

From: Getachew Tesfaye
To: DAFLUCAS Ronda M.
Date: 5/22/2007 1:06:17 PM
Subject: Draft RAI-2, Software Program Manual Topical Report

Ronda,
Attached please find a draft of the second round of RAIs for the Software Program Manual Topical Report (ANP-10272). We will have our technical staff available to discuss them with you as soon as you are ready. Please call me with a proposed date and time for the telecon.

Thanks,
Getachew Tesfaye
Project Manager
NRO/DNRL/NAR1

CC: Norbert Carte; Tarun Roy

Mail Envelope Properties (46532309.568 : 24 : 8846)

Subject: Draft RAI-2, Software Program Manual Topical Report
Creation Date 5/22/2007 1:06:17 PM
From: Getachew Tesfaye

Created By: GXT2@nrc.gov

| Recipients | Action | Date & Time |
|---|---------------|------------------------|
| areva.com PM Ronda.Daflucas (DAFLUCAS Ronda M.) | Transferred | 5/22/2007 1:06:26 |

| | | |
|--|-----------|-------------------|
| nrc.gov OWGWPO01.HQGWDO01 PM NNC CC (Norbert Carte) | Delivered | 5/22/2007 1:06:21 |
|--|-----------|-------------------|

| | | |
|---|-----------|-------------------|
| nrc.gov TWGWPO03.HQGWDO01 PM TCRI CC (Tarun Roy) | Delivered | 5/22/2007 1:06:19 |
|---|-----------|-------------------|

| Post Office | Delivered | Route |
|--------------------|----------------------|--------------|
| OWGWPO01.HQGWDO01 | 5/22/2007 1:06:21 PM | nrc.gov |
| TWGWPO03.HQGWDO01 | 5/22/2007 1:06:19 PM | nrc.gov |

| Files | Size | Date & Time |
|--|-------------|------------------------|
| MESSAGE | 763 | 5/22/2007 1:06:17 PM |
| DRAFT RAI - SOFTWARE PROGRAM MANUAL TR.wpd | 30364 | 5/22/2007 12:57:46 PM |

Options

| | |
|-----------------------------|----------|
| Auto Delete: | No |
| Expiration Date: | None |
| Notify Recipients: | Yes |
| Priority: | Standard |
| ReplyRequested: | No |
| Return Notification: | None |

| | |
|---------------------------|----------|
| Concealed Subject: | No |
| Security: | Standard |

| | |
|-------------------------|--------------------|
| To Be Delivered: | Immediate |
| Status Tracking: | Delivered & Opened |

DRAFT

SECOND REQUEST FOR ADDITIONAL INFORMATION (RAI)

ANP-10272, "SOFTWARE PROGRAM

MANUAL FOR TELEPERM XSTM SAFETY SYSTEMS

TOPICAL REPORT" (TAC NO. MD3971)

PROJECT NUMBER 733

- RAI 29) Will the second U.S. EPR be programmed from scratch, or will software from the first U. S. EPR be reused or adapted for the second? If reuse or adaption is intended, then how is it described in the SPM?

AREVA has stated, in a public meeting, that the application software for the U.S. EPR will be developed in the US. The software development process described in ANP-10272, "Software Program Manual TELEPERM XS Safety Systems Topical Report" (SPM) seems to describe a design from scratch process for application software. However, it is anticipated that one application may contain enough similarities to another that it could appear to be cost effective to start with one application and modify it to make another (e.g. 1st U.S. EPR to 2nd U.S. EPR). Will application software be reused, or adapted from one application to create another? If reuse of application software is anticipated, then please describe how the SPM addresses it. Will the first U.S. EPR application programs be programmed from scratch in the U.S. or will they reuse some of the application code from prior European designs?

- RAI 30) Please describe the process that will be followed to adapt the software development plans to the version of TELEPERM XS (TXS) that will be used.

The versions of hardware and software described in the TXS Topical Report (TR) will not be used for U.S. EPR or other US applications. However, this has not been explicitly stated by AREVA. Does the SPM assume that the TXS platform that will be used is the one that has been approved? If not, please describe the version of TXS that the SPM is applicable to. Also, if the applicable version TXS is not a currently approved version, then please describe the plans to adapt the SPM to the approved version that will be used.

- RAI 31) Please describe how the SPM is coordinated with the processes and procedures used to establish reasonable assurance that the desire product will be produced.

10 CFR 50 Appendix B: 'The pertinent requirements of this appendix apply to all activities affecting the safety-related functions of those structures, systems, and

Enclosure

components; these activities include designing, purchasing, fabricating, handling, shipping, storing, cleaning, erecting, installing, inspecting, testing, operating, maintaining, repairing, refueling, and modifying. As used in this appendix, "quality assurance" comprises all those planned and systematic actions necessary to provide adequate confidence that a structure, system, or component will perform satisfactorily in service.' Therefore the software development plans are part of the quality assurance (QA) program. However, the SPM does not describe how the software development plans fit into the rest of the AREVA QA program. Please describe how the software development plans are coordinated with the QA program. Please be sure to identify the applicable approved Appendix B program.

- RAI 32) Please describe how the SPM ensures that the software development plans produced will satisfy the acceptance criteria identified in Branch Technical Position (BTP) No. 14.

BTP No. 14 identifies acceptance criteria for process planning. These acceptance criteria are grouped into three groups of characteristics: Management, Implementation, & Resource. The SPM does not seem to contain requirements that these desirable characteristics are achieved.

- RAI 33) Please describe any suggestions that AREVA will provide to the customers on how to address cyber security in the latter life cycle phases.

SPM Section 9.3 says: "The guidance of Regulatory Guide 1.152 is implemented as follows: ... Items C.2.6 through C.2.9 specify guidance to be addressed by the customer and do not apply to AREVA NP." However, it is expected that some aspects of cyber security are TXS specific, and therefore AREVA may be in the best position to provide recommendations on TXS specific cyber security measures in latter life cycle phases.

- RAI 34) Please describe the process models that will be used and the types of simulations that will be conducted in the software development process.

SPM Section 1.4 says: "SIVAT ... Process models can also be linked into the simulator to perform closed-loop tests." This statement says what can be done. However, it is not clear what will be done, or what is required by the SPM to be done.

SPM Section 4.3.6 says: "The SIVAT testing and its results confirm that the software design is consistent with a basis from the safety analysis." Is it currently planned to use process models and simulate each function credited in the Safety Analysis Report (SAR)? If not, please explain the analysis used to bridge the gap between what will be tested and what will be credited.

- RAI 35) Please describe the development process of the Simulation based Validation Tool (SIVAT).

Section 5.1.2 of the TELEPERM XS Topical Report (TXS TR) says: "The

development of each component and of each tool shall follow a development process, which consist of six phases ..." The SPM describes the use of the SIVAT tool. The SIVAT tool was not described in the TXS TR. Please describe how the development process of the SIVAT addresses the requirements in the TXS TR.

- RAI 36) Please describe any cyber security assessments of TXS and any associated actions to address concerns identified. Note: The response to this question may contain safeguards information and if so, must be treated appropriately.

Cyber security concerns can be addressed either in hardware or in software. The TXS system may have cyber security concerns that have been identified in previous assessments. AREVA must have a plan to address these concerns, and to the extent that these concerns are addressed in software, then the plans that will be developed in accordance with the SPM must address these concerns. Please describe how the plans developed in accordance with the SPM will address cyber security concerns.

- RAI 37) Please describe how the SPM addresses the need to update the software development plans.

NUREG-0800 Chapter 7, Branch Technical Position (BTP) No. 14 assumes that a certain process will be followed in developing digital computer-based instrumentation and control systems. This process includes three aspects 1) development of project specific plans 2) following the plans, and 3) assessing that the results produced are acceptable. BTP No. 14 provides acceptance criteria for each of these aspects. The following paragraphs are included to demonstrate that the BTP No. 14 concept of the plans is that they are project specific and adaptable.

Section A.3.1.2 of BTP No. 14 contains a definition of the implementation characteristics, which includes: "Schedule - The time order of events necessary to achieve the purpose of the planning document, given either as absolute dates ..." A schedule that includes absolute dates is applicable to project specific activities and not to project neutral items.

Section A.3.1.3 of BTP No. 14 contains a definition of the resource characteristics, which includes: "Budget - The financial resources necessary to carry out the work." A plan that includes a budget is applicable to project specific activities and not to project neutral ones.

Section A.3.1.3 of BTP No. 14 contains a definition of the resource characteristics, which includes: "Personnel - The numbers ... of personnel required to carry out the work defined in the planning document." A plan that includes the number of personnel is applicable to project specific activities and not to project neutral ones.

NUREG/CR-6101 says: "Planning activities result in the creation of a number of documents that are used to control the development process." The implication is that planning activities are documented in plans. It is anticipated that each project

will be planned.

Section B.3.1.1 of BTP No. 14, "Acceptance Criteria for Software Management Plan (SMP)," identifies that Regulatory Guide 1.173 endorses IEEE Std 1074-1995, subject to provisions listed. IEEE Std 1074-1995 Clause 3.1.6, "Plan Project Management," says: "As new or revised Input Information is received in this Activity, project plans shall be updated and further project planning shall be based upon these updated plans."

Section B.3.1.10 of BTP No. 14, "Software Verification and Validation Plan (SVVP)," identifies that Regulatory Guide 1.168, Revision 1, endorses IEEE Std 1012-1998, "IEEE Standard for Software Verification and Validation," as providing methods acceptable to the staff for meeting the regulatory requirements as they apply to verification and validation of safety system software, subject to the exceptions listed. IEEE Std 1012-1998, Section 5.1.1 says: "The management of V&V activities is performed in all software life cycle processes and activities. This activity continuously reviews the V&V Effort, revises the SVVP as necessary based upon updated project schedules and development status ..."

Section B.3.1.10 of BTP No. 14, "Software Configuration Management Plan (SCMP)," identifies that Regulatory Guide 1.169, "Configuration Management Plans for Digital Computer Software Used in Safety Systems of Nuclear Power Plants," endorses IEEE Std 828-1990, "IEEE Standard for Configuration Management Plans," as providing an acceptable approach for planning configuration management. IEEE Std 828-1990 Section 2.6, "SCM Plan Maintenance," says: "The Plan should be reviewed at the start of each project software phase, changed accordingly, and approved and distributed to the project team."

RAI 38)

Please explain how the SPM describes the incorporation of information from the new nuclear plant implementation process.

In the letter that Areva sent to the U.S. NRC submitting the SPM for review, AREVA stated: "AREVA NP intends to use the Software Program Manual to support digital safety instrumentation and control (I&C) system upgrades at operating nuclear plants and digital safety systems for new nuclear plants." However, the SPM does not describe how the information produced as part of the 10 CFR 52 licensing process is used in the software development process. What information relative to the software development process will be in the certified design? Where will that information be located? How will the information in the certified design be used in the software development process? What information relative to the software development process will be in the Combined Operating Licence (COL)? Where will that information be located? How will the information in the COL be used in the software development process?