WBN2Public Resource

From: Poole, Justin
Sent: Monday, December 12, 2011 10:47 AM
To: Arent, Gordon
Cc: Clark, Mark Steven; WBN2HearingFile Resource
Subject: DRAFT Request for Additional Information Regarding Open Item 98
Attachments: DRAFT Request for Additional Information on Open Item 98 - EICB - December 2011.docx

Gordon,

In reviewing TVA's September 1, 2011, letter, the staff has come up with the attached questions. Please review to ensure that the RAI questions are understandable, the regulatory basis is clear, there is no proprietary information contained in the RAI, and to determine if the information was previously docketed. If further clarification is needed, and you would like to discuss the questions in a conference call, let us know. Please also let me know how much time Tennessee Valley Authority (TVA) needs to respond to the RAI questions. This email does not convey a formal NRC staff position, and it does not formally request for additional information.

Justin C. Poole
Project Manager
NRR/DORL/LPWB
U.S. Nuclear Regulatory Commission
(301)415-2048
email: Justin.Poole@nrc.gov

Hearing Identifier: Watts_Bar_2_Operating_LA_Public
Email Number: 628

Mail Envelope Properties (19D990B45D535548840D1118C451C74DC8B2CAC6EB)

Subject: DRAFT Request for Additional Information Regarding Open Item 98
Sent Date: 12/12/2011 10:47:16 AM
Received Date: 12/12/2011 10:47:21 AM
From: Poole, Justin

Created By: Justin.Poole@nrc.gov

Recipients:
"Clark, Mark Steven" <msclark0@tva.gov>
Tracking Status: None
"WBN2HearingFile Resource" <WBN2HearingFile.Resource@nrc.gov>
Tracking Status: None
"Arent, Gordon" <garent@tva.gov>
Tracking Status: None

Post Office: HQCLSTR02.nrc.gov

Files	**Size**	**Date & Time**
MESSAGE	833	12/12/2011 10:47:21 AM
DRAFT Request for Additional Information on Open Item 98 - EICB - December 2011.docx	27359	

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

Watts Bar 2 Common Q PAMS Secure Development and Operational Environment
SSER 23 Appendix HH Action Item 98
Requests for Additional Information

The following RAIs are regarding the Watts Bar 2 Common Q PAMS Secure Development and Operational Environment. The action associated with this review area is captured in SSER 23 Appendix HH, Action Item 98 (ML11270A306). TVA submitted documents (reference below) on September 1, 2011 to address this item.

1. Platform Development – The US Nuclear Regulatory Commission staff notes that the Common Q platform was subject to commercial grade dedication and that a topical report on the platform was reviewed and approved by the staff (ML003740165). However, at the time of the staff's previous review, no evaluation was performed regarding the secure development environment for the Common Q platform and the staff is aware that the platform has undergone changes. Regulatory Guide 1.152, Revision 3, which is cited by the licensee as being used to conform to establishing a secure development environment, contains regulatory positions related to ensuring that superfluous features are not present in software-based safety systems that could present the potential for degrading the reliable operation of the system.

   a) Since the Common Q platform was originally designed to potentially serve in several different plant applications, please provide references for and a description of any analyses that were performed to determine if there are any superfluous functions or features resident on the platform (i.e., in any of the platform software or software-driven components, such as PLCs) that are not utilized by the Common Q platform or post accident monitoring system (PAMS) application, as well as a summary of the results of such analyses. If any unnecessary functions or features were identified, please explain what measures were taken to resolve any potential impact on the Common Q platform or PAMS application operation (i.e., were features disabled, removed or determined by analysis not to have potential to impact operations?). [e.g., the staff notes that in Attachment 9 of the September 1, 2011, Request for Additional Information responses (ML11257A050), it is stated that the Function Enable keyswitch on the Operators Module was not installed for the Watts Bar Unit 2 PAMS application, and that the Operator's Module has no connection to a printer.]

   b) It is essential that the Common Q platform operating system software be maintained in a fashion that protects it from unauthorized changes. Please confirm that WNA-LI-00058-WBT-P, Rev. 3, Sections 2.2.1 and 2.2.2 (ML110950334) describe the changes made to the platform. If not, please provide a description of changes made (including removal of unnecessary features) to the Common Q operating system software since it was initially subject to commercial grade dedication and analyses were performed of the features resident on the platform. Please describe the processes followed to ensure that only authorized changes have been made.

   c) WCAP-17427-P, Revision 1 (ML11257A061) states that the approved version of the QNX software is protected by a CRC stamp to ensure that the correct configuration is

d) used. For the WBN2 PAMS application, provide documentation indicating your confirmation that the CRC stamp for QNX was verified to be the correct version intended for use.

e) WCAP-17427-P, Revision 1 states that the AC160 software is under strict configuration controls and that any changes are jointly approved by Westinghouse and ABB. Please confirm that the summary of changes provided in Section 2.2.2 of WNA-LI-00058-WBT-P, Revision 3 (ML110950334) accurately reflects modifications since dedication. Also, please describe what measures were taken to ensure that the correct, commercially-dedicated version of AC160 software is installed on the WBN2 PAMS system.

2) Application Development – Staff reviewed WCAP-17427-P, Revision 1 and found it to be largely consistent with APP-GW-J0R-012, Revision 1 (ML102170268 dated June 2010). However, much of the processes described are in future-tense and it is not clear to the staff what actions were accomplished for this particular Watts Bar Unit 2 PAMS application development to establish a secure development environment. WCAP-17427-P, Rev 1 (ML11257A061 dated August 2011) describes the security assessment for the Common Q PAMS for Watts Bar Unit 2.

a. In Section 2.2.3.1.1.a, the statement is made that the Westinghouse Quality Management System (QMS) "will be" followed to ensure documents from hardware and software development efforts are adequately protected. Specifically, the section states that documents are to be stored in the Enterprise Document Management System (EDMS).

i) Please identify what documents related to the Common Q platform development (relevant to the Watts Bar 2 PAMS) are protected under the QMS / EDMS.

ii) Please identify what documents related to the Watts Bar 2 PAMS development are protected under the QMS/EDMS.

b) In Section 2.2.3.1.1.b, discussions of controls contained in the Software Program Manual are detailed. Please provide a confirmatory statement that the Watts Bar 2 PAMS development process conformed to these controls.

c) In Section 2.2.3.2, items 2. and 3. are identical. Please clarify if one of these items is intended to state something else.

d) In Section 2.2.3.2, the statement is made that during the implementation phase, software "shall be" code reviewed by IV&V using a defined checklist for adherence to coding standards and application requirements. Please clarify if this step was performed for the Watts Bar Unit 2 PAMS application. Please clarify if WNA – VR-00283-WBT-P, Rev.4 (ML110770540) contains this record. If not, please provide a reference for the code review results and provide a statement indicating the findings of the review.

e) In Section 2.3.1.5, the statement is made that the security requirements "shall be" verified and validated as part of the overall system requirements. Please clarify if this step was performed for the Watts Bar Unit 2 PAMS application. Please clarify if WNA – VR-00283-WBT-P, Rev.4 (ML110770540) contains this record. If not, please provide a reference for the results of the V&V of the security requirements and provide a statement indicating the findings of the V&V.

f) In Section 2.4.1, the statement is made that an assessment of the PAMS "will be" performed to verify that requirements for security controls are implemented correctly in the design. Please clarify if this step was performed for the Watts Bar Unit 2 PAMS application. Please clarify if WNA – VR-00283-WBT-P, Rev.4 (ML110770540) contains this record. If not, please provide a reference for the results of the V&V of the security requirements and provide a statement indicating the findings of the assessment.

g) In Section 2.5.1.1, the statement is made that an IV&V assessment "will be" performed of the security requirements during the implementation phase and that any anomalies will be documented. Please clarify if this step was performed for the Watts Bar Unit 2 PAMS application. Please clarify if WNA – VR-00283-WBT-P, Rev.4 (ML110770540) contains this record. If not, please provide a reference for the results of the IV&V of the security requirements. Please provide a brief summary of any anomalies found and, if there were any, please confirm that they were resolved in accordance with the Software Program Manual processes.

h) In Section 2.5.3, IV&V Phase Summary Report and Software Release Records are given as outputs of the implementation phase. Please confirm if WNA-VR-00283-WBT P, Rev 4 (ML110770540) is the appropriate IV&V Phase Summary Report Record. Please provide a reference for Software Release Records documents and submit on docket.

   i) In Section 2.5.3, the statement is made that the code is maintained in a "locked" area of the configuration control system. Please provide further detail regarding the "locked" area of the configuration control system. (e.g., is the code stored on a removable media and physically locked somewhere? Or, is the code on an isolated computer or network and protected by software controls?).

j) In Section 2.6 (and its subsections), testing activities are described in future-tense. Please provide a brief summary of the testing results as they pertain to security requirements for the system. Do WNA-TR-02451-WBT (ML110950332) and WNA-VR-00283-WBT-NP, Rev4 (ML110770538) represent this evidence? If not, please provide references for the documents identified in Section 2.6.3 and submit on docket.

3. Secure Operational Environment – In order to establish compliance with IEEE-603 Clauses 5.6.3 and 5.9, the staff needs to ensure that a secure operational environment has been established for the proposed digital safety system. Regulatory Guide 1.152, Revision 3 - which the licensee has indicated it used to conform to these requirements - provides applicable regulatory positions.

   a. Please provide a description of the analyses performed to establish what digital systems are connected to the PAMS, what behaviors those systems are capable of either in a normal or failed operating state and what measures were taken in the PAMS design or Watts Bar operations to ensure its reliable operation in the presence of those potentially adverse behaviors.
   b. Please provide a description of the analyses performed to establish what points of physical and logical access are present to allow interaction with the PAMS and what measures were taken in the PAMS design or Watts Bar operations to provide assurance that only authorized personnel can access the system.
   c. The "Watts Bar Nuclear Unit 2 Common Q Post Accident Monitoring System Conformance to the Secure Development and Operational Environment

Requirements of Regulatory Guide 1.152 Revision 3" document (ML11257A050 dated September 1, 2011) describes the licensee's activities relative to SDOE.

i. In Section 1.e (on page 7), it is noted that the testing of the Maintenance and Test Panel (MTP) software data diode function was included in the CIT/FAT and that the software data diode is the "qualified" isolation device. Please provide a summary of testing performed for this software data diode (i.e., did the testing consist of just the "data storm" testing or were there other tests?). Also, please elaborate on what is intended by the term "qualified" (i.e., Does it indicate that it has been formally tested? Or is there some other pedigree implied by the term?)

ii. In Section 2.a.i.(1) (on page 8), the statement is made that the touch screen on the Operators Modules could change constants or alarm setpoints if the Function Enable keyswitch was placed in the 'enable' position. In Section 1. b of the same document, it is noted that the Function Enable keyswitch was not installed on the Operators Module for the PAMS. Please confirm that the Operators Panel does not possess a Function Enable keyswitch. [Note: Sections 2.a.i.(2) and 2.a.vi.(1) also mention the Function Enable keyswitch in regard to the Operators Module.]

iii. In Section 2.a.v (on page 9), use of a hardware data diode is noted. Please clarify if this is the device referenced in the response to RAI 14b submitted on July 30, 2010 (ML102160349). If not, please provide information on the specific hardware used (i.e., vendor and model number).