

REQUEST FOR ADDITIONAL INFORMATION (RAI)

OCONEE NUCLEAR STATION, UNITS 1, 2, AND 3 (OCONEE)

DIGITAL UPGRADE OF REACTOR PROTECTIVE SYSTEM (RPS) AND ENGINEERED

SAFEGUARDS PROTECTIVE SYSTEM (ESPS)

The Nuclear Regulatory Commission (NRC) staff's questions in this RAI are developed from the review of the license amendment request (LAR) dated January 31, 2008, and the NRC staff's May 2008 visit to Oconee. Please provide a response to each question first writing the question followed by the Duke Energy Carolinas, LLC's (Duke's) response to those questions. If the requested information has already been provided to the NRC staff, please specifically identify where this information is located in the docketed documentation.

MAY 2008 Trip Report Items

The May 2008 trip report dated July, 23, 2008 (ML081900197), identified the following action items and questions under different topics:

Diversity and Defense-in-Depth (D3)

1. Please provide a description of how adding diverse low-pressure injection (LPI) and high-pressure injection (HPI) have changed the results and conclusion of the D3 analysis.
2. Please provide setpoints for actuation of the LPI and HPI systems that were used in the D3 analysis.
3. Please provide a summary of the D3 assessment that includes the following:
 - (a) Explanation that the two-minute reactor trip has always been a part of the Oconee licensing basis and is currently required with the RPS/ESPS system and will continue to be required after the new digital system is installed.
 - (b) Description of what diverse indications are available to the operator and describe any affect that a software common mode failure would have on operator interpretation of the event.
 - (c) Describe the built-in conservatism of the D3 best-estimate analysis program regarding the analyzed plant responses to Chapter 15 design-basis accidents (DBAs) with a software common cause failure (SWCCF).
4. Please provide a qualitative discussion of the expected outcome of events where fuel damage occurs.

Communications

5. Please provide data verifying the one-way communication link of the Port Tap with the external plant data systems.
6. Please provide documentation to demonstrate that the isolation communication processor is on the SVE2 board.

The NRC staff was provided a copy of the December 13, 2006 (ML070080325), briefing slides on the digital replacement project that in part, addressed safety-related (SR) inter-channel and SR channel to non-SR systems data communications. Please provide an explanation for the following questions to facilitate the NRC staff's understanding of the Oconee Teleperm XS (TXS) platform design features.

7. Slide 5 - The 3rd bullet says that "only static memory allocation is used." Please explain when this allocation is done, and how it is controlled. Is either static or dynamic memory re-allocation performed at any time after the original compiling from the "C" code?
8. Slide 23 - This slide shows the communications method used to demonstrate independence. The slide shows the safety function processors, DPRAM, SL21 boards, and the SLLM. The SL21 is labeled as the buffer circuit. Is there an interposing communications processor, and if so, where is it located? Please provide a circuit diagram or schematic showing the interposing communications processor, and its connections to other circuits.
9. Slide 24 - This slide shows a figure from Annex G of the Institute of Electrical and Electronics Engineers (IEEE) Std 7-4.3.2. This annex was not indorsed by the staff, because use of a buffer circuit without an interposing communications processor was considered insufficient isolation. Is this method of isolation the one used for the Oconee digital safety system?
10. Slide 27 - The 3rd bullet says the cyclic data transfer has a predefined package size, constant bus load and age monitoring.
 - (a) Please define the package size and show the bit allocation for the message. Is this a standard bus protocol, and if so, which is it?
 - (b) Please define the bus load, show what it is, and how often a message is sent. Define what units are on the bus, and under what conditions each is the bus master.
 - (c) How is the checksum generated, and how is the message age monitoring accomplished?
 - (d) How does usage of a bus meet the Interim Staff Guidance (ISG) 4 requirement that all communications be point-to-point?
11. Slide 27 - The 4th bullet says there is no dynamic allocation of resources. Is there static allocations of resources?

12. Slide 27 - The 7th bullet mentions a simple type of multi-tasking. Please define the multi-tasking, and show how it is done without using interrupts. The bullet also mentions the service commands. What commands are considered service commands, how are they sent to the safety processor, and under what conditions.
13. Slide 28 - The 7th step of the cyclic operations is shown as “write output data.” Is this considered inter-channel or safety to non-safety communications. Please show all output data possible, and where it is written to. If this data can go to more than one place, show how the routing is accomplished.
14. Slide 29 - This slide shows the cyclic signal processing. Please provide a detailed description of each of the elements, including bit size and allocation, time for each portion of the processing, and a description of how each portion is generated and used.
15. Slide 30:
 - (a) The 1st bullet says that a fiber optic medium is used. Is this two fibers, each with one-way transmission, or a single fiber with two-way transmission?
 - (b) The 3rd bullet speaks of avoidance and independent control. How is this done? If channel A and channel B are communicating, where is the data stored? Is the communications processor synchronized with the safety processor, and if so, how?
 - (c) The 5th bullet mentions “not-a-number checking.” What is this, and how is this done?
 - (d) The 6th bullet states that on-line validation limits the propagation of faulty data. How does this on-line validation differentiate between faulty data and data rapidly changing from a rapidly changing plant condition?
16. Slide 32:
 - (a) The 1st bullet states there is a “separate logical MicroNET communications channel for each message.” Is the separate channel a physical point-to-point transfer, or is this a logical point-to-point transfer?
 - (b) The 1st bullet also mentions a “unique MicroNET communications interface.” Please define this interface in detail.
 - (c) The 3rd bullet mentions the standard header. Please provide the size, bit definition and coding for each of these portions of the header. Where and how is each of these generated?
 - (d) The 4th bullet states “Message size determined individually for each message ...” Please list the different types of messages, what the message size is, how this message size was determined, and what the content of each message is, by bit definition.
17. Slide 37 - This slide discusses the received message checking.

- (a) Is this checking done by the interposing communications processor or by the safety processor?
 - (b) The 3rd check shown is for sequence number. What occurs if a sequence number is skipped?
 - (c) How many numbers must be skipped to trigger a communications fault?
 - (d) Is there a memory of missed messages, that is, what would happen if every other message was missed?
18. Slide 38 - This slide discusses message age monitoring. When ONE_MISS status is present, how long will the previous message be used? This seems to indicate only one cycle, but the staff had previously been told the previous message could be used for 200 ms.
19. Slide 39 - This slide on message age monitoring says an error situation will exist if a data message is not received by the runtime environment (RTE) for two or more cycles.
- (a) Is this two or more cycles of the interposing communications processor or of the safety processor?
 - (b) How are the two processors synchronized?
20. Slide 42 - This slide has a green box which says "Use of inter-channel communications does not create new interfaces, it simply changes the location of the interconnections."
- (a) Does this mean that the inter-channel communications and safety to non-safety communications use the same buffers, fiber optic lines, etc.? If this is true, would this also mean that there is one bus or LAN for both types of communications, and therefore there are non-safety devices on the bus or LAN used for inter-channel communications?
 - (b) Please justify this, and show how point-to-point communications are used.
21. Slide 44 - The 3rd bullet of this slide states that an alarm indication is initiated by the on-line signal validation.
- (a) Will this alarm trigger a limited condition of operation (LCO)? If not, why?
 - (b) What will be done by the operators or technicians in response to this alarm?
22. Slide 45 - This slide shows error information from the TXS being transferred to the service unit and alarms. Please describe in detail how this is done, and what equipment is involved.
23. Slide 46 - This slide shows a wide black line extending horizontally from each SAA1. What is it?

24. Slide 48 - The 2nd bullet of this slide states that the 2nd min/2nd max logic will prevent an “overly conservative spurious trip.”
 - (a) Can this feature mask a sensor failure?
 - (b) Will a sensor failure still result in an LCO for the respective channel?
25. Slide 51 - This slide discusses the automated channel check logic.
 - (a) Please list all equipment and logic checked during the current (analog system) channel checks, and compare this to the equipment and logic which would be checked by an automated channel check.
 - (b) Does the current channel check test the sensor wires to the trip system, and will this still be checked by the automated channel check?
26. Slide 54:
 - (a) The drawing seems to indicate that communications between the various TXS RPS/ESF channels and the voters is via the Monitoring and Service Interface (MSI). Is this correct?
 - (b) The drawing shows an ethernet switch between the Netoptics unit and the service unit. What is the function of this switch? What other devices are attached to this switch?
 - (c) Please define the boundary of the safety to non-safety border.
27. Slide 58:
 - (a) The staff believes this is a logic view, and not a physical representation of the logic. Please confirm this understanding.
 - (b) If this is correct, the failure of an input line would also be a failure of that line wherever it is physically used. What are the other uses of this line, and how are the additional subsequent failures taken into account?
28. Slide 60 - This slide shows that the parameter change enable key switch does not, as required by ISG #4, create a “physical cable disconnect, or by means of keylock switch that either physically opens the data transmission circuit or interrupts the connection by means of hardwired logic”, but rather sets a bit in a register. Why is this permissible, and why is this type of logic used in a safety-related system.
29. Slide 63 - This slide shows data flow for various types of messages. Does the notation →CPU) or (CPU→) refer to the MSI, and if so, why was this not shown in that manner?
30. Slide 64:

- (a) Are the yellow lines Profibus between the various RPS channels and the MSI/RPS E?
 - (b) There is a vertical black line connecting the service unit, the TXS gateway and the line from the MSI / RPS E. This line extends beyond those units. Please define this line, and list all devices attached to this line, or which could be attached to this line in other applications.
31. Slide 65 - This slide states that signaling messages are assembled in phase 6 of every cycle (see slide 35, 1st sub-bullet). Does this mean all messages to all devices are assembled in phase 6, and sent in phase 7? Please provide an exact description of what occurs in every part of phases 6 and 7, in what order, and how this order is controlled.
32. Slide 66:
- (a) The 1st bullet discusses information commands allowed during normal operations. The read back and request for repeated transmission would indicate there is two-way communications between the non-safety service unit and the safety system during normal operation, even when the key switch is not released. Please confirm this.
 - (b) The 5th sub-bullet mentions “trace data for Ocone.” What is this and how is it used?
33. Slide 68 - The 5th sub-bullet on this slide states that service commands are accepted for execution if the “Service command is permitted for execution in the current RTE operation mode.” Please list each service command, and under what conditions could it be executed. Of particular interest are those service commands which could be executed with the TXS on-line and performing its safety function.
34. Slide 69:
- (a) This slide mentioned protocols for communications independence for two-way communications. Please provide the definition of those protocols.
 - (b) The 4th sub-bullet states that there is no “strong” response time requirement. What is the response time requirement?
 - (c) Please define, in detail, the signaling messages mentioned in the 5th sub-bullet.
35. Slide 71:
- (a) Please redraw this slide to show exactly where and how each task is entered and exited. What triggers the departure from each task?
 - (b) How is the time available for the self-test task determined, and by what?
36. Slide 75 - This slide discusses communication with the service unit. Please describe the isolation of the service unit from other non-safety plant equipment, and how that isolation will be maintained.

37. Slide 78:

- (a) The 1st bullet and sub-bullet says the RTE is “similar” to the RTE of function computers. Please explain what “similar” means, and specifically point out any differences.
- (b) Please provide an exact definition, format, bit assignment, and method of formatting for each type of data, service and signaling message, and when each is used.
- (c) The 4th bullet mentions the one-way communications device. Please describe this device in detail, and in particular, provide sufficient information so the staff can confirm the one-way nature of this device.

ISG 4), staff positions # 3, 9, 10, 11,12, 14, 18, 19, and 20 in Enclosure 3 of Supplement 2, “Position Paper on Alignment of Oconee RPS/ESPS with ISG#4 (AREVA Document No. 51-9076647)” need additional information to sufficiently address the ISG Staff positions as follows:

38. Staff position #3 states: “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. Receipt of information that does not support or enhance the safety function would involve the performance of functions that are not directly related to the safety function. Safety systems should be as simple as possible. Functions that are not necessary for safety, even if they enhance reliability, should be executed outside the safety system. A safety system designed to perform functions not directly related to the safety function would be more complex than a system that performs the same safety function, but is not designed to perform other functions. The more complex system would increase the likelihood of failures and software errors. Such a complex design, therefore, should be avoided within the safety system.”

Since the staff has not received the previously requested detailed message formats and bit assignments, please provide this information along with an explanation of how each of these messages enhances the performance of the safety function. Particular care should be given to the reason why this enhancement is necessary, and why this method was chosen, and how it is necessary and related to the safety function.

39. Staff position # 9 states: “Incoming message data should be stored in fixed predetermined locations in the shared memory and in the memory associated with the function processor. These memory locations should not be used for any other purpose. The memory locations should be allocated such that input data and output data are segregated from each other in separate memory devices or in separate pre-specified physical areas within a memory device.”

Please describe how the memory locations within the shared memory are allocated and fixed. The staff has been told this occurs when the software is compiled, but does not understand how this is done, how the memory allocation is fixed, what would occur if more memory is allocated than is physically present, and how the transmitting and receiving units know what the allocation is, and how to use that data.

40. Staff position # 10 states: "Safety division software should be protected from alteration while the safety division is in operation. On-line changes to safety system software should be prevented by hardwired interlocks or by physical disconnection of maintenance and monitoring equipment." This section goes on to state: "A workstation (e.g. engineer or programmer station) may alter addressable constants, setpoints, parameters, and other settings associated with a safety function only by way of the dual processor/shared memory scheme described in this guidance, or when the associated channel is inoperable. Such a workstation should be physically restricted from making changes in more than one division at a time. The restriction should be by means of physical cable disconnect, or by means of keylock switch that either physically opens the data transmission circuit or interrupts the connection by means of hardwired logic."

The staff understands that the Areva TXS system proposed for use at Oconee uses key switches that sets a bit within memory, and does not use a physical disconnect. This would appear to conflict with staff guidance. Please explain why the TXS system should be approved. Include in the discussion any additional protection which may exist, or what additional protection will be provided by Oconee, beyond the normal key protection, sign-out requirements, and administrative activities which would also be used for a physical disconnect key switch.

41. Staff position # 11 states: "Provisions for interdivisional communication should explicitly preclude the ability to send software instructions to a safety function processor unless all safety functions associated with that processor are either bypassed or otherwise not in service. The progress of a safety function processor through its instruction sequence should not be affected by any message from outside its division. For example, a received message should not be able to direct the processor to execute a subroutine or branch to a new instruction sequence."

Please provide a detailed description of how interdivisional communication explicitly precludes the ability to send software instructions to a safety function processor, and how receipt of a message about the unavailability of a sensor will not direct the processor to branch to a new instruction sequence.

42. Staff position # 12 states: "Communication faults should not adversely affect the performance of required safety functions in any way."

Please provide the detailed message formats and bit assignments, with an analysis of how an error in each part of the message would be detected. This information is similar to that requested for staff position # 3.

43. Staff position # 14 states: "Vital communications should be point to point by means of a dedicated medium (copper or optical cable). In this context, "point to point" means that the message is passed directly from the sending node to the receiving node without the involvement of equipment outside the division of the sending or receiving node. Implementation of other communication strategies should provide the same reliability and should be justified."

The TXS system proposed for use at Oconee does not appear to use point-to-point communications, please provide a detailed description of the communications methods used. In particular, please show any instances where more than one communications link used the same wires or fiber, any instance where the same communications port or

hardware is used, or where more than one communications link used the same software to process the data.

44. Staff position # 18 states: "Provisions for communications should be analyzed for hazards and performance deficits posed by unneeded functionality and complication."

Please provide this analysis.

45. Staff position # 19 states: "If data rates exceed the capacity of a communications link or the ability of nodes to handle traffic, the system will suffer congestion. All links and nodes should have sufficient capacity to support all functions. The applicant should identify the true data rate, including overhead, to ensure that communication bandwidth is sufficient to ensure proper performance of all safety functions. Communications throughput thresholds and safety system sensitivity to communications throughput issues should be confirmed by testing."

Please show how Oconee identified the true data rate, including overhead, to ensure that communication bandwidth was sufficient to ensure proper performance of all safety functions. Please provide the information on the true data rate and overhead. In addition, please show how this was tested.

46. Staff position # 20 states: "The safety system response time calculations should assume a data error rate that is greater than or equal to the design basis error rate and is supported by the error rate observed in design and qualification testing."

Please provide these calculations and design-basis data error rate, and how this was tested.

Software Program Manual

47. Please provide the copy of Office Instruction, OI-1457, "TELEPERM XS Software Quality Assurance Plan," that is applicable to the Oconee RPS/ESPS project.
48. Please provide the latest applicable copy of AREVA NP Inc. Document No. 51-9001942-004, "Oconee Nuclear Station, Unit 1 RPS/ESPS Controls Upgrade Software Generation and Download."

Verification and Validation (V&V)

49. Please provide a detailed description of the Duke review and oversight activities of the Oconee safety system V&V efforts, which were performed by its vendor.

Factory Acceptance Test (FAT)

50. Please provide an explanation of what documentation is impacted by the change in the testing strategy, summarizing the impact, and providing a schedule for the submittal of the revision to these documents.

Exceptions

51. Please provide the documentation identifying all standards used by the supplier and any deviations from these standards, including any associated acceptability determination.

Changes

52. Please provide an explanation of the changes to the TXS system since the TXS Topical Report that includes a fact-based explanation of changes, and an explanation of how these facts can be combined to arrive at an acceptability determination.

Quality Management Plan

53. Please provide an explanation of the Duke review of documentation produced by its vendor, and of Duke's vendor audit activities: (a) a detailed explanation of the activities requested, (b) providing examples of the issues identified by Duke, and (c) how issues were resolved.

LAR Review Items- Questions on Software

General Questions

54. (a) What conventions are followed to identify requirements within:
- (1) AREVA NP Inc. Office Instructions (OIs)
 - (2) Project-Specific Plans
 - (3) Software Requirements Specifications (SRSs)
- (b) Where are these conventions documented?

These questions have been misunderstood in the past, and therefore clarification is provided in the form of a definition and examples.

Convention: a: usage or custom
b: a rule of conduct or behavior
c: an established technique, practice, or device

Examples: ANSI/IEEE Std 829-1983: "The words *shall*, *must* and the imperative form identify the mandatory material within this standard. The words *should* and *may* identify optional material."

IEEE Std 1219-1998: "The words *shall* and *must* identify the mandatory (essential) material within this standard. The words *should* and *may* identify optional (conditional) material."

ANSI/IEEE Std 1008-1987: "The word *must* and imperative verb forms identify the mandatory material within this standard. The words *should* and *may* identify optional material."

55. In defining the inputs for the software development effort, Duke produced:
- 1 OSC-8623, "RPS & ESPS System Functional Description," also identified by AREVA NP Inc., Doc. No. 32-5061401-006.
 - 2 OSC-8695, "Unit 1 Software Parameters for TXS Plant Protection System," also identified by AREVA NP Inc., Doc. No. 32-507267-002

OSC-8623 requires that “Actual in-plant setpoints are listed in OSC-8695...” The RTM shows OSC-8695 as input to the SRS, which is an input to the Software Design Description (SDD); however, OSC-8695 could not have been created without using the SDD as an input; the SDD is listed as an input to OSC-8695.

Please describe the role and use of OSC-8695 in the software development process.

Supplement 2 Questions

The following questions were identified during the review of Supplement 2 (ML081260167).

56. NUREG-0800 (SRP), Chapter 7, Branch Technical Position 7-14, Section B.3.1.1 contains acceptance criteria for Software Management Plans. Supplement 2 does not describe the documentation of the plan for software management.

Please provide a description of how the SRP acceptance criteria associated with the Software Management Plan (SMP) are addressed in the LAR and its supplements.

57. NUREG-0800 (SRP), Chapter 7, Branch Technical Position 7-14, Section B.3.1.2 contains acceptance criteria for Software Development Plans. Supplement 2 does not describe the documentation of the plan for software development.

Please provide a description of how the SRP acceptance criteria associated with the Software Development Plan (SDP) are addressed in the LAR and its supplements.

Requirements Traceability Matrix (RTM) Questions

An RTM is one effective way to assure that all requirements have been implemented. Oconee has used an RTM (AREVA NP Inc., Document No. 51-9062040-002) for this assurance. The following questions regarding the RTM were identified during the review process, and are based on the following three quotations from AREVA NP Inc’s, documents.

The Software Verification and Validation Plan (SVVP), AREVA NP Inc., Doc. No. 51-9010419-005, states:

Proprietary [[

]]

]]

The Requirements Verification and Validation (V&V) Activity Summary Report, AREVA NP Inc., Doc. No. 51-9056720-001, states (Section 4.1.1.4, page 22):

Proprietary [[.

]]

58. Oconee Calculation OSC-8623, Rev. 5 (also called AREVA NP Inc., Doc. No 32-5061401-006), “RPS &ESFAS System Functional Description” states: “Actual in-plant setpoints are listed in OSC-8695...” The SVVP requires that the requirements from the software parameters document be traced in the software requirements traceability analysis, and that each requirement traced be cut and past into the RTM.

- (a) The software parameters document (AREVA Doc No. 32-5072673-001) is referenced as a source of requirements in the Oconee RTM, but most of its requirements are not included in the RTM. Please explain why.
- (b) Section 4.1.1.2 of Requirements Verification and Validation (V&V) Activity Summary Report, AREVA NP Inc., Doc. No. 51-9056720-001, does not identify that the software parameters document was used in the software requirements traceability analysis. Please explain why.

SDD Section 3.4 states: "The ONS Parameter Calculation OSC-8695 ... defines the necessary values for those parameters associated with plant specific design basis information."

- (c) Please describe how it was verified, and documented, that these "actual in-plant setpoints" have been implemented in the RPS/ESPS system.
 - (d) Please identify the location in the LAR and associated documentation that demonstrates that these "actual in-plant setpoints" have been verified as being implemented in the design, or provide such documentation.
59. The Requirements V&V Activity Summary Report does not identify, as an open item, that "actual in-plant setpoints," identified in OSC-8695, are not incorporated into the Software Requirements Matrix (SRM); please explain why.
60. Many individual requirements (e.g., setpoint and parameter values from OSC-8695) are not copied verbatim into the RTM; please explain why.
61. Tracing of the Availability Requirement.
- (a) The RTM contains one entry for the requirement in SRS Section 3.2.2, "Availability." The text of this requirement in the RTM is just the title of the section. The RTM traces this entry to SDD Section 5.0, "DESCRIPTION OF THE ATTACHMENTS;" however, SDD Section 5.0 does not contain information specific to the implementation of this requirement. Please explain why.
 - (b) Please provide an explanation of the traces to inappropriate sections and how this was addressed by V&V.
62. The RTM contains one entry for all of the requirements in SRS Section 3.2.3, "Security and Access Control." The text of this requirement in the RTM is just the title of the section. The RTM traces this entry to SDD Section 4.2, "RPS Trip #2;" however, SDD Section 4.2 is empty (i.e., "reserved for future use").

Please explain how the Security and Access Control requirements are documented in and traced to the SDD?

Software Requirements Specification (SRS) Questions

The following questions are a result of reviewing the Software Requirements Specification (SRS) -- "Oconee Nuclear Station, Unit 1 RPS ESFAS Controls Upgrade Software Requirements Specification," AREVA NP Inc., Doc. No. 51-9054435-002.

63. The SRS states (Section 2.6, page 46):

Proprietary [[

]]

- (a) What document (i.e., what Title & Document No.) will contain the final setpoint and parameter values?
- (b) How will it be verified and validated that the final setpoint and parameter values are properly implemented in the RPS/ESPS system installed at the site?
- (c) When will the final setpoint and parameter values be input into the deliverable system and associated documentation?
- (d) Please describe the relationship between the core operating limits report (COLR) calculations, COLR values, and the software parameters document.

64. The SRS states (Section 1.2, page 20):

Proprietary [[

]]

- (a) Please explain what “developed and maintained at the same level” means. That is, does it mean that this software is developed and maintained by including the same design features, and following the same analytical techniques, and procedural measures as for safety-related software?
- (b) Does it mean that this software will be traced with the same RTM methodology?

The SVVP (AREVA Doc No. 51-9010419-005) states (Section 4.6.6.2, page 24):

Proprietary [[

]]

The NRC noted that it is not an accepted practice to credit “line-by-line code review” instead of software functional testing of safety-related software; therefore, TXS Gateway software does not seem to be treated as safety-related as required by the SRS.

- (c) Please explain the apparent conflict between these two proprietary quotations.

65. The SRS contains the following two requirements (see statements containing the verb “shall”) that do not appear to be in the SDD; the SRS states (Section 1.2):

Proprietary [[

]]

The Software Verification and Validation Plan (SVVP), AREVA NP Inc., Doc. No. 51-9010419-005, states (Section 5.2.1, page 29):

Proprietary [[

]]

- (a) The text of the two requirements above are not included in the SRM portion of the RTM (51-9062040-002, "Oconee Nuclear Station, Unit 1 RPS ESFAS Controls Upgrade Requirements Traceability Matrix Report"); please explain why.

The RTM depicts (See Attachment F, page 2) that the requirements of the SRS are traced to the SDD.

- (b) How are the two SRS requirements, quoted above, implemented within the SDD?

Verification and Validation (V&V) Questions

The following questions are a result of reviewing the Software Verification and Validation Plan (SVVP), AREVA NP Inc., Doc. No. 51-9010419-005, and the Requirements Verification and Validation (V&V) Activity Summary Report, AREVA NP Inc., Doc. No. 51-9056720-001

66. RG 1.172 requires that: "[An SRS must be Correct, Unambiguous, Complete, Consistent, Ranked for importance and/or stability, verifiable, modifiable, and traceable.]"

The SVVP does not require that the software requirements are evaluated against the RG 1.172 criteria; the SVVP states (Section 5.2.1, page 29, Task No. 2):

Proprietary [[

]]

Please provide an evaluation of how the criteria used by V&V provides an acceptable method of complying with the regulations addressed by RG 1.172.

67. The SVVP requires that the requirements in SRS (51-9054435-002) be evaluated for testability; the SVVP states (Section 5.2.1, Task 2, page 29):

Proprietary [[

]]

The Requirements V&V Activity Summary Report documents the testability evaluation performed by V&V and concludes that the requirements are testable, and does not include any open items for requirements that are not testable. The Requirements V&V Activity Summary Report states (Section 4.1.1.4, page 31):

Proprietary [[

]]

In contrast to the quotations above, the SRS (51-9054435-002) contains requirements that are not testable, as demonstrated by the three examples below:

Proprietary [[

]]

Please explain the testability conclusion in the Requirements V&V Activity Summary Report in light of the fact that the SRS contains requirements that are not testable.

Software Configuration Management Plan (SCMP) Questions

The following questions are a result of reviewing the Software Configuration Management Plan (SCMP) – AREVA NP Inc., Document No. 51-90064444-005.

68. The SCMP states that the guidance of Regulatory Guide 1.169, “Configuration Management Plans for Digital Software Used in Safety Systems of Nuclear Power Plants,” is followed (Section 1.1, page 15):

Proprietary [[

]]

In a conference call, Oconee stated that the phrase “follows the guidance of” should not be understood to mean that the actions in the guidance document were done, “[because there is no requirement to do the things described in a guidance document]”; therefore this quotation is ambiguous in that it is not clear what is done. Oconee also stated that the term “conforms to” is used when all guidance is done.

Does the SCMP conform to Regulatory Guide 1.169 (i.e., is all of the guidance done)? If not, please clarify what alternative actions have been taken and explain how this is equivalent to the applicable RG 1.169 criteria.

69. There are different conventions that are at times followed in the documentation of requirements. One convention is that a requirement is stated only once. Another convention is to present information relevant to a particular concern in a particular document; this presentation can be called a view. With multiple views comes the possibility of presenting some of the same information in more than one place. The combination of these two conventions is sometimes accomplished by stating a

requirement in one place (e.g., using “shall”) and describing it in all other places (e.g., using “is”).

The SCMP states (see Section 3.2.2, page 35):

Proprietary [[

]]

This statement does not contain the word “shall;” is this statement a requirement?

70. The SCMP contains two definitions regarding “configuration audits”: “Function Configuration Audit”, and “Physical Configuration Audit.” The body of the SCMP uses a third term “Configuration Audit;” the SCMP states (Section 3.4.1, page 38):

Proprietary [[

]]

Regulatory Guide 1.169 Section C.1.4, “**Configuration Audit**,” states: “IEEE Std 610.12-1990 refers the definition of configuration audit to two other audits without specifying whether one or both definitions are meant. In the context of an audit for delivery of a product, a configuration audit includes both a functional configuration audit and a physical configuration audit.”

- (a) Does the term “configuration audit” on page 38 of the SCMP refer to: “Functional Configuration Audit”, “Physical Configuration Audit”, or both?
- (b) Please describe how the review of the Code Configuration Document addresses the “Functional Configuration Audit” and “Physical Configuration Audit” as defined in the SCMP.
- (c) What documentation describes the designed configuration of all software that is part of the safety-related software portion of the TXS System?

Software Integration Plan (SIntP) Questions

The Standard Review Plan (SRP) documents that a description of the contents of a Software Integration Plan (SIntP) is contained in NUREG/CR-6101. The SRP states (NUREG-0800 Chapter 7, Branch Technical Position No. 7-14 Section B.3.1.4, "Software Integration Plan"):

"NUREG/CR-6101, Section 3.1.7, 'Software Integration Plan,' and Section 4.1.7, 'Software Integration Plan,' contain guidance on SIntPs."

NUREG/CR-6101 states (Section 3.1.7):

"Software integration actually consists of three major phases: integrating the various software modules together to form single programs, integrating the result of this with the hardware and instrumentation, and testing the resulting integrated product. During the first phase, the various object modules are combined to produce executable programs. These programs are then loaded in the second phase into test systems that are constructed to be as nearly identical as possible to the ultimate target systems, including computers, communications systems and instrumentation. The final phase consists of testing the results, and is discussed in another report..."

71. Please provide an explanation of how the various RPS/ESPS integration activities address the SRP acceptance criteria for a SIntP. This explanation should include a cross reference that explains how RPS/ESPS project documentation addresses the full scope of integration as described by NUREG/CR-6101.
72. Supplement 4 states that "FAT fulfills the requirements for system integration ... testing" and that "additional application software integration test cases are added to the scope of FAT to satisfy IEEE Std 1012-1998 validation requirements for application software integration testing." The "testing" aspects of FAT could be considered to address the testing the resulting integrated product; however the docketed FAT plan does not mention integration testing.

Please provide integration testing documentation.

Software Installation Plan (SInstP) Questions

The SInstP address the installation of the integrated system into the target environment (e.g., installation at the nuclear power plant); the SRP states (NUREG-0800, Chapter 7, Branch Technical Position No. 7-14, Section B.3.1.5, "Software Installation Plan"):

"NUREG/CR-6101, Section 3.1.8, 'Software Installation Plan,' and Section 4.1.8, 'Software Installation Plan,' contain guidance on SInstPs."

NUREG/CR-6101 states (Section 4.1.8):

"The Software Installation Plan governs the process of installing the completed software product into the production environment. There may be a considerable delay between the time the software product is finished and the time it is delivered to the utility for installation.

Without an Installation Plan, the installation may be performed incorrectly, which may remain undetected until an emergency is encountered. If there is a long delay between

the completion of the development and the delivery of the software to the utility, the development people who know how to install the software may no longer be available.”

73. NUREG-0800 (SRP), Chapter 7, Branch Technical Position 7-14, Section B.3.1.5 contains acceptance criteria for Software Installation Plans.

Supplement 2 Table 2, “Disposition of References to the SPM from the ONS RPS/ESPS LAR,” identifies that the Software Installation Plan is addressed by the Oconee “Software Generation and Download Procedure [AREVA NP Inc. Doc. No. 51-9001942-004].”

The Software Generation and Download Procedure does not contain site-specific installation instructions.

Please describe the planned site installation activities and associated documentation.

LAR Review Items---- Question on TSs and Design

74. Section 9.3 in Enclosure 2 states that a quantitative availability analysis (32-5061241-00, not included in table 1-2) and a qualitative analysis (included in table 1-2) are utilized for calculating the probabilities of failure, and estimates of reliability and availability. The “operating history and reliability data is provided as the basis for the proposed test intervals.” This section also states that the availability analysis did not include the TXS output relays and that it will be revised to include the output relays and the results of the failure modes effects analysis (FMEA).

Please submit the quantitative availability analysis which includes the output relays and the results of the FMEA.

75. Section 9 in Enclosure 2 provides justification for changing the technical specifications (TSs) channel functional test interval from the current requirement of 45 days on a staggered test basis to an interval of 18 months plus 25%. In this section, Duke stated that this interval is consistent with the recommended surveillance testing provided in Topical Report EMF-2341(P) which was reviewed by the NRC as part of their review of the TXS topical report. The document 51-9044432-003, “Oconee Nuclear Station RPS/ESPS Surveillance change justification” supports the proposed interval. In Section 1 of Enclosure 2, Duke referenced various sections of EMF-2341(P) for channel functional test and stated, “Logic System Functional Tests are accomplished by Continuous self monitoring.”

However, the NRC staff’s Safety Evaluation Report (SER) on the TXS topical report referenced EMF-2341(P) and stated in Section 4.2 as follows:

“The report describes measures to be implemented in safety I&C systems configured with a TXS architecture to comply with requirements for channel checks, functional tests, channel calibration verification tests, response time verification tests, and logic system functional tests.

The measures include:

- Periodic verification (during refueling outages) of accuracy and time constants of the analog input modules

- Continuous self-monitoring and on-line diagnostics to verify proper functioning of digital systems and to ensure integrity of the installed application and system software
- Periodic actuation of output channel interposing relays - The reactor trip function is tested at the same surveillance test interval as current technical specifications (typically quarterly) and the engineered safety features actuation system (ESFAS) function is tested consistent with the licensee's refueling outage (typically 15 to 24 months).

As defined in the [Advanced Light Water Reactor (ALWR)] Standard Technical Specifications, a logic system functional test is a test of all required logic components (i.e., all required relays and contacts, trip functions, solid-state logic elements, etc.) of a logic path, from as close to the sensor as practicable up to, but not including, the actuated device, to verify operability. The logic system functional test may be performed by means of any series of sequential, overlapping, or total system steps so that the entire logic system is tested.

For some applications, interposing relays may be used in the logic component. The licensee should test those relays in accordance with the existing TS requirements. It is prudent to verify the logic system functions at least every refueling outage. This is a plant-specific action item along with the plant-specific technical specification requirements."

Please provide a detailed explanation of how continuous self monitoring of the instrumentation channel, which ends at the target system hardware (TXS Processor), will perform periodic functional testing of logic system and interposing relays as identified in the above statements of the staff SER. Also please submit AREVA document 51-9044432-003, "Oconee Nuclear Station RPS/ESPS Surveillance Change Justification," referenced in Section 9.4.

76. The Oconee current TSs definition of channel functional test requires OPERABILITY verification, including required alarms, interlocks, display, and trip functions. The LAR has proposed changing this definition as follows:
- Analog and bistable channels - the injection of simulated or actual signals into the channel as close to the sensor as practicable to verify OPERABILITY of all devices in the channel required for channel OPERABILITY.
 - Digital computer channels – the use of diagnostic programs to test digital computer hardware and the injection of simulated process data into the channel to verify channel OPERABILITY of all devices in the channel required for channel OPERABILITY.

The current TSs definition specifies the "functions to be tested for operability verification" whereas the proposed change does not specify what are "all devices in the channel required for channel operability." Please explain this discrepancy and revise the proposed definition. Please note that the LAR Enclosure 1, Figure 2.2-1 identifies boundaries of a channel.

77. LAR Enclosure 1 page 2-8 and AREVA NP Inc., Doc. No. 51-9029108-003 page 21 (item 3 of LAR Enclosure 6), show Reactor Trip Relay Logic with two S451 digital output

modules in each of the four channels; whereas, AREVA NP Inc., Doc. No. 51-5065423-07 page 33 (item 14 in Table 1-2 of LAR) shows four modules per channel. Please explain the difference and function of these modules. Are these modules operating in a Master/ checker configuration as the two SVE2 processing modules in each ESFAS voter subsystems?

78. LAR Section 2.7.2 references Table 2.7-2 for a summary and discussion of the changes to software and references Table 2-4 for a summary of software revisions, since TXS SER. Table 2-4 is included in the submittal while Table 2.7-2 is missing. Please provide Table 2.7-2.
79. DLPIAS manual actuation capability, as explained in LAR Section 2.4.2.1, includes an Emergency Override pushbutton to permit a redundant capability to prevent inadvertent operation of the LPI pumps. Please explain and justify why a similar capability is not provided in DHPIAS. Also, identify as to what administrative controls will be established for the use of these override push buttons, how long the DASs will be allowed to be overridden, and will the affected RPS/ESPS channels be operable during the period of the DAS override? How will the DAS operability status be indicated?
80. LAR Section 4.2.2 lists RG 1.118, Revision 3 to provide the regulatory requirements for the proposed change. Revision 3 of RG 1.118 endorsed IEEE Std. 338-1987 which states in Section 5 (13), "where practical, means shall be included in the design to prevent the simultaneous application of any bypass condition to redundant channels or load groups during testing."

LAR Enclosure 6, item 3 (AREVA NP Inc., Doc. No. 51-9029108-003) in Section 4, lists various operational modes such as TXS parameter change enable mode, RPS shutdown bypass mode, RPS instrument input channel manual bypass mode, and ESFAS voter manual bypass mode. The key-switches of these bypass modes are administratively controlled and there are no hardware or software interlocks between channels. Please identify the means to prevent the simultaneous application of any bypass condition to redundant channels or load group during testing , as required by IEEE-338

81. According to the network architecture described in LAR Enclosure 1 and slides 23, 31, and 34 in the December 13, 2006, presentation, SL21 data link is used for communication between RPS/ESPA channels and uses a token for giving authority to each channel to send data. For a lost token condition, which sometimes happens, it is not clear how response time, deterministic procedure and fail-safe criteria are met. The token re-making time would delay the response time used in an accident analysis, and/or may affect the deterministic property and the accident analysis. Please explain how this token passing instead of a point-to-point communication meets the safety criteria and maintains the accident analysis results. Please explain how this is comparable to ISG #4 criteria regarding point-to-point communications between safety channels.
82. According to LAR Enclosure 1 (fig.2.1-2/2.2-1) and AREVA NP Inc. Doc. No. 51-9029108-003, Profibus L2 data link is used in inter-channel communication when each safety channel sends their input signal to 2.MIN/2.MAX Function Block of redundant channels, and when each channel send its bi-stable output to the redundant channel trip relays.

Please explain if the token passing process is also used in the case of transmission of the bi-stable output from one channel to the redundant channels trip relays and provide the following information:

- (a) Whether the two Profibus L2 data links, used in 2.MIN/2.MAX Function Block and bi-stable output, use the same token or it is a different token.
- (b) What is the recovery process when the token is lost?.

Please provide documentation to confirm deterministic communication.

83. LAR Section 2.2.1 states, "The TXS SNV1 Signal Multiplier Modules provide isolated analog outputs which are independent of the TXS processors. These isolated outputs provide signals to control board indicators, recorders, and to the non-safety Integrated Control System (ICS)." This statement does not include isolated and independent signals to DLPIAS and DHPIAS. However, Figures 2.4-1 and 2.4-2, respectively, for DLPIAS and DHPIAS show buffered 1E to non-1E signals from TXS to DLPIAS/ DHPIAS.

Please confirm that the initiation signal from the respective SNV1 to DLPIAS/ DHPIAS is isolated and independent of the TXS processor.

84. LAR Section 2.5.3 states:

"TXS service unit serves the following functions:

- Monitoring the system state,
- Reading and acknowledging on line error and state messages,
- Modifying online parameters,
- Performing period tests,
- Error detection and fault diagnostics, and
- Central reloading of software after design changes"

Functions such as, modifying online parameters, performing period testing, and central reloading of software have potential to adversely affect the safety functions. For these functions, the data exchange between safety system and non-safety systems should be processed in a manner that does not adversely affect the safety function.

Please identify the design provided in the TXS for prevention of this potential adverse effect of performing these functions on the safety system. Are these functions performed automatically or manually in a bypass mode using a software or hard-wired switch?