/053/054/055/056) are interlocked. One of the two common 1.b supply valves (KAB30 AA049/050) and one of the two common 1.b return valves (KAB30 AA051/052) must be closed prior to opening the CIVs from the common 2.b header (KAB30 AA053/054/055/056), and vice versa. The functional logic is shown on Figure 7.6-2.
>
> To maintain cooling to the RCP thermal barriers, an interlock function is required to open the CIVs on the common header removed from service (common 1.b or 2.b) when a CIV on the common header in service (common 2.b or 1b, respectively) is closed. The functional logic is shown on Figure 7.6-12.

Questions:

1. The dark division vertical lines on Figures 7.6-2 and 7.6-12 are incorrectly drawn and should be corrected.

07.01-69

Provide clarification and corrections to US EPR Tier 2 FSAR Section 7.3 and 7.6.

In accordance with 10 CFR50 Appendix A and GDC 44, cooling water must have the capability to transfer heat from systems, structures, systems, and components (SSCs) important to safety to an ultimate heat sink during both normal and accident conditions, with suitable redundancy, assuming a single active component failure coincident with either the loss of offsite power or loss of onsite power.

Based on the staff's review of US-EPR FSAR Revision 5, the following questions are needed related to the component cooling water system (CCWS) and SSCs important to safety. FSAR discrepancies were noted when reviewing Tier 2 Sections 9.2.2 (CCWS); 7.3.1, “Engineered Safety Features Systems;” and 7.6, “Interlock Systems Important to Safety”.

FSAR Tier 2 Section 9.2.2.6.1.3, “CCWS Non-Safety-Related Functions,” states:

> In case of a failure to close of a switchover valve on the initial train or lack of opening of a switchover valves on the final train, another switchover is automatically done to the initial configuration.
>
> In case a CIV fails to open on the final header, another transfer is automatically performed back to the initial configuration.

Question:

1. The staff was unable to find the two logics described above in Tier 2 FSAR Sections 7.3 or 7.6.

07.01-70

Provide clarification and corrections to US EPR Tier 2 FSAR Sections 7.3, 7.6, and 9.2.8.

In accordance with 10 CFR50 Appendix A and GDC 44, cooling water must have the capability to transfer heat from systems, structures, systems, and components (SSCs) important to safety to an ultimate heat sink during both normal and accident conditions, with suitable redundancy, assuming a single active component failure coincident with either the loss of offsite power or loss of onsite power.

Based on the staff's review of US-EPR FSAR Revision 5, the following questions are needed related to the safety chilled water system (SCWS), and SSCs important to safety. FSAR discrepancies were noted when reviewing Tier 2 Sections 9.2.8 (SCWS); 7.3.1, “Engineered Safety Features Systems;” and 7.6, “Interlock Systems Important to Safety”.

FSAR Tier 2 Section 9.2.8 describes many I&C functions; however, these functions are not adequately described or cross referenced to FSAR Sections 7.3 or 7.6.

FSAR Tier 2 Section 9.2.8.6, “Instrumentation Requirements,” states:

The following automatic functions represent generic steps in train switchover to be performed or validated as a result of the abnormal condition in the affected train:

1. Standby train prerequisites are met for train startup.
2. Cross-tie MOVs are open-validate MOV position.
3. Start standby train pump 1.
4. Start standby train pump 2.
5. Start standby train chiller unit.
6. Enable the control loop for differential pressure across the evaporator, which starts system flow regulation by the bypass control valve in the standby train.
7. Enable the pressure monitoring loop for system pressure.

Annunciation occurs on automatic switchover.

Questions:

1. The logic described above (items 1 through 7) are not clearly described in Section 7.6.1 or Figures 7.6-5, 7.6-6, 7.6-7, and 7.6-8.

2. References from Section 9.2.8 to I&C Figures 7.6-5, 7.6-6, 7.6-7, and 7.6-8 does not exist and should be added to the FSAR.

07.01-71

Provide clarification and corrections to US EPR Tier 2 Figures 7.6-5, 7.6-6, 7.6-7, and 7.6-8 and FSAR Section 7.6.1.

In accordance with 10 CFR50 Appendix A and GDC 44, cooling water must have the capability to transfer heat from systems, structures, systems, and components (SSCs) important to safety to an ultimate heat sink during both normal and accident conditions, with suitable redundancy, assuming a single active component failure coincident with either the loss of offsite power or loss of onsite power. Based on the staff's review of US-EPR FSAR Revision 5, the following questions are needed related to the safety chilled water system (SCWS), and SSCs important to safety. FSAR discrepancies were noted when reviewing Tier 2 Sections 9.2.8 (SCWS); 7.3.1, “Engineered Safety Features Systems;” and 7.6, “Interlock Systems Important to Safety”.

FSAR Tier 2 Section 9.2.8.6, “Instrumentation Requirements,” states:

If the pressure falls to MIN-3, the following measures are initiated automatically for the affected train:

1. Chilled water system “Protection OFF” alarms. The MIN-3 system pressure setpoint trip occurs before the pressure corresponding to the minimum required available NPSH is reached.
2. Refrigeration unit shuts down.
3. Chilled water circulating pump shuts down.

Question:

1. The logic described above (item 1 through 3) is not described in Section 7.6.1 or Figures 7.6-5, 7.6-6, 7.6-7, and 7.6-8. This should be added to the FSAR.

07.01-72

Provide clarification and corrections to US EPR Tier 2 Figures 7.6-5, 7.6-6, 7.6-7, and 7.6-8 and FSAR Section 7.6.1.

In accordance with 10 CFR50 Appendix A and GDC 44, cooling water must have the capability to transfer heat from systems, structures, systems, and components (SSCs) important to safety to an ultimate heat sink during both normal and accident conditions, with suitable redundancy, assuming a single active component failure coincident with either the loss of offsite power or loss of onsite power.

Based on the staff's review of US-EPR FSAR Revision 5, the following questions are needed related to the safety chilled water system (SCWS), and SSCs important to safety. FSAR discrepancies were noted when reviewing Tier 2 Sections 9.2.8 (SCWS); 7.3.1, “Engineered Safety Features Systems;” and 7.6, “Interlock Systems Important to Safety”.

FSAR Tier 2 Section 9.2.8.6, “Instrumentation Requirements,” states:

> Running pumps will trip on a pump fault, chiller fault, low evaporator flow (MIN-2), or MIN-3 pressure in the expansion tank. In the event of a running pump trip on a pump fault when the cross-tie valves are shut and the division train is operating separate from the other division pair, then the second pump is on stand-by and starts when the SCWS fills to the normal operating pressure band in the expansion tank. In the event of a DBA with LOOP, the running pumps automatically restart under the EDG loading sequence. The pumps in the opposite train start if the running pumps fail.

Question:

1. The logic described above is not described in Section 7.6.1 or Figures 7.6-5, 7.6-6, 7.6-7, and 7.6-8. This should be added to the FSAR.

07.01-73

Provide clarification and corrections to US EPR Tier 2 FSAR 7.6.1 and 9.2.8.

In accordance with 10 CFR50 Appendix A and GDC 44, cooling water must have the capability to transfer heat from systems, structures, systems, and components (SSCs) important to safety to an ultimate heat sink during both normal and accident conditions, with suitable redundancy, assuming a single active component failure coincident with either the loss of offsite power or loss of onsite power.

Based on the staff's review of US-EPR FSAR Revision 5, the following questions are related to the safety chilled water system (SCWS), and SSCs important to safety. FSAR discrepancies were noted when reviewing Tier 2 Sections 9.2.8 (SCWS); 7.3.1, “Engineered Safety Features Systems;” and 7.6, “Interlock Systems Important to Safety”.

FSAR Tier 2 Section 9.2.8.2.2, “Component Description” states:

> SCWS Trains 1 and 4 each has eight fans used for heat removal from the air cooled chiller refrigeration units. These fans are located in the safeguards buildings.

Question:

1. The starting of the eight fans and associated logic are not described in Sections 7.6.1 or 9.2.8. This should be added to the FSAR.

07.01-74

Describe how remote access to the Process Information and Control System (PICS) is not possible. Specifically, describe what provisions are employed, either through the configuration of the firewall or through other provisions in the I&C system design, to prevent remote access to the PICS from the plant business network.

10 CFR 52.47(a)(2), “Contents of applications; technical information”, states, in part, with regard to systems, structures and components (SSCs) that the description shall be sufficient to permit understanding of the system designs. US-EPR FSAR, Tier 2 Section 7.1.1.3.2 states, “Redundant firewalls are provided for unidirectional transfer of information from the PICS to plant business networks. Remote access to the PICS is not possible.” This section does not describe what provisions are available to ensure that remote access is not possible or how the firewall is configured as one-way to the plant business networks. Provide a description of how remote access to the PICS is not possible from plant business networks. Specifically, what provisions within the design ensure that remote access to the PICS is not possible from the plant corporate network. In addition, describe what provisions will be implemented to ensure that the firewall is one-way in order to prevent inadvertent access (e.g. remote access, testing) to the PICS. Furthermore, describe how these provisions will be verified in the as-built design.

07.01-75

Describe how the Process Information and Control System (PICS) connection addresses the guidance of Digital I&C Interim Staff Guidance (D I&C ISG)-04 to meet the requirements of IEEE Std. 603-1991 Clause 5.6.3.

IEEE Std. 603-1991, Clause 5.6.3 states that “the safety system design shall be such that credible failures in and consequential actions by other systems, as documented in 4.8 of the design basis, shall not prevent the safety systems from meeting the requirements of this standard.” D I&C ISG-04 provides guidance on non-safety system communication with safety systems. Specifically, Section 1 of D I&C ISG-04 provides guidance on data communication between non-safety systems and safety systems and Section 3 of D I&C ISG-04 provides guidance on use of multidivisional control and display stations to control plant equipment in more than one safety division. Since the PICS provides multidivisional control of safety equipment through a data communications link to the Priority Actuation and Control System (PACS), the PICS would need to address the guidance of Section 1 and Section 3 of D I&C ISG-04 to demonstrate compliance to IEEE Std. 603-1991 Clause 5.6.3. As stated in Tier 2 Section 7.1.1.3.2 of the

US-EPR FSAR, "the design for PICS complies with the design principles in DI&C-ISG-04..." This section does not include design information on how the PICS conforms to this ISG. Specifically, no information was provided to demonstrate how each criteria within Section 1 and 3 of this ISG was addressed. Examples include no description of how the design addresses Section 1.2 and Section 1.3 of ISG-04 which state that "The safety function of each safety channel should be protected from adverse influence from outside the division of which that channel is a member..." and "A safety channel should not receive any communication from outside its own safety division unless that communication supports or enhances the performance of the safety function." Another example is that the FSAR does not describe how the design conforms to Section 3.5 of ISG-04 which states that "The results of malfunctions of control system resources (e.g., workstations, application servers, protection/control processors) shared between systems must be consistent with the assumptions made in the safety analysis of the plant..." Provide a description of how the PICS conforms to each criteria within Section 1 and 3 of ISG-04.

07.01-76

Staff requests applicant to clarify the use of Operational I&C Disable Switches (OPDIS) in use for credited manual operator actions.

10 CFR 52.47(a)(2), “Contents of applications; technical information”, states, in part, with regard to systems, structures and components (SSCs) that the description shall be sufficient to permit understanding of the system designs. On Page 7.1-73 of US EPR FSAR Tier 2, Revision 5, the applicant states the following:

“The Operational I&C Disable switch will be necessary for an AOO or PA for which the operator used credited SICS component-level commands to mitigate the event.”

The staff requests the applicant clarify the following:

1. Under Section 15.0.0.3.7 of US EPR FSAR Tier 2, Revision 5, should this distinction be made when referring to credited operator actions?

2. Should this distinction be made in Section 7.3 of US EPR FSAR Tier 2, Revision 5? For example, the applicant states on page 7.3-2 that, “For an extra borating system (EBS) malfunction event, the component-level controls on SICS are credited to terminate EBS.” Even though the SICS controls are credited, to ensure that the credited actions are effective, would the operator need to enable the OPDIS?

07.01-77

Applicant to clarify design information on FSAR Figures 7.6-5 – 7.6-8

10 CFR 52.47(a)(2), “Contents of applications; technical information”, states, in part, with regard to systems, structures and components (SSCs) that the description shall be sufficient to permit understanding of the system designs. For US EPR FSAR Tier 2, Revision 5, figures 7.6-5 through 7.6-8, clarify the following:

1. Provide additional information on the boxed symbol titled, “Black box standby mode”
    a. What information does this item represent for the system?
    b. Is this symbol and its information related to the “Blackbox Internal Fault” shown in US EPR FSAR Tier 2, Revision 4, Section 7.6?

2. For the system denoted as “Train ‘X’ LOOP Restart Failure”, if this input demonstrates that the train that is active fails to start after a LOOP, then clarify why this input would not lead directly to a switchover, or why this input wouldn’t directly feed into the downstream ‘AND’ gate logic?

07.01-78

Clarify the acceptability of using an analysis to demonstrate acceptable performance of self testing features in order to close related Inspections, Tests, Analyses, and Acceptance Criteria (ITAACs). This question is related to RAI 505, Question 7.1-44.

10 CFR 52.47(b)(1), "Contents of applications; technical information", states, in part, the application must contain the proposed inspections, tests, analyses and acceptance criteria that are sufficient to provide reasonable assurance that, if met, a facility would be constructed and operated in conformity with the design certification. US EPR FSAR Tier 1, Revision 5, Table 2.4.1-7(Protection System [PS]) ITAAC Item 4.26 and US EPR FSAR Tier 1, Revision 5, Table 2.4.4-4 (Safety Automation System [SAS[) ITAAC Item 4.20 shows the confirmation of credited self-testing features performance for both safety systems. Within the Inspections, Tests, Analyses (ITAs) for both items, the applicant states, in part, that analyses or a combination of type tests and analyses will be performed to demonstrate self-testing features performance. The staff is concerned that the applicant considers providing an analysis alone as a sufficient means of performing an ITAAC given the safety significance of these design features, and that the self-testing features are not passive design features. The automated and credited self-testing features for both PS and SAS are in continuous operation. Similar to ITAAC Item 4.27 on Table 2.4.1-7, the staff considers testing to be the appropriate means to verify that self-testing features properly respond to faults for which they are designed to address. The applicant is to address the following questions:

1. If the applicant considers providing an analysis to be a sufficient ITA, describe the type of analysis and how it would provide a sufficent verification of self-testing features.

2. Justify why analysis is necessary, in lieu of testing, to address an ITAAC for a safety-related application that is in continuous operation.

07.01-79

Clarify the potential discrepancy between commitment wording and acceptance criteria for Safety Automation System (SAS) Inspections, Tests, Analyses, and Acceptance Criteria (ITAAC) Item 4.18.

10 CFR 52.47(b)(1), "Contents of applications; technical information", states, in part, the application must contain the proposed inspections, tests, analyses and acceptance criteria that are sufficient to provide reasonable assurance that, if met, a facility would be constructed and operated in conformity with the design certification. US EPR FSAR Tier 1, Table 2.4.4-4, ITAAC Item 4.18, Revision 5, in the commitment wording states, in part,

"The ESF and EAS functions are removed when input signals that represent the completion of the ESF and EAS functions are present"

The acceptance criteria wording states, in part that,

"The ESF and EAS functions remain following removal of the signal. The ESF and EAS functions are removed when the ESF and EAS functions are manually reset."

Applicant to address the following questions:

1. IEEE Std. 603-1991, Clause 5.2, "Completion of Protective Actions" states, in part, that deliberate operator action shall be required to return the safety system to normal. Does the commitment wording description meet this requirement?

2. Does the applicant consider the commitment wording and acceptance criteria, as currently written to be correct in addressing Clause 5.2?

07.01-80

Clarify the safety functions of the Process Information and Control System (PICS) and the Inspections, Tests, Analyses, and Acceptance Criteria (ITAAC) to verify its performance.

10 CFR 52.47(b)(1), "Contents of applications; technical information", states, in part, the application must contain the proposed inspections, tests, analyses and acceptance criteria that are sufficient to provide reasonable assurance that, if met, a facility would be constructed and operated in conformity with the design certification. For US EPR FSAR Tier 1, Section 2.4.10, "PICS", Revision 5, the staff requests clarification on the following items:

1. Item 3.6 refers to "safety function" of PICS with regards to EMI/RFI performance. Clarify what safety functions PICS is performing.

2. There does not appear to be an ITAAC item that verifies all the control functionality available on the PICS. If AREVA intends the PICS to be used during normal, AOO and PAs, then there should be an ITAAC item that verifies the PICS can control and display status of the equipment available from the PICS. Clarify where in the FSAR PICS controls for safety and/or non-safety functions are verified in ITAAC space.

07.01-81

Describe the fault tolerance attributes of the Process Information and Control System (PICS) Server Units (SUs).

10 CFR 52.47(a)(2), "Contents of applications; technical information", states, in part, with regard to systems, structures and components (SSCs) that the description shall be sufficient to permit understanding of the system designs. US EPR DCD FSAR Tier 2, Section 7.1.1.3.2, "Process Information and Control System), Revision 5, page 7.1-24, states,

"The Server Units are configured in a distributed redundancy. The redundancy of the two servers is established through a software package which combines the physical resources of two servers into a single operating environment with redundancy of the underlying hardware and data. The operating environment evaluates the status of the redundant server units. In the event of a detected malfunction, the function is switched to the corresponding reserve server unit. The server units operate in lockstep providing redundancy of hardware, data and networks for automated fault management."

The staff requests the applicant address the following clarifying questions:
1. Provide information on how a faulted SU's data communications are blocked or restricted from continuing once a fault is detected.
2. Considering the redundant SUs operate in a unified software-based environment, provide more information on how a fault or error on one SU is prevented or restricted from compromising or corrupting the non-faulted SU's performance and data communications.
3. Has the applicant applied similar design attributes to other areas in the US EPR I&C design?

07.01-82

Applicant to address the following clarifying questions regarding the Process Automation System (PAS) and the Diverse Actuation System (DAS).

10 CFR 52.47(b)(1), "Contents of applications; technical information", states, in part, the application must contain the proposed inspections, tests, analyses and acceptance criteria (ITAACs) that are sufficient to provide reasonable assurance that, if met, a facility would be constructed and operated in conformity with the design certification. Within US EPR FSAR Tier 1, Chapter 2, Revision 5, the applicant added a new Tier 1 ITAAC entry for the PAS. For US EPR FSAR Tier 1, Section 2.4.9, "PAS", Revision 5, the staff requests clarification on the following items:

1. ITAAC Item 3.3 states, "PAS equipment listed in Table 2.4.9-1 can perform its safety function when subjected to electromagnetic interference (EMI) and radio-frequency interference (RFI)." According to ITAAC Item 1.0, PAS is a non-safety related system. Clarify the above-statement when it refers to performing its "safety function". Does the PAS perform some safety functions or are there certain PAS components/equipment that are safety related?

2. Regarding ITAAC Item 3.1 on Table 2.4.9-2, how will control function segmentation verification be performed for the PAS? Is there a means to verify control function allocation to various PAS CUs from the PICS?

    a. Does ITAAC Item 3.1 also take into account safety control function segmentation as well?

3. Regarding Table 2.4.9-2, there does not appear to be an ITAAC item that verifies the automatic functions performed by the PAS. Does the applicant intend to use other mechanical system ITAACs (e.g. Feedwater) to collectively verify PAS automatic control functionality or is there another means that the applicant is verifying the functionality of the three subsystems of PAS?

Regarding US EPR FSAR Tier 1, Section 2.4.24, "DAS", Revision 5, does this system have any supporting self-diagnostic and/or self-monitoring features?

07.01-83

Provide a revision to the U.S. EPR FSAR that is consistent with the FSAR mark up pages submitted on March 16, 2012, in response to RAI 505, Question 07.05-10. FSAR mark-ups included in the March 16, 2012 response to RAI 505, Question 07.05-10, stated "PAM variables are provided in the MCR to perform Type A, B, and C accident management functions." The staff found this acceptable. It is noted, however, that Revision 4 of the U.S. EPR FSAR is inconsistent with the FSAR mark-up pages included with the March 16, 2012, response to RAI 505, Question 07.05-10. This inconsistency was raised at public meetings. This inconsistency needs to be addressed in the applicants' forthcoming revision of the U.S EPR FSAR. The following italics indicate the applicant's typographical error; *"PAM variables are provided on the PICS operator workstation in the MCR to perform Type A, B, and C accident management functions."* The applicant provided FSAR Revision 5 on July 13, 2013. The staff reviewed Revision 5 of the U.S. EPR FSAR and determined that the error is still there and needs to be corrected by the applicant.