

Review of ANP-10272, Revision 1, Software Program Manual for Teleperm XS Safety Systems

11 Major Concerns That Was Previously Identified

1) Revisions

The staff has received numerous requests for additional information (RAI) responses, many of which modify the SPM, and some of which may conflict with earlier responses. For this reason, AREVA is requested to designate the exact changes which will be made in response to each RAI question. Also, due to the extent of changes, it is necessary for the staff to have a revision of the TR on the docket to facilitate further review. The revision should incorporate past RAI responses as well as modifications associated with the topics discussed in this letter.

Update: This issue is adequately addressed.

2) Scope

Which portions of the SPM are mandatory and what portions are optional? The response to RAI 66 was not clear. The staff needs to clearly understand what is being sought for approval.

Update:

The response did not address the issue raised by RAI 66, which, therefore, remains open. That initial question states "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."

3) Specification And Coding Environment (SPACE)

SPACE is not safety-related. In the TXS Topical Report SER, SPACE was approved as part of an overall life cycle process. SPACE is required to have verification and validation (V&V) of its output including the SPACE functional block diagrams adequately and appropriately represent the Software Design Description (SDD). Acceptable V&V of application software was credited but not the capability of SPACE. The SPM needs to be revised to appropriately address SPACE.

Update: This issue is adequately addressed.

4) Scope of AREVA NP Software Development Procedures

Applicant's response to RAI 7 states that the "AREVA GmbH procedures do not apply to the development of TXS application software for U.S. projects." The staff requested clarification in the SPM, to what systems, processes and tools, the AREVA NP GmbH software development procedures for the SPM apply.

Review of ANP-10272, Revision 1, Software Program Manual for Teleperm XS Safety Systems

Areva response stated "Section 3.4 described the use of Operating Instructions to implement the Software Program Manual for work done in the U.S. for the implementation of TELEPERM XS projects. Section 4.0 was modified to note that the procedures described in Section 5 of the TELEPERM XS Topical Report apply to the TELEPERM XS platform development work performed in Germany

Update: This issue is adequately addressed.

5) Conformance to Guidance

The staff needs to know if "conforms to the guidance" is the same as 100% compliance. Staff needs to have a clear understanding of what guidance documents and standards will be followed, and to what degree they will be followed. The staff cannot approve the SPM without a clear understanding of what is being approved. For example, the response to RAI 72 did not discretely answer the conformance to guidance question.

Update:

Examples have been corrected and Section 3.6 definition of "shall" is consistent with 2009 IEEE Standards Style Guide. This issue is adequately addressed.

6) Verification and Validation (V&V)

AREVA takes exception to IEEE Std 1012 in that the applicant says component verification and validation testing is not mandatory. Justify this exception. Also, it should be clear from the SPM that the V&V Manager determines the scope of V&V activities as opposed to Technical Manager and Quality Assurance, see RAI 71, and the final system testing is the responsibility of the V&V group.

Update:

- 1) In the revised SPM, the exception to component testing, as an explicit exception to IEEE STD 1012, has been removed. A statement has been added "The combination of TELEPERM XS generic qualification testing and project-specific testing addresses all of the testing activities in IEEE Std 1012-1998, as shown in Table 13-1." Table 13-1 shows all component testing is done under the generic TXS testing. Therefore, the staff interprets this as all component testing is done under the generic TXS process and procedures, no new components will be developed under the application software process as described in the SPM. AREVA is to confirm this.
- 2) The SV&V plan was changed to "The Technical Manager and the QA organization are responsible for reviewing the Software Verification and Validation Plan to assess its appropriateness to the scale and complexity of the project." This is not acceptable; per RAI 86 the staff did provide some flexibility by the following suggestions; "The QA and V&V organizations are the only organizations with any authority over the Verification and Validation Plan. The design technical manager is not independent, and could be influenced by non-quality factors such as cost or scheduling issues. The V&V and QA organizations can, however, request the consultation of other organizations and managers,

Review of ANP-10272, Revision 1, Software Program Manual for Teleperm XS Safety Systems

such as the design technical manager, in collecting information from which to base their determination. If this is the intent of the SPM language, it should be modified to clearly state that relationship." Therefore the only organizations that can be responsible for the SV&V plan are the V&V and QA organizations. The Technical manager can only advise.

Section 2.1.6 of the SPM stated that the Testing Function was performed by software engineers. This section was removed. Section 11.8, now states the V&V personnel are responsible for preparation of the software and system validation test documents and may get assistance from the design groups as allowed but under direction of V&V group. This issue is adequately addressed.

7) Software Configuration Management

AREVA takes exception to IEEE Standard 828 in that the applicant states a separate software configuration management organization, including a configuration control board (CCB), is not required. Justify this exception. For example, AREVA should provide an analysis of each task required of a software configuration management organization as defined by IEEE 828, and then assign these tasks appropriately. Included would be a procedure on how project meetings and Design Review Boards will perform the same tasks as a CCB.

Update:

Per the revised SPM, AREVA NP now uses CCBs after the Application Software has been developed to the baseline stage. The SPM now states the Project Engineer is chairman of the Application Software Configuration Control Board and serves with the software supervisor and the Lead Software Designer as members of the board. Participation by QA and the Verification and Validation Group is typically included to ensure compliance with project requirements.

For any review board or special organization established for performing SCM activities on this project, the Plan shall describe its:

- a) Purpose and objectives;
- b) Membership and affiliations;
- c) Period of affectivity;
- d) Scope of authority;
- e) Operational procedures.

It appears that this issue is adequately addressed in the SPM. However, the use of a Configuration Control Board as stated in the SPM is not consistent with how the CCB would be implemented in the new SCMP OI 1460-10. Specifically, OI 1460 makes convening a CCB optional depending on the significance of the functional change to the application. SPM, Section 12.2.2, states that AREVA NP uses Configuration Control Boards for the development of TELEPERM XS Application Software for control of changes to functional requirements after the Application Software has been developed to the baseline stage. OI 1460-10 says that use of CCB is optional so this comment is not resolved.

Review of ANP-10272, Revision 1, Software Program Manual for Teleperm XS Safety Systems

8) SIVAT

If AREVA NP plans to credit SIVAT in the software V&V stage of the software lifecycle, AREVA NP should provide documentation demonstrating that SIVAT was developed to a quality software development process.

At the January 15, 2009 meeting, AREVA NP proposed to revise the SPM to describe a software V&V process without crediting SIVAT. The proposal would allow the option of using SIVAT once the quality of the tool has been adequately demonstrated and approved by the NRC staff. If AREVA NP plans to move forward with the proposal, the option for using a software verification and validation tool should at a minimum provide a description (i.e., scope and purpose) of how the optional tool would be used in software V&V.

Update:

References to SIVAT have been removed from the SPM up to Appendix B. This includes removal of SIVAT in the definitions, discussion in the Application Software Validation Testing, Tools for Verification and Validation Testing as well as the Software Configuration Management Plan. Up to Appendix B, the only reference to a simulation test tool is an "NRC approved simulation test tool." However, in Appendix B, it is stated "The Software Program Manual describes the specific system qualification process for TELEPERM XS projects in the U.S. This process uses the SIVAT tool, as described below." Therefore, this appears to the staff to be an inconsistent reference to SIVAT. AREVA is requested to revise the SPM to address SIVAT consistently.

9) Software Safety Analysis

As an exception to the SRP, BTP HICB-14, AREVA had identified that it does not intend to use a software safety organization nor does it perform a specific analysis of the application software to detect hazards.

Update:

Revision 1 of the SPM now states there is a Software Safety Plan and the Technical Manager is responsible for it although there is no Software Safety Team or organization. The staff has the following issues to be resolved with regards to this plan:

- I. BTP HICB-14 states that the SSP should include a requirement that a safety analysis be performed and documented on each of the principal documents; requirements, design descriptions and source code.
- II. BTP HICB-14 states that the SSP should identify all documentation required for the proper and safe operation of the software.
- III. The SSP discusses the use of the SPACE tool. BTP HICB-14 states that all tools used to carry out the application software development should be discussed, and in particular, a description of the method for preventing inadvertent introduction of hazards by the use of all projects tools.

Review of ANP-10272, Revision 1, Software Program Manual for Teleperm XS Safety Systems

- IV. Also, BTP HICB-14 states that the SSP should define the safety-related activities to be carried out for each set of life cycle activities, from requirements through operation and maintenance.

10) Other Software Tools

Identify whether other software tools (examples: FunBase, cmp_code and rediff) are credited in software development process. If credited, applicant should provide acceptable demonstration of software quality. If not credited, discussion of the tools should be removed or it should be clearly stated that such tools are not credited for software development.

Update:

The addition of Section 4.2 provided a listing of development support tools that are "part of" the SPACE Engineering Tool. But this section does not attempt to demonstrate software quality of these tools. The description of these should include if they were written and developed by AREVA at the same time, and part of, the SPACE engineering tool, predeveloped or a COTS item. The listing does not include rediff or identify this is a complete listing (can the SPACE tool be substituted for or if any compilers or software loaders be used?)

11) Other Issues

V&V organization should be responsible for the preparation of test plans and not the software development organization. It should be made clear that V&V personnel should perform all V&V functions, they can be assisted by other personnel, but the duty, responsibility and implementation belong to the V&V organization.

Update

The responsibility for the V&V functions has been clarified to identification of the V&V organization. This issue is adequately addressed.

The Quality Assurance Manager manages the Software Quality Assurance Plan not the technical manager. Additionally, see RAI 76, concerning the role of Quality Assurance Manager.

Update:

Section 5.2 (formerly Section 2.1) now states the "The Technical Manager is responsible for ensuring that all project work is performed in accordance with the applicable QA processes and procedures, as required by the AREVA NP Quality Management Manual.

However, as RAI 76 originally stated; "The language of the SPM seems to indicate the Technical Manager is assuming the responsibilities of the Quality Assurance Manager. If this is the case the NRC would then determine if acceptability of such a justification." This was predicated on the statement, still in the SPM, "The Technical Manager manages the Software Quality Assurance Plan." The NRC review guidance for this is in Section B.3.1.3.4 of BTP 7-14 which states "The organization of the software QA organization should be checked to ensure that there is sufficient authority and

Review of ANP-10272, Revision 1, Software Program Manual for Teleperm XS Safety Systems

organizational freedom, including sufficient independence from cost and schedule to ensure that the effectiveness of the QA organization is not compromised. IEEE Std 1028-1988 can be used as guidance.”

AREVA NP should clarify of how and who can close open items in the open item database.

Update:

The SPM does not address the closure of open items. This must be modified to state that an open item can only be closed by the individual or group that individual belongs to.

There should be assurances that no unused code is present versus no used code is run on any processor.

Update:

The SPM now states “The use of the SPACE Engineering Tool ensures that no unused code is inserted in the Application Software.” This issue is adequately addressed.

Review of ANP-10272, Revision 1, Software Program Manual for Teleperm XS Safety Systems

ADDITIONAL CONCERNS

12) Software Test Plan

Section 4.5.8, Software Test Plan, states "The test plan is prepared during the detailed design phase of the software development life cycle." However, it does not indicate the organization or personnel responsible preparing the test plan. Also, per IEEE Std 1012-1998, testing is the responsibility of the V&V group. AREVA is to identify how Section 3.3.7, Testing, meets these guidelines with the testing team performing hardware checkouts but the V&V group should be identified as the responsible organization.

Also, BTP 7-14 states the procedure for specifying the associated released code with the associated testing documentation should be identified.

Roles and responsibilities are not defined. What organization is responsible for preparing test specification and test development, and what organization will perform the test activity?

If roles and responsibilities are to be delineated at the Test Specification level, then some guidance would be expected in the Software Test Plan to ensure compliance with the Standards. Even though the SPM lists separate activities, it is silent on the acceptability of combining activities.

SPM, Section 11.8, states that the V&V group is responsible for preparation of the software and system validation test documents, and that V&V group may get assistance from the software and hardware design groups (under the direction of the V&V group) for preparation of validation test specifications, procedures, and reports and the performance of test tasks.

From Figure 11-1: Test Document Work Flow and Control Points, it is not clear who will actually write the test cases. Will it be the V&V organization or the matrix support personnel? What is involved in the "packaging of document"?

13) Document Standards

Function Diagram Standards – states that "The verification and validation activities include the independent verification that the SDD conforms to the functional requirements and design constraints." To further explain the process there should be identification that another part of V&V is to insure that the SPACE function block diagrams adequately and appropriately represent the SDD. Is this described or explained in another part of the SPM?

14) Software Management Plan

BTP 7-14 states "The SMP should ensure that quality assurance budgets, safety budgets, and V&V budgets not be subject to expropriation by the software development organization, in order to maintain financial independence of these assurance activities." However, in the SMP, the project manager is responsible for "the adequate budgeting,

Review of ANP-10272, Revision 1, Software Program Manual for Teleperm XS Safety Systems

scheduling, and staffing of the project software activities described in this report, including the timely acquisition of independent Verification and Validation resources for the project.” How is financial independence maintained with one person responsible for both the software development and independent V&V resource acquisition?

Personnel resources for each project phase should be listed in the SMP per BTP 7-14. AREVA should identify who is responsible for that activity.

15) Software Development Plan

The SDP should describe the mechanisms for tracking the risk factors and implementing contingency plans per BTP 7-14. Risk factors that should be included include system risks, mechanical/electrical hardware integration, risks due to size and complexity of the product, the use of predeveloped software, cost and schedule, technological risk, and risks from program interfaces (maintenance, user, associate contractors, subcontractors, etc.). If these are identified elsewhere in the SPM, please identify specifically where there can be located.

Project schedules are mentioned as being developed as part of the project plans with no further information as to their content. Per BTP 7-14 these should include reviews, milestones and audits to avoid unexpected schedule delays.

The SDP should describe the software development environment, including tools such as software design aids, compilers, loaders, and subroutine libraries. If these are found in other plans, that should be pointed out. The SDP should require that tools be qualified with a degree of rigor and level of detail appropriate to the safety significance of the software which is to be developed using the tools. Another option is to take credit for V&V.

16) Software Quality Assurance Plan

Section 5.5, Software Audits, states the audits conform to the guidance of IEEE Std 1028-1997, as endorsed by Regulatory Guide 1.168, except where the guidance conflicts with the AREVA NP Quality Management Manual. These conflicts should be identified here or some other method of identification should be noted. The staff will have to review these to determine the level of compliance with Reg Guide 1.168.

17) Software Integration Plan

Regulatory Guide 1.173, endorses IEEE Std 1074-1995, and within that standard states that “the Software Requirements and the Software Detailed Design should be analyzed to determine the order for combining software components into an overall system, and that the integration methods should be documented.” AREVA is requested to identify, in the SPM, if the Software Generation and Download Procedure document includes the order in which software components are combined and loaded into the system or if there are other documents which identify this.

The SMP should identify the software organization, if there is one, or if the personnel implementing the plan are part of the development organization which is acceptable per the guidance of BTP 7-14.

Review of ANP-10272, Revision 1, Software Program Manual for Teleperm XS Safety Systems

The SMP identifies that the Software Generation and Download Procedure controls and documents the generation of each Application Software release but does not state if that procedure identifies or records successful completion of the installation, and what integration tests are performed. If physical integration is done during the pre-FAT stage, there should be identification if any testing is done at this stage and distinguish the differences if there is any credit done for integration testing in the FAT stage.

18) Software Installation Plan

The SInstP states the Software Design Group implements the Software Generation and Download Procedure. The Verification and Validation personnel can also install the software during the system test phase. Is software installed only using this procedure, under all circumstances? Per BTP 7-14, the SInstP should describe the boundaries between the software installation organization and the broader safety system installation organization. Reporting channels should be described. Since the software is being installed in hardware, the personnel performing this installation should be a mix of the software and hardware personnel. The critical part of the software installation is the system test (Note: per IEEE Std 1012-1998, Final System testing is considered a V&V test, and is the responsibility of the V&V group). It is acceptable for the installation to be performed by the development organization or by the customer. If installation is performed by the customer, then the delineation of responsibility between the development organization and the customer should be defined in such a way that misunderstanding in communications between the two organizations are kept to a minimum.

Checks should be required to ensure that the computer system is functional, that the sensors and actuators are functional, that all cards are present and installed in the correct slots. These should be part of the SInstP, per BTP 7-14, as well as plans for installation of software on installed systems in operating plants should recognize the need to declare all affected functions inoperable according to the plant's technical specifications before proceeding with installation, and to conduct appropriate return-to-service testing before declaring the modified function operable.

Installation tools should be qualified to with a rigor and level of detail appropriate to the safety significance of the software which is to be installed using the tools. Use of the Teleperm Service unit and the Maintenance Laptop is identified but not what software, including operating systems, is loaded the security methods or these how these tools were qualified and if these are the only installation tools necessary should be identified.

19) Software Maintenance and Operations Plan

This plan should describe the boundaries between the software maintenance organization and other company organizations. Reporting channels should be described should list the general functions that the software maintenance organization will be expected to perform, and provide general information on obtaining field trouble reports.

The software tools should be identified and also be qualified, and should be identical to those used during the original design. The SmaintP should have some provisions for

Review of ANP-10272, Revision 1, Software Program Manual for Teleperm XS Safety Systems

qualifying a new revision of the tools, if the original versions of the tools are no longer available.

The staff does not understand the intent to combine the Maintenance and Operations Plans. That is an option that can be done at AREVA's request; however the guidelines from BTP 7-14 and IEEE 1074 on Operations plans should also be included. Section B.3.1.8 should be reviewed to include the listed Management, Implementation and Resource Characteristics of the Software Operations Plans. These include, but not limited to:

- Specify operator interface stations and actions required to support operation.
- Describe the procedures necessary to start, operate and stop the software system.
- Should require a list of error messages, giving a description of the error indication, the
- probable interpretation of the error indication, and steps to be taken to resolve the situation

20) Software Verification and Validation Plan (SVVP)

If SIL Level scheme is not defined in SVVP, how can a reviewer ensure that the safety software will meet the minimum requirements of SIL 4 equivalent?

Specific V&V activities are not defined. How will V&V activities integrate with the Phases of SW life cycle?

V&V Activity Summary Reports are not defined or described in the SVVP.

21)

Will all TXS applications use the same software life cycle (SLC) model? IEEE 1074 requires that the SLC model Processes, Inputs and Output activities be defined in the SPM. OI 1456-03 does this but the SMP section of the SPM doesn't.

22)

To what degree has conformance to the referenced standards been accomplished in the SPM? Where exceptions to the Standards are taken, where is the justification noted? Would it be possible to perform a requirements traceability analysis between the SPM and the various standards used to develop it? Request that AREVA NP to include standards and Regulatory Guide traceability within the RTM matrix program.

23)

Many of the Standards requirements can only be verified by review of the implementation documents which are not referenced in the SPM. What method would the Staff use to confirm these requirements? Staff assumes that OI documents would not be docketed, so would the staff need to do on-site audits to get access to them?

Review of ANP-10272, Revision 1, Software Program Manual for Teleperm XS Safety Systems

24)

What methods would be used to ensure consistency is established and maintained between the SPM and the various OI's that constitute the implementing instructions for the SPM? There should be some sort of audit provision for this included in the SPM. The NRC could perform verification inspections per ITAAC, or DAC to ensure that the requirements of the SPM were met. There could also be a tracing mechanism between the SPM and the OI's to ensure compliance.

25)

Safety Evaluations are dependent on both the vendor planning documents and the licensee's planning and implementation documents. The use of the SMP would standardize the vendor side of things but each applicant would still need to provide a set of application specific documents to cover the licensee side.

For example, SW Configuration management becomes the licensee's responsibility once the system is turned over from the vendor. In this case, the staff would like to review the SW CM plans to determine that adequate CM control will be maintained through this transition and into the O&M phase of the software. The same applies for other aspects of the SW such as V&V, SQA, and SSP.

26)

In Chapter 5.14.1, AREVA NP stated that risk management process *satisfies* the requirements in IEEE STD 7-4.3.2-2003 clause 5.3.6, as endorsed by Regulatory Guide 1.152. Can applicant use consistent wording for meeting a requirement? In other parts of the SPM, "conforms" was used.

27)

In Chapter 7, AREVA NP stated that physical software integration occurs at the pre-FAT stage, when the application software is loaded on the TXS processors, and that the project-specific FAT Plan covers the approach and activities associated with the Software and Hardware Integration. What is a pre-FAT stage, and how is it different from FAT.