

NRR-PMDAPEm Resource

From: Minarik, Anthony
Sent: Monday, April 13, 2015 7:47 AM
To: Bryan, Robert H Jr (rhbryan@tva.gov)
Cc: Arent, Gordon (garent@tva.gov); Poole, Justin; Dion, Jeanne
Subject: Questions from EICB on Draft Test Plan (Closure of HH-083)
Attachments: HH-083 Questions from NRC-EICB WBN U2 4-13-2015.docx

Bob,

Please see the attached document with detailed questions from EICB on the draft Test Plan submitted by TVA.

Anthony Minarik
301-415-6185

Office of Nuclear Reactor Regulation (NRR)
Division of Operating Reactor Licensing (DORL)
Watts Bar Special Projects Branch (LPWB)

Normal Hours:
0600-1545: Mon-Fri

Hearing Identifier: NRR_PMDA
Email Number: 1994

Mail Envelope Properties (Anthony.Minarik@nrc.gov20150413074600)

Subject: Questions from EICB on Draft Test Plan (Closure of HH-083)
Sent Date: 4/13/2015 7:46:59 AM
Received Date: 4/13/2015 7:46:00 AM
From: Minarik, Anthony

Created By: Anthony.Minarik@nrc.gov

Recipients:

"Arent, Gordon (garent@tva.gov)" <garent@tva.gov>
Tracking Status: None
"Poole, Justin" <Justin.Poole@nrc.gov>
Tracking Status: None
"Dion, Jeanne" <Jeanne.Dion@nrc.gov>
Tracking Status: None
"Bryan, Robert H Jr (rhbryan@tva.gov)" <rhbryan@tva.gov>
Tracking Status: None

Post Office:

Files	Size	Date & Time
MESSAGE	342	4/13/2015 7:46:00 AM
HH-083 Questions from NRC-EICB WBN U2 4-13-2015.docx		34034

Options

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

NRR/DE/EICB Comments Regarding Closure of Open Item 83 in Watts Bar Unit 2 Safety Evaluation Report NUREG-0847, Supplement 23

In Supplement 23 of NUREG-0847(ADAMS Accession No. ML1206A499), TVA was to confirm to the NRC the completion of a data storm test on the DCS. This was identified as Open Item 83. Per Section 7.7 of the Standard Review Plan, the NRC staff is directed to perform an evaluation of the effects of control system failures on plant safety. The review is required to 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. One aspect of control system failure of concern is the potential for a failure within a data communications network that is connected to multiple control systems. It may be possible for such a failure to simultaneously prevent two or more control systems from properly functioning in such a manner that results in the plant being put into a condition that has not been previously analyzed in the SAR. TVA has proposed to conduct a network data storm test to confirm that the control systems associated with the functions described in FSAR Section 7.7.1.11.1 will continue to perform their required control functions with a failed communication network without any plant upset.

In order for the staff to close Open Item 83, the staff needs to understand the benefits and limitations of any testing that is performed to demonstrate that it is not possible (or very unlikely) for a data communications fault occurring on a common control system network to simultaneously prevent two or more control systems from properly functioning in such a manner that results in the plant being put into a condition that has not been previously analyzed in the SAR. With regard to the draft test procedure provided by TVA to date, the staff has additional questions to aid in its understanding of the test that has been proposed.

- 1) TVA is requested to provide a copy of the data storm test plan, which establishes the requirements, general methodology, test objectives, and acceptance criteria for the test. The plan should provide the reasons why the proposed test procedure will conclusively demonstrate the objectives of the test are satisfied. There should be a description of the required analysis of the test data resulting from performance of the test that would support (or how it may not support) the final conclusion. The test plan information should also include these specific objectives:
 - a. How the results will support the segmentation analysis and, particularly, the conclusion that the events listed in NUREG-0847, Section 7.7.1.4.4.1, items (1) through (8), will not be caused by the propagation of failures. Also confirmation should be provided that the failures of one control processor (CP) pair are limited to outputs failing high, low, or as is.
 - b. NUREG-0847 also states that: "The test will demonstrate conformance to Clause 6.3 of IEEE Std. 603-1991 by proving that the Foxboro I/A mesh will not propagate failures from one segment to another and cause a plant upset." The test then shall specifically state Clause 6.3 of IEEE Std. 603-1991 is met and the

propagation of failures does not take place beyond the Foxboro I/A meshnetwork from one segment to another.

- c. Finally, the test should confirm that a failed communication network, which includes consideration of the effects of both network action and inaction, will permit the system to continue to function and will not cause plant conditions more severe or not previously identified in the analysis of anticipated operational occurrences in Chapter 15 of the SAR.
- 2) The NRC staff requests a network diagram that depicts the associated control system workstations, switches, firewalls, and connectivity of the following systems on the control network:
 - a. Feedwater Flow/Steam Generator Level Control System
 - b. Feedpump Turbine Speed Control system
 - c. Condenser Steam Dump valve/loss of load interlock controls
 - d. Atmospheric steam dump valve controls
 - e. SG PORV controls
 - f. Pressurizer Pressure, Level, charging, letdown spray, cold overpressure mitigation controls
 - g. Auxiliary Control system
- 3) The NRC staff also requests a table that relates the associated switches and ports to the names of the control systems listed above would be very helpful in understanding the procedure supplied.
- 4) See specific comments ATTACHMENT 1: Comments to "WBN U2 Foxboro I/A Network Storm Test," Procedure No. ?,

Comments to:
WBN U2 Foxboro I/A Network Storm Test
Procedure No.?
DRAFT

General Comments:

- 1) In each of the Broadcast and Multicast tests, the description reads “This test will verify system performance” and data is recorded but no acceptance criteria is identified for the generated or destination network traffic at the given ports.
- 2) Only Test 6.5, “Aux Control Room CP Broadcast Storm Testing,” makes a statement that would be considered a test objective. That test states: “This test will verify that the broadcast limit settings for the FCPs and WSs are functioning correctly.” The remaining tests should identify a similar specific objective.
- 3) Also, each of these tests say to “document system performance observed” (e.g. Workstation ___ Normal ___ Smurf). It is not clear what type of entry is required. Is it a matter of simple acceptance or if data is requested to be entered in those spaces.

4) Specific Comments:

Comment	Section	Description	Comment
a. Comment on test requirements and criteria	All Sections	Acceptance Criteria	With the exception of verifying the “0-100%” in X seconds, there are no adequate testing requirements or acceptance criteria identified in the procedure. Where will these be described?
b.	Attachments/Forms	Lists 7 items in this category	Only Attachments 1, 2 & 3 are included.
c.	5. Special Tools & Equipment	Test Indicator; 0 – 100% scale	Further information is necessary on what this equipment is. (e.g., name, inputs, what it measures etc.).
d.	5. Special Tools & Equipment	Network Sniffer – PC with Ethereal or Wireshark installed	If Ethereal is installed, the libpcap packet capture library software should be or may already be installed. However, it is not clear if the intent is to simply capture packet information, but rather what to check for.

Comment	Section	Description	Comment
e.	6.1.1.11 Test Step	Obtain printout of CP6TEST compound and blocks and attach in Attachment 3	Wireshark captures packets and lets you examine their contents. It is not clear what the test is requesting or what the inspection criteria are.
f.	6.1.1.13 Test Step	Verify that the output from W20614 CH 8 sweeps from 0-100% in approx. X seconds.	What is the intent of identifying "X" seconds? Is this to be determined later? How will this be determined? How was the value for "X" determined? Is it different for different components?