SummerRAIsPEm Resource

From: Gleaves, Bill
Sent: Monday, June 20, 2016 1:01 PM
To: SummerRAIsPEm Resource
Subject: FW: Draft RAIs for Common Q LAR - Public Meeting June 23, 2016
Attachments: Draft-RAIs-LAR-15-017.docx

From: Betancourt, Luis
Sent: Thursday, June 16, 2016 5:19 PM
To: Patel, Chandu; Gleaves, Bill
Cc: Harbuck, Craig; Roggenbrodt, William; Dias, Antonio; Curtis, David; Dixon-Herrity, Jennifer; Hoellman, Jordan; Caldwell, Robert
Subject: Draft RAIs and Audit Plan for Common Q LAR - Public Meeting June 23, 2016

Chandu and Bill,

Attached please find staff's draft RAIs which the NRC staff intends to discuss in the public meeting on June 23, 2016.

Draft RAIs
Attached are the draft RAIs of Vogtle's LAR 15-017, "Update of Common Q Platform Software Program Manual and Topical Report," for your review and comment. These draft RAIs will be used to facilitate the discussion in the public meeting on June 23, 2016. Note that these draft RAIs have not yet gone through management review.

The purpose of the meeting will be to discuss these with the License and then refine the draft RAIs before management review. The deadline for DEIA/ICE to submit the draft RAIs to DNRL/LB4 is July 1, 2016.

Hearing Identifier: Summer_COL_eRAIs
Email Number: 140

Mail Envelope Properties (a986b67dea16428ea2647be1e00d98de)

Subject: FW: Draft RAIs for Common Q LAR - Public Meeting June 23, 2016
Sent Date: 6/20/2016 1:00:35 PM
Received Date: 6/20/2016 1:00:36 PM
From: Gleaves, Bill

Created By: Bill.Gleaves@nrc.gov

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

Post Office: HQPWMSMRS02.nrc.gov

Files	**Size**	**Date & Time**
MESSAGE	1051	6/20/2016 1:00:36 PM
Draft-RAIs-LAR-15-017.docx	51506	

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

Draft Request for Additional Information on License Amendment Request: "Update of Common Qualified Platform Software Program Manual and Topical Report"

Date of Revision: 06-16-16

Vogtle LAR 15-017: ML16046A009
Summer LAR 13-35: ML16067A145

Disclaimer

The purpose of this document is to facilitate the discussion between the U.S. Nuclear Regulatory Commission (NRC) staff and representatives of Southern Nuclear Operating Company (SNC), the Licensee for Vogtle Electric Generating Plant (VEGP) Units 3 and 4; and South Carolina Electric & Gas Company (SCE&G), the Licensee for Virgil C. Summer Nuclear Station (VCSNS) Units 2 and 3 for the public meeting on June 23, 2016 (ML16141A081). The purpose of this meeting is to discuss the NRC staff's draft request for additional information (RAI) related to the NRC staff's review of the request for license amendment: "Update of Common Qualified (Common Q) Platform Software Program Manual (SPM) and Topical Report." Although this document contains the NRC staff's draft RAIs for the requested amendment, additional RAIs may be identified as a result of the discussions from the public meeting. In addition, some of the draft RAIs shown below may be eliminated as a result of the discussions from the public meeting.

The draft RAIs have not yet gone through the formal review process.

Enclosure 2, "Plant-Specific Action Item and Generic Open Item Dispositions for WCAP-16096, Revision 4 and WCAP-16097, Revision 3"

10 CFR 50.55a(a)(1) requires that structures, systems, and components must be designed, fabricated, erected, constructed, tested, and inspected to quality standards commensurate with the importance of the safety function to be performed.

10 CFR 50, Appendix A, GDC 1, "Quality Standards and Records," requires in part that systems and components important to safety be designed, fabricated, erected, and tested to quality standards commensurate with the importance of the safety functions to be performed. Where generally recognized codes and standards are used, they should be identified and evaluated to determine their applicability, adequacy, and sufficiency, and should be supplemented or modified as necessary to ensure a quality product consistent with the required safety function.

GDC 4, "Environmental and Dynamic Effects Design Basis," states that structures, systems, and components important to safety shall be designed to accommodate the effects of, and to be

compatible with, the environmental conditions associated with normal operation, maintenance, testing, and postulated accidents, including loss-of-coolant accidents.

GDC 21, "Protection System Reliability and Testability," states that the protection system shall be designed for high functional reliability and in-service testability commensurate with the safety functions to be performed.

WCAP-16097: Common Q Topical Report – Plant-Specific Action Items (PSAI)

1. WCAP-16097, PSAI 6.18 (Pages 5-6 of Enclosure 2):

   10 CFR 50.36 sets forth requirements for technical specifications to be included as part of the operating license for a nuclear power facility.

   WCAP-16097, "Common Qualified Platform Topical Report," Plant-Specific Action Item (PSAI) 6.18 states that "…*administrative controls must be in place to ensure that changes to setpoints are only performed while the system is not being relied upon to perform its safety functions. In addition, the affected division of the Common Q safety system must be declared inoperable prior to implementation of setpoint changes.*" To address WCAP-16097 PSAI 6.18, the Licensee proposes to add a new Tier 2 Subsection 7.1.2.14.3, "Operational Process," to describe the software operations plan and the administrative controls within it. The proposed markups for this new Subsection (see page 9 of Enclosure 4) states:

   > A software operations plan includes administrative controls to require that the PMS and its division room are in the appropriate configuration prior to making setpoint changes. This includes requiring a channel to be bypassed prior to making setpoint changes for reactor trip or ESFAS functions. In addition, the PMS division is declared inoperable prior to making setpoint changes for blocks and resets. The administrative controls prevent the protection and safety monitoring system division room environment from interfering with protection and safety monitoring system equipment when plant personnel are making setpoint changes. The administrative controls account for local emissions from nearby equipment and activities (e.g., welding) while the maintenance test cabinet (MTC) door is open.

   In addition, the disposition to WCAP-16097 PSAI 6.18, states, in part that:

   > Since the PMS division will remain operational during setpoint changes for reactor trip and ESFAS actuation functions, as described above, the PMS division room environment needs to be considered when opening the MTC door to make setpoint changes.

   The requested amendment does not provide a discussion any specific details on how the administrative controls for implementing setpoint changes will affect the Technical

Specifications. In addition, the NRC staff did not find adequate design information in the requested amendment to fully understand how the setpoint changes will be modified for both reactor trip and engineered safety features actuation functions in the various configurations that may exist across sub-channels and across other divisions, (e.g. one sub-channel bypassed, the other sub-channel fully operational, while the remainder of the safety divisions are operational etc.) within the Common Q portion of the Protection and Safety monitoring System (PMS). Therefore, the NRC staff requests the Licensee to:

(1) Describe how the administrative controls for implementing setpoint changes will affect the Technical Specifications for the affected PMS division.

(2) Describe how the voting logic in the other PMS divisions would be affected for all reactor trip and engineered safety features actuation functions while implementing setpoint changes under all different operating conditions.

(3) In reviewing Section 2.2.6, Maintenance and Test Panel Subsystem of WCAP-16675, "AP1000™ Protection and Safety Monitoring System," Revision 5, the NRC staff understands there is one 'Function Enable' switch within each of the divisionally based Maintenance and Test Panels (MTPs). The text describes, in part, "*When the Function Enable keyswitch is disabled, all surveillance test conditions are removed and all external inputs to the safety system functions are restored*." In using this statement as a basis, it appears that when the "Function Enable "switch is taken to the "Enable" position that surveillance test conditions for both sub-channels have the potential to be inserted and all, or many, of the external inputs to the division have been disabled.

Please describe what exact controls are deemed sufficient by the Licensee to ensure that, in the presence of a system designed for division-based maintenance, as evidenced by a singular Function Enable switch per division and not two separate switches, that at least one sub-channel within the given division will remain operational.

(4) The proposed markups for Tier 2 Subsection 7.1.2.14.3, states, in part, that:

> …In addition, the PMS division is declared inoperable prior to making setpoint changes for <u>blocks and resets</u>…

Is this meant to include permissive signals that permit manual bypass of associated Function(s)?

(5) The proposed markups for Tier 2 Subsection 7.1.2.14.3, states, in part, that:

> Since the PMS division <u>will remain operational during setpoint changes</u> for reactor trip and ESFAS actuation functions…

Please define what is meant by “operational” in the text shown above?

Update the requested amendment accordingly.

2. WCAP-16097, PSAI 6.20 (Page 6 of Enclosure 2)

WCAP-16097 PSAI 6.20 states that *“A Licensee implementing an application based upon the Common Q platform that utilizes fiber optic cables to connect HSL's between safety divisions shall ensure that all plant specific environmental qualification requirements for this cabling are met.”* The disposition of WCAP-16097 PSAI 6.20 states:

> For the AP1000, this issue was already included in the scope of the WCAP-16097 PSAI 6.4 disposition in APP-GW-GLR-017.

From the information contained in the disposition for WCAP-16097 PSAI 6.4 at APP-GW-GLR-017, it is not clear to the NRC staff how the plant specific environmental qualification requirements for the fiber optic cables are met. The NRC staff request the Licensee to further demonstrate how WCAP-16097 PSAI 6.20 is met.

3. WCAP-16097, PSAI 6.24 (Page 8):

WCAP-16097 PSAI 6.24 states that *“A licensee implementing an application based upon the Common Q platform that relies on the FPDS to perform safety critical functions shall perform an evaluation to address the added reliance on the FPDS to accomplish the required safety functions. The affects of not having the necessary information available on the FPDS during the design basis event should be considered and addressed in this evaluation*.” The disposition of WCAP-16097, PSAI 6.24 states, in part, that:

> The evaluation concluded that the only safety critical functions based on the Common Q platform that rely on the Flat Panel Display System (FPDS) are those design basis events (DBE) that require operator action. The DBE are for Anticipated Operational Occurrences. No DBEs are limiting Design Basis Accidents. For these three DBEs, the information necessary for the operator to take action is captured on the FPDS and on alternate, non-safety related sources.

The NRC staff requests the Licensee to identify the three design basis events (DBE) that require operator action. In addition, please identify the alternate non-safety related sources and describe the effects of not having the necessary information available on the Flat Panel Display System during the DBEs.

WCAP-16096: Common Q Software Program Manual – Plant-Specific Action Items

1. WCAP-16096, PSAI 2 (Pages 11-12 of Enclosure 2):

   WCAP-16096, "Software Program Manual for Common Q™ Systems," PSAI 2 states that "*The Common Q SPM only includes the Software Life Cycle Process Planning Documentation as outlined in SRP BTP 7-14, Section B.2.1. As such, the plant-specific documentation outlined in SRP BTP 7-14, Sections B.2.2, "Software Life Cycle Process Implementation," and B.2.3, "Software Life Cycle Process Design Outputs," is to be evaluated separately for any application that references the Common Q SPM.*"

   BTP 7-14, Section B.2.2, "Software Life Cycle Process Implementation," provides guidance to evaluate the software lifecycle process implementation. BTP 7-14, Section B.2.2, states that one or more sets of reports should be available for each of the following activity groups: requirements, design, implementation, integration, validation, installation, and operations and maintenance.

   The disposition of WCAP-16096 PSAI 2 states, in part, that:

   > These reports cover the following activities: requirements, implementation, integration, validation, installation, and operations and maintenance.

   From the information contained in the requested amendment, the NRC staff was not able to confirm any reports for the design activity. The NRC staff requests the Licensee to document the design activity in the requested amendment.

Enclosure 3, "Common Q Platform Software Program Manual and Topical Report Alternatives and Justification"

10 CFR 50.55a(a)(1) requires that structures, systems, and components must be designed, fabricated, erected, constructed, tested, and inspected to quality standards commensurate with the importance of the safety function to be performed.

10 CFR 50, Appendix A, GDC 1, "Quality Standards and Records," requires in part that systems and components important to safety be designed, fabricated, erected, and tested to quality standards commensurate with the importance of the safety functions to be performed. Where generally recognized codes and standards are used, they should be identified and evaluated to determine their applicability, adequacy, and sufficiency, and should be supplemented or modified as necessary to ensure a quality product consistent with the required safety function.

WCAP-16096: Common Q Software Program Manual Alternatives

1. Common Q SPM Sections, "Glossary of Terms: Project Quality Plan," and 4.3.2.1, "Initiation (Concept) Phase – (Page 2 of Enclosure 3)

   The Licensee proposes an alternative to Common Q SPM Sections, "Glossary of Terms: Project Quality Plan," and 4.3.2.1, "Initiation (Concept) Phase." The alternative proposes to delete the following text from the Common Q SPM:

   > Any alternatives to the SPM processes or additional project specific information for the SQAP, SVVP, SCMP or SOMP shall be documented and justified in the PQP.

   The justification of the alternative states:

   > The Project Plan identifies the Software Development Plan as the location for the SPM alternatives and justifications. The Software Development Plan also identifies itself as the companion document to the Project Plan. Both of these documents are approved by the Quality Organization.

   The Licensee proposes to use the Software Development Plan as the location for the SPM alternatives to the SPM processes or additional project specific information for the SQAP, SVVP, SCMP or SOMP. The NRC staff requests the Licensee to:

   (1) Provide the relationship of the Project Plan and the Software Development Plan. Are these two documents at the same level of hierarchy?

   (2) Demonstrate why is acceptable to use Software Development Plan instead of the Project Plan as the location for the SPM alternatives to the SPM processes and/or additional project specific information.

   (3) Provide a justification for removing the Common Q SPM text shown above.

2. Common Q SPM Section 4.3.2.6, "Site Installation and Checkout Phase – (Page 3 of Enclosure 3)

   The Licensee proposes an alternative to Common Q SPM Section 4.3.2.6, "Site Installation and Checkout Phase." The alternative proposes to develop the site test plan in accordance with the overall digital I&C test strategy to support installation testing and the Initial Test Program. The justification of the alternative states:

   > A separate schedule is developed that governs the overall scheduling of AP1000 site testing. Site test planning is initiated during PMS development, but

independent of any particular PMS development phase. This is an appropriate approach for a new build project.

The preparation of the site test plan is initiated during the requirements phase to support evaluation of requirement testability on-site. The Licensee needs to demonstrate why the site test planning is independent of any particular PMS development phase.

3. Common Q SPM Section 9.2.3, "Control" – (Page 6 of Enclosure 3)

In the alternative to Common Q SPM Section 9.2.3, "Control," the Licensee proposes to designate the Software Lead to confirm the AP1000 PMS software changes. Section 5.4.3.1.5, "Engineering Project Manager," of the SPM states that EPMs and Platform Leads may delegate the performance of necessary tasks to other persons but remain responsible for their execution. The NRC staff requests the Licensee to:

(1) Provide the organizational charts for the Platform Lead and the Software Lead.

(2) Describe how the Platform Lead will remain responsible for the execution of the AP1000 PMS software changes.

4. SPM Section 11.4, "Corrective Action" – (Page 7 of Enclosure 3)

In the alternative to Common Q SPM Section 11.4, "Corrective Action," the Licensee proposes to document the corrective actions in the Common Q Automation Issue Tracking System (RITS), and for the independent RITS reviewer to close out the report. The NRC staff requires additional information in order to determine if an adequate level of independence has been established. Please provide a listing of all reporting relationships established to demonstrate that an adequate level of separation exists between the design team and the independent RITS reviewer.

5. Common Q SPM Section 12, "Secure Development and Operational Environment Plan" – (Page 8 of Enclosure 3)

10 CFR 50.55a(h), "Protection and Safety Systems," requires compliance with the requirements of IEEE Std. 603-1991, which is a system-level standard that contains requirements related to access controls. IEEE Std. 603-1991, Clause 5.9, provides access control requirements for safety systems.

The Licensee proposes to exclude WCAP-16096, Section 12, "Secure Development and Operational Environment Plan," from being incorporated by reference into the UFSAR. The justification of the alternative to Section 12, "Secure Development and Operational Environment Plan" states:

The AP1000 PMS Computer Security Plan is specific for AP1000 and has been determined to be an acceptable method used to demonstrate how computer security is incorporated into the design and development of AP1000 safety systems. The AP1000 PMS Computer Security Plan is consistent with the Common Q SPM incorporated by reference information and, therefore, should be used in place of any Section 12 references made within the Common Q SPM.

The NRC staff requests the Licensee to document in the requested amendment the differences between the AP1000 PMS Computer Security Plan and WCAP-16096, Section 12.

WCAP-16097: Common Q Topical Report Alternatives

1. Table A3-2, "Common Q Topical Report Alternatives" – (Page 10 of Enclosure 3)

   The Licensee proposes to remove the revision number for the WCAP-17266 reference from the TR Section, "Reference." The justification of the alternative states:

   > Removing the revision number for the WCAP-17266 reference is consistent with how the Common Q SPM references this document. WCAP-17266 is not an input into WCAP-16097, but a lower-level process document. Therefore, identifying a revision number is unnecessary. This document will continue to meet the commitment in WCAP-16097, Revision 3, Section 12 which requires it to describe the screening and evaluation process for determining what Common Q platform changes are available for audit, and which changes require re-submission to the NRC.

   The NRC staff requests the Licensee to identify which high-level process document will ensure errors are properly identified, captured, tracked, resolved and placed into a records management system to ensure the issue is available for historical reference.

Enclosure 5, "Resolution of Common Q NRC Items"

In the Record of Changes for Revision 2 of APP-GW-GLR-017, the Licensee states that DCD markups were updated to reference Revisions 1 and 2 of APP-GW-GLR-017. However, the NRC staff found changes to Sections 7.1.2.3, 7.1.2.8, "Communication Functions," 7.1.6, "Combined License Information"; 9A3.1.2.5.2, "Safe Shutdown Evaluation"; and the newly added Subsection 9A.3.1.2.8.4, "Safe Shutdown Evaluation." These DCD markups were not discussed in Enclosure 1 of the letter. The NRC staff requests the Licensee to describe the nature of the changes.