

Public Meeting to Discuss U.S. EPR Design Certification I&C Chapter 7 Path Forward for Closure of Open Items

Chris Doyel
Rockville, Maryland
November 15, 2012



Purpose and Background

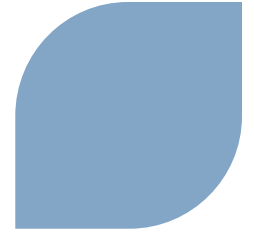
► Purpose

- ◆ Present schedule for U.S. EPR FSAR I&C Chapter 7 open item resolution
- ◆ Confirm agreement with the NRC on the I&C Chapter 7 path to closure technical approach for U.S. EPR Design Certification
- ◆ Identify future NRC/AREVA interaction opportunities

► Background

- ◆ May 2012 Schedule Letter
 - Identifies commitment dates for outstanding open items
- ◆ New Issues
 - RAI 555 Questions 7.1-53, 7.1-54, and 7.1-55

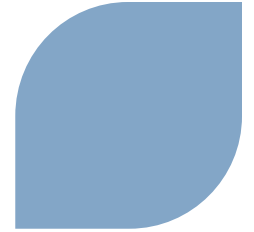
Status Summary of I&C Chapter 7 Open Items



* NRC to confirm agreement on status

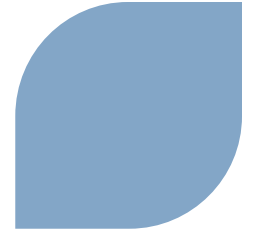
RAI	Question No.	Topic/Subject	Status *
505	07.01-33	SPND	Open
505	07.01-34	Details on the "maintenance laptop" and "test machine"	5/9/12 A
505	07.01-35	SAS Logics and FMEA	Open
505	07.01-36	SAS Voting	Open
505	07.01-37	SAS ITAAC	4/11/12 A
505	07.01-38	System recovery from a 'loss of power condition'	4/17/12 A
505	07.01-39	Self-Test Features	Open
505	07.01-40	failed self-test run	5/22/12 A
505	07.01-41	Define the terms such as 'halted', 'disabled' and 'out of service'	3/16/12 A
505	07.01-42	SAS is now covered by the scope of ANP-10315	1/19/12 A
505	07.01-43	SICS ITAAC	11/22/11 A
505	07.01-44	Self-testing Functionality	Open
505	07.01-45	PACS self-testing features	4/19/12 A
505	07.01-46	Operation I&C Disable Switch	4/27/12 A
505	07.01-47	PACS response time testing	5/22/12 A

Status Summary of I&C Chapter 7 Open Items



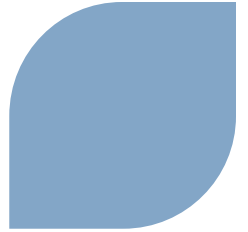
RAI	Question No.	Topic/Subject	Status
505	07.01-48	SAS compliance with IEEE Std. 603-1998	7/20/12 A
505	07.01-49	SAS compliance with IEEE Std. 603-1998, Clauses 6.6 and 6.7	5/29/12 A
505	07.01-50	Identify the approved version of Topical Report ANP-10272	4/18/12 A
505	07.01-51	Multiple TXS processor operating states	5/22/12 A
505	07.03-37	Turbine Trip Function	12/15/11 A
505	07.03-38	Compliance with IEEE Std. 603-1998, Clause 4	4/17/12 A
505	07.04-15	SICS - remote shutdown station	12/15/11 A
505	07.05-10	PAM - Regulatory Guide (RG) 1.97	3/16/12 A
505	07.05-11	COL Information Item for PAMS list	12/15/11 A
505	07.07-23	PICS environmental qualification	11/22/11 A
505	07.08-43	DAS and PS credited human diversity	12/15/11 A
505	07.08-44	Manual reactor coolant pump (RCP) trip	1/10/12 A
505	07.08-45	PS subsystem diversity descriptions	12/15/11 A

Status Summary of I&C Chapter 7 Open Items



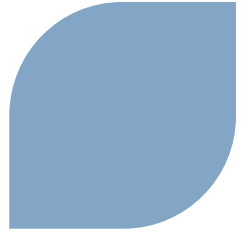
RAI	Question No.	Topic/Subject	Status
505	07.08-46	IEEE-603-1998, Clause 4.I - ITAAC	3/16/12 A
505	07.08-47	DAS test at power	4/3/12 A
505	07.08-48	SCDS credited quality assurance descriptions	1/10/12 A
505	07.08-49	Credited DAS "software structure"	12/15/11 A
505	07.09-71	SAS voting logic	4/27/12 A
505	07.09-72	Service Unit isolation switch	4/18/12 A
506	14.03.05-25 thru 14.03.05-42	SRP Section: 14.03.05 - Instrumentation and Controls - Inspections, Tests, Analyses, and Acceptance Criteria	Last - 5/30/12 A
512	07.08-50	SAS Common Cause Failure	7/20/12 A
542	07.01-52	Watchdog Timer	Open
555	07.01-53	PAS Failures	Open
555	07.01-54	Priority Module	Open
555	07.01-55	Operational I&C Disable Switches	Open

AREVA Plan to respond to Open Items



- ▶ **RAI 505, Question 7.1-33**
- ▶ **RAI 505, Question 7.1-35**
- ▶ **RAI 505, Questions 7.1-36, 39, and 44**
- ▶ **RAI 542, Question 7.1-52**
- ▶ **RAI 555, Question 7.1-54**
- ▶ **RAI 555, Question 7.1-55**
- ▶ **RAI 555, Question 7.1-53**

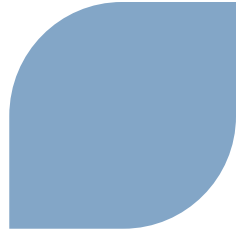
AREVA Plan to respond to RAI 505 Q 07.01-33



▶ The undetected failure of the most limiting SPND

- ◆ Refer to Public Meeting, October 4th, 2012 on AREVA
Approach to Detecting Failure of SPNDs – Closure Plan
to Respond to RAI 505 Question 07.01-33**

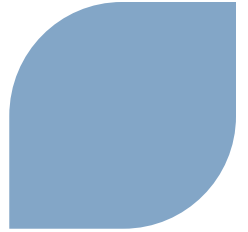
AREVA Plan to respond to RAI 505 Q 07.01-35



► SAS Logics and FMEA

- ◆ All follow-up question responses incorporated in final RAI draft response sent to NRC on 10/11/12. Pending NRC feedback.
- ◆ AREVA will revise the Component Cooling Water System/SAS Logic Diagrams based on initial NRC feedback.

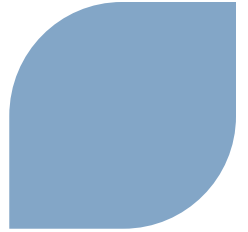
AREVA Plan to respond to RAI 505 Q 07.01-36, 07.01-39, 07.01-44



▶ SAS Voting, Self-Test Features, and Self-Testing Functionality

- ◆ Separate presentation given today, November 15, 2012.**

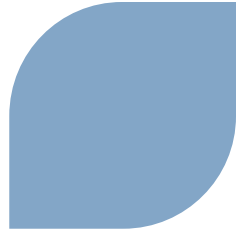
AREVA Plan to respond to RAI 542 Q 7.1-52



► Watchdog Timer

- ◆ AREVA will provide a description and diagrams illustrating how the Teleperm XS watchdog timer would be able to execute the reactor trip function if all Actuation Logic Unit (ALU) processors lock-up, and describe the dependency on the ALU software and hardware to perform its functions.
- ◆ AREVA will update ANP-10315P Self Testing Technical Report to provide the watchdog timer details requested in this RAI.

AREVA Plan to respond to RAI 555 Q 7.1-54

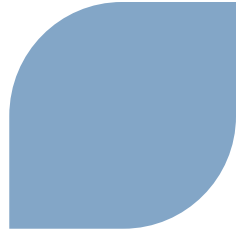


► Provide an analysis of the priority logic scheme for the U.S. EPR I&C systems

◆ AREVA will update the U.S. EPR FSAR to provide:

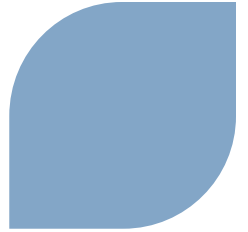
- Description of latched and unlatched implementation in I&C systems
- How a latched actuation signal confirms completion of the function
- Design criteria of manual and automatic unlatching
- Design criteria for implementing latching and unlatching
- Explanation of latching in the PACS
- Design criteria for the use of pulse signals
- How time delays are implemented
- Describe the failures of time delays
- Diagram(s) for the priority logic of the PACS

AREVA Plan to respond to RAI 555 Q 7.1-54



- ◆ **AREVA will update Technical Report ANP-10315P to provide:**
 - Discussion of how latching/unlatching functionality is verified
- ◆ **AREVA will provide an explanation of specific examples of how the systems interface with each other through the priority logic for certain functions in the RAI response.**

AREVA Plan to respond to RAI 555 Q 7.1-55

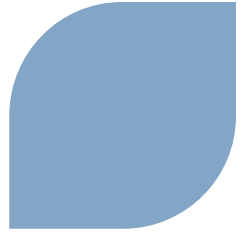


► Operational I&C Disable Switches (OPDIS)

◆ AREVA will update the U.S. EPR FSAR to include:

- When the OPDIS switch is used
- OPDIS consideration in safety analysis
- OPDIS switch's effects on the PAS and PICS
- OPDIS implementation in PACS
- Implementation of voting on the OPDIS switches
- SICS manual component level interface with PAS
- Surveillance requirement for OPDIS

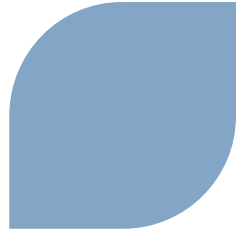
AREVA Plan to respond to RAI 555 Question 7.1-53



- ▶ **PAS/PICS Failures Affecting Safety Related Equipment**
 - ◆ **“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.”**

AREVA Plan to respond to RAI 555

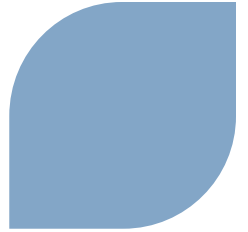
Question 7.1-53



Specifically, the staff requested the following:

- 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 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.**

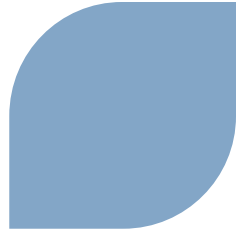
AREVA Plan to respond to 7.1-53 Current Design Approach



► Postulated failures of non-safety-related control systems are considered in Chapter 15 analyses of AOOs and PAs

- ◆ Postulated failures for Chapter 15 analyses of Anticipated Operational Occurrences (AOOs) and Postulated Accidents (PAs) are described in Section 15.0 of Standard Review Plan
 - Evaluation of AOOs and PAs must consider performance of credited protection or safety systems, including the effects of most limiting single active failure.
 - *Single Failure*. “An occurrence that results in a components loss of capability to perform its intended safety functions.”
 - *Common-Mode Failure*. “The result of an event which, because of dependencies, causes a coincidence of failure states of components in two or more separate channels of a redundant system, leading to the failure of the defined system to perform its intended function.”

AREVA Plan to respond to 7.1-53 Current Design Approach

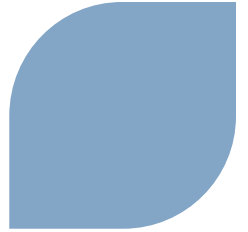


► Non-Safety-Related Control System Failures Postulated for U.S. EPR

- ◆ U.S. EPR non-safety-related control systems are not credited for the mitigation of any Chapter 15 AOOs or PAs. U.S. EPR safety-related control systems are credited for the mitigation of Chapter 15 AOOs and PAs.
- ◆ Postulated failures of non-safety-related control systems can affect mitigation of Chapter 15 AOOs and PAs in two ways: (1) non-safety-related (NSR) to safety-related (SR) control system interactions, and (2) NSR control system actions.

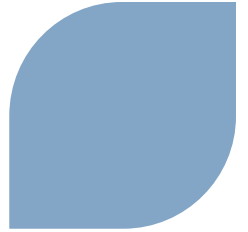
AREVA Plan to respond to 7.1-53

Current Design Approach



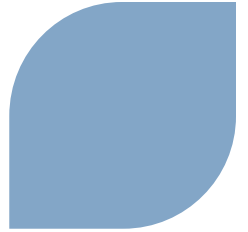
1. Non-safety-related to safety-related control system interactions
 - PICS/PAS can provide component level commands (e.g., open MSIV) and group commands (e.g., start safety injection) to safety-related plant equipment.
 - Single failures of safety-related equipment only are postulated in Chapter 15 safety analysis.
 - Effects of non-safety-related control system failures are treated as initiating events and limited to spurious actuation of at most one train of safety-related equipment for one function.
2. Non-safety-related control system actions
 - PICS/PAS provide indication and control of non-safety-related plant equipment.
 - Failures of PICS/PAS affecting non-safety-related plant equipment are included as a part of the Chapter 15 initiating events (e.g., feedwater heater bypass valve opens causing overcooling event).
 - Effects of non-safety-related control system failures are treated as initiating events and limited to spurious actuation of at most one train of non-safety-related plant equipment for one function.

AREVA Plan to respond to 7.1-53 NRC Guidance for Digital I&C



- ▶ From ISG-4, Rev. 1, STAFF POSITION, 3.1 Independence and Isolation, 5. Malfunctions and Spurious Actuations:
- ▶ Safety and control processors should be configured and functionally distributed so that a single processor malfunction or software error will not result in spurious actuations that are not enveloped in the plant design bases, accident analyses, ATWS provisions, or other provisions for abnormal conditions. This includes spurious actuation of more than one plant device or system as a result of processor malfunction or software error. *The possibility and consequences of malfunction of multiple processors as a result of common software error must be addressed.*
- ▶ No single control action (for example, mouse click or screen touch) should generate commands to plant equipment. Two positive operator actions should be required to generate a command.

AREVA Plan to respond to 7.1-53 NRC Guidance for Digital I&C



- ▶ **From ISG-4, Rev. 1, STAFF POSITION, 3.1 Independence and Isolation, 5. Malfunctions and Spurious Actuations: Cont'd**
- ▶ Stations which are not safety-related should be shown to produce no spurious actuations and to have no adverse effect upon any safety-related equipment or device as a result of a design basis condition, both during the condition and afterwards. *If spurious or abnormal actuations or stoppages are possible as a result of a design basis condition, then the plant safety analyses must envelope those spurious and abnormal actuations and stoppages.*
- ▶ **From Standard Review Plan 7.7**
- ▶ Effects of control system failures – The review should confirm that the failure of any control system component or any auxiliary supporting system for control systems does not cause plant conditions more severe than those described in the analysis of anticipated operational occurrences in Chapter 15 of the SAR. This evaluation should address failure modes that can be associated with digital systems such as software design errors as well as random hardware failures. *(The evaluation of multiple independent failures is not intended.)*

AREVA Plan to respond to 7.1-53

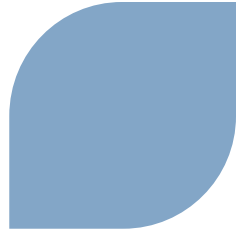
► AREVA will clarify the requirements of PAS and PICS in accordance with NRC guidance in ISG-04 as follows:

1. The existing PAS design meets the requirements of ISG-04 with respect to minimizing the potential for multiple spurious failures. The PAS design utilizes the principles of :

- Redundancy
- Independence
- Segmentation
- Physical Separation
- Electrical Isolation and Separation
- For software, uses the same processes and procedures as safety related software per ISG-04

These requirements will be added to the FSAR Section 7.1.1.4.6
Process Automation System.

AREVA Plan to respond to 7.1-53

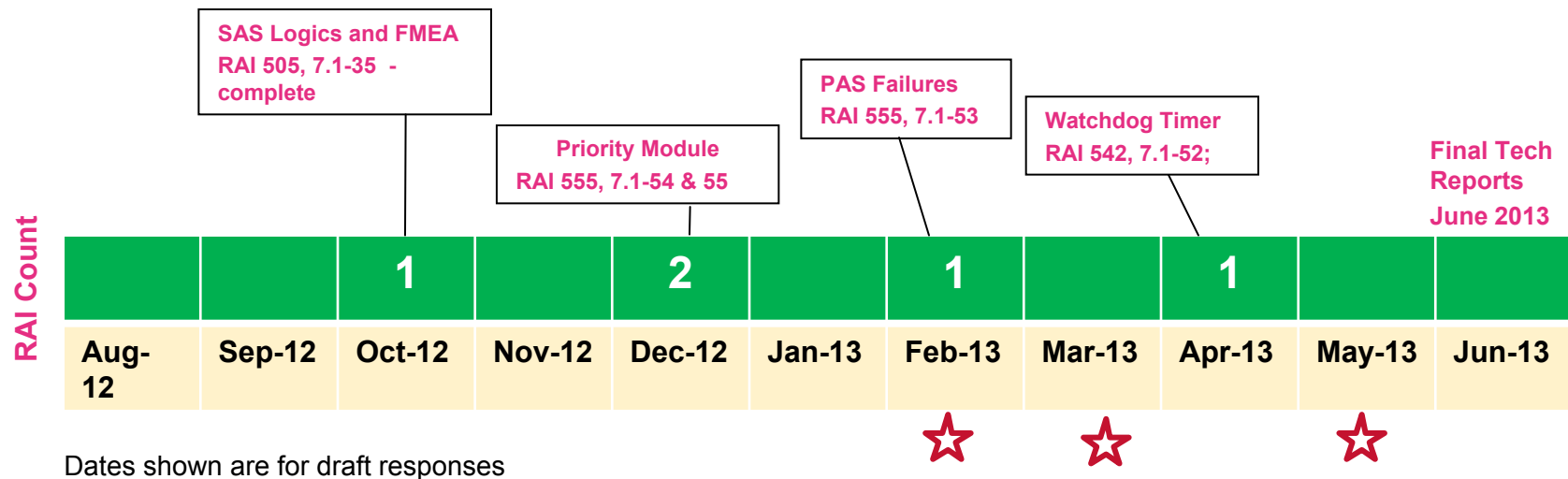


2. The existing PICS design meets the requirements of ISG-04 with respect to minimizing the potential for multiple spurious failures. The PICS design utilizes the principles of :
 - Two operator actions where appropriate (see ISG-04)
 - Redundancy
 - Independence
 - EMI/RFI Qualification
 - Electrical Isolation and Separation

These requirements will be added to the FSAR Section 7.1.1.4.6
Process Automation System.

3. U.S. EPR Tier 1 will be revised to include an ITAAC for PICS and PAS confirming the design requirements listed in items 1 and 2.

U.S. EPR FSAR I&C Chapter 7 Timeline



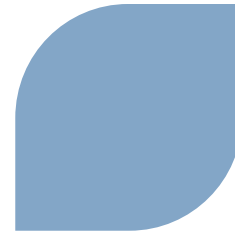
★ = Proposed NRC Interaction (audit) opportunity

Schedule of I&C Chapter 7 Open Items

RAI	Question No.	Topic/Subject	Draft to NRC	Final to NRC
505	07.01-35	SAS Logics and FMEA	10/11/2012 A	11/13/2012
505	07.01-36	SAS Voting	5/1/12 A	12/19/2012*
505	07.01-39	Self-Test Features	3/22/12 A	12/19/2012*
505	07.01-44	Self-testing Functionality	3/5/12 A	12/19/2012*
542	07.01-52	Watchdog Timer	4/25/2013	6/28/2013
555	07.01-53	PICS/PAS Failures	2/1/2013	4/1/2013
555	07.01-54	Priority Module	12/20/2012	2/21/2013
555	07.01-55	Operational I&C Disable Switches	12/20/2012	2/21/2013
N/A	N/A	ANP-10304 D3 Tech Report – Rev 6	N/A	6/28/2013
N/A	N/A	ANP-10315 Self Test Tech Report – Rev 2	N/A	6/28/2013
N/A	N/A	ANP-10309 PS Tech Report – Rev 5	N/A	6/28/2013
N/A	N/A	ANP-10310 Priority Module Tech Report – Rev 2	N/A	6/28/2013

* Responses were previously sent final and will be updated to reflect NRC feedback, if required.

Interaction Opportunities



► NRC/AREVA Interaction Opportunities

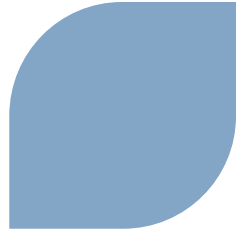
◆ Telecons

- Technical Meetings/Telecons [as needed]
 - Discuss NRC feedback on RAI responses

◆ Audits and Public Meetings

- February 2013 Audit of RAI 505; RAI 555 – Q 7.1-54 & 55
- March 2013 Audit of RAI 555 – Q 7.1-53
- May 2013 Audit of RAI 542 – Q 7.1-52

Acronyms



- ▶ AOO – Anticipated Operational Occurance
- ▶ ATWS – Anticipated Transient without SCAM
- ▶ COL – Combined Operating License
- ▶ DAS – Diverse Actuation System
- ▶ FMEA – Failure Modes and Effects Analysis
- ▶ FSAR – Final Safety Analysis Report
- ▶ I&C – Instrumentation and Control
- ▶ IEEE – Institute of Electrical and Electronic Engineering
- ▶ ISG – Interim Staff Guidance
- ▶ ITAAC - Inspections, Tests, Analyses, and Acceptance Criteria
- ▶ MSIV – Main Steam Isolation Valve
- ▶ PA – Postulated Accident
- ▶ PACS – Priority and Actuator Control System
- ▶ PAM – Post Accident Monitoring
- ▶ PAS - Process Automation System
- ▶ PICS - Process Information and Control System
- ▶ PS - Protection System
- ▶ RAI – Request for Additional Information
- ▶ SAS - Safety Automation System
- ▶ SICS - Safety Information and Control System
- ▶ SPND - Self Powered Neutron Detector
- ▶ SU - Service Unit
- ▶ TXS - Teleperm XS