**From:** Getachew Tesfaye
**To:** DAFLUCAS Ronda M.
**Date:** 8/2/2007 6:43:14 AM
**Subject:** Draft RAI 3, Software Program Manual Topical Report

Ronda,
Attached please find a draft of the third 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
Sr. Project Manager
NRO/DNRL/NARP

**CC:** Lois James; Norbert Carte

**Mail Envelope Properties** (46B1B542.F16 : 24 : 8846)

| | |
|---|---|
| **Subject:** | Draft RAI 3, Software Program Manual Topical Report |
| **Creation Date** | 8/2/2007 6:43:14 AM |
| **From:** | Getachew Tesfaye |
| **Created By:** | GXT2@nrc.gov |

| **Recipients** | **Action** | **Date & Time** |
|---|---|---|
| areva.com | Transferred | 8/2/2007 6:43:47 AM |
| Ronda.Daflucas (DAFLUCAS Ronda M.) | | |
| nrc.gov | | |
| OWGWPO01.HQGWDO01 | Delivered | 8/2/2007 6:43:20 AM |
| NNC CC (Norbert Carte) | Opened | 8/2/2007 8:40:04 AM |
| nrc.gov | | |
| OWGWPO04.HQGWDO01 | Delivered | 8/2/2007 6:43:20 AM |
| LMJ CC (Lois James) | Opened | 8/2/2007 6:52:39 AM |

| **Post Office** | **Delivered** | **Route** |
|---|---|---|
| | | areva.com |
| OWGWPO01.HQGWDO01 | 8/2/2007 6:43:20 AM | nrc.gov |
| OWGWPO04.HQGWDO01 | 8/2/2007 6:43:20 AM | nrc.gov |

| **Files** | **Size** | **Date & Time** |
|---|---|---|
| MESSAGE | 791 | 8/2/2007 6:43:14 AM |
| DRAFT RAI-3 SOFTWARE PROGRAM MANUAL TR.wpd | 47697 | 8/2/2007 6:41:06 AM |

**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**

THIRD REQUEST FOR ADDITIONAL INFORMATION (RAI)

ANP-10272, "SOFTWARE PROGRAM

MANUAL FOR TELEPERM XSTM SAFETY SYSTEMS

TOPICAL REPORT" (TAC NO. MD3971)

PROJECT NUMBER 733

RAI 39) Where are the software security activities for each phase specified?

Section 9.3, "Security and Disaster Recovery," states: "As recommended by Regulatory Guide 1.152 ... software security activities are specified for each phases of the application software development life cycle." However this section does not say where these activities are specified.

RAI 40) How are the planning activities of the Technical Manager documented?

Section 2.1.1, "Technical Manager," states: "The technical manager is responsible for software planning, technical development, integration, installation, and testing of the TELEPERM XS application software."

RAI 41) Please describe the activities associated with the integration of the software with the hardware.

Section 1.2, "AREVA NP Coverage of BTP HICB-14," describes the installation activity after the testing activities (i.e after SIVAT testing in the design phase and Factory Acceptance Testing in the testing phase), and associates the installation activities with Commissioning. Therefore the term "installation" is understood to refer to system installation at the plant. What term (e.g. "software installation") is used to refer to those activities of loading the software onto the target hardware at the factory prior to Factory Acceptance Testing (FAT)? What term (e.g. "software integration") is used mean the integration of the application software with the system software, in the development environment?

Table 1-1, "AREVA NP Coverage of BTP HICB-14," states that the Integration Plan is discussed in Section 2.0, "ORGANIZATION," of the SPM. It is understood that this "Integration Plan" is intended to address the acceptance criteria of the SRP associated with the Software Integration Plan (SIntP) as described in Section B.3.1.4 of Branch Technical Position (BTP) No. 14.

Section 2.0 states: "Because AREVA NP uses the approved SPACE tool to automatically generate the application software and the SPACE tool produces software that is designed to work with the system software of the TELEPERM XS

system, no software integration effort is required between the system software and application software. Therefore, a separate software integration organization or software installation organization is not necessary."

Regulatory Guide 1.73, "Developing Software Life Cycle Processes for Digital Computer Software Used in Safety Systems of Nuclear Power Plants," endorses, subject to the exception listed in the regulatory position, IEEE Std 1074-1995. IEEE 1074 Section 5.3.8.3, "Description [of performed integration]," states: "If the system includes both hardware and software components, the system integration may be included as part of this Activity." Since all TXS system will contain both hardware and software, please describe where system integration is considered (e.g. planned).

Chapter 7, "Instrumentation and Controls ," of NUREG-0800, "Standard Review Plan for the Review of Safety Analysis Reports for Nuclear Power Plants," contains BTP No. 14, "Guidance on Software Reviews for Digital Computer-Based Instrumentation and Control Systems." Section B.3.1.4.1 of BTP No. 14, Revision 5 Dated March 2007, states: "The SIntP [Software Installation Plan] should include a general description of the software integration process and of the hardware/software integration process."

RAI 42) Please describe the activities associated with the installation of a TXS system.

Section 2.1.5, "I&C Engineers," states: "The I&C engineers also install the software prior to the factory acceptance test, and installation and commissioning." Therefore there appear to be two times that software is installed, and one time that the system is installed. Correct?

Section B.3.1.5.2, "Implementation Characteristics of the SInstP," of BTP No. 14, Revision 5 Dated March 2007, states: "The SInstP should describe procedures for software installation, for combined hardware/software installation, and systems installation." However Section 2.0 of the SPM TR does not appear to address any of these aspects.

RAI 43) Please describe how the Software Operation and Maintenance Plan (SOMP) follows the guidance of IEEE 1074.

Section 7.0, "SOFTWARE OPERATIONS AND MAINTENANCE PLAN," states: "The Software Operations and Maintenance Plan follows the life cycle planning for operations and maintenance guidance of IEEE 1074." However, Section C.2 of RG 1.173 states: "IEEE Std 1074-1995 is an organizing standard that ensures that activities deemed important to software quality are performed and related properly to each other; it does not provide detailed information regarding the implementation of specific life cycle activities."

RAI 44) Please clarify text the states that IEEE 1074-1995 presents a software development life cycle model.

Section 9.0, "SOFTWARE DEVELOPMENT DOCUMENTATION," states: "The

software development life cycle at AREVA NP has been mapped to the software life cycle model presented in IEEE 1074." However, Section 2.1, "Overview," of IEEE Std 1074-1995 states: "While this standard neither dictates nor defines a specific software life cycle (SLC) or its underlying methodologies, it does require that an SLCM be chosen and used."

RAI 45) Where are the Application Life Cycle Activities referred to in the header row of the Table in the Appendix to the SPM TR described?

How do the activities described in the appendix related to the phases described in Section 1.2, "TELEPERM XS Application Software Life Cycle Overview?"

How do the "II.E Create Project Plan" and "III.G Create Software Life Cycle" life cycle activities in the appendix related to the SPM TR and the software development plans?

RAI 46) Please provide an evaluation that discusses how the lower SIL classifications proposed in Section 1.3, "Software Classification," provide an acceptable method of complying with those rules or regulations of the Commission, or portions thereof, that underlie the corresponding SRP acceptance criteria.

Section 1.3 states: "The portions of the application software that do not perform design basis accident mitigation functions directly may be classified with a lower SIL classification that is appropriate to the relative importance to safety ..." However, Section 5.3.3 of IEEE Std 7-4.3.2-2003 states: "... V&V requirements for the highest integrity level (level 4) apply to systems developed using this standard ..."

Section 1.3 also states: "A criticality analysis determines the appropriate SIL classifications and assigns the classifications following the guidance of IEEE 1012 ..., which is endorsed by Regulatory Guide 1.168 ..., and the AREVA NP Plan for Software Development in Section 9." However, Section C.1 of RG 1.168 states: "Software used in nuclear power plant safety systems should be assigned integrity level 4 or equivalent, as demonstrated by a mapping between the applicant or licensee approach and integrity level 4 as defined in IEEE Std 1012-1998."

RAI 47) Please explain how the Software Training Plan (STrngP) is addressed.

Section 1.0, "INTRODUCTION," states: 'Table 1-1 shows how the suggested plans from BTP HICB 14 are addressed." Table 1-1 states that the training plan is implemented in Section 8.0, "CUSTOMER SOFTWARE TRAINING PLAN,".' However, Section 8.0 states: "The customer training plan is included as a part of the project plan." Is the STrngP in Section 8.0 or in the project plan?

Section 8.0 also states: "The AREVA NP operating instructions that implement the customer training plan control the specifics of the training provided to the customer." Is the STrngP implemented in Section 8.0 or in operating instructions?

Are operating instructions included in the project plan (e.g. by reference)?

Section 8.3, "Responsibilities," refers to "internal implementing procedures". What is the relationship between operating instructions and internal implementing procedures? Can these procedures be identified now?

Section 8.4, "Measurements," states: "The implementing documents of the customer training plan ensure that feedback is gathered and incorporated into the training process." What are the implementing documents and how are they related to the other document identified?

RAI 48) Please explain how many training plans there are and how they fit together.

Table 1-1 refers to a "training plan". The title of Section 8.0 refers to a "Customer Software Training Plan". The body of Section 8.0 refers to: "AREVA NP customer training plan," "customer's training plan," and "project training plan."

Has a project training plan been produced for the U.S. EPR? Note: Section 8.0 states: "The customer's training plan and specification are referenced to produce a project training plan..."

For the U.S. EPR, what is the "customer's training plan?" Since Areva is pursuing a design certification that is not related to any specific customer; is it appropriate for there to be an Areva document that contains the same material that might otherwise be found in a customer's training plan? What is that document?

RAI 49) What specific operating instructions implement each plan?

Table 1-1 identifies that certain plans are implemented by "Operating Instructions". However the specific operating instructions that implement each plan have not been identified. How are the operating instructions related to the AREVA NP Administrative Procedures referenced in Section 12.0, "REFERENCES."

RAI 50) How is operator training addressed?

The training described seems to address the functioning of the TXS components. However, operator training on the delivered system does not seem to be addressed. Please explain.

RAI 51) Regarding Response to RAI No. 1: Please explain the difference between verification that a code generator worked correctly and validation of the application software.

RETRANS was used to confirm "correct application of the tool for code generation." This is in effect verification that the code generator worked properly. RETRANS is a code generation tool verification tool, not a software validation tool. One may be able to say that the RETRANS analysis validated the proper operation of the code generation tool, but RETRANS was never used to validate application software.

**Note:** The point here is not to get confused about what verification and validation are, as Areva and the U.S. NRC may have different definitions for these two terms. The point is that RETRANS and SIVAT are understood to do completely

different things.

It is understood that the TXS TR explained that the proper operation of the code generators was ensured by type testing and verification of specific applications using RETRANS, as explained below. As explained in RAI No. 1: TXS TR Section 2.4.3.3.3 states: 'As a diverse measure to detect potential software faults not found by the means described in Section 3.2.1, the verification tool "RETRANS" developed by GRS-ISTec is used as an independent testing tool.' Section 3.2.1, "Software Type Test," states: "The basic intention of type-tests is to separate out tests and inspections that are independent of a specific application from those that are specific to the safety needs of a particular power plant." TXS TR Section 3.2.1.3, "Scope of Components," states: "... in addition to type-testing the on-line components of TELEPERM XS, the tools used to automatically generate parts of the on-line software are type-tested."

How many revisions has each tool, involved in the automatic code generation of the application software, undergone since RETRANS was last used?

SIVAT is a simulation tool that allows the application software to be tested prior to installation into the target hardware.

RAI 52) Regarding Response to RAI No. 1: What is the input to the SIVAT? Does SIVAT take as an input, the C code generated by the code generators, or does it use the generators and run them against the project database?

Is the code then adapted such that it can run as a model in the simulation control system? That is to say, is the code test using SIVAT, exactly the same as that which will run on the target platform?

RAI 53) In the TXS TR, a set of methods was used to develop and test the code generation tools, and these methods were deemed to require additional application specific testing using RETRANS. Have those methods changed? If not, then why does Areva now feel that these same methods no longer require the application specific testing?

RAI 54) Regarding Response to RAI No. 1: Please explain how the change from using RETRANS to verify code generation to SIVAT to Validate application software, does not constitute a change in the TXS System design principles and methods for safety related applications as described in the TXS TR.

RAI 55) Regarding Response to RAI No. 1: What is the latest version of AREVA NP Report No. NGLP/2004/en/0094, "TELEPERM XS Simulation - Concept of Validation and Verification."

RAI 56) Regarding Response to RAI No. 1: Was there a documented plan that defined what constituted the "introductory phase", and when this phase terminated?

RAI 57) Regarding Response to RAI No. 1: Please provide the documented evaluation that determined that RETRANS was no longer needed?

RAI 58) Regarding Response to RAI No. 1: What TXS systems have been built, and which ones were part of the "introductory phase" (i.e. which ones used RETRANS).

RAI 59) Regarding Response to RAI No. 1: Please describe any instances where a system tested using SIVAT did not perform as expected after construction. Please also describe any associated corrective actions.

RAI 60) Regarding Response to RAI No. 2: Please describe, and identify the associated sections in the TXS TR, that contain any guidance or requirements for the application software development process.

The response to RAI No. 2 is very informative. However, the intent of the original question was not addressed. Section 2.1 of the U.S. Digital Protection System Topical Report states: "The NRC's approval of the TXS platform as a qualified, generic digital I&C platform also constitutes approval of the TXS system design principles and methods for safety-related applications that were documented in ..." If the Areva believes that the TXS TR did not contain guidance or requirements for the application software development process, then please say so explicitly.

Note 1: The description of the use of RETRANS in the TXS TR is applicable to the application software development process.

Note 2: The description in Section 2.4, "Reliability," of the TXS TR contains implications for the application development process.

Since the SPM does not reference any TXS TR guidance or requirements for application software development, it is assumed that Areva is not crediting any prior approval of guidance or requirements governing application software development. Is this correct?

RAI 61) Regarding Response to RAI No. 3: What documentation contains the "Functional Diagrams"?

Are the functional diagrams printed and included into a document? Or are they only visible through the Specification and Coding Environment (SPACE) tool.

RAI 62) Regarding Response to RAI No. 3: What procedures control the software requirements specification (SRS)?

The Response to RAI No. 5 states: 'The term "Software Requirements Specification" in ANP-10272 directly correlates to the term "Software Requirements Specification," as described in Section 2.2.2.7 in the NRC safety evaluation report (SER) for the TXS topical report.'

Section 2.2.2.7 in the NRC SER for the TXS topical report states: 'The software requirements specifications are controlled by Siemens Engineering Procedure FAW-3.4, "Contents and Structure of System Specifications for Software Components," and FAW-3.5, "Contents and Structure of Design Documents for Software Components." FAW-3.4 describes the process to be used for converting the system requirements into software specifications. FAW-3.5 describes the technical processes for converting the software specification into a module structure

that may be used for implementing the software requirements.'

Therefore it is understood that the engineering procedures described in the TXS TR are applicable to the SRSs developed under the SPM. Correct?

RAI 63) Regarding Response to RAI No. 3: What procedures control the Software Design Descriptions (SDDs)?

The Response to RAI No. 5 states: 'The term "Software Design Description" in the SPM directly correlates to the term "Software Design Description" described in Section 2.2.2.9 in the NRC safety evaluation report (SER) for the TXS TR.'

Section 2.2.2.9 in the NRC SER for the TXS TR states: 'The processes controlling the software design description are specified in Siemens Engineering Procedure FAW-3.5, "Contents and Structure of Design Documents for Software Components," and FAW-3.6, "Contents and Structure of Implementation Documents for Software Components." FAW-3.5 describes the process by which the software specification is translated into the software design description. FAW-3.6 describes the process by which the software design description is implemented.'

Therefore it is understood that the engineering procedures described in the TXS TR are applicable to the SDDs developed under the SPM. Correct?

RAI 64) Regarding Response to RAI No. 5: Where will the Functional Requirements Specification be addresses?

The response to RAI No. 5 states: "...In general, the functional requirements for the safety-related digital protection and control systems are drawn from the Final Safety Analysis Report for operating plants and the Design Control Document for certified designs. ..." Is the correct understanding of this answer that the functional requirements specification will not be included in the documentation submitted as part of the DCD application?

Presumably the design can not be completed before the required functionality is specified. Therefore does Areva NP intend to use Design Acceptance Criteria (DAC) for the specification of the functional requirements? Does Areva NP intend the specification of the functional requirements to be included in the Combined Operating License (COL) application material? Does Areva NP intend the specification of the functional requirement to be addressed in Inspection Test Analysis and Acceptance Criteria (ITAAC)?

RAI 65) Regarding Response to RAI No. 6: Please explain why the NRC should make a determination of the acceptability of the SPM prior to receiving the evaluation of the SPM against the SRP.

10 CFR 50.34(h) states: "Applications ... shall include an evaluation of the facility against the SRP in effect on May 17, 1982 or the SRP revision in effect six months prior to the docket date of the application, whichever is later." Since any application that may reference the SPM will be submitted after August 2007, the current version

of the SRP would be applicable, and not the version that was applicable at the time the SPM was submitted.

The response to RAI No. 6 states: 'AREVA NP evaluated ANP-10272 and other internal work processes and procedures against BTP HICB-14 as part of the development of the topical report. BTP HICB-14 was the version that was in effect at the time ANP-10272 was submitted to NRC for review. The results of conformance assessment are documented in AREVA NP document 51-9047411-000, "Alignment of the TXS System Application Software Program, as described in the Software Program Manual, with Branch Technical Position HICB-14." '

RAI 66) Regarding Response to RAI No. 9: Please describe the convention for documenting requirements in the Software Program Manual.

The response to RAI No. 9 is very informative and will be considered in the review of any Operating Instructions and project-specific plans that are submitted for review. However, the intent of the original question was not addressed. The Abstract of the SPM states: "This Software Program Manual describes the requirements and objectives for the following plans ..." It is the desire of the reviewer to identify the requirements in the SPM, and make a determination of the acceptability of the SPM, based on the requirements that it imposes on lower tier documents. The reviewer has not been able to identify any convention that is being followed to distinguish between descriptive material and the statement of requirements for lower tier documents. This was the basis for the original question.

RAI 67) Regarding Response to RAI No. 9: Please clarify the convention that Areva NP uses for identifying requirements in programmatic documents.

The response to RAI No. 9 states: 'AREVA NP uses the term "shall" to denote requirement statements in Operating Instructions and project-specific plan documents. The AREVA NP Procedures and Policies Dictionary defines shall as "Denotes a requirement." The term "shall" is used in the Operating Instructions and project-specific plans to implement the ANP-10272 requirements.'

However, Areva NP has also stated in ANP-10266 Revision 1: '... implementing procedures and instructions implement the QAP.' Therefore the SPM and the QAP are similar programmatic documents that are implemented by procedures, instructions or plans. However, the QAP uses "shall" to identify requirements and the SPM does not. Please explain this apparent inconsistency.

RAI 68) Regarding Response to RAI No. 9: Please identify number of requirements that the SPM places on each lower tier document.

The reviewer will look at a section, and try to determine the number of requirements in that section. In order for the requirements to be unambiguously stated, Areva and the U. S. NRC should arrive at the same number of requirements. Subsequently, the U.S. NRC may look at the lower tier documents in order to determine whether they satisfy the requirements of the SPM.

RAI 69) Regarding Response to RAI No. 33: Please explain the discrepancy between the Areva position that Regulatory Guide 1.152 and NEI 04-04 Revision 1 provide consistent guidance and the consensus(Industry and U.S. NRC) position that the two documents provide inconsistent guidance.

The response to RAI No. 33 states: 'AREVA NP recognizes that the Nuclear Energy Institute has issued document NEI 04-04, "Standard Cyber Security Program for Operating Reactors," to address a method of compliance pending rule change 10 CFR 73.55(m), "Digital computer and communication networks." This document addresses the topics associated with items C.2.6 through C.2.9 from Regulatory Guide 1.152, "Criteria for Use of Computers in Safety Systems of Nuclear Power Plants," Revision 2. '

However, it appears that there is consensus between the Nuclear Industry and the NRC that: "Regulatory Positions 2.1 - 2.9 of RG 1.152 and NEI 04-04 provide conflicting guidance for implementing cyber security requirements for safety systems at nuclear power plants." (i.e. See Problem No. 1 at the bottom of page 4 of ML071900253)

RAI 70) Regarding Response to RAI No. 33: Please provide a detailed description of how NEI 04-04 Revision 1 addresses Regulatory Guide 1.152 Position 2.9.