From: Getachew Tesfaye
To: DAFLUCAS Ronda M.
Date: 3/22/2007 8:20:10 AM
Subject: Draft RAI - Software Program Manual TR

Ronda,
Attached please find the subject draft RAIs. 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.
Getachew Tesfaye
Project Manager
NRO/DNRL/NAR1

CC: John Smith; Joseph Colaccino; Larry Burkhart

Mail Envelope Properties (4602747A.544 : 24 : 8846)

Subject: Draft RAI - Software Program Manual TR
Creation Date 3/22/2007 8:20:10 AM
From: Getachew Tesfaye

Created By: GXT2@nrc.gov

Recipients	**Action**	**Date & Time**
areva.com	Transferred	3/22/2007 8:20:33 AM
Ronda.Daflucas (DAFLUCAS Ronda M.)		
nrc.gov		
OWGWPO01.HQGWDO01	Delivered	3/22/2007 8:20:18 AM
LJB3 CC (Larry Burkhart)		
nrc.gov		
OWGWPO03.HQGWDO01	Delivered	3/22/2007 8:20:17 AM
JXC1 CC (Joseph Colaccino)	Opened	3/23/2007 8:39:10 AM
nrc.gov		
TWGWPO02.HQGWDO01	Delivered	3/22/2007 8:20:10 AM
jms7 CC (John Smith)	Opened	3/22/2007 10:09:25 AM

Post Office	**Delivered**	**Route**
		areva.com
OWGWPO01.HQGWDO01	3/22/2007 8:20:18 AM	nrc.gov
OWGWPO03.HQGWDO01	3/22/2007 8:20:17 AM	nrc.gov
TWGWPO02.HQGWDO01	3/22/2007 8:20:10 AM	nrc.gov

Files	**Size**	**Date & Time**
MESSAGE	659	3/22/2007 8:20:10 AM
AREVA Software Program Manual TR Draft RAI.wpd	49337	3/22/2007 8:05:24 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

SUBJECT: REQUEST FOR ADDITIONAL INFORMATION REGARDING THE US EPR SOFTWARE PROGRAM MANUAL TELEPERM XS SAFETY SYSTEM TOPICAL REPORT (SPM) (TAC MD3971)

By letter dated December 21, 2006 (ML063610098) Areva requested the review and approval of ANP-10272, "Software Program Manual TELEPERM XS Safety Systems Topical Report" (ML063610100). The following information is requested to understand the intended implementation of the software development program.

1) **Question Summary:** Explain why the RETRANS verification tool that is described in the TELEPERM XS Topical Report (TXS TR) is not described in the SPM.

Full Text: It is basically understood that the use of the RETRANS tool allowed the code generator to be accepted without exaggerated quality verification demands. For example, TXS TR Section 2.4.3.3.3 says: '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. The generated code can be analyzed by **RETRANS** to identify the function block modules and reveal the connections between them. The result of this process should yield the information elements contained in the design database as input on the SPACE editor for engineering the I&C functions. A comparison of the result of the validator analysis with the content of the design database for the I&C functions confirms correct application of the tool for code generation and **relieves the code generator of exaggerated quality verification demands** ...'

2) **Question Summary:** Explain how the application software development process described in the SPM relates to the one described in the TXS TR.

Full Text: The description in the TXS TR and associated SER describe tools and procedural requirements that do not appear to be identified in the SPM. Does the SPM replace, modify, or augment and supplement the application software development process described in the TXS TR? Please explain.

3) **Question Summary:** Describe how the SPM terms "logic diagrams," "Functional Requirements Specification," "Software Requirements Specification," and "Software Design Description" relate to terms already defined in the TXS TR (i.e. Function Diagram & Software Specification).

Full Text: Does the SPM "Software Requirements Specification" correspond to the TXS TR "Software Specification?" For example, in Section 9.1.3, it says: "The SDD uses functional blocks similar to the SPACE tool database to translate the requirements from the SRS into logic diagrams. These logic diagrams form the basis of the software logic. The logic diagrams show the inputs, how those inputs are manipulated, and the resulting outputs. Once completed, these diagrams are redrawn in the SPACE tool to generate the code." Therefore are the logic diagrams on the SPM the same thing as the function block diagrams in the TXS TR?

4) **Question Summary:** Describe how the SPM terms "component," "software modules," and "subsystems," relate to terms already defined in the TXS TR (i.e. Function Block, Function Diagram, & Function Diagram Group Modules).

Full Text: The TXS TR uses several terms to describe software pieces and assemblies of software pieces: Function Block modules (FB-module), Function Diagram modules (FD-modules), Function Diagram Group modules (FDG-modules), and application. It appears that the term "component" is used in the TXS TR to refer mostly to system software items and hardware items. In terms of the application software, it appears that the smallest indivisible thing is a FB-module. An application can consist of up to two FDG-modules that, in turn, can consist of FD-modules that, in turn consist of FB-modules. A FB-module is referring to the implementation of a function block - a box on a function diagram. A FD-module can be thought of as the implementation of a function diagram (consisting of one or more pages). The term "application" is used to refer to what is loaded on one function processor (excluding system software). In UML 1.1, a component represents implementation items, such as files and executables. In UML 2, components are considered autonomous, encapsulated units within a system or subsystem that provide one or more interfaces. So a component is probably not an application. In Section 6.0 it says: "One area of exception with regard to the IEEE Standard 1012 is that component verification and validation test execution is not considered to be mandatory, but verification of any component testing performed is mandatory. ... The AREVA NP approach to component testing (called simulation testing) is discussed in section 6.2.7.4.1." However, Section 6.2.7.4.1 does not mention "component." In addition, in Section 6.2.4 it says: "When differing software integrity levels are assigned within the project, the Software Verification and Validation Plan documents the Safety Integrity Level assignment to individual software components, such as requirements, detailed functions, software modules, subsystems ..." How are "requirements" a form of "individual software components?" Therefore it is not clear what software piece or assembly of software pieces is being referred to as a component.

5) **Question Summary:** Describe how the SPM addresses the documentation of the specific design basis of each safety system.

Full Text: IEEE Std 603-1991 Section 4 requires that the specific design basis of a safety system be established. However, the SPM does not describe where this design basis is documented. For example, Section 9.1.4 says: "Each identifiable requirement in the SRS is traceable backwards to the system requirements and either the design bases or regulatory requirements that it satisfies." Therefore each feature is checked to ensure that it is required (i.e. no extra functionality), but where is it checked that all requirements are implemented in the SRS?

6) **Question Summary:** Describe how Areva intends to address conformance to the standard review plan (SRP).

Full Text: 10 CFR 50.34(h) requires an evaluation against the SRP. Therefore each licensee must provide an evaluation of the software development plans against NUREG-0800 Chapter 7, Branch Technical Position (BTP) No. 14. The SPM is an appropriate

document to address conformance with the SRP.

7) **Question Summary:** Describe the requirements on the Functional Requirements Specification (FRS).

Full Text: Section 9.1.1, "Functional Requirements Specification," does not place any requirements on the form or content of the FRS, nor does it identify any guidance that is followed in producing this document.
However, Section 2.2.2.4 of the TXS SE has identified associated procedural requirements that may be applicable to the FRS: '... FAW-3.4, "Contents and Structure of System Specifications for Software Components" ...'

8) **Question Summary:** Describe the requirements associated with the Software Design Descriptions (SDD).

Full Text: Section 9.1.3, "Software Design Description," describes only one aspect of a SDD, the function block/logic diagrams. The SDD must contain material other than just block/logic diagrams. For example: 1) Additional requirements on the SDD are contained in Section 9.4.2, "Coding Standards," and in Section 9.4.3, "Logic Structure Standards." 2) Section 2.2.2.4 of the TXS SE says: "... FAW-3.5, "Contents and Structure of Design Documents for Software Components,"... FAW-3.5 describes the process by which the software specification is translated into the SDD. FAW-3.6 describes the process by which the SDD is implemented. ..."

9) **Question Summary:** Describe the conventions for documenting requirements.

Full Text: Section 9.1.2 identifies IEEE 830 as providing guidance for the Software Requirements Specification (SRS). This standard contains guidance on broadly accepted practices in requirements documentation. The guidance can be applied to any document that contains requirements, for example the SPM. However it is not clear what standards or conventions are followed in the SPM and associated plans, with respect to requirements documentation. For example: The SPM does not contain a single "shall." The SPM does contain twelve (12) "must's." Are there twelve (12) requirements in the SPM?

10) **Question Summary:** Describe how the Failure Modes and Effects Analysis (FMEA), as described in Section 4.3.3 of the SPM, will follow the guidance of IEEE 379-2000.

Full Text: It is not clear if Areva means that the FMEA document shall conform to all of the requirements in IEEE 379-2000. Will the FMEA also follow the recommendations and permissions in IEEE 379-2000. Note: IEEE 379 refers to IEEE 352 for reliability analysis. IEEE 352 contains guidance for FMEAs. However, Section 4.3.3 says: "The FMEA follows the guidance of IEEE 379..."

11) **Question Summary:** Describe the difference in meaning of the various conformance claims.

Full Text: The SPM claims conformance to certain criteria in different ways, and it is not

clear whether these difference in terminology reflect differences in meaning (if so, how), or simply are different for linguistic diversity and readability reasons. For example:
1) Section 3.1 says: "The Software Quality Assurance Plan fulfills the requirements for a software quality assurance plan in accordance with IEEE 730 ... but must be considered along with the AREVA NP Quality Management Manual and the Quality Assurance reviews and audits for complete fulfillment of the IEEE requirements." This statement seems to say both: a) that the SQAP conforms to IEEE 730 and b) that it does not do so completely. Please explain.
2) Section 9.1.2 says: "The SRS is written following the content and format recommendations of IEEE 830, which is endorsed by Regulatory Guide 1.172." Therefore it is understood that Section 9.1.2 requires that each "shall" and "must" in the modified standard is followed. It would be more clear to say that the SRS shall conform to the guidance in RG 1.172.

12) **Question Summary:** Describe how the logic diagrams in the SDD are redrawn.

Full Text: Section 9.1.3 says that the logic diagrams in the SDD are redrawn in the SPACE tool. Is this redrawing done by a human being, or is it done by a software tool?

13) **Question Summary:** Describe the project specific plans that will be created for each project.

Full Text: The SPM and associated plans describe a program that is augmented and supplemented with project specific plans. However it is not clear what specific plans are required to augment and supplement the SPM and associated plans in order to address all of the NRC requirements and guidance. Nor is it clear what is expected to be in each project specific plan. The use of the term "plan" to describe programmatic aspects and also project specific aspects is confusing. The fact that both programmatic and project specific plans exist for SCMP and SVVP make it hard to determine, when only SCMP or SVVP is used, which one is being referred to. It is suggested that programmatic documents use the term "program" and that project specific documents use the word "plan." For example, the following section say:
ABSTRACT: "The combination of the Software Program Manual and the five plans listed above, which are implemented in AREVA NP operating instructions, constitute a program ..."
Section 5.1.2: "A project plan or specific Software Configuration Management Plan would cover ..."
Section 5.2.2: "...Any special agreed upon requirements are incorporated into the project plan ... These configuration status accounting reports are published periodically at the frequency established in the project plan. ... and document this verification and validation activity in accordance with the project-specific verification and validation plan."

14) **Question Summary:** The requirements to identify changes between revision of documents are not addressed in the SPM. Describe the requirements to identify changes between two revision of a document.

15) **Question Summary:** Describe the software quality metrics used.

Full Text: The SPM makes reference to "software quality metrics" but does not describe which specific metrics will be used. For example, Section 5.3.9 says: "The open item tracking system is also the primary source of statistical information for software quality metrics."

16) **Question Summary:** Describe what "operating instructions" are and how they are used.

Full Text: It appears from the use of the term "operating instructions" in the SPM, that they can be like QA procedures (i.e. programmatic in nature) and at times that they can be project specific. However it is not clear how or when an operating instruction is programmatic and when it is project specific.

17) **Question Summary:** Describe why the specific metrics are used?

Full Text: Typically metrics are part of a metrics program, and have relatively little value when first applied. It is only through programmatic development that metrics have value. For example, it is not obvious why the following metrics measure the effectiveness of V&V: 1) "History of project deliverables compared to schedule commitments," 2) "Total number of verification and validation open items in the open item backlog as a function of calendar time," and 3) "Length of time to close a verification and validation open item after identification." For example is it good or bad to have a lot of V&V open items in the backlog? (Good: V&V is finding stuff faster than design can fix it; Bad: V&V is not closing the items after design has fixed them or V&V is not working with design)

18) **Question Summary:** Describe the meaning of "project."

Full Text: When reference is made to project specific plans, it is not clear if there is a set of plans produced for each contract (i.e. a new plant), a set of plans is produced for each system (i.e. ESF), or a layers of plans at the project and system levels are produced.

19) **Question Summary:** Describe the difference in meaning between the following terms: safety goals, software risk, software hazard, and software error.

Full Text: From the way that these terms are used by Areva, it is not clear what distinction Areva is making between the meaning of these terms. It should be noted that proper operation in accordance with design, and safety are generally considered two distinct concepts. For example, a revolver is a highly reliable piece of equipment, but is questionably safe. In addition, safety is a system issue, not strictly a software issue. Therefore ensuring that the software functions as designed, and ensuring that the system is safe are two distinct types of evaluations. Of course, errors in the implementation of a design can be unsafe, but this is not the only way that an item can be unsafe. For example, single event effects are one way that faults can be created in a properly programmed system. The proper handling of faults is desirable. However, Section 4.0 says: "AREVA NP uses SIVAT testing of the application software generated by the SPACE tool to detect errors that would prevent the software from fulfilling its safety function. SIVAT testing, coupled with the FMEA, response time analysis, and

FAT are sufficient to ensure that there are no software hazards."

20) **Question Summary:** Describe how the software safety plan is implemented in the context of the system safety program.

Full Text: Since the software safety plan "follows the concepts IEEE 1228," and since IEEE 1228 says that the software safety program is implemented within the system safety program, clarification of how the Areva program addresses this aspect is desired. However, Section 4.0 says: "SIVAT testing, coupled with the FMEA, response time analysis, and FAT are sufficient to ensure that there are no software hazards."

21) **Question Summary:** Clarify Areva's concept of the requirements for defense-in-depth and diversity with respect to manual controls.

Full Text: It is not clear what Areva believes to be required with respect to manual controls and Defense-in-Depth and Diversity. The SRP (NUREG-0800) was last updated in 1997. In 1999 10CFR50.55a(h) requires that safety systems meet the requirements of IEEE 603-1991. IEEE 603 Section 6.2 requires a manual means to initiate each function that is required of the safety system. IEEE Section 6.2.1 requires that the manual means, associated with an automatic means, be implemented in a diverse manner. The implication is that all of these manual means are of the same quality as the automatic means. In addition, Branch Technical Position No. 19 "Guidance for Evaluation of Defense-in-Depth and Diversity in Digital Computer-Based Instrumentation and Control Systems" basically says that if the safety system is implemented as a programmable system, then a Defense-in-Depth and Diversity analysis is required, since programmable systems are vulnerable to common cause failures. This analysis may conclude that a diverse system is also required. Therefore if the safety system manual controls are implemented using software, then a diverse set of manual controls may also be required. However, Section 4.3.1 says: "The diversity and defense-in-depth analysis is performed to assess the adequacy of diversity afforded by the system design, to ensure that adequate defense-in-depth has been provided in the design, and to verify that the displays and manual controls for critical safety functions initiated by operator action are diverse from computer systems used in the automatic portion of the reactor protection and engineered safety features actuation systems."

22) **Question Summary:** Describe the software safety analysis methods, tools and techniques (MTT) that will be used to implement the Software Safety (SS) Plan (SSP), and what work products these MTTs will be applied to.

Full Text: Conceptually IEEE 1228 requires various software safety analyses to be performed (i.e. SS Requirement Analysis, SS Design Analysis, ...) and that the specific types be identified. In the SSP (SPM Section 4), Areva describes eight (8) safety analysis activities: 1) Diversity and Defense in Depth Analysis; 2) Application Software Requirements Traceability Matrix; 3) Failure Modes and Effects analysis; 4) Response Time Analysis; 5) Verification and Validation Reports; 6) Software Test Report and SIVAT testing; 7) Criticality Analysis; and 8) Factory Acceptance Test Report. However, each of these is addressed by different guidance as is explained below. Therefore it is

not clear what activities are required by the SSP (i.e. not required elsewhere). If all activities are performed in accordance with a plan or procedure, what activities would not be performed if the SSP were eliminated?
1) BTP-19 provides guidance to the staff for reviewing a Defense-in-Depth an Diversity analysis.
2) The acceptance criteria for the Software Quality Assurance Plan (SQAP) says that the SQAP should ensure that traceability is maintained throughout all phases, and an RTM is one way of documenting this.
3) IEEE 603 Section 5.15 requires a reliability analysis, and NUREG-0800 Section 7.1-C contains the guidance for reviewing this analysis. An FMEA is considered one way to address this requirement.
4) Response time is a functional or performance requirement, and ensuring that an application responds in the required time period has traditionally not been considered a safety analysis activity.
5) BTP-14 provides acceptance criteria for Software Verification and Validation Plans.
6) Testing can be addressed under SCMP, SVVP, & SQAP.
7) Not much guidance exists regarding graded levels of quality. Basically everything in a safety system should be of high quality. It is not clear how a criticality classification of software is relevant to safety. Where or how is the Safety Integrity Level of a module considered?
8) Testing can be addressed under SCMP, SVVP, & SQAP.
However, Section 4.0 says: "The plan follows the concepts of IEEE 1228 but does not fully comply ... AREVA NP does not use a software safety organization nor does it perform a specific analysis of the application software to detect hazards." Please explain.

23) **Question Summary:** Describe how the "consideration" of the extended FMEA, as described in Section 4.3.3 of the SPM, follows the guidance of IEEE 379-2000.

Full Text: IEEE Std 379 does not mention an extended FMEA, and therefore it is not clear how the extended FMEA can follow IEEE 379. It is not clear if Areva means that the extended FMEA document shall conform to all of the requirements in IEEE 379-2000. Will the extended FMEA follow the Recommendations and permissions in IEEE 379-2000? How will it be documented that "consideration was given?" IEEE 379 refers to IEEE 352 for reliability analysis. However IEEE 352 does not mention an extended FMEA. However, Section 4.3.3 says: 'On a project to project basis, consideration is given to performing a limited analysis of multiple random hardware and software failures, that is an "extended Failure Modes and Effects Analysis" as recommended by IEEE 379.' Please explain.

24) **Question Summary:** Describe the relationship between tasks that address the Single Failure analysis and Reliability Analysis requirements.

Full Text: IEEE 603 Section 5.1 contains requirements for the safety system to perform all safety functions in the presence of single failures (therefore an analysis is implied), and Section 5.15 contains requirements for reliability analysis. Both sections refer to IEEE 352 and 577 for guidance on reliability analysis. IEEE 352 describes an FMEA, as one step in a system reliability analysis. Therefore it is not clear if the FMEA is intended

to address, in part, both single failure and reliability analysis requirements. For example Section 4.3.3 says: "The FMEA examines the effects of random single failures on the ability of the safety system to perform its required safety functions." Please explain.

25) **Question Summary:** Describe how the Areva software development program addresses the scale (e.g. size and duration) of a project implemented under it.

Full Text: Software development projects can be of many sizes, and durations. It is expected that the importance of certain documentation will vary with differences in size and duration of the project. However, it is not clear what programmatic means exist to address the scale of a project. Partly this issue could be addressed by describing the software development program in the context of the system design and development. For example, a plant-wide digital I&C design would require more documents and more document types than a single system modernization. However this additional documentation may not be considered part of the software development process. The software development program is a part of system development, and it is hard to determine that the software development program is complete without knowing what is addressed in the system development program.

26) **Question Summary:** Describe how the Areva software development program addresses the different implementation contexts (e.g. design certification vs modernization) of a project implemented under it.

Full Text: The letter that submitted the SPM to the NRC identified that it was intended that the SPM would be referenced by both existing plant modernization projects, and by the US EPR design certification (DC). However the SPM does not describe how these two implementation contexts (i.e. modernization vs DC) are treated differently.

27) **Question Summary:** Describe the configuration management process for changing a setpoint in the protection system when it is in operation.

Full Text: It is understood that a setpoint change is essentially a software change. It is not clear how the software configuration management plan (SCMP) addresses these changes.

28) **Question Summary:** Explain how the SPM addresses the configuration of parameters and definition of trace data that can be set through the runtime environment (RTE) when in the PARAM operating mode.

Full Text: The TXS TR (in Section 3.1.3.4) described four operation modes (OPERTION, PARAM, TEST, & DIAGNOSIS). It is possible to permanently change the functioning of the processor module when not in the OPERATION mode. However it is not clear how the documentation of these changes are addressed in the Software Configuration Management Plan (SCMP). It is expected that setpoint changes will be made using these features, correct?