Public Meeting to Discuss NRC Comments on Responses to RAI Set 505, Question 7.1-36, 39, and 44

Duc Phan, Chris Doyel
Rockville, Maryland
November 15, 2012

EPR™ by AREVA

AREVA

Purpose and Background

Purpose

- Present resolution to NRC comments on responses to RAI set 505, Questions 7.1-36, 39, and 44
- Confirm agreement with the NRC on the resolutions to NRC comments

Background

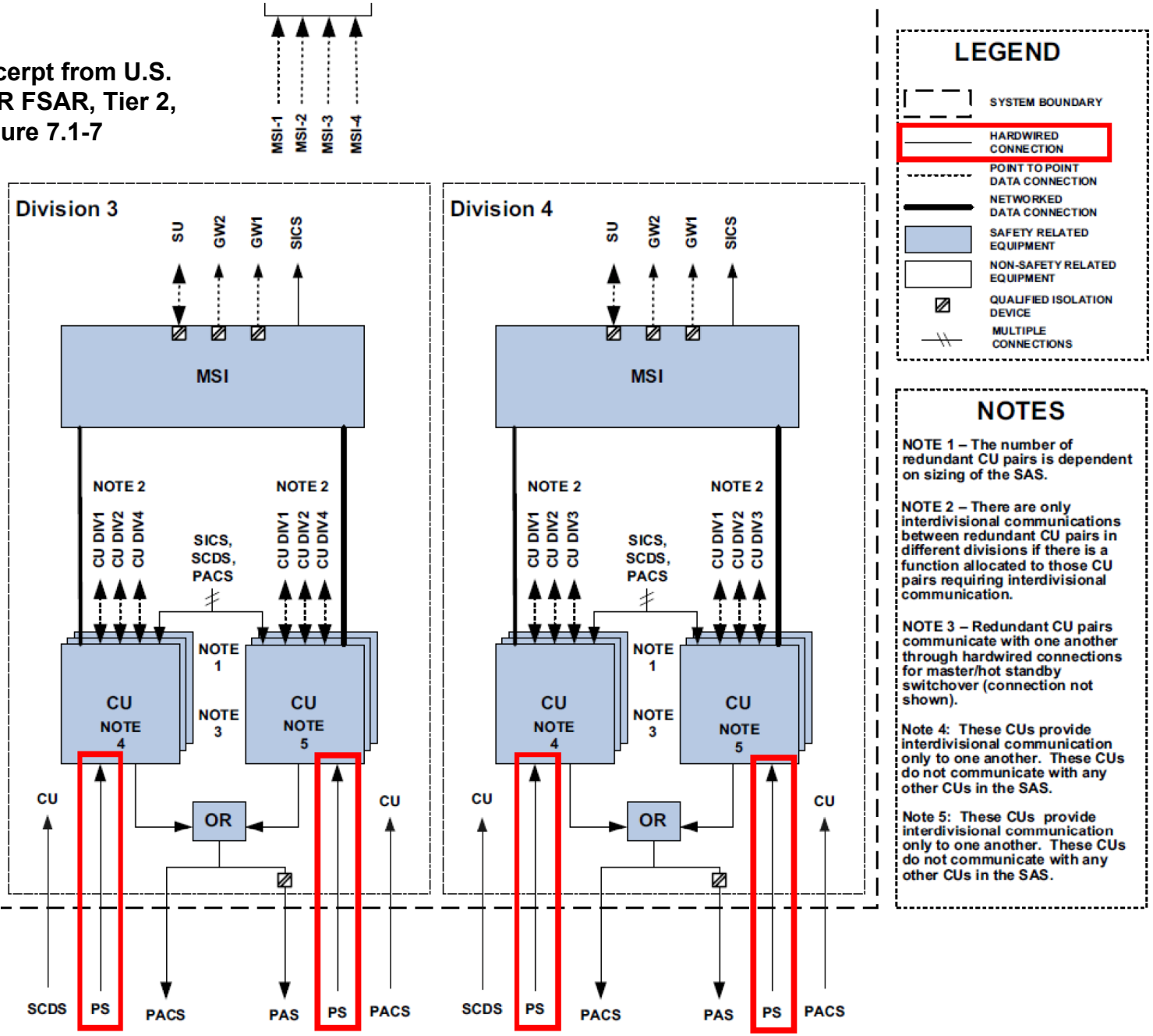
- Final response to RAI 505 7.1-36 was provided on April 27, 2012
- Final response to RAI 505 7.1-39 was provided on May 22, 2012
- Final response to RAI 505 7.1-44 was provided on May 9, 2012
- RAI Set 505 additional follow-up comments received from NRC on August 14, 2012

Comments on RAI 505

RAI 505, Question 7.1-36

- **1. For Figure 7.1-7 [*shown on slide 4*], for each CU in which the PS feeds into the CU, what type of connection does this line denote? It doesn't appear to be a hardwired connection nor a networked connection based strictly on the drawing legend on the side of this figure.**
  - The connections from the PS to the SAS are hardwired connections. This is shown in U.S. EPR FSAR, Tier 2, Figure 7.1-7 and denoted in the drawing legend.

Excerpt from U.S. EPR FSAR, Tier 2, Figure 7.1-7



NOTES

NOTE 1 – The number of redundant CU pairs is dependent on sizing of the SAS.

NOTE 2 – There are only interdivisional communications between redundant CU pairs in different divisions if there is a function allocated to those CU pairs requiring interdivisional communication.

NOTE 3 – Redundant CU pairs communicate with one another through hardwired connections for master/hot standby switchover (connection not shown).

Note 4: These CUs provide interdivisional communication only to one another. These CUs do not communicate with any other CUs in the SAS.

Note 5: These CUs provide interdivisional communication only to one another. These CUs do not communicate with any other CUs in the SAS.

Comments on RAI 505 Cont'd

- **2. Regarding Note 2 on Figure 7.1-7 [*shown on slide 4*]: Besides voting and system interlocks, what other functions require interdivisional communication?**
  - Engineered Safety Features (ESF) Control, Essential Auxiliary Support (EAS) Control, and Interlock functions are performed by SAS. Interdivisional communication is provided when required, for voting across divisions or due to the divisional power allocation to the mechanical and electrical portions of the system. U.S. EPR FSAR Tier 2, Table 7.1-5 lists all SAS functions and explains why interdivisional communication is required for selected functions ("Interdivisional Communications" column).

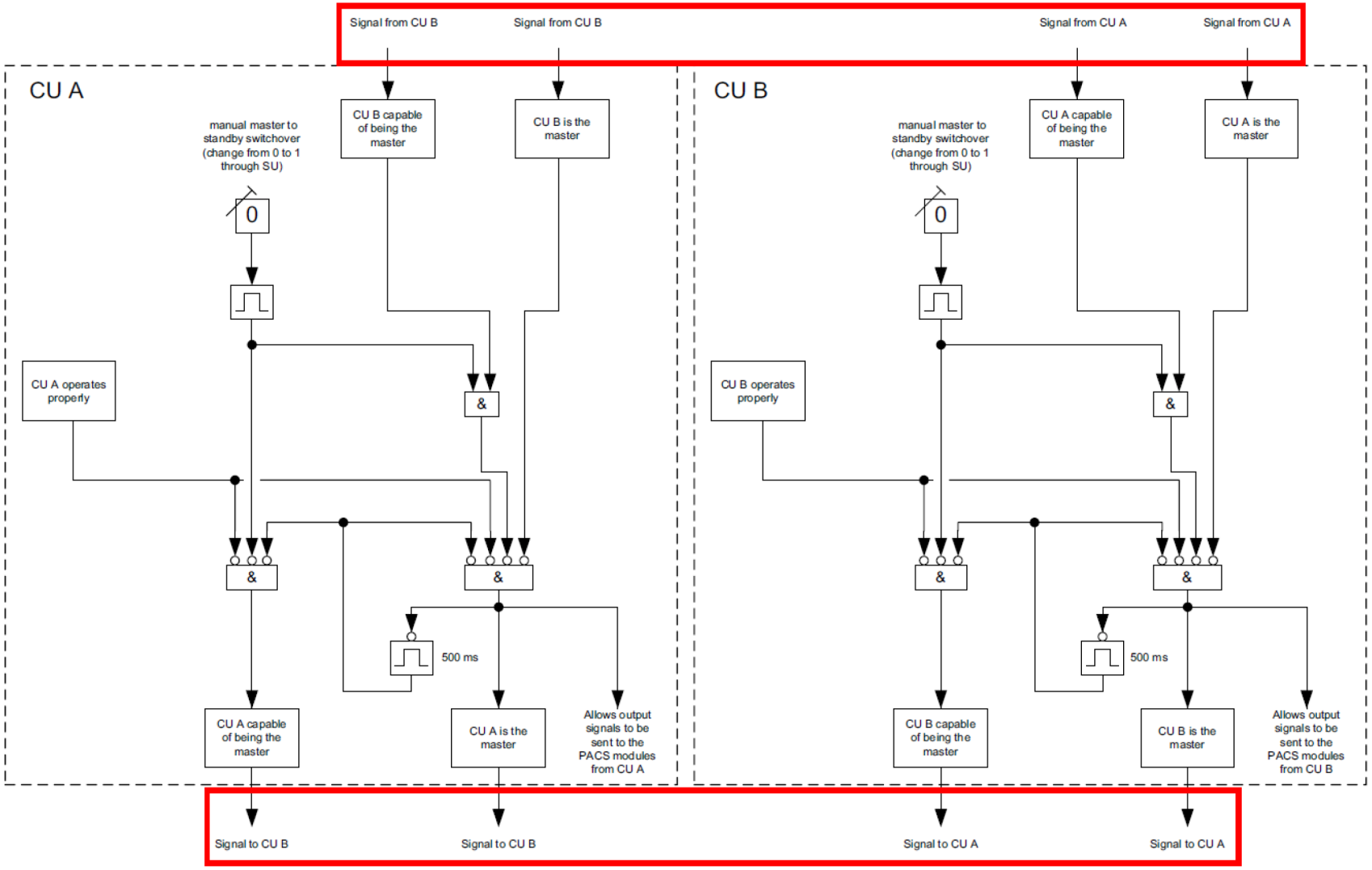
System[1]	Function Name[2]	Function Safety Basis[3]	Interdivisional Communications[4]
Main Steam System (MSS)	Steam Generator MSRCV Regulation during Pressure Control (Figure 7.3-12)	This function is described in Sections 7.3.1.3.4 and 10.3.	The MSRIV closed position is detected via 2 out of 4 voting (the position switches are associated with Div 1 through 4).
Residual Heat	RHR Isolation Valves	This function is described	NO

Excerpt from U.S. EPR FSAR Tier 2, Table 7.1-5

Comments on RAI 505 Cont'd

- **3. Regarding Figure 7.1-29 (Master/Standby Logic) [*shown on slide 7*] and 7.1-7(SAS Architecture) and Note 3 [*shown on slide 4*]: Where are the hardwired connections mentioned in Note 3 represented on Figure 7.1-29? All connections on the logic appear to be networked. Note 3 states that redundant CU pairs communication through hardwired connections. Also, what type of communication is conferred over the hardwired connection?**
  - Note 3 of U.S. EPR FSAR, Tier 2, Figure 7.1-7 states, "Redundant CU pairs communicate with one another through hardwired connections for master/hot standby switchover (connection not shown)." The connections between the CUs on U.S. EPR FSAR, Tier 2, Figure 7.1-29 are hardwired. Discrete (e.g. ON/OFF or 1/0) values are passed between the master and hot standby CUs through hardwired connections. U.S. EPR FSAR, Tier 2, Figure 7.1-29 is meant to show the master/hot standby switchover logic and not the hardware design.

Excerpt of U.S. EPR FSAR, Tier 2, Figure 7.1-29



Comments on RAI 505 Cont'd

- **4. Regarding Figure 7.1-7 [*shown on slide 4*]: Clarify the relationship between SAS and PAS due to the figure showing an output from SAS to PAS. According to Table 7.1-4, the connection between SAS and PAS is a hardwired connection to, "Provide for coordination of logic between SAS and PAS (if needed)."**
  - The connection from SAS to PAS is a one way hardwired and isolated connection (shown on U.S. EPR FSAR, Tier 2, Figure 7.1-7) to send SAS information to PAS. Some functions of PAS may require inputs from SAS to execute its functionality (e.g. CCWS Emergency Leak Detection Function sends signal to disable CCWS Normal Operation Switchover if you have a leak). A description will be added to U.S. EPR FSAR, Tier 2, Section 7.1 to add clarification on the SAS to PAS connection.

Comments on RAI 505 Cont'd

- **5. Regarding Figure 7.1-29 [*shown on slide 7*], explain the significance of 500ms delay time. Is there a technical basis for this amount of time?**
  - There is no significance to the exact value of the 500ms. The 500ms prevents a CU from switching between master and hot standby within a short period of time. This ensures that both CUs have ample time to switch over to master or hot standby before having the ability to switch again. This amount of time was based on engineering judgment and experience from the European designs.
- **6. Regarding FSAR markup p. 7.1-23, second bullet, is "range monitoring" the same thing as the automated channel comparison function detailed in ANP-10315P?**
  - Range monitoring described in U.S. EPR FSAR, Tier 2, Section 7.1 is different than the channel check function detailed in ANP-10315P. Range monitoring is the detection if the sensor has provided a value outside of the calibrated range (e.g. 4-20mA) and flagging that sensor value as faulty. The channel check function is a comparison of multiple like parameters to determine if there is a deviation that exceeds an established limit. If there is a deviation, then it will result in an alarm in the MCR. A within range failure of a sensor will not be detected by range monitoring, but will be alarmed through the channel check function.
  - The range monitoring function will be clarified in the U.S. EPR FSAR, Tier 2, Section 7.1.1.4.2.

Comments on RAI 505 Cont'd

- **7. FSAR markup page 7.1-19, second bullet from top of page: What are the "subordinate modules"?**
  - A SAS CU is composed of a function processor, communication modules, input modules, and output modules. The function processor acts as the "brains" of the CU, and the subordinate modules are the communication, input, and output modules. Subordinate modules are connected to the function processor to provide specific capabilities (e.g. Profibus communication, Ethernet communication, Analog Outputs).
  - The use of subordinate modules will be clarified in the U.S. EPR FSAR, Tier 2, Section 7.1.1.4.2.
- **8. Applicant states, "Each CU blocks its own outputs through the software of the CU." Explain how the system is protected if a failure happens such that a CU does not block its own output. Does the failure analysis bound this type of failure?**
  - If a CU does not block it's own outputs, then the divisional redundancy or the master CU within the division protects the system from a single failure. The worst case scenario is if a CU has a spurious output and does not block its own output. This condition is covered by the SAS failure modes and effects analysis (FMEA) as a undetected spurious failure.

Comments on RAI 505 Cont'd

RAI 505, Question 7.1-39

- **1. Applicant does not provide a methodology, as part of any testing that provides a programmatic means to verify self-testing periodically to meet the guidance of BTP 7-17. This would be inconsistent with how the applicant has treated the other PS/SAS/ RPMS and even DAS functionalities.**
  - Verification of self-test functionality is incorporated in the extended self-test. That test is described in a couple of places in ANP-10315P. The markup of that report for Revision 2 was submitted to the NRC in Supplement 19 of the response to RAI 505, Question 7.1-44. The extended self-test is run periodically. This test has been included in the Technical Specifications as a refueling test requirement. Successful performance of this test verifies the functionality of the cyclic self-test software. Detailed descriptions of the tests run as a part of the extended self test and the periodic self tests are included in the Revision 2 markup of ANP-10315P.

Comments on RAI 505 Cont'd

- **2. Applicant does not provide any additional information in ANP-10315P that demonstrates that surveillance testing or any periodic testing takes into account verifying self test functionality.**
  - See response to question 1.

Comments on RAI 505 Cont'd

- **3. The applicant's response relies heavily on the self testing software features themselves to verify their own operability and/or correct operation both software and hardware. In particular, for HW such as the watchdog timer (WDT), the applicant relies on the self testing software to verify its operation while the WDT uses a hardwired signal to do such things as initiate a reactor trip and self testing does not extend to hardwired component connections. There is a Phase 4 RAI concerning the Watchdog Timer functionality so until this RAI is received, its verifiability will be in question. Will not receive till 6/28/13. For example, if the SU changes the operating state of a function processor to Functional Test, that function processor would alter its data messages and receiving function processor, upon receiving those new messages would disregard them. Would this be an example of an independent way, in this case a human being initiating a change at the SU, of verifying self-testing functionality?**
  - The example suggested by the NRC would not fully test the functionality of the self-test. Therefore, it does not represent a full verification of the self-test features. The extended self-test provides the full verification of the self-test features.
  - The watchdog timer operation will be answered as part of RAI 542, Question 7.1-52.

Comments on RAI 505 Cont'd

- **4. Not clear how Channel comparison testing aspect is checked periodically. This comparison takes places in divisional gateways, they are NSR and not within the scope of Figure 2-1 of ANP-10315P, which shows the scope of surveillance testing. Important because applicant is crediting this function to replace daily/quarterly channel checks that are standard operating practices.**
  - In order to eliminate cross channel communication, the channel comparisons have been moved to the gateways that are on the communications network and receive but do not transmit information from PS or SAS. Whatever the requirement from Tech Specs is for a channel check on identical readings from the plant can be made either in the gateways or the servers, and alarm criteria set up to notify the operator if any of the readings go out of specification. AREVA will add a requirement in the Technical Specifications to verify the performance of the channel check every 31 days.

Comments on RAI 505 Cont'd

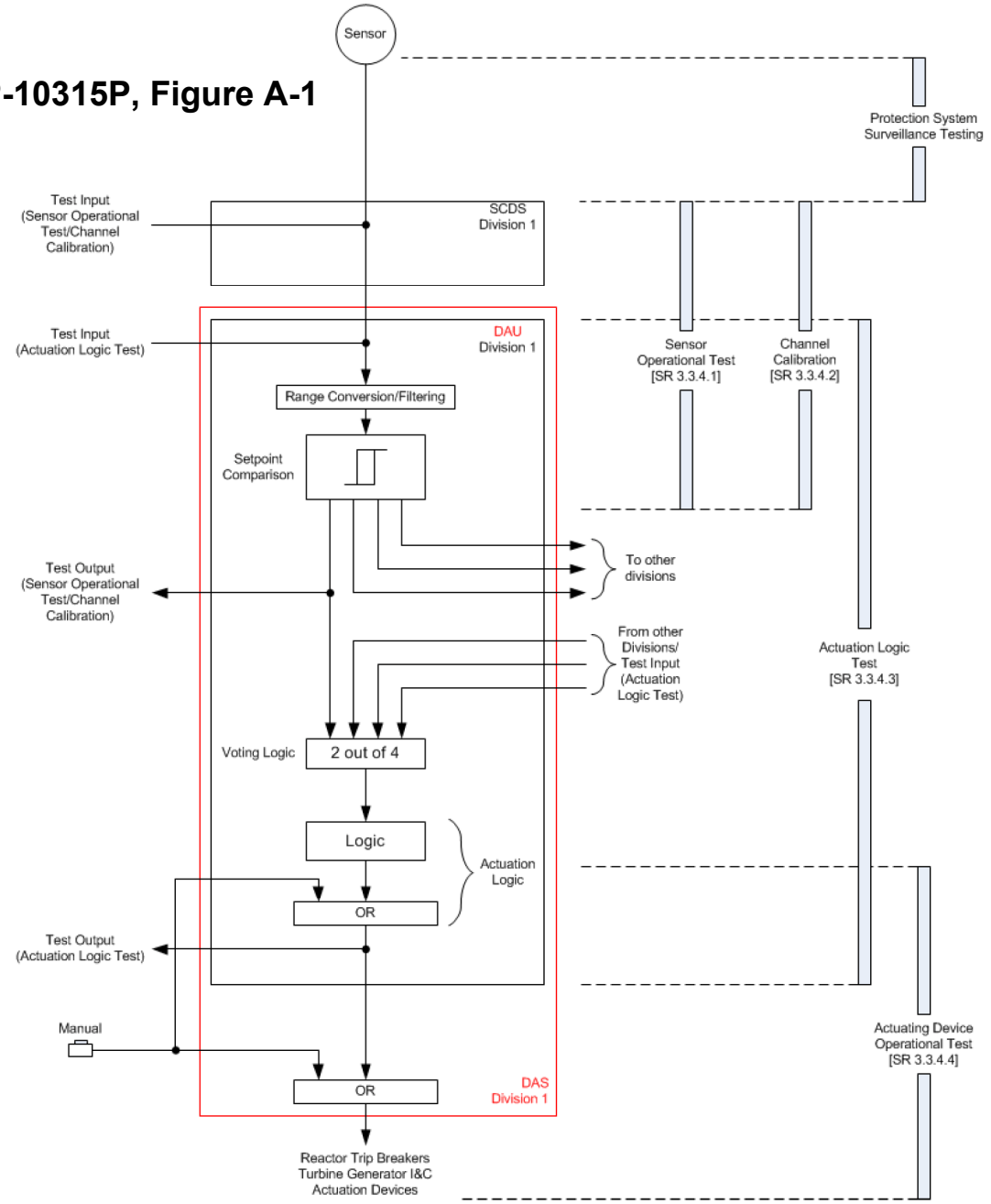
- **5. If things such as software/firmware/hardware changes are performed, how do the proposed indirect verifications ensure that credited self-testing is either unchanged, or provides the same level of detection in the presence of new or modified software/firmware/hardware?**
  - In the TXS platform, any changes that have to be made will require a plant modification. For those changes, appropriate testing will have to be done on the same level as the initial testing. The modification will have to contain whatever changes are necessary to also change the self testing software. This process will need to be similar to the process for doing the initial testing at the factory.
  - Changes to the operating system may or may not require changes to the self testing software.
  - Changes to the application software will be tested using SIVAT before installation, and any changes to the CRC sum of the memory section will need to be factored into the self testing.
  - These changes will be accomplished in accordance with the AREVA Software Program Manual, ANP-10272.

Comments on RAI 505 Cont'd

RAI 505, Question 7.1-44 (ANP-10315P)

- **1. For Figure A-1 [*shown on slide 17*], refer to the OR gate at bottom of figure. Does this device exist outside or inside DAS logic? Does the Manual signal go to this or gate or does it actually run through the DAS logic?**
  - The OR gate at the bottom of ANP-10315P, Figure A-1 is included as a part of DAS. The manual signal goes through both the DAS logic (inside the DAU) and this OR gate outside of the Diverse Actuation Unit (DAU). This figure and U.S. EPR FSAR Tier 2, Figure 7.1-13 will be revised to include the OR gate within the DAS system boundary.

Excerpt from ANP-10315P, Figure A-1



Comments on RAI 505 Cont'd

- **2. Regarding Appendix A – DAS: Per ANP-10304, DAS has associated setpoints that actuate after the PS. If so, why does the new DAS surveillance not take into account verifying this, and/or verifying some level of performance such as response time testing?**
  - ANP-10315P was created to describe the details of the surveillance testing defined by U.S. EPR FSAR, Tier 2, Chapter 16 (Technical Specifications). The DAS calibration surveillance verifies the setpoints in DAS. There is no DAS surveillance for response time testing. This is consistent with the ESBWR and APWR Technical Specifications.

Comments on RAI 505 Cont'd

- **3. Regarding Figure 2-5 – ESFAS No-Go Test – According to this drawing, this logic only tests for ESF/SAS functionality. Does this testing logic also include testing for SAS normal functions as well, such as CCWS Interlocking functions, etc.? Is this logic applicable to ALL SAS functions?**
  - The test configuration shown in ANP-10315P, Figure 2-5 applies to all SAS functions. ANP-10315P will be revised to reflect the fact that Figure 2-5 is a No-Go test configuration that applies to all SAS functions.
- **4. Referring to Page 2-41, what surveillance does the PACS loss of power testing fall under? Appendix C does not specify this.**
  - The PACS loss of power testing was included in the response to RAI Set 505, Question 7.1-45. This was to fulfill the requirements of IEEE 603-1998 Clause 5.5. A loss of power testing is not required in Technical Specifications. It is required in functional startup testing. The loss of power testing for I&C systems is addressed in U.S. EPR FSAR, Tier 2, Section 14.2. The PACS testing in Section 14.2 will be revised to include loss of power testing similar to the PS and SAS sections.

Comments on RAI 505 Cont'd

- **5. Referring to Table 2-5, second column, "Failures undetected by inherent features", what types of failures are represented? For the fourth column, what types of failures are represented?**
  - In ANP-10315P Table 2-5, the column titled "Failures undetected by inherent features" refers to failures that are not detected by the self-test features as part of the system software. An example is the temporary fault of RAM cells (e.g. a data error written into the RAM). This may affect the execution of a function, but may not be detectable by the self-test of the RAM because the RAM will be overwritten periodically.
  - In ANP-10315P Table 2-5, the column titled "Failures that are non-functional (failure does not prevent proper performance)" refers to failures that do not prevent the equipment from providing the proper execution of the function. Some examples of this are, failures of the LEDs resulting in wrong indication of operating status and a failure of the reset pushbutton (not used during normal operation).
  - Definitions for the column headings will be included in ANP-10315P.

Comments on RAI 505 Cont'd

- **6. Referring to Section 2.2.6.8, page 2-29: Discussion needs to be added on how a passed self test provides reasonable assurance of operability as the applicant committed to adding previously.**
  - A statement will be revised in ANP-10315P, Section 2.2.6.8 to say, "The self-monitoring functions confirm proper functioning of the safety function processors, the integrity of the installed code**, and provides reasonable assurance of operability**."

Schedule

- **Schedule for providing revised responses is provided in the presentation for closure of open items.**