AREVA

April 29, 2011
NRC:11:039

Document Control Desk
U.S. Nuclear Regulatory Commission
Washington D.C. 20555-0001

Comments on Draft Safety Evaluation for Topical Report ANP-10303P, Revision 1, "SIVAT: TELEPERM XS™ Simulation Validation Test Tool Topical Report," (TAC No. ME1503)

Ref. 1: Email, Holly Cruz (NRC) to Gayle Elliott (AREVA NP Inc.), "Draft Safety Evaluation for AREVA NP Inc. for Topical Report (TR) ANP-10303P, Revision 1, 'SIVAT: TELEPERM XS™ Simulation Validation Test Tool Topical Report' (TAC No. ME1503)," March 22, 2011.

The NRC released a draft safety evaluation (SE) on ANP-10303P, Revision 1, and requested that AREVA NP Inc. (AREVA NP) review the document for proprietary material and for any factual errors.

AREVA NP has reviewed the draft SE provided in Reference 1 and has determined that the draft safety evaluation contains information that was identified in the topical report as being proprietary information. AREVA NP is also providing comments for consideration. A marked-up copy of the draft SE is provided in Attachment A showing the proprietary information and AREVA NP comments. Attachment B provides a summary table of the proprietary information and comments.

AREVA NP considers some of the material contained in the enclosed to be proprietary. As required by 10 CFR 2.390(b), an affidavit is enclosed to support the withholding of the information from public disclosure. Proprietary and non-proprietary versions of the enclosed are provided.

If you have any questions related to this submittal, please contact Ms. Gayle Elliott, Manager, Product Licensing. She may be reached by telephone at 434-832-4695 or by e-mail at Gayle.Elliott@areva.com.

Sincerely,

Pedro Salas, Manager
Corporate Regulatory Affairs

Enclosures

cc: H.D. Cruz
Project 728

T007
NRR

AREVA NP INC.
An AREVA and Siemens company

3315 Old Forest Road, P.O. Box 10935, Lynchburg, VA 24506-0935
Tel.: 434 832 3000 - www.areva.com

AFFIDAVIT

COMMONWEALTH OF VIRGINIA)
) ss.
CITY OF LYNCHBURG)

1. My name is Gayle F. Elliott. I am Manager, Product Licensing, for AREVA NP Inc. (AREVA NP) and as such I am authorized to execute this Affidavit.

2. I am familiar with the criteria applied by AREVA NP to determine whether certain AREVA NP information is proprietary. I am familiar with the policies established by AREVA NP to ensure the proper application of these criteria.

3. I am familiar with the AREVA NP information contained in the attachment to a Letter from Pedro Salas (AREVA NP) to Document Control Desk (NRC), entitled "Comments on Draft Safety Evaluation for Topical Report ANP-10303P, Revision 1, 'SIVAT: TELEPERM XS™ Simulation Validation Test Tool Topical Report', (TAC No. ME1503)," NRC:11:039, dated April 29, 2011 and referred to herein as "Document." Information contained in this Document has been classified by AREVA NP as proprietary in accordance with the policies established by AREVA NP for the control and protection of proprietary and confidential information.

4. This Document contains information of a proprietary and confidential nature and is of the type customarily held in confidence by AREVA NP and not made available to the public. Based on my experience, I am aware that other companies regard information of the kind contained in this Document as proprietary and confidential.

5. This Document has been made available to the U.S. Nuclear Regulatory Commission in confidence with the request that the information contained in this Document be withheld from public disclosure. The request for withholding of proprietary information is made in

accordance with 10 CFR 2.390. The information for which withholding from disclosure is requested qualifies under 10 CFR 2.390(a)(4) "Trade secrets and commercial or financial information."

6. The following criteria are customarily applied by AREVA NP to determine whether information should be classified as proprietary:

(a) The information reveals details of AREVA NP's research and development plans and programs or their results.

(b) Use of the information by a competitor would permit the competitor to significantly reduce its expenditures, in time or resources, to design, produce, or market a similar product or service.

(c) The information includes test data or analytical techniques concerning a process, methodology, or component, the application of which results in a competitive advantage for AREVA NP.

(d) The information reveals certain distinguishing aspects of a process, methodology, or component, the exclusive use of which provides a competitive advantage for AREVA NP in product optimization or marketability.

(e) The information is vital to a competitive advantage held by AREVA NP, would be helpful to competitors to AREVA NP, and would likely cause substantial harm to the competitive position of AREVA NP.

The information in the Document is considered proprietary for the reasons set forth in paragraphs 6(b) and 6(c) above.

7. In accordance with AREVA NP's policies governing the protection and control of information, proprietary information contained in this Document have been made available, on a limited basis, to others outside AREVA NP only as required and under suitable agreement providing for nondisclosure and limited use of the information.

8. AREVA NP policy requires that proprietary information be kept in a secured file or area and distributed on a need-to-know basis.

9. The foregoing statements are true and correct to the best of my knowledge, information, and belief.

____

SUBSCRIBED before me this 29th

day of April, 2011.

____

Sherry L. McFaden
NOTARY PUBLIC, COMMONWEALTH OF VIRGINIA
MY COMMISSION EXPIRES: 10/31/14
Reg. # 7079129

SHERRY L. MCFADEN
Notary Public
Commonwealth of Virginia
7079129
My Commission Expires Oct 31, 2014

DRAFT SAFETY EVALUATION BY THE OFFICE OF NUCLEAR REACTOR REGULATION

TOPICAL REPORT ANP-10303P

"SIVAT: TELEPERM XS™ SIMULATION VALIDATION TEST TOOL TOPICAL REPORT"

AREVA NP, INC.

PROJECT NO. 728

1.0 INTRODUCTION

By letter dated June 11, 2009 (Reference 1), "Request for Review and Approval of ANP-10303P, 'SIVAT: TELEPERM XS™ Simulation Validation Test Tool Topical Report'," AREVA NP Inc.[1] submitted "SIVAT: TELEPERM XS™ (TXS) Simulation Validation Test Tool Topical [(TR)] Report" that would allow the use of SIVAT as a software validation tool for the development of safety-related applications for the TXS system. On December 28, 2009, the U.S. Nuclear Regulatory Commission (NRC) issued (Reference 2), "Acceptance for Review of AREVA NP, Inc. 'SIVAT: TELEPERM XS™ Simulation Validation Test Tool Topical Report'."

Deleted: TXS

Deleted: ,

Deleted: Letter of a

Deleted: the

By letter dated September 1, 2010 (Reference 3), AREVA NP submitted Revision 1 to TR "SIVAT: TELEPERM XS™ Simulation Validation Test Tool Topical Report" in response to Requests for Additional Information by the NRC staff (Reference 4).

Deleted: TXS

Deleted: "AREVA NP Response to

Deleted: "

2.0 REGULATORY EVALUATION

Because the SIVAT tool is not designed to be installed in operating nuclear power plant systems and therefore does not itself perform safety functions, much of the guidance available for digital safety systems does not directly apply to this SE. Nevertheless, the following regulatory requirements and guidance were considered by the NRC staff in its review of the application due to the important Verification and Validation (V&V) functions that the SIVAT tool will support for the actual TXS application software that will perform safety functions in nuclear power plants:

Title 10 of the *Code of Federal Regulations* (10 CFR) Part 50 establishes the fundamental regulatory requirements with respect to the domestic licensing of nuclear production and utilization facilities. Specifically, Appendix A, "General Design Criteria [(GDC)] for Nuclear Power Plants," to 10 CFR Part 50 provides, in part, the necessary design, fabrication, construction, testing, and performance requirements for structures, systems, and components important to safety.

The regulation at 10 CFR 50.55a(h), "Protection and Safety Systems," requires compliance with Institute of Electrical & Electronics Engineers (IEEE) Standard (Std.) 603-1991, "IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations," and the correction sheet dated January 30, 1995. For nuclear power plants with construction permits issued before

1. AREVA NP (Inc) is a designation used in this report to refer to the AREVA NP organization responsibility for the design of U.S. projects using the TELEPERM XS System. This organization is based in Alpharetta, Georgia.

ENCLOSURE

January 1, 1971, the applicant/licensee may elect to comply instead with its plant-specific licensing basis. For nuclear power plants with construction permits issued between January 1, 1971, and May 13, 1999, the applicant/licensee may elect to comply instead with the requirements stated in IEEE Std. 279-1971, "Criteria for Protection Systems for Nuclear Power Generating Stations." IEEE Std. 603-1991, Clause 5.1, requires in part that "...safety systems shall perform all safety functions required for a design-basis event in the presence of: (1) ...any single detectable failure within the safety systems concurrent with all identifiable but non-detectable failures." IEEE Std. 279-1971, Clause 4.2, requires in part that "...any single failure within the protection system shall not prevent proper protective action at the system level when required."

SIVAT is being proposed as a tool to be used to support the V&V activities associated with safety-related software, therefore, its use will be relied upon to provide reasonable assurance that the requirements of the following GDC's are being met by the safety-related software of systems designed within the AREVA TXS platform.

GDC-10, "Reactor Design," requires that the reactor core and associated coolant, control, and protection systems be designed with appropriate margin to assure that specified acceptable fuel design limits are not exceeded during any condition of normal operation, including the effects of anticipated operational occurrences (AOOs).

GDC-13, "Instrumentation and Control," requires that instrumentation shall be provided to monitor variables and systems over their anticipated ranges for normal operation, for AOOs, and for accident conditions as appropriate to assure adequate safety, including those variables and systems that can affect the fission process, the integrity of the reactor core, the reactor coolant pressure boundary, and the containment and its associated systems. Appropriate controls shall be provided to maintain these variables and systems within prescribed operating ranges.

GDC-20, "Protective System Functions," requires that the protection system be designed to do two things. There are: (1) to initiate automatically the operation of appropriate systems including the reactivity control systems in order to assure that specified acceptable fuel design limits are not exceeded as a result of AOOs and (2) to sense accident conditions and to initiate the operation of systems and components important to safety.

GDC-21, "Protection System Reliability and Testability," requires that the system be designed for high functional reliability and in service testability with redundancy and independence sufficient to preclude loss of the protection function from a single failure and preservation of minimum redundancy despite removal from service of any component or channel.

GDC-22, "Protection System Independence," requires that the system be designed so that natural phenomena, operating, maintenance, testing, and postulated accident conditions do not result in loss of the protection function.

GDC-23, "Protection System Failure Modes," requires that the system be designed to fail to a safe state in the event of conditions such as disconnection, loss of energy, or postulated adverse environments.

3.0 TECHNICAL EVALUATION

3.1 SIVAT System Description

The Simulation Validation Test Tool called SIVAT is a high quality non-safety software simulation tool that was developed by AREVA NP for the purpose of providing V&V support for the development of project related TXS safety-related application software. [

] System functionality aspects that cannot be tested in this simulation environment must be tested through other means which are not within the scope of this SE.

The objective of SIVAT is to provide assurance that the applicable functional requirements established by the process engineers are correctly translated into Function Diagrams (FDs) without errors and to provide assurance that the software that was automatically generated from these FDs provides the required functionality in terms of the input and output response of the system.

Process models which are described within the SIVAT TR (Reference 11) can also be linked into the simulator in order to perform system closed-loop tests. The use of closed-loop simulation testing to complete V&V activities for safety-related application software cannot be evaluated or approved by the NRC within this SE because of the uncertainties associated with the use of process models. These models have not been submitted to the NRC for review and are not within the scope of this SE. This SE does not, however, preclude the use of SIVAT to perform closed-loop tests to support system qualification.

SIVAT is designed to support TXS Application Software V&V activities and to increase the likelihood of early detection of Application Software faults. Thus, the NRC staff acknowledges that the use of SIVAT can serve to reduce project risks in the earlier stages of the software development process.

Deleted: the

3.1.1 How SIVAT Works

[

] The process for generating safety-related software using SPACE has previously been evaluated by the TXS Platform Reference TR Safety Evaluation "Acceptance for Referencing of Licensing Topical Report EMF-2110(NP), Revision 1, "TELEPERM XS™: A Digital Reactor Protection System" (Reference 5).

Figure 3.1 below illustrates the process that is used to generate safety-related code for system installation as well as the code that is to be run within SIVAT.

[ ]

Figure 3-1: SIVAT Code Generation Process Illustration

[ ]

[ ]

3.1.2 Using SIVAT to Verify Safety System Application Software

The process of verifying the correctness of Application Software using SIVAT involves comparing simulated function diagram integrated component performance with specified system requirements. The verification of Application Software is complete when all specified requirements for a safety system can be objectively demonstrated to be satisfied.

Verification of Application Software establishes reasonable assurance that the Application Software is accomplishing all of the functions that are specified by the software requirements.

Deleted: safety system

Deleted: s

Deleted: block

Deleted: s

Deleted: n

Deleted: application

Deleted: s

Deleted: s

3.1.3 Using SIVAT to Validate Safety System Application Software

Validation of safety-related software performance using SIVAT is accomplished by analyzing the simulated system performance and making a qualitative determination of whether the system adequately fulfills its safety function requirements.

Validation of software establishes reasonable assurance that the software accomplishing its functions in a correct manner.

Comment [g1]: Section 3.1.3 should also state information about the SDD such as "Verifying the Application Software functionality, specified in the Software Design Description (SDD) is tested to validate that the software elements correctly implement software requirements."

3.1.4 SIVAT Verification and Validation Test Example (Oconee RPS/ESPS system Function FU0007)

[ ]

[ ]

Table 3-1: Oconee SIVAT Test Document References

[ ]

[

]

Figure 3-2: RCS High Outlet Temperature Trip Simplified Function Diagram

[

]

Table 3-2: Test Parameters and Expected Values

Deleted: Table¶

[

]

The test results for the test case example are shown in Table 3-3 below:

Comment [g2]: Provide reference to where the test results were derived from like the other tables. If this information was not derived from a reference document, then specify that it is a representation of an Oconee Data File.

Table 3-3: SIVAT Oconee RPS/ESPS FU0007 Test Results Data File

Deleted: NPP

[

]

[

]

[ ]

Figure 3-4: Example of Oconee Test Incident Report Entry

Deleted: Example 3-1

[

]

3.2 Software Life Cycle Planning Process

Comment [g3]: The Software Life Cycle Planning Process in Section 3.2 associated with the SIVAT tool development done by AREVA NP GmbH also provides information about the Operations and Training plans executed by AREVA NP Inc. that are not associated with the SIVAT tool Development by AREVA NP GmbH. This section should provide an explanation of which organization is associated with what section based upon the audit information and also what the SIVAT TR states.

This section evaluates the planning documentation associated with the SIVAT tool development.

Deleted: software

Proposed digital safety-related I&C equipment that uses the TXS platform will be required to conform to IEEE Std. 603-1991 "Criteria for Safety Systems for Nuclear Power Generating Stations." SIVAT will be used as a tool to assure conformance with several of these standards requirements; therefore, a separate IEEE Std. 603 conformance evaluation was conducted. Refer to Section 3.4, "Conformance with IEEE Std. 603-1991," of this SE for details concerning conformance of the SIVAT tool with applicable portions of this standard.

Among the standards referenced in the Standard Review Plan (SRP) NUREG-0800 and Branch Technical Position (BTP) 7-14, IEEE Std.7-4.3.2-2003, "Criteria for Digital Computers in Safety *Systems of Nuclear Power Generating Stations," provides specific requirements concerning the* development of software. Although SIVAT software is not actually used in safety systems, it supports the performance of V&V activities that are required for the qualification of application software that is installed in the safety systems of nuclear power plants. Because of this, several of the clauses within IEEE Std. 7-4.3.2 are directly applicable to SIVAT. Refer to Section 3.5, "Conformance with IEEE Std. 7-4.3.2-2003," of this SE for details concerning the applicant's conformance with this standard.

3.2.1 SIVAT Software Management Plan

The SRP NUREG-0800, BTP 7-14, Section B.3.1.1, provides acceptance criteria for software management plans (SMP). This section states that Regulatory Guide (RG) 1.173 endorses IEEE Std. 1074-1995, "IEEE Standard for Developing Software Life Cycle Processes," and that Clause 3.1.6, "Plan Project Management," contains an acceptable approach to SMP. Clause 3.1.6 states that the SMP should include planning for support, problem reporting, risk management, and retirement.

The SMP used by AREVA NP GmbH[2] to facilitate management of the SIVAT tool is contained in Section 5.0 "SIVAT Management Plan" of the "TELEPERM XS™ Simulation Validation Test Tool (SIVAT) Topical Report ANP-10303P Revision 1" (Reference 11). This document provides a methodology for documenting quality assurance (QA) elements of software and data associated with the SIVAT tool.

Deleted: V&V

The SIVAT *tool was developed under the same QA program and software lifecycle development* process and procedures that were previously evaluated for TXS system software in the TXS platform reference SE (Reference 5). That report concluded that Engineering procedure FAW-TXS-1.1, "Phase model for the development of Software Components for TXS," was compatible to IEEE Std. 1074, "Developing Life Cycle Process," and was therefore acceptable. The applicant has also stated that engineering procedure FAW-TXS-1.1 has not changed since the TXS platform reference SE (Reference 5) was issued in May of 2000.

Deleted: safety evaluation report

The SIVAT tool was developed based on a requirements specification and a TS document in accordance with the FAW-TXS-1.1 engineering procedure. A thread audit was performed in Alpharetta, Georgia, on May 8, 2010, through May 10, 2010, in order to confirm compliance with the approved software development life cycle processes. During this audit (Reference 13), as documented in the "Trip Report for U. S. Nuclear Regulatory Commission (NRC) Staff's Thread Audit at AREVA for SIVAT Simulation Tool," several TSs were selected and traced from the development documentation through to the implementation and verification activities as defined by the process. The results of this audit discovered no significant quality issues or process discrepancies with the development of the SIVAT tool.

Deleted: program

No supporting specification documentation for the front end or Graphical User Interface (GUI) portion of the SIVAT tool was produced during the development process. Therefore, those functions that are performed by this GUI could not be traced during the audit. This GUI

Deleted: simulator

Deleted: of this application

Deleted: application

Deleted: *application*

---

[2] AREVA NP GmbH is a designation used in this report to refer to the AREVA NP organization responsibility for the TELEPERM XS System development. This organization is based in Erlangen, Germany.

performs a minimal set of tasks, for each requirement that the NRC staff chose to trace that was being performed by this GUI, the NRC staff was able to observe that the function was performed satisfactorily via SIVAT demonstration activities. The NRC staff concluded that no simulator functions that the V&V process invokes are performed by the GUI without readily available confirmation that the GUI performed these tasks satisfactorily.

Deleted: application

Based upon the review of the SIVAT software development lifecycle, which is the same process that was reviewed and approved by the NRC for the TXS platform, the NRC staff has determined that the SIVAT SMP is of sufficient quality to provide a reasonable expectation for the development of software suitable for use as a tool to support the performance of V&V activities for TXS based safety-related Application Software. The NRC staff also concludes that *implementation of this plan has resulted in a program that is effective in identifying and* addressing software quality issues associated with the SIVAT tool.

Deleted: s

Deleted: simulation

3.2.2 SIVAT Software Development Plan

The acceptance criteria for a Software Development Plan (SDP) are contained in the SRP, BTP 7-14, Section B, 3.1.2. This section states that RG 1.173, "Developing Software Life Cycle Processes for Digital Computer Software Used in Safety Systems of Nuclear Power Plants," endorses IEEE Std. 1074-1995, "IEEE Standard for Developing Software Life Cycle Processes," subject to exceptions listed, as providing an approach acceptable to the NRC staff, for meeting the regulatory requirements and guidance as they apply to development processes for safety system software and that Clause 5.3.1. of IEEE Std. 7-4.3.2-2003 contains additional guidance on software development.

The SDP used by AREVA NP GmbH to facilitate development of the SIVAT tool is contained in Section 6.0, "SIVAT Development Plan" of the TXS simulation test tool SIVAT TR (Reference 11). The Software Life Cycle Model (SLCM) for the SIVAT tool is defined in the same program and software lifecycle development process and procedures that were previously evaluated for TXS system software in the TXS platform reference SE (Reference 5). AREVA NP GmbH, uses *a phase model for the software lifecycle which closely follows the waterfall model defined in* Section 2.3.1 of NUREG/CR-6101, "Software Reliability and Safety in Nuclear Reactor Protection Systems." As was previously stated in Section 3.2.1 of this SE, the TXS simulation validation test tool SIVAT TR concluded that engineering procedure FAW-TXS-1.1, "Phase model for the development of Software Components for TXS" was compatible to IEEE Std. 1074, "Developing Life Cycle Process" and was therefore acceptable.

Deleted: V&V

The SIVAT SDP adequately addresses the software lifecycle development planning activities of IEEE Std. 1074-1995 because it is based upon the previously approved TXS software development processes. The NRC staff concludes that the SDP used for the SIVAT simulation test tool provides a development process, which promotes high functional reliability and design quality of SIVAT software that is suitable for its intended use.

3.2.3 SIVAT Software Quality Assurance Plan

Section B.3.1.3 of BTP 7-14 provides guidance in evaluating Software Quality Assurance Plans (SQAP). The SQAP shall conform to the requirements of 10 CFR Part 50, Appendix B, and the applicant's overall QA program. Stated in 10 CFR Part 50, Appendix B, the applicant shall be responsible for the establishment and execution of the QA program. The applicant may delegate the work of establishing and executing the QA program, or any part thereof, but shall retain responsibility for the QA program. The SQAP would typically identify which QA procedures are applicable to specific software processes, identify particular methods chosen to implement QA procedural requirements, and augment and supplement the QA program as needed for software. Clause 5.3.1 of IEEE Std. 7-4.3.2-2003, which is endorsed by RG 1.152, Revision 2, provides guidance on software QA. Clause 5.3.1 of IEEE Std. 7-4.3.2-2003 states that computer software shall be developed, modified, or accepted in accordance with an approved SQAP consistent with the requirements of IEEE/EIA Std. 12207.0-1996, and that guidance for developing software QA plans can be found in IEEE Std. 730-2002, "Standard for Software Quality Assurance Plans."

The SQAP used by AREVA GmbH to establish the necessary processes that ensure that the SIVAT software attains a level of quality commensurate with its importance to safety is contained in Section 7.0, "SIVAT Quality Assurance Plan" of the TXS simulation test tool SIVAT TR (Reference 11). The SIVAT tool was developed under the same QA program and life cycle process that was previously evaluated for TXS system software in the TXS platform reference SE (Reference 5). The following procedures were utilized by the SIVAT development team to implement Appendix B quality controls for the SIVAT tool.

1. FAW-TXS 1.5 was used to implement configuration management requirements.
2. FAW-TXS 2.2 was used to implement documentation requirements.
3. FAW-TXS 4.1 was used to implement system integration requirements.
4. FAW-TXS 4.2 was used to govern review guidelines for the development of SIVAT

The changes that have been made to the above engineering procedures were subsequently documented in the response to Request for Additional Information (RAI) 52 of the "Oconee RPS/ESPS RAI responses" (Reference 12). The NRC staff evaluated the changes to these procedures and determined that the safety conclusions that were based on the conformance to IEEE Std. 730-2002, "Standard for Software Quality Assurance Plans," and IEEE Std. 1074-1995, "Standard for Developing Software Life Cycle Processes," have not been compromised because of these procedure changes. In addition, specific V&V activities relating to software QA described in Section 14 of the SIVAT TR (Reference 11) were applied to the development of the SIVAT tool.

Deleted: opical

Deleted: eport

The NRC staff has determined that the quality controls that these procedures implement meet the applicable requirements of 10 CFR Part 50, Appendix B, for a software V&V tool. The NRC staff also determined that the SIVAT QA plan as implemented by these procedures conforms to IEEE Std. 730-2002, "Standard for Software Quality Assurance Plans," and IEEE Std. 1074-1995, "Standard for Developing Software Life Cycle Processes," Clause 3.3 as endorsed by RG 1.173. The NRC staff therefore considers the SIVAT QA plan to be acceptable.

3.2.4 SIVAT Software Integration Plan

Section B.3.1.4 of BTP 7-14 provides guidance in evaluating Software Integration Plans (SIntP). Clause 5.3.7 of IEEE Std. 1074-1995, which is endorsed by RG 1.173, provides an acceptable approach to an integration plan. Clause 5.3.7 states that during the plan integration activity, the software requirements and the software design description are analyzed to determine the order of combining software components into an overall system. BTP 7-14, Section B.3.1.4.1 asks for a description of the software integration process and the software integration organization.

[

]

[ ]

Figure 3-5: SIVAT Integration Software Elements

Deleted: 4

[

]

[

]

The SIVAT SIntP describes the software integration processes involved with incorporating TXS system software into SIVAT. The plan also states which group is responsible for the integration activities. As set forth above, the SIntP adequately addresses the software integration planning activities of BTP 7-14, and the NRC staff finds the SIntP acceptable.

3.2.5 SIVAT Software Installation Plan

The acceptance criteria for a SIntP are contained in the SRP, BTP 7-14, Section B.3.1.5, "Software Installation Plan." IEEE Std. 1074-1995, "IEEE Standard for Developing Software Life Cycle Processes," Clause 6.1 which is endorsed by RG 1.173 provides an acceptable approach for software installation plans. IEEE Std. 1074-1995, Clause 6.1.1, states an installation consists of the transportation and installation of the software system from the development environment to the target environment. It includes the necessary software modifications, checkout in the target environment, and customer acceptance. If a problem arises, it must be identified and reported. BTP 7-14, Section B.3.1.5.4, states that there should be approved procedures for software installation, for combined hardware and software installation, and systems installation. Further guidance is provided in NUREG/CR-6101, Section 3.1.8, "Software Installation Plan," and Section 4.1.8, "Software Installation Plan," that contains a sample outline of an installation plan.

Deleted: n

[

]

3.2.6 SIVAT Software Maintenance Plan

The acceptance criteria for a Software Maintenance Plan are contained in the SRP BTP 7-14, Section B.3.1.6, "Software Maintenance Plan (SMaintP)." The section states that NUREG/CR-61 01, Section 3.1.9, "Software Maintenance Plan," and Section 4.1.9, "Software

Maintenance Plan," contain guidance on SMaintP. These sections break the maintenance into three activities: failure reporting, fault correction, and re-release procedures.

The SMaintP provided by AREVA to facilitate the maintenance of the SIVAT tool is contained in Section 10.0 "SIVAT Software Maintenance Plan" of the TXS simulation test tool SIVAT TR (Reference 11).

Deleted: V&V

Identification of the need to maintain SIVAT software is performed by the various user organizations which include AREVA NP Inc. These software change requests are transmitted to the SIVAT development organization AREVA NP GmbH for incorporation into the tool. The processes for making changes to SIVAT software which include maintenance of software configuration control are described in Section 15.0 of the SIVAT TR (Reference 11). These processes are evaluated in Section 3.2.11 of this SE. The SIVAT problem reporting processes are described in Section 5.4 of the SIVAT TR (Reference 11).

Deleted: .

The SIVAT SMaintP defines a process for maintaining the SIVAT software including identification of the need for changes to software, processing software revisions to accomplish the changes and V&V activities to provide assurance that the changes made do resolve the initiating issues. The NRC staff has determined that the SIVAT SMaintP as defined within the SIVAT TR (Reference 11) is consistent with the guidance of SRP BTP 7-14, Section B.3.1.6, "Software Maintenance Plan." The SIVAT SMaintP is therefore acceptable.

Deleted:

3.2.7 SIVAT Operations Plan

The acceptance criteria for a software operations plan (SOP) are contained in the SRP, BTP 7-14, Section B.3.1.8, "Software Operations Plan." This section states that the primary aspect is completeness. It adds that the operations plan needs to address the security of the system, and in particular, the means used to ensure that there are not unauthorized changes to hardware, software, and system parameters, and that there is monitoring to detect penetration or attempted penetration of the system.

The SIVAT operations plan used by the AREVA NP Inc. to facilitate the operation of the SIVAT V&V tool is contained in Section 11.0 "SIVAT Operations Plan" of the TXS simulation test tool SIVAT TR (Reference 11).

Deleted: software

Deleted: GmbH

Deleted: Software

The SIVAT Operation Plan provides a general description of the operation of SIVAT. This discussion includes a description of the types of V&V integration and functional testing that SIVAT is used to support. Section 11.2 of the TR (Reference 11) lists and discusses the limitations associated with SIVAT simulation. [

Deleted: SOP

]

[

]

The NRC staff determined that the management, implementation, and resource characteristics of the SIVAT Operations Plan are adequate. The security of the system is accomplished via independent V&V activities and through software configuration control measures. The organizational structure, which includes the V&V organization as well as the Software Design Group that is needed to control the software operations, is defined within the SIVAT SOP. The NRC staff has determined that the SIVAT Operations Plan as defined within the SIVAT TR (Reference 11) is consistent with the guidance of SRP, BTP 7-14, Section B.3.1.8, "Software Operations Plan". The SIVAT Operations Plan is therefore acceptable.

Deleted: SOP

Deleted: Software

Deleted: SOP

3.2.8 SIVAT Training Plan

The acceptance criteria for a software training plan are contained in the SRP, BTP 7-14, Section B.3.1.7, "Software Training Plan." This section states that RG 1.173 endorses IEEE Std. 1074-1995, "IEEE Standard for Developing Software Life Cycle Processes." Clause 7.4 of that standard, "Training Process," contains an approach relating to planning for training. SRP BTP 7-14, Section B.3.1.7, also states that NUREG/CR-6101, Section 3.1.10, "Software Training Plan," contains further guidance on Software Training Plans.

Clause A.1.2.6 of IEEE Std. 1074-1995, requires different types of training depending on the need. It states that training tools, techniques, and methodologies shall be specified, and that the planning shall include developing schedules, estimating resources, identifying special resources, staffing, and establishing exit or acceptance criteria. This planning shall be documented in the Training Planned Information.

The SIVAT training plan used by the AREVA NP Inc. to facilitate training of V&V personnel in the use of the SIVAT V&V tool is contained in Section 12.0, "SIVAT Training Plan" of the TXS simulation test tool SIVAT TR (Reference 11). This plan describes a method for ensuring that the training needs for the use of SIVAT are achieved. The training plan describes training organizational responsibilities, methods used to accomplish SIVAT training, training resources available to support SIVAT training, and training requirements for personnel who perform tasks that involve use of SIVAT.

Deleted: software

Deleted: GmbH

The NRC staff determined that the management implementation and resource characteristics of the software training plan are satisfactory. The NRC staff concludes that this training plan is compliant with the requirements of IEEE Std. 1074-1995 and is therefore acceptable.

3.2.9 Software Safety Plan (SSP)

The acceptance criteria for a SSP are contained in the SRP, BTP 7-14, Section B.3.1.9, "Software Safety Plan" and Section B.3.2.1, "Acceptance Criteria for Safety Analysis Activities." These sections state that the SSP should provide a general description of the software safety effort, and the intended interactions between the software safety organization and the general system safety organization. It further states that NUREG/CR-6101, Section 3.1.5, "Software

Safety Plan," and Section 4.1.5, "Software Safety Plan," contain guidance on SSP. Further guidance on safety analysis activities can be found in NUREG/CR-6101 and RG 1.173, Section C.3, "Software Safety Analyses."

The SSP used by the AREVA NP GmbH to facilitate software safety activities for the SIVAT tool is contained in Section 13.0 "SIVAT Software Safety Plan" of the TXS simulation test tool TR (Reference 11). The SIVAT tool does not modify the actual application software code that is loaded into the TXS safety processors. The NRC staff therefore agrees that SIVAT cannot directly create a safety hazard affecting safety functions. The accuracy and fidelity of SIVAT test results are however relied upon for the satisfactory completion of application specific software safety tasks such as Validation Testing.

> **Comment [g4]:** The SSP would be used by both AREVA GmbH and AREVA NP Inc. in different aspects. This section should provide an explanation of which organization is associated with what section based upon the audit information and also what the SIVAT TR states.

> **Deleted:** V&V

[

]

The NRC staff concludes that the SIVAT SSP as defined in the SIVAT TR (Reference 11) provides adequate assurance that the software safety activities which rely upon the SIVAT tool outputs will resolve safety issues presented during the design and development of the TXS Application Software. The NRC staff also determined that adequate processes are in place to insure that software hazards which cannot be detected by SIVAT due to the limitations of simulation will be identified and corrected through means of V&V that do not rely on SIVAT. These limitations are defined in Section 3.6 of the SIVAT TR (Reference 11). The SIVAT SSP is therefore acceptable.

> **Deleted:** safety

> **Deleted:** a

> **Deleted:** s

3.2.10 SIVAT Verification and Validation Plan (SVVP)

The acceptance criteria for SVVP are contained in the SRP, BTP 7-14, Section B.3.1.10, "Software Verification and Validation Plan," and Section B.3.2.2, "Acceptance Criteria for Software Verification and Validation Activities." These sections state that RG 1.168, "Verification, Validation, Reviews, and Audits for Digital Computer Software Used in Safety Systems of Nuclear Power Plants," Revision 1, endorses IEEE Std. 1012-1998, "IEEE Standard for Software Verification and Validation," as providing methods acceptable to the NRC staff for meeting the regulatory requirements as they apply to V&V of safety system software. This section also states that further guidance can be found in RG 1.152, Revision 2, Section C.2.2.1, "System Features," and NUREG/CR-6101, Sections 3.1.4 and 4.1.4. Verification is defined as the process of determining whether the products of a given phase of the development cycle fulfill the requirements established during the previous phase.

The simulator based application software validation process is described in the TXS reference TR (Reference 15) "TELEPERM XS™: A Digital Protection System: Platform Reference Topical Report EMF-2110(NP) (A) Revision 1" Section 2.4.3.3.2 "Simulator-Based Validation".

The SVVP used by AREVA NP GmbH to facilitate software V&V activities for the SIVAT V&V tool is contained in Section 14.0, "SIVAT Software Verification and Validation Plan," of the TXS simulation test tool SIVAT TR (Reference 11). This plan describes methods used by AREVA

NP GmbH to ensure the correctness of the SIVAT tool software.

The procedures that are used by AREVA to perform software verification activities associated with SIVAT are the same procedures that are used for the development of the TXS platform software. These procedures were previously evaluated by NRC staff in the TXS platform reference SE (Reference 5). That SE found that these procedures specify the areas of application, the organizational responsibilities, requirements for independent V&V (IV&V) activities, and requirements for documentation. These procedures are compatible with IEEE Std. 1012-1998, "Software Verification and Validation Plans," and are, therefore, acceptable.

Deleted: P

Deleted: R

3.2.11 SIVAT Configuration Management Plan (SCMP)

The acceptance criteria for SCMP are contained in the SRP, BTP 7-14, Section B.3.1.11, "Software Configuration Management Plan," and Section B.3.2.3, "Acceptance Criteria for Software Configuration Management Activities." These sections state that RG 1.173, "Developing Software Life Cycle Processes for Digital Computer Software Used in Safety Systems of Nuclear Power Plants," endorses IEEE Std. 1074-1995, "IEEE Standard for Developing Software Life Cycle Processes," Clause A.1.2.4, "Plan Configuration Management," and RG 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," and provides an acceptable approach for planning configuration management. SRP, BTP 7-14, Section B.3.1.11, further states that additional guidance can be found in IEEE Std. 7-4.3.2-2003, "IEEE Standard Criteria for Digital Computers in Safety Systems on Nuclear Power Generating Stations," Clause 5.3.5, "Software configuration management," and in Clause 5.4.2.1.3, "Establish configuration management controls." NUREG/CR-6101, Section 3.1.3, "Software Configuration Management Plan," and Section 4.1.3, "Software Configuration Management Plan," also contain guidance.

Comment [g5]: The SCMP would be used by both AREVA GmbH and AREVA NP Inc. in different aspects. This section should provide an explanation of which organization is associated with what section based upon the audit information and also what the SIVAT TR states.

The SCMP used by AREVA NP GmbH to facilitate software configuration management activities for the SIVAT tool is contained in Section 15.0, "SIVAT Configuration Management Plan" of the TXS simulation test tool TR (Reference 11). This plan describes the methods that are used to maintain the SIVAT software in a controlled configuration. All SIVAT software and associated documentation are classified as configuration items in the TXS projects for which they are used. As such, configuration control for these items is maintained.

Deleted: V&V

Deleted: Software

In order to evaluate the effectiveness of the SCMP the NRC staff reviewed the configuration controls which were used during the Oconee RPS/ESPS system SIVAT validation testing activities. During the SIVAT audit conducted on June 8th through 10th, 2010 (Reference 13), the NRC staff verified that the SIVAT configuration information was documented in the Oconee test documentation (References 6, 7, 8, & 9). [

]

SIVAT was developed under the same configuration management processes that are used for the development of safety-related TXS software. The SCMP describes process changes that have been made since the NRC's approval of the AREVA NP GmbH software configuration management process in 2000 (Reference 5, Section 2.2.5). The following list is a summary of these changes:

1. A Change Control Board was added to the process.
2. Additional clarifying details were included for the description of Configuration Management Tasks.
3. The requirements of Type Tests for the TXS system platform were added.

The NRC staff has reviewed these changes and has concluded that the software configuration management processes remain compatible with IEEE Std. 828-1990 and are therefore, acceptable.

3.2.12 SIVAT Test Plan (STP)

The acceptance criterion for STP is contained in the SRP, BTP 7-14, Section B.3.1.12, "Software Test Plan," and in Section B.3.2.4, "Acceptance Criteria for Testing Activities." These sections state that both RG 1.170, "Software Test Documentation for Digital Computer Software Used in Safety Systems of Nuclear Power Plants," that endorses IEEE Std. 829-1983, "IEEE Standard for Software Test Documentation," and RG 1.171, "Software Unit Testing for Digital Computer Software Used in Safety Systems of Nuclear Power Plants," that endorses IEEE Std. 1008-1987, "IEEE Standard for Software Unit Testing," identify acceptable methods to satisfy software unit testing requirements.

The STP used by AREVA NP GmbH to facilitate software test activities which utilize the SIVAT tool is contained in Section 16.0, "SIVAT Test Plan," of the TXS simulation test tool SIVAT TR (Reference 11). Currently, testing has been completed for SIVAT Release 1.2.4. The STP outlines the methods that will be used to test future releases of SIVAT. These methods involve testing simulated system response to input, output, and state data measured during factory acceptance tests of on-line systems in the test field. The acceptance criteria for these test results are that the simulated and on-line systems must exhibit the same functional behavior as indicated by the test data. The scope of testing is defined in the STP and includes change request Implementation test component and a tool integration component. SIVAT test documentation is developed and maintained in accordance with IEEE Std. 829-1983. Based on AREVA NP's commitment to meeting IEEE Std. 829-1983 and IEEE Std. 1008-1987, the NRC staff finds the SIVAT STP acceptable.

3.2.13 ERBUS Test Field Simulator Testing

Section 3.7 of the TR describes simulation in the test field using a test field simulator called ERBUS. ERBUS is a computer-assisted test system for TXS test field application. The ERBUS system generates analog and digital signals, which are wired directly into the TXS hardware during factory testing activities. In addition, system output analog and digital signals are wired to input channels of the ERBUS system for the purpose of monitoring system outputs during test performance.

AREVA stated that "The description of ERBUS was included for completeness, since the same simulator control system that is used for SIVAT also runs on the Simulator Control Unit used in the test field." Refer to RAI's 13 and 14 (Reference 4) for additional information regarding the use of ERBUS.

ERBUS testing is described as testing that is performed following the manufacture of the cabinet in the test field. Figure 3-13 of the TR also illustrates ERBUS testing as testing that is

Deleted: Software

Deleted: V&V

Deleted: Software

Comment [g6]: Specify which TR describes the ERBUS: SIVAT or TXS platform reference SE.

Comment [g7]: Specify which TR provides Figure 3-13: SIVAT or TXS platform reference SE.

performed independently from the use of SIVAT. This description of the ERBUS testing process is considered by the NRC staff to be informative. Though the NRC staff recognizes ERBUS testing as a means of performing verification testing of system aspects that are not tested within SIVAT, the NRC staff did not evaluate the ERBUS based test processes.

3.3 SIVAT Code Adaptation Process Evaluation

[

]

3.4 Conformance with IEEE Std. 603-1991, "IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations"

This standard establishes criteria to be applied to those systems required to protect the public health and safety by functioning to mitigate the consequences of design-basis events. SIVAT software does not directly perform such functions, however it will be used to ensure that these functions as implemented on the TXS platform do meet the functional and design criteria for the power, instrumentation, and control portions of nuclear power generating station safety systems. The NRC staff therefore considers the practices for design and evaluation of safety system performance and reliability outlined in this standard to be relevant to the SIVAT Tool.

Deleted: application

3.4.1 Safety System Designation (IEEE Std. 603-1991, Section 4)

SIVAT does not perform safety-related functions nor is it required to protect the public health and safety by functioning to mitigate the consequences of design-basis accidents. The SIVAT Tool is therefore designated as a non-safety-related tool. Even so, a development process which includes a requirements basis has been established for the design of SIVAT. This design is available as was demonstrated during the thread audit conducted in Alpharetta, Georgia on June 8th through 10th (Reference 13) and via the requirements documentation submitted to the NRC in support of this SE, "TELEPERM XS Simulation Tools - Translation of Selected Chapters

Deleted: application

Deleted: application

from Requirements and Design Specification Documents from the Initial Development" (Reference 17).

3.4.2 Safety System Criteria (IEEE Std. 603-1991, Section 5)

SIVAT is not used to maintain plant parameters within acceptable limits established for each design-basis event. SIVAT may be used to validate that TXS Application Software performs these functions. The NRC staff concludes that when used in accordance with established validation policies and procedures, the SIVAT Tool does provide reasonable assurance that such functions can be achieved by the TXS safety system applications being tested.

Deleted: safety
Deleted: a
Deleted: s
Deleted: do
Deleted: validation t

SIVAT is not required to meet the single failure criterion of Section 5.1 of IEEE Std. 603-1991.

3.4.3 Sense and Command Features Functional and Design Requirements (IEEE Std. 603-1991, Section 6)

SIVAT is not relied upon for the performance of sense and command features by the TXS safety systems, therefore the requirements of this section do not apply to SIVAT.

3.4.4 Execute Feature Functional and Design Requirements (IEEE Std. 603-1991, Section 7)

SIVAT is not relied upon for the performance of executive features by the TXS safety systems, therefore the requirements of this section do not apply to SIVAT.

3.4.5 Power Source Requirements (IEEE Std. 603-1991, Section 8)

The SIVAT Tool is not required to meet the power source requirements of this section because SIVAT is not required to be operational during the performance of safety functions by TXS safety systems.

Deleted: system

3.5 Conformance with IEEE Std. 7-4.3.2-2003, "IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations"

IEEE Std. 7-4.3.2 establishes additional computer specific requirements to supplement the criteria and requirements of IEEE Std. 603. Software Tools are defined within IEEE Std. 7-4.3.2 as follows:

Software tools: A computer program used in the design, development, testing, review, analysis, or maintenance of a program or its documentation. Examples include compilers, assemblers, linkers, comparators, cross-reference generators, decompilers, editors, flow charters, monitors, test case generators, integrated development environments, and timing analyzers.

Though software simulators are not explicitly listed within this definition, the NRC staff considers the SIVAT software package to be a software tool because it is used to support the testing of safety-related programs.

Deleted: simulator

Section 5.3, "Quality," of IEEE Std. 7-4.3.2 states that "in addition to the requirements of IEEE Std. 603, the following activities necessitate additional requirements that are necessary to meet the quality criterion: Use of software tools." These additional requirements are:

The SQAP shall address the software tools for the system development and maintenance as follows.

If software tools are used during the lifecycle process of safety-related software, one or both of the following methods shall be used to confirm outputs of that software tool are suitable for use in safety-related systems:

a) The output of the software tool shall be subject to the same level of V&V as the safety-related software, to determine that the output of that tool meets the requirements established during the previous lifecycle phase.

b) The tool shall be developed using the same or an equivalent high quality lifecycle process as required for the software upon which the tool is being used as described in this subclause (5.3) or commercially dedicated as in 5.17, to provide confidence that the necessary features of the software tool function as required.

Formatted: Bullets and Numbering

Though the SIVAT Tool is not a safety-related software package, it was developed using a software lifecycle process equivalent to the process that is used to develop TXS safety-related Application Software. The NRC staff conducted an audit of the SIVAT development process (Reference 13) which included tracing of several requirements to program implementation and testing. The results of this audit in addition to the operating experience with SIVAT usage indicated that a quality process was being used to provide a reasonable level of assurance that the SIVAT tool outputs are representative of the expected performance of the safety-related software upon installation into plant equipment.

Deleted: program

Deleted: program

Deleted: TXS software

The output of the SIVAT tool is the test data that is collected during the SIVAT test execution. This data is assessed by V&V personnel during the test results evaluation activity as described in Section 3.1.4 above to determine if the test acceptance criteria have been satisfied. The NRC staff concludes that the intent of method as described above is being met by the SIVAT testing processes that are being used to validate TXS safety-related software.

Software tools used to support the software lifecycle process of safety-related software shall be controlled under configuration management. See Section 3.2.11 of this SE for the NRC staffs' evaluation of the SCMP for SIVAT.

3.6 Software Requirements Traceability

The definition of a Requirements Traceability Matrix (RTM) is contained in Standard Review Plan (SRP), BTP 7-14, Section A.3, definitions, and states: "An RTM shows every requirement, broken down in to sub-requirements as necessary, and what portion of the software requirement, software design description, actual code, and test requirement addresses that system requirement." This is further clarified in Section B.3.3, "Acceptance Criteria for Design Outputs," in the subsection on Process Characteristics. This section states that an RTM, that needs to show every requirement, should be broken down in to sub-requirements, as necessary. The RTM should show what portion of the software requirements specification, software design description (SDD), actual code, and test requirement addresses each system requirement.

Though no RTM was used for the development of SIVAT, the NRC staff conducted a thread audit which included a number of requirements selected from the TELEPERM XS Simulation Tool Requirements and Design Specification Documents (Reference 17). During this audit AREVA NP staff was able to track the implementation of the selected software requirements through each phase of the SIVAT design process. The results of this audit are documented in the audit report (Reference 13).

Deleted: of

Deleted: SIVAT software r

Deleted: d

Deleted: various

Software Requirements Traceability also applies to the development of test requirements for an application which uses SIVAT for validation testing. During the thread audit, the NRC staff asked AREVA to discuss and evaluate how requirements traceability to the SIVAT test documentation and test results would be established and maintained. [

]

Deleted: t

The V&V requirements RTM attachment of the RTM report was provided as an example of how software requirements would be traced to the SIVAT test specification and test procedure documents. The RTM functional requirements specifications coverage attachment of the RTM provides an analysis of the requirements tracing effort which includes an assessment of the level of requirements coverage provided for the particular project.

The NRC staff concludes that SIVAT simulation based validation testing activities can be safely integrated into the planned requirements tracing processes and is therefore acceptable.

3.7 Limitations of SIVAT Testing

[

]

During the SIVAT audit, the NRC staff discussed and evaluated how each of these simulation limitations would be subsequently verified and validated via means that do not rely on SIVAT. AREVA NP also provided a presentation on the subject of limits of simulation (Reference 19), "TELEPERM XS Perspectives on Limitations of SIVAT Testing." This included the history of the SIVAT simulation tool and provided an explanation of why the limits of simulation exist. The NRC staffs' evaluation concluded that AREVA NP does have the necessary processes and programs to affect supplementary testing activities through the means of factory acceptance tests if the equipment has not been installed into a plant, and through site acceptance tests performed on installed plant equipment. Refer to Section 4.2 of the SIVAT thread audit trip report (Reference 13) for additional details of this evaluation.

Deleted: e

4.0 CONCLUSION

The NRC has concluded, based on the considerations discussed above, that:

1. There is reasonable assurance that the health and safety of the public will not be endangered by the use of the SIVAT software simulation tool for validation testing activities in the proposed manner.

2. Such activities will be conducted in compliance with the Commission's regulations.

3. The issuance of amendments which credit the use of SIVAT to support validation testing activities of TXS safety-related Application Software will not be inimical to the common defense and security or the health and safety of the public.

Formatted: Bullets and Numbering

Deleted: TXS

Deleted: s

5.0 LIMITATIONS AND CONDITIONS

Based on the forgoing considerations, the NRC staff concludes that the use of SIVAT is acceptable with limitation and conditions described as follows:

1. [ ]

   System functionality aspects that cannot be tested in this simulation environment must be tested through other means which are not within the scope of this SE.

2. The use of closed-loop simulation testing to complete V&V activities for safety-related application software cannot be evaluated or approved by the NRC within this SE because of the uncertainties associated with the use of process models. These models have not been submitted to the NRC for review and are not within the scope of this SE. This SE does not, however, preclude the use of SIVAT to perform closed-loop tests to support system qualification.

3. The SIVAT tool was developed under the same program and software lifecycle development process and procedures that were previously evaluated for TXS system software in the TXS platform reference SE (Reference 5). That report concluded that Engineering procedure FAW-TXS-1.1, "Phase model for the development of Software Components for TXS," was compatible to IEEE Std. 1074, "Developing Life Cycle Process," and was therefore acceptable. The applicant has also stated that engineering procedure FAW-TXS-1.1 has not changed since the TXS platform reference SE (Reference 5) was issued in May of 2000.

4. The SIVAT SOP provides a general description of the operation of SIVAT. This discussion includes a description of the types of V&V integration and functional testing that SIVAT is used to support. Section 11.2 of the TR (Reference 11) lists and discusses the limitations associated with SIVAT simulation. [ ]

Comment [g8]: Specify section 11.2 of which TR: SIVAT or TXS platform reference SE..

5. The NRC staff also determined that adequate processes are in place to insure that software hazards which cannot be detected by SIVAT due to the limitations of simulation will be identified and corrected through means of V&V that do not rely on SIVAT. These limitations are defined in Section 3.6 of the SIVAT TR (Reference 11).

6. ERBUS testing is described as testing that is performed following the manufacture of the cabinet in the test field. Figure 3-13 of the TR also illustrates ERBUS testing as testing that is performed independently from the use of SIVAT. This description of the ERBUS testing process is considered by the NRC staff to be informative. Though the NRC staff recognizes ERBUS testing as a means of performing verification testing of system aspects that are not tested within SIVAT, the NRC staff did not evaluate the ERBUS based test processes.

6.0 REFERENCES

1. Gardner, Ronnie L., AREVA letter to Document Control Desk, NRC, "Request for Review and Approval of ANP-10303P, 'SIVAT: TELEPERM XS™ Simulation Validation Test Tool Topical Report'," June 11, 2009, ADAMS Accession No. ML091680619.
2. Rosenberg, Stacey L., NRC letter to Ronnie L. Gardner, AREVA, "Acceptance for Review of AREVA NP, Inc. 'SIVAT: TELEPERM XS™ Simulation Validation Test Tool Topical Report'," December 28, 2009, ADAMS Accession No. ML093491029.
3. Gardner, Ronnie L., AREVA letter to Document Control Desk, NRC, "Request for Review and Approval of ANP-10303P, Revision 1, 'SIVAT: TELEPERM XS™ Simulation Validation Test Tool Topical Report'," September 1, 2010, ADAMS Accession No. ML102460054.
4. Gardner, Ronnie L., AREVA letter to Document Control Desk, NRC, "Response to Request for Additional Information Regarding ANP-10303, 'SIVAT: TELEPERM XS™ Simulation Validation Test Tool Topical Report'," May 5, 2010, ADAMS Accession No. ML101270267.
5. Richards, Stuart A., NRC letter to James F. Mallay, Siemens Power Corporation, "Acceptance for Referencing of Licensing Topical Report EMF-2110(NP), Revision 1, 'TELEPERM XS: A Digital Reactor Protection System'," May 5, 2000, ADAMS Accession No. ML003711856.
6. AREVA NP document 62-9014734-002, Oconee Nuclear Station, Unit 1 RPS/ESFAS Controls Upgrade Application Software Function Module Test Specification.
7. AREVA NP document 63-9014738-003, Oconee Nuclear Station, Unit 1 RPS/ESFAS Controls Upgrade Application Software Functions Test Procedure.
8. AREVA NP document 51-9027244-002, Oconee Nuclear Station, Unit 1 RPS/ESFAS Controls Upgrade Application Software Test Report.
9. AREVA NP document 51-9027208-001, Oconee Nuclear Station, Unit 1 RPS/ESFAS Controls Upgrade Software Unit Test Incident Report 51-9027208-001.
10.
11. AREVA NP, TR ANP-10303P, Revision 1, "SIVAT: TELEPERM XS™ Simulation Validation Test Tool Topical Report,". ADAMS Accession No. ML102460055.

Deleted: "
Deleted: "
Deleted: 6
Deleted: the
Deleted: "
Deleted: "
Deleted: "
Deleted: "
Deleted: "
Deleted: "
Deleted: "
Deleted: "
Deleted: 62-9014734-002
Deleted: 63-9014738-003
Deleted: SIVAT
Deleted: 51-9027244-002
Deleted: SIVAT
Deleted: <#>AREVA NP Inc., AREVA NP document 51-9052960-003, 'Oconee Nuclear Station, Units 1, 2, and 3 RPS/ESFAS Controls Upgrade Factory Acceptance Test Plan. ¶
Formatted: Bullets and Numbering
Deleted: . Inc.

12. Baxter, Dave, Oconee Nuclear Station Response to RAIs to Document Control Desk, NRC, "Oconee, Units 1, 2, and 3, Response to Request for Additional Information for License Amendment Request for Reactor Protective System/Engineered Safeguards Protective System Digital Upgrade, Technical Specification Change No. 2007-09, Supp. 5.," September 30, 2008, ADAMS Accession No. ML082800268.

13. "Trip Report for U. S. Nuclear Regulatory Commission (NRC) Staff's Thread Audit at AREVA for SIVAT Simulation Tool," June 30, 2010.

14. TELEPERM XS SIVAT-TXS Simulation Based Validation Tool User Manual TXS-1047-76-V2.1.

15. Siemens Power Corporation Nuclear Division, "TELEPERM XS: A Digital Protection System," May 2000, ADAMS Accession No. ML003732662.

16. AREVA NP document 51-9003307-00 , Oconee Nuclear Station, Units 1, 2 & 3 - RPS/ESFAS Controls Upgrade Simulation Based Validation Tool (SIVAT) Test Plan.

Deleted: Technical Report

17. "TELEPERM XS Simulation Tools -Translation of Selected Chapters from Requirements and Design Specification Documents from the Initial Development," July 9, 2010, ADAMS Accession No. ML102070250.

18. "Integration of SIVAT into Requirements Traceability Matrix," June 8, 2010, ADAMS Accession No. ML101730088.

19. "TELEPERM XS Perspectives on Limitations of SIVAT," Testing June 8, 2010, ADAMS Accession No. ML101730087.

Principal Contributor: Richard Stattel

Date: