AREVA

SIVAT: TELEPERM XS™ Simulation Validation Test Tool

ANP-10303NP-A
Revision 1

Topical Report

June 2012

AREVA NP Inc.

UNITED STATES
NUCLEAR REGULATORY COMMISSION
WASHINGTON, D.C. 20555-0001

June 15, 2012

Mr. Pedro Salas, Manager
Site Operations and Regulatory Affairs
AREVA NP Inc.
3315 Old Forest Road
Lynchburg, VA 24501

SUBJECT: FINAL SAFETY EVALUATION FOR AREVA NP, INC. (AREVA) ANP-10303P, REVISION 1, "SIVAT: TELEPERM XS™ SIMULATION VALIDATION TEST TOOL TOPICAL REPORT [TR]" (TAC NO. ME1503)

Dear Mr. Salas:

By letter dated June 11, 2009 (Agencywide Documents Access and Management System (ADAMS) Accession No. ML091680619), AREVA submitted its ANP-10303P, Revision 1, SIVAT: TELEPERM XS™ Simulation Validation Test Tool Topical Report (TR) to the U.S. Nuclear Regulatory Commission (NRC) staff. By letter dated August 9, 2011, an NRC draft safety evaluation (SE) regarding our approval of ANP-10303P, Revision 1, was provided for your review and comments. By letter dated April 29, 2011, AREVA commented on the draft SE. The NRC staff's disposition of AREVA comments on the draft SE are discussed in the attachment to the final SE enclosed with this letter.

The NRC staff has found that ANP-10303P, Revision 1, is acceptable for referencing in licensing applications that would allow the use of SIVAT as a software validation tool for the development of safety-related applications for the TELEPERM XS™ system to the extent specified and under the limitations delineated in the TR and in the enclosed final SE. The final SE defines the basis for acceptance of the TR.

Our acceptance applies only to material provided in the subject TR. We do not intend to repeat our review of the acceptable material described in the TR. When the TR appears as a reference in license applications, our review will ensure that the material presented applies to the specific plant involved. License amendment requests that deviate from this TR will be subject to a plant-specific review in accordance with applicable review standards.

In accordance with the guidance provided on the NRC website, we request that AREVA publish accepted proprietary and non-proprietary versions of this TR within three months of receipt of this letter. The accepted versions shall incorporate this letter and the enclosed final SE after the title page. Also, they must contain historical review information, including NRC requests for additional information and your responses. The accepted versions shall include a "-A" (designating accepted) following the TR identification symbol.

NOTICE: The Enclosure transmitted herewith contains proprietary information. When separated from the Enclosure, this document is decontrolled.

If future changes to the NRC's regulatory requirements affect the acceptability of this TR, AREVA and/or licensees referencing it will be expected to revise the TR appropriately, or justify its continued applicability for subsequent referencing.

Sincerely,

Sher Bahadur, Deputy Director
Division of Policy and Rulemaking
Office of Nuclear Reactor Regulation

Project No. 728

Enclosure 1: Non-Proprietary Final SE
Enclosure 2: Proprietary Final SE

FINAL 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. (AREVA)[1] submitted the "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.'"

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

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(a)(1) requires, in part, that systems and components be designed, tested, and inspected to quality standards commensurate with the safety function to be performed.

ENCLOSURE 1

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

FINAL 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. (AREVA)[1] submitted the "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.'"

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

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(a)(1) requires, in part, that systems and components be designed, tested, and inspected to quality standards commensurate with the safety function to be performed.

ENCLOSURE 1

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

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 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 quality assurance criteria are being met by the safety-related software of systems designed within the AREVA TXS platform.

The regulation at 10 CFR Part 50, Appendix B, Criterion III, "Design Control," requires, in part, that for safety-related Systems, Structures or components (SSCs), quality standards be specified and that design control measures shall provide for verifying or checking the adequacy of design.

The regulation at 10 CFR Part 50, Appendix B, Criterion XI, "Test Control," requires, in part, that a test program be established to demonstrate that safety-related systems and components will perform satisfactorily in service.

The regulation at 10 CFR Part 50, Appendix B. Criterion XII, "Control of Measuring and Test Equipment" requires that measures shall be established to assure that tools, gages, instruments, and other measuring and testing devices used in activities affecting quality are properly controlled, calibrated, and adjusted at specified periods to maintain accuracy within necessary limits.

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 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 SIVAT TR is being reviewed by the NRC because AREVA has included provisions for SIVAT simulation based testing activities within their TXS software development life cycle processes. In regards to software tool usage, BTP 7-14 states "if the output of any tool cannot be proven to be correct, the tool itself should be developed or dedicated as safety-related, with all the attendant requirements." Since the outputs of the SIVAT application will be used as a means of verifying software functionality and the SIVAT application is not safety-related, the NRC staff determined that this evaluation was necessary in order to establish a basis for the validity of these outputs.

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.

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 safety system application software using SIVAT involves comparing simulated function diagram integrated component performance with specified system requirements. The verification of software is complete when all specified requirements for a safety system application 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.

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 application software establishes reasonable assurance that the software is accomplishing its functions in a correct manner.

3.1.4 SIVAT Verification and Validation Test Example

[

]

[

]

3.2 Software Life Cycle Planning Process

This section evaluates the planning documentation associated with the SIVAT tool development by AREVA GmbH, and its use on a project by AREVA.

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.

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.

The SIVAT tool was developed based on a requirements specification and a technical specification 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 technical specifications 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 SIVAT development program.

---

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

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

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.

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, provides 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.

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 QA Plan

Section B.3.1.3 of BTP 7-14 provides guidance in evaluating Software QA 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.

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.

[

]

[

]

[

]

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 software installation plan 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 indentified 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.

[

]

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).

Identification of the need to maintain SIVAT software is performed by the various user organizations which include AREVA. 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. 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.

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 is consistent with the guidance of SRP BTP 7-14, Section B.3.1.6, "Software Maintenance Plan." The SIVAT SMaintP is therefore acceptable.

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 AREVA 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).

The SIVAT Operations 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. [

]

[

]

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 IV&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 Software Operations Plan as defined within the SIVAT TR 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.

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 Plan Information.

The SIVAT training plan used by AREVA 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.

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.

[

]

The NRC staff concludes that the SIVAT SSP as defined in the SIVAT TR 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 safety 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. The SIVAT SSP is therefore acceptable.

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 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 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.

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.

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.

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 conducted by AREVA. During the SIVAT audit conducted on June 8^{th} through 10^{th}, 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 STP defines the scope of testing, including change request implementation and tool integration. SIVAT test documentation is developed and maintained in accordance with IEEE Std. 829-1983. Based on AREVA'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 SIVAT TR (Reference 11) 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 questions 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 SIVAT 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.

3.3 [

]

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.

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 application. 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 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 safety 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.

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

Section 5.3 of IEEE Std. 603-1991 states in part that "safety system equipment shall be tested in accordance with the prescribed quality assurance program."

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). SIVAT test 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, Section 3.2.12 of this SE.

The NRC staff determined that the quality controls used for the SIVAT application testing meet the applicable requirements of 10 CFR 50 Appendix B for a software V&V tool.

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.

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 application to be a software tool because it is used to support the testing of safety-related programs.

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.

Though the SIVAT tool is not a safety-related software application, 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.

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 staff was able to track the implementation of various software requirements through each phase of the SIVAT design process. The results of this audit are documented in the audit report (Reference 13).

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. [

]

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 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 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.

3.8 Regulatory Compliance Evaluation Summary

10 CFR 50.55a(a)(1)

10 CFR Part 50, Appendix B, Criterion III:

The software QA plan is used by the AREVA NP GmbH to establish the necessary processes that ensure that the SIVAT software attains a level of quality commensurate with its importance to safety. 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 procedures utilized by the SIVAT development team to implement Appendix B quality controls for the SIVAT tool meet the applicable requirements of 10 CFR 50 Appendix B for a software V&V tool.

10 CFR Part 50, Appendix B, Criterion XI:

SIVAT, when used in conjunction with the TXS Software Test Plan, provides an acceptable environment to facilitate performance of safety-related software validation test activities. Furthermore, the NRC staff determined that the SIVAT tool when used within the restrictions outlined in Section 3.7 of this SE provides an acceptable means for verifying or checking the adequacy of TXS software designed for safety-related applications of nuclear power plants.

10 CFR Part 50. Appendix B. Criterion XII:

The SIVAT Tool does not require calibration or periodic adjustments. The primary measures to assure that SIVAT remains properly controlled at required periods to maintain confidence in its performance and outputs are proper software configuration management (Section 3.2.11 of this SE), design process controls (Section 3.2.2 of this SE), and control of tool usage through the approved procedures (Sections 3.2.7 & 3.2.10 of this SE). Each of these aspects of SIVAT control has been evaluated and the NRC staff has determined that these control measures provide reasonable assurance that SIVAT will be maintained within acceptable limits of performance.

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.

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 TXS 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 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 SIVAT TR (Reference 11) lists and discusses the limitations associated with SIVAT simulation. [

   ]

4. 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).

5. 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 the 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 document 62-9014734-002, Oconee Nuclear Station, Unit 1 RPS/ESFAS Controls Upgrade Application Software Function Module Test Specification.
7. AREVA document 63-9014738-003, Oconee Nuclear Station, Unit 1 RPS/ESFAS Controls Upgrade Application Software Functions Test Procedure.
8. AREVA document 51-9027244-002, Oconee Nuclear Station, Unit 1 RPS/ESFAS Controls Upgrade Application Software Test Report.
9. AREVA document 51-9027208-001, Oconee Nuclear Station, Unit 1 RPS/ESFAS Controls Upgrade Software Unit Test Incident Report.
10. AREVA document 51-9052960-003, 'Oconee Nuclear Station, Units 1, 2, and 3 RPS/ESFAS Controls Upgrade Factory Acceptance Test Plan.
11. AREVA, TR ANP-10303P, Revision 1, "SIVAT: TELEPERM XS™ Simulation Validation Test Tool Topical Report," ADAMS Accession No. ML102460055.
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 document 51-9003307-00, Oconee Nuclear Station, Units 1, 2 & 3 - RPS/ESFAS Controls Upgrade Simulation Based Validation Tool (SIVAT) Test Plan.
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:

RESOLUTION OF COMMENTS BY THE OFFICE OF NUCLEAR REACTOR REGULATION REGARDING THE DRAFT SAFETY EVALUATION FOR AREVA NP, INC. TOPICAL REPORT ANP-10303P, "SIVAT: TELEPERM XS™ SIMULATION VALIDATION TEST TOOL TOPICAL REPORT" PROJECT NO. 728

This Attachment provides the U.S. Nuclear Regulatory Commission (NRC) staff's review and disposition of the comments made by AREVA NP, Inc. (AREVA) on the draft safety evaluation (SE) for the AREVA Topical Report (TR) ANP-10303P, "SIVAT TELEPERM XS™ Simulation Validation Test Tool Topical Report," (Agencywide Documents and Management System (ADAMS) Accession No. ML112930222). AREVA provided its comments in a letter dated April 29, 2012 (ADAMS Accession No. ML111260687).

SUMMARY TABLE OF PROPOSED CHANGES TO AREVA TR DRAFT SE, PROPRIETARY REVIEW COMMENTS

Comment No.	Page No.	Line	AREVA Reviewer	AREVA Comment	NRC Response
1	3	7-9	Taylor	Proprietary Information	Proprietary Information withheld in Final SE
2	3	34-38	Taylor	Proprietary Information	Proprietary Information withheld in Final SE
3	4	1	Taylor	Proprietary Information	Proprietary Information withheld in Final SE
4	4	4	Taylor	Proprietary Information	Proprietary Information withheld in Final SE
5	4	4-10	Taylor	Proprietary Information	Proprietary Information withheld in Final SE
6	5	12-18	Taylor	Proprietary Information	Proprietary Information withheld in Final SE
7	6	10-27	Taylor	Proprietary Information	Proprietary Information withheld in Final SE
8	6	1-23	Taylor	Proprietary Information	Proprietary Information withheld in Final SE
9	6-7	25-30	Taylor	Proprietary Information	Proprietary Information withheld in Final SE
10	7	(6)31-(7)1	Taylor	Proprietary Information	Proprietary Information withheld in Final SE
11	7	4-13	Taylor	Proprietary Information	Proprietary Information withheld in Final SE
12	8	17	Taylor	Proprietary Information	Proprietary Information withheld in Final SE
13	8	2-3	Taylor	Proprietary Information	Proprietary Information withheld in Final SE
14	8	6-9	Taylor	Proprietary Information	Proprietary Information withheld in Final SE
15	9	11-16	Taylor	Proprietary Information	Proprietary Information withheld in Final SE
16	9	1-22	Taylor	Proprietary Information	Proprietary Information withheld in Final SE
17	13	24-38	Moniri	Proprietary Information	Proprietary Information withheld in Final SE
18	14	1-3	Taylor	Proprietary Information	Proprietary Information withheld in Final SE

Comment No.	Page No.	Line	AREVA Reviewer	AREVA Comment	NRC Response
19	14	5-16	Taylor	Proprietary Information	Proprietary Information withheld in Final SE
20	15	1-9	Taylor	Proprietary Information	Proprietary Information withheld in Final SE
21	15	31-42	Moniri	Proprietary Information	Proprietary Information withheld in Final SE
22	16	39-48	Moniri	Proprietary Information	Proprietary Information withheld in Final SE
23	17	1-4	Moniri	Proprietary Information	Proprietary Information withheld in Final SE
24	18	13-18	Moniri	Proprietary Information	Proprietary Information withheld in Final SE
25	19	37-40	Moniri	Proprietary Information	Proprietary Information withheld in Final SE
26	21	6-27	Taylor	Proprietary Information	Proprietary Information withheld in Final SE
27	24	13-19	Moniri	Proprietary Information	Proprietary Information withheld in Final SE
28	24	32-38	Taylor	Proprietary Information	Proprietary Information withheld in Final SE
29	25	20-21	Taylor	Proprietary Information	Proprietary Information withheld in Final SE
30	25	44-47	Moniri	Proprietary Information	Proprietary Information withheld in Final SE

SUMMARY TABLE OF PROPOSED CHANGES TO AREVA TR DRAFT SE, COMMENTS

Comment No.	Page No.	Line No.	AREVA Reviewer	AREVA Comment	NRC Comment
1	1	13	Taylor	The date of June 11, 2009, does not match the date in Reference 1, of June 6, 2009. Please clarify.	Reference date changed.
2	1	13	Taylor	The title of Reference 1, in quotes, should match the title of Reference 1 on Page 26 of the SE.	Title changed.
3	1	18	Taylor	The title of Reference 2, in quotes should match the title of Reference 2, on Page 26, of the SE.	Title changed.
4	1	21	Taylor	The title of Reference 3, in quotes should match the title of Reference 3, on Page 26, of the SE.	Title changed.
5	3	6	Taylor	Line should state: "developed by AREVA NP for the....".	AREVA NP, Inc. designated as AREVA throughout SE.
6	3	19	Taylor	Consistency should be used for the name of the Topical Report, use SIVAT Topical Report or SIVAT TR and add (Reference 11) to the sentence. This is throughout the document.	Reference noted. Consistency verified.
7	3	28	Taylor	Revise line to state: "Thus, the NRC Staff..."	Comment incorporated.
8	3	34	Taylor	Revise line to state: [ ]	Comment incorporated.
9	3	36	Taylor	Revise like Comment 8.	Comment incorporated.

SUMMARY TABLE OF PROPOSED CHANGES TO AREVA TR DRAFT SE, COMMENTS

10	4	6	Taylor	Revise line to state: [ ]	Comment incorporated.
11	4	13	Taylor	Revise line to state: [ ]	Editorial comment not incorporated at the discretion of the technical reviewer.
12	4	18-19	Taylor	[ ]	Comment incorporated.
13	4	20	Taylor	Revise Section 3.1.2 title to state: "Verify Safety System Application Software".	Comment incorporated.
14	4	22	Taylor	Consider using a standard term for safety system software like "Application Software". This is throughout the document.	Consistency verified.
15	4	23	Taylor	Revise line to state: "simulated function ~~block~~ diagram...".	Comment incorporated.
16	4	24	Taylor	Revise line to state: "The verification of Application Software is complete...".	Editorial comment not incorporated at the discretion of the technical reviewer.
17	4	25	Taylor	Revise line to state: "~~an application~~ safety system can be...".	Editorial comment modified at the discretion of the technical reviewer.
18	4	27	Taylor	Revise line to state: "Verification of Application Software establishes reasonable assurance that the Application Software is...".	Editorial comment modified at the discretion of the technical reviewer.

19	5	1	Taylor	Revise Section 3.1.3 title to state: "...Validate Safety System Application Software".	Comment incorporated.
20	5	3-5	Taylor	Section 3.1.3 also should 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."	Comment not incorporated at the discretion of the technical reviewer.
21	5	11	Taylor	Revise line to state: "(Oconee RPS/ESPS System Function FU0007)".	Comment incorporated.
22	5	13-14	Taylor	Revise line to state: [ ] This is according to the LAR submittal, (Reference 12).	Editorial comment modified at the discretion of the technical reviewer.
23	5	13-17	Taylor	A discussion should be added to explain that this information is representative of typical SIVAT documentation and that the documentation format may vary from project to project, however the critical attributes will be present in the documentation, (i.e., expected results may be represented differently).	Comment incorporated.

24	5	18-19	Taylor	Table 3-1, identifies the Oconee Factory Acceptance Plan. This should be Reference 16, the Simulation Test Plan.	Comment incorporated.
25	5	25	Taylor	[ ]	Comment incorporated.
26	6	23	Taylor	Revise Title of Figure 3-2, to state: "RCS High Outlet Temperature Trip Simplified Function ~~Block~~ Diagram".	Comment incorporated.
27	6	29	Taylor	Revise line to state: [ ]	Editorial comment modified at the discretion of the technical reviewer.
28	7	2	Taylor	Revise Title of Table 3-2, to state: "Test Parameters and Expected Values ~~Table~~".	Comment incorporated.
29	7	8	Taylor	Revise line to state: [ ]	Editorial comment not incorporated at the discretion of the technical reviewer.
30	7	9	Taylor	Revise line to state: [ ]	Editorial comment not incorporated at the discretion of the technical reviewer.

31	7	9	Taylor	Revise line to state: [ ]	Editorial comment not incorporated at the discretion of the technical reviewer.
32	7	11	Taylor	Upon completion of the test case, the test data file is plotted graphically and analyzed. The test data file is also opened to verify that the bistable changed state. Consider specifying the plotting of data.	Comment not incorporated at the discretion of the technical reviewer.
33	7	12-13	Taylor	Revise line to state: [ ]	Editorial comment modified at the discretion of the technical reviewer.
34	7	17	Taylor	Revise Title of Figure 3-3, to state: [ ]	Comment incorporated.
35	8	1	Taylor	Revise line to state: "The test results for the test case example are…".	Editorial comment not incorporated at the discretion of the technical reviewer.
36	8	1	Taylor	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.	Comment not incorporated at the discretion of the technical reviewer.
37	8	4	Taylor	Revise Title of Table 3-3, to state: "SIVAT Oconee RPS/ESPS FU0007 Test Results Data File".	Comment incorporated.

38	8	15	Taylor	Revise line to state: [ ]	Editorial comment not incorporated at the discretion of the technical reviewer.
39	9	22	Taylor	Revise Example 3-1, to Figure 3-4.	Editorial comment not incorporated at the discretion of the technical reviewer.
40	9	35	Taylor	Revise line to state: [ ]	Editorial comment not incorporated at the discretion of the technical reviewer.
41	9	42	Taylor	Consistency should be used for the name of the SIVAT software tool. A recommendation is, "SIVAT tool".	Consistency verified.
42	9	42-43	Taylor	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 Topical Report states.	Comment incorporated.
43	10	20	Taylor	Revise line to state: "...management of the SIVAT ~~V&V~~ tool...".	Comment incorporated.

44	10	26	Taylor	Revise line to state: "...was developed under the same QA program and...".	Editorial comment not incorporated at the discretion of the technical reviewer.
45	10	27-28	Taylor	Revise line to state: "...TXS system software in the TXS platform reference ~~safety evaluation report~~ SE ..."	Comment incorporated.
46	10	43	Taylor	Revise line to state: "discrepancies with the development of the SIVAT ~~program~~ tool".	Editorial comment modified at the discretion of the technical reviewer.
47	10	46	Taylor	Revise line to state: "portion of the SIVAT ~~simulator~~ tool was produced during the development process ~~of this application~~.".	Editorial comment modified at the discretion of the technical reviewer.
48	10	47	Taylor	Revise line to state: "Therefore, those functions that are performed by this ~~application~~ GUI could not...".	Comment incorporated.
49	11	1	Taylor	Revise line to state: "This ~~application~~ GUI performs...".	Comment incorporated.
50	11	4-5	Taylor	Revise line to state: "...invokes are performed by the GUI ~~application~~ without readily available...".	Comment incorporated.
51	11	12	Taylor	Revise line to state: "...TXS safety-related application software..." .	Editorial comment modified at the discretion of the technical reviewer.
52	11	14	Taylor	Revise line to state: "...associated with the SIVAT ~~simulation~~ tool.".	Comment incorporated.

53	11	27	Taylor	Revise line to state: "...development of the SIVAT ~~V&V~~ tool is...".	Comment incorporated.
54	11	28	Taylor	Consistency should be used for the name of the SIVAT Topical Report.	Consistency verified.
55	11	34-35	Taylor	Consistency should be used for the name of the SIVAT Topical Report.	Consistency verified.
56	12	15	Taylor	Consistency should be used for the name of the SIVAT Topical Report.	Consistency verified.
57	12	33	Taylor	Consistency should be used for the name of the SIVAT Topical Report.	Consistency verified.
58	13	18-19	Taylor	Consistency should be used for the name of the SIVAT Topical Report.	Consistency verified.
59	13	26	Taylor	Revise line to state: "...TXS safety-related ~~plant~~ application software..." .	Editorial comment modified at the discretion of the technical reviewer.
60	13	30	Taylor	If comments 37 and 38 are accepted, change Figure 3-4, to Figure 3-5.	Editorial comment not incorporated at the discretion of the technical reviewer.
61	13	31	Taylor	Revise line to state: [———]	Comment incorporated.
62	14	3	Taylor	If comments 38 and 39 are accepted, change Figure 3-4 to Figure 3-5.	Editorial comment not incorporated at the discretion of the technical reviewer.

63	14	8	Taylor	Revise line to state: [ ]	Comment incorporated.
64	14	15-16	Taylor	Revise line to state: [ ]	Editorial comment not incorporated at the discretion of the technical reviewer.
65	15	1-9	Taylor	Should these objectives mirror the objectives within Section 3.3 of the SIVAT Topical Report?	Editorial comment not incorporated at the discretion of the technical reviewer.
66	15	32	Taylor	Revise line to state: [ ]	Editorial comment not incorporated at the discretion of the technical reviewer.
67	15	32-33	Taylor	Consistency should be used for the name of the SIVAT Topical Report.	Consistency verified.
68	15	39-40	Taylor	Revise line to state: [ ]	Editorial comment modified at the discretion of the technical reviewer.
69	16	4	Taylor	Revise line to state: "...maintenance of the SIVAT ~~V&V~~ tool is...".	Comment incorporated.
70	16	5-6	Taylor	Consistency should be used for the name of the SIVAT Topical Report.	Consistency verified.
71	16	9	Taylor	Remove second period from AREVA NP Inc..	Comment incorporated.

72	16	12	Taylor	Consistency should be used for the name of the SIVAT Topical Report.	Consistency verified.
73	16	14	Taylor	Consistency should be used for the name of the SIVAT Topical Report.	Consistency verified.
74	16	20	Taylor	Consistency should be used for the name of the SIVAT Topical Report.	Consistency verified.
75	16	21	Taylor	Revise line from SMaint P to SMaintP, delete extra space.	Comment incorporated.
76	16	32	Taylor	Revise line to state: "...SIVAT ~~software~~ Operations Plan used by AREVA NP ~~GmbH~~ Inc.to facilitate the operation...".	Editorial comment modified at the discretion of the technical reviewer.
77	16	33	Taylor	Revise line to state: "...Section 11.0 "SIVAT ~~Software~~ Operations Plan"	Editorial comment modified at the discretion of the technical reviewer.
78	16	34	Taylor	Consistency should be used for the name of the SIVAT Topical Report.	Consistency verified.
79	16	36	Taylor	Revise line to state: "SIVAT Operations Plan ~~SOP~~ ...".	Comment incorporated.

80	16	40-41	Taylor	Revise line to state: "…for full qualification of a safety-related application software. Those aspects of a ~~safety~~ application software which cannot be…".	Editorial comment not incorporated at the discretion of the technical reviewer.
81	17	1-4	Taylor	Revise line to state: [——————————] Also, a discussion of how the V&V engineers compare the testing results to the software requirements would be beneficial prior to a discussion of requirement traceability.	Editorial comment not incorporated at the discretion of the technical reviewer.
82	17	7	Taylor	Revise line to state: "of the SIVAT Operations Plan ~~SOP~~…".	Comment incorporated.
83	17	11	Taylor	Revise line to state: "…that the SIVAT ~~Software~~ Operations Plan as defined…"	Editorial comment not incorporated at the discretion of the technical reviewer.
84	17	11	Taylor	Consistency should be used for the name of the SIVAT Topical Report.	Consistency verified.
85	17	13	Taylor	Revise line to state: "the SIVAT Operations Plan ~~SOP~~ …".	Comment incorporated.
86	17	30	Taylor	Revise line to state: "…SIVAT ~~software~~ Training Plan used by AREVA NP ~~GmbH~~ Inc.to facilitate training…".	Comment incorporated.

87	17	31-32	Taylor	Consistency should be used for the name of the SIVAT Topical Report.	Consistency verified.
88	18	5	Taylor	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 Topical Report states.	Comment not incorporated at the discretion of the technical reviewer.
89	18	5-6	Taylor	Revise line to state: "...SIVAT ~~V&V~~ tool is contained in ...".	Comment incorporated.
90	18	13	Taylor	Revise line to state [ ]	Editorial comment modified at the discretion of the technical reviewer.
91	18	16	Taylor	Revise line to state: [ ]	Editorial comment not incorporated at the discretion of the technical reviewer.
92	18	20	Taylor	Consistency should be used for the name of the SIVAT Topical Report.	Consistency verified.
93	18	22	Taylor	Revise line to state: "...TXS ~~safety~~ application software..." .	Editorial comment not incorporated at the discretion of the technical reviewer.
94	18	26	Taylor	Consistency should be used for the name of the SIVAT Topical Report.	Consistency verified.

95	18	47-48	Taylor	Consistency should be used for the name of the SIVAT Topical Report.	Consistency verified.
96	18	48	Taylor	Revise line to state: "...used by AREVA NP GmbH to ensure...".	Editorial comment not incorporated at the discretion of the technical reviewer.
97	19	3	Taylor	Revise line to state: "...NRC staff in the TXS platform reference ~~SER~~..."	Editorial comment modified at the discretion of the technical reviewer.
98	19	26	Taylor	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 Topical Report states.	Comment not incorporated at the discretion of the technical reviewer.
99	19	27	Taylor	Revise line to state: "...SIVAT V&V tool is contained in Section 15.0, "SIVAT ~~Software~~ Configuration Management Plan ...".	Comment incorporated.
100	19	39-40	Taylor	Revise line to state: [———]	Comment incorporated.
101	19	44	Taylor	Revise line to state: "...the AREVA NP GmbH software configuration management...".	Comment incorporated.
102	20	10	Taylor	Revise Section 3.2.12 title to state: "SIVAT ~~Software~~ Test Plan".	Comment incorporated.

103	20	21-22	Taylor	Revise line to state: "...utilize the SIVAT ~~V&V~~ tool is contained in Section 16.0, "SIVAT ~~Software~~ Test Plan," of the...".	Editorial comment not incorporated at the discretion of the technical reviewer.
104	20	22-23	Taylor	Consistency should be used for the name of the SIVAT Topical Report.	Consistency verified.
105	20	36	Taylor	Specify which TR describes the ERBUS, SIVAT or TXS platform reference SE?	Comment incorporated.
106	20	49	Taylor	Specify which TR provides Figure 3-13, SIVAT or TXS platform reference SE?	Comment incorporated.
107	21	27	Taylor	Specify section 3.6 of which TR, SIVAT or TXS platform reference SE?	Comment incorporated.
108	21	38	Taylor	Revise line to state: "...in this standard to be relevant to the SIVAT ~~application~~ Tool".	Editorial comment modified at the discretion of the technical reviewer.
109	21	43-44	Taylor	Revise line to state: "The SIVAT ~~application~~ Tool is therefore designated as a non-safety-related ~~application~~ tool.".	Editorial comment modified at the discretion of the technical reviewer.
110	22	7	Taylor	Revise line to state: "...that TXS ~~safety~~ application software ~~do~~ performs..." .	Editorial comment modified at the discretion of the technical reviewer.

111	22	9	Taylor	Revise line to state: "... the SIVAT ~~validation~~ Tool does provide ...".	Editorial comment modified at the discretion of the technical reviewer.
112	22	28	Taylor	Revise line to state: "The SIVAT ~~system~~ Tool is not required...".	Editorial comment modified at the discretion of the technical reviewer.
113	22	45	Taylor	Revise line to state: "The SIVAT ~~simulator~~ software package to be a software tool...".	Editorial comment modified at the discretion of the technical reviewer.
114	23	21	Taylor	Revise line to state: "Though the SIVAT ~~program~~ Tool is not a safety-related ~~program~~ software package...".	Editorial comment modified at the discretion of the technical reviewer.
115	23	22	Taylor	Revise line to state: "...TXS safety-related application software..." .	Comment incorporated.
116	23	42	Kohli	Revise sentence to read: " ...Standard Review Plan (SRP) ..."	Comment incorporated.

117	24	1	Kohli	Revise sentence to read: "... software requirements specification, software design description (SDD)..."	Editorial comment modified at the discretion of the technical reviewer.
118	24	4-8	Kohli	Revise sentence to read: "... 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.	Editorial comment modified at the discretion of the technical reviewer.
119	24	10	Kohli	Revise sentence to: " Software Requirements Traceability ..."	Editorial comment modified at the discretion of the technical reviewer.
120	24	16	Kohli	Revise sentence to: [ ]	Editorial comment not incorporated at the discretion of the technical reviewer.
121	24	45	Taylor	Revise line to state: "...AREVA NP does have the...".	Editorial comment not incorporated at the discretion of the technical reviewer.
122	24	46	Taylor	Revise line to state: "program to affect supplementary...".	Comment incorporated.

123	25	12	Taylor	Revise line to state: "...TXS safety-related application software..." .	Comment incorporated.
124	25	21	Taylor	Revise line to state: [ ]	Editorial comment not incorporated at the discretion of the technical reviewer.
125	25	43	Taylor	Specify section 11.2 of which TR, SIVAT or TXS platform reference SE???	Comment incorporated.
126	25	46	Taylor	Revise line to state: [ ]	Comment incorporated.
127	26	34	Taylor	Revise line to state: "6. AREVA NP document, 62-9014734-002 , Oconee Nuclear Station, Unit 1 RPS/ESFAS Controls Upgrade Application Software Function Module Test Specification".	Editorial comment modified at the discretion of the technical reviewer.
128	26	36	Taylor	Revise line to state: "7. AREVA NP document, 63-9014738-003, Oconee Nuclear Station, Unit 1 RPS/ESFAS Controls Upgrade Application Software Functions Test Procedure".	Editorial comment modified at the discretion of the technical reviewer.
129	26	38	Taylor	Revise line to state: "8. AREVA NP document, 51-9027244-002, Oconee Nuclear Station, ~~SIVAT~~ Unit 1 RPS/ESFAS Controls Upgrade Application Software Test Report..." .	Editorial comment modified at the discretion of the technical reviewer.
130	26	39	Taylor	Revise line to state: "9. AREVA NP document, 51-9027208-001, Oconee Nuclear Station, ~~SIVAT~~ Unit 1 RPS/ESFAS Controls Upgrade Software Unit Test Incident Report.	Editorial comment modified at the discretion of the technical reviewer.

131	26	40	Taylor	The FAT Plan Reference in Table 3-1, was removed in Comment 24. Remove Reference.	Editorial comment not incorporated at the discretion of the technical reviewer.
132	26	42	Taylor	For consistency, change AREVA NP. Inc., to AREVA NP document, or vice versa.	Consistency verified.
133	27	8	Taylor	Reference 14, is the SIVAT Manual from AREVA NP GmbH. AREVA NP Inc. also has a document number for this document. This is a generic licensing question of how the documents were transmitted to the NRC. If it was an AREVA NP Inc. document, please correct the reference information.	Editorial comment not incorporated at the discretion of the technical reviewer.
134	27	12	Taylor	Revise line to state: "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.	Editorial comment modified at the discretion of the technical reviewer.

AREVA

October 26, 2010
NRC:10:098

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

Request for Review and Approval of ANP-10303P, "SIVAT: TELEPERM XS™ Simulation Validation Test Tool Topical Report"

Ref. 1: Letter, Ronnie L. Gardner (AREVA NP Inc.) to Document Control Desk (NRC), "Request for Review and Approval of ANP-10303P, SIVAT: TELEPERM XS™ Simulation Validation Test Tool Topical Report," NRC:09:063, June 11, 2009.

Ref. 2: Letter, Stacey L. Rosenberg (NRC) to Ronnie L. Gardner (AREVA NP Inc.), "Acceptance for Review of AREVA NP, INC. SIVAT: TELEPERM XS™ Simulation Validation Test Tool Topical Report (TAC NO. ME1503)," December 28, 2009.

Ref. 3: Letter, Ronnie L. Gardner (AREVA NP Inc.) to Document Control Desk (NRC), "Review of ANP-10303PI SIVAT: TELEPERM XS™ Simulation Validation Test Tool Topical Report (TAC NO. ME1503)," NRC:10:001, January 4, 2010.

Ref. 4: Letter, Ronnie L. Gardner (AREVA NP Inc.) to Document Control Desk (NRC), "Response to Request for Additional Information Regarding ANP-10303, 'SIVAT: TELEPERM XS™ Simulation Validation Test Tool Topical Report' (TAC No. ME1503)," NRC:10:041, May 5, 2010.

Ref. 5: Letter, Ronnie L. Gardner (AREVA NP Inc.) to Document Control Desk (NRC), "Review of ANP-10303P, SIVAT: TELEPERM XS™ Simulation Validation Test Tool Topical Report (TAC NO. ME1503)," NRC:10:057, June 17, 2010.

Ref. 6: Letter, Ronnie L. Gardner (AREVA NP Inc.) to Document Control Desk (NRC), "Review of ANP-10303P, SIVAT: TELEPERM XS™ Simulation Validation Test Tool Topical Report (TAC NO. ME1503)," NRC:10:067, July 20, 2010.

Ref. 7: Letter, Ronnie L. Gardner (AREVA NP Inc.) to Document Control Desk (NRC), "Request for Review and Approval of ANP-10303P, Revision 1, "SIVAT: TELEPERM XS™ Simulation Validation Test Tool Topical Report," NRC:10:076, September 1, 2010.

AREVA NP Inc. (AREVA NP) requested the NRC's review and approval of AREVA NP ANP-10303P, Revision 1, "SIVAT: TELEPERM XS™ Simulation Validation Test Tool Topical Report in Reference 7. The review history for ANP-10303P is identified in References 1 through 6.

The NRC conducted an audit in Alpharetta, GA. The audit was performed to provide additional support for the safety evaluation for ANP-10303P. One of the objectives of the audit was an evaluation of the software test methodology described in the SIVAT Topical Report. The NRC reviewed the following documents as part of that audit objective:

- Document 51-9027244-002 Oconee Nuclear Station, Unit 1 RPS/ESFAS Controls Upgrade Application Software Test Report
- Document 51-9027208-001 Oconee Nuclear Station, Unit 1 RPS/ESFAS Controls Upgrade Application Software Test Incident Report

In an October 19, 2010 e-mail request, NRC (Holly Cruz) requested that these two documents be submitted on the docket in support of the NRC review.

The requested information is provided as enclosures to this letter. The information in the documents is illustrative of the AREVA NP test documentation that is produced for software testing performed with the SIVAT Test Tool. The information is not intended to represent any design or licensing information regarding the Oconee Nuclear Plant. AREVA NP considers the material contained in the topical report to be proprietary. As required by 10 CFR 2.390(b), an affidavit is enclosed lo support the withholding of the information from public disclosure. Nonproprietary versions of these documents are not provided based on the guidance in Information Notice 2009-07. Proprietary versions of the requested documents are enclosed.

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

Sincerely,

Ronnie L. Gardner

Ronnie L. Gardner, Manager
Corporate Regulatory Affairs
AREVA NP Inc.

Enclosures

cc: H. D. Cruz
R. Subbaratnam
Project 728

UNITED STATES
NUCLEAR REGULATORY COMMISSION
WASHINGTON, D.C. 20555-0001

October 18, 2010

Mr. Ronnie L. Gardner, Manager
Corporate Regulatory Affairs
AREVA NP Inc.
3315 Old Forest Road
P.O. Box 10395
Lynchburg, VA 24506-0935

SUBJECT: REQUEST FOR ADDITIONAL INFORMATION RE: AREVA NP, INC TOPICAL REPORT (TR) ANP-10303P, REVISION 0, "SIVAT: TELEPERM XS ™ SIMULATION VALIDATION TEST TOOL" (TAC NO. ME1503)

Dear Mr. Gardner:

By letter dated June 11, 2009 (Agencywide Documents Access and Management System Accession No. ML091680619), AREVA submitted for U.S. Nuclear Regulatory Commission (NRC) staff review TR ANP-10303P, Revision 0, "SIVAT: TELEPERM XS ™ Simulation Validation Test Tool Topical Report." Upon review of the information provided, the NRC staff has determined that additional information is needed to complete the review. On May 10, 2010, Alan Meginnis, AREVA Product Licensing Manager, and I agreed that the NRC staff would receive your response to the enclosed Request for Additional Information (RAI) questions within 30 days of the issuance of this letter. In addition, AREVA requested the opportunity to review the RAI questions for proprietary information, prior to public release. We will delay placing the RAI questions in the public document room for a period of 10 working days from the date of this letter to provide you with the opportunity to comment on the proprietary aspects. If you believe that any information in the enclosure is proprietary, please identify such information line-by-line and define the basis pursuant to the criteria of Section 2.390 of Title 10 of the *Code of Federal Regulations* (10 CFR). After 10 working days, the RAI questions will be made publicly available. If you have any questions regarding the enclosed RAI questions, please contact me at 301-415-1053.

Sincerely,

Holly Cruz, Project Manager
Licensing Processes Branch
Division of Policy and Rulemaking
Office of Nuclear Reactor Regulation

Project No. 728

Enclosure:
As stated

REQUEST FOR ADDITIONAL INFORMATION

LICENSE TOPICAL REPORT FOR SIVAT SIMULATION VERIFICATION AND VALIDATION TOOL

TAC Number ME1503

Instrumentation and Controls Branch

1. In Section 3.0 of the topical report (TR), the statement is made that "... the I&C functionality represented in the TXS [(TELEPERM XS)] Application Software can be *completely verified* with SIVAT [(Simulation Validation Test Tool)]." However, Section 3.6 of the TR lists a series of limitations of the simulation, several of which could impact the ability of the tool to verify the I&C functionality of a TXS application. Please define what is meant by this statement and explain how the limitations of simulation listed in Section 3.6 do not invalidate this statement.

2. In Section 3.2 of the TR, the Specification and Coding Environment (SPACE) code generator is described as being *qualified.* Please explain what is meant by this. Though the SPACE tool was described in the reference TXS topical report as well as the safety evaluation performed by the NRC, there is no mention of a qualification level achieved by these efforts.

   The TXS SE concluded that "...SPACE (specification and coding environment) tool for designing and assembling safety-related applications has the capability and safeguards to ensure that the implementation of the application programs can be successfully accomplished on a plant-specific basis."

   The staff understands that the SPACE tool has not been qualified as being Safety Related nor was it developed to the equivalent standards necessary for Software Integrity Level (SIL) 4 software. Please confirm that the qualification level stated in this TR is consistent with the conclusions made in the referenced TXS safety evaluation.

3. In Section 3.3 of the TR "Objectives for the SIVAT tool", the first listed objective makes reference to "... the original TELEPERM XS Application Software C code ..." and states that this same code is used for the SIVAT tool. It is evident that the SIVAT application is very different from the TXS application Software code as the objectives for each have little in common. How is it possible that the same code can be used to accomplish the objectives for the TXS application and the SIVAT tool programs?

4. In Section 3.3 of the TR "Objectives for the SIVAT tool", the second feature of the SIVAT tool listed states that "No *functional modifications* of the TELEPERM XS Application Software C code" are made. However, the staff understands that some changes are made to the application code prior to it being executed within the simulator. Section 16.1 describes the changes made to the TXS code as; "The code is slightly adapted in order to use the centrally managed memory of the simulator instead of the memory of the online systems." Please clarify what is meant by a *functional modification* within this context and explain why the changes that are made to the application code are not considered to be *functional modifications.*

ENCLOSURE

5. In Section 3.4 "TELEPERM XS Simulation Methodology, the second paragraph states that "... the Model provides an exact representation of the Original Application Software." Because non-functional modifications are being made to the application software code prior to it being executed within the simulator, this statement appears to be inconsistent. The following paragraphs' statement that this code is adapted accordingly also seems to conflict with this exact representation statement. This statement appears to be contradictory. Please provide clarification of this statement and justification for this claim.

6. The third paragraph of Section 3.5 "Simulation of communication" states that the MicroNET network system, which is relied upon by the TXS for communication of messages between processors by the runtime environment, is hardware based and is not simulated. The section also goes on to explain that message transfer functions are *implemented in a simplified manner.* This appears to be a significant limitation of the simulation environment because TXS applications are heavily reliant on communications between the various modules of the system yet there is no mention of this in Section 3.6 "Limitations of Simulation." Please explain why AREVA does not consider the simplified manner in which system communications are being implemented within the simulator to be a Limitation of Simulation.

7. Section 3.3.5 "TELEPERM XS Malfunctions" lists three types of functions used to simulate malfunctions. These three malfunction types do not appear to be capable of simulating all failures that can occur to a TXS system. Malfunctions such as the following are not described:

   a. Memory errors,
   b. Specific communication link faults,
   c. Signal faults,
   d. Power Degradation,
   e. Faults associated with specific Function Block or a Function Block, and
   f. Partial failure or degraded operation of a TXS central processing Unit (CPU).

   Please explain how TXS malfunctions that are not within the three types described in this section would be accounted for.

8. The description of the three types of functions used to simulate malfunctions listed in Section 3.5.5 does not explain how these failures are to be applied to an application under simulation.

   For example, what message would the "failure of a message" function be applied to? Can this function be applied to all, some, or just one specific message within the application? Can specific input or output (I/O) modules or selected signals within an I/O module be selected for the "failure of an I/O module" functions or would the function being switched on just fail all of the systems I/O modules?

   Please provide a more detailed description of these functions to help the staff to understand exactly what system malfunctions can be tested during simulation and to identify what additional malfunction types would need to be tested when the application is loaded onto TXS hardware.

9. In Section 3.5.5, the symptoms of a failed CPU are described and activation of the Failure of a complete "TELEPERM XS CPU" function would simulate these symptoms. This implies that there is only one mode of failure for the TXS CPU. If this is not the case, then would it also be possible to simulate the symptoms for CPU failure modes other than the one described in this section?

   Please provide additional information on the postulated failure modes for a TXS CPU and explain how simulation tests performed using SIVAT would provide an adequate means of ensuring that the safety system would be able to complete the required safety functions in the event of such a failure. If SIVAT testing cannot be used to test this level of system functionality, then this additional Limit of Simulation should be included in Section 3.6 of the TR.

10. Section 3.5.7 of the TR describes the Test Principals used for implementing SIVAT tests and it provides an example of how test cases would be formulated and run on an application using the SIVAT tool. The section does not, however, discuss the methods or processes that would be used to generate these test cases. Please provide a description of exactly how the test specification is developed and explain the criteria that would be used to develop test cases, which are to be run on SIVAT. Also, explain what criteria would be used to determine which test cases could be run on SIVAT verses test cases that would need to be run on TXS hardware due to the limitations of simulation described in Section 3.6.

11. Since the TELEPERM XS analysis tool, "cpuload," referenced in Section 3.6 has not been evaluated or approved for use as a qualified Verification & Validation (V&V) tool by the NRC, it cannot be used as a sole means of ensuring that CPU load requirements are met. Therefore, test field verification should be a required activity for all applications developed using the TXS platform. Please explain how the requirements for CPU Load testing will be met for TXS applications.

12. The CPU restart Limit of Simulation is described in Section 3.6 as having been performed as part of the TELEPERM XS generic qualification process. Since this process was completed for the TXS platform, the test results should be available. Please provide a description of these tests and a summary of the test results. (Optionally, the NRC staff could review these records during a future audit.)

13. Section 3.7 of the TR describes Simulation in the Test Field using ERBUS[1]. ERBUS testing is described as testing that is performed following the manufacture of the cabinet in the test field. Figure 3-13 also illustrates ERBUS testing as testing that is performed independently from the use of Validation by SIVAT. Please explain the relevance of ERBUS in relation to the Validation Testing activities associated with SIVAT. This section appears to be informative in nature and not necessarily relevant to the qualification of SIVAT as a Verification and Validation (V&V) tool.

14. In the last paragraph of Section 3.7.3, a limitation to ERBUS Test field simulation is described and a conclusion that "...no response time measurements can be done using

---

[1] The name of a computer-assisted test system for TELEPERM XS test field application (test field simulator).

this system" is made yet no other field test program is mentioned in the TR. Since response time testing is listed as a limitation for both the SIVAT simulation and the ERBUS field test simulator, please explain how time response testing will then be accomplished for a TXS application.

15. In regard to SIVAT compliance to BTP 7-14 in Section 4.11 of the TR, the statement: "system characteristics not tested by SIVAT are either tested during the TXS generic qualification testing process, verified with other TXS analysis tools, or *validated during system validation testing...*"presents a circular argument since the SIVAT tool itself is being used to support TXS software validation. Please explain how characteristics which are not tested by SIVAT such as those listed in Section 3.6 will be subsequently tested during system validation testing when SIVAT itself is being used to perform system validation testing.

16. In Section 5.4 "Problem Reporting" of the SDP, the first paragraph describes the scope of problem reporting as "... discrepancies regarding the use of the TELEPERM XS SIVAT tool for validation testing of Application Software developed by AREVA NP for use in safety-related I&C applications deployed in the U.S.". It is un-clear to the staff as to whether this scope applies to problems associated with the SIVAT tool, problems associated with TXS application software, or problems associated with both types of application. Please explain the intended scope for Problem Reporting within the context of the SIVAT SDP Section 5 of the TR. Include a description of how errors associated with the SIVAT tool will be identified, processed, and resolved.

17. Section 7.1 "SIVAT Quality Assurance Plan" states "SIVAT was developed under the same QA program and software lifecycle development process as described in the TELEPERM XS Topical Report." That topical report evaluated the procedures FAW 3.4, 3.5, and 3.6 and sited these procedures as basis for its safety conclusion. Please explain why it is acceptable to credit the Lifecycle development process described in the TXS topical report when the FAW 3.6 procedure that was used as a basis for the safety evaluation was determined to be *not applicable to the development of SIVAT Software* in Section 6.1.2 of the SIVAT TR. Please also explain why the procedures FAW 3.4 and 3.5 are not referenced in the SIVAT TR and describe how the processes covered by these procedures are being otherwise performed in an acceptable manner for SIVAT.

18. In Section 11.1 "Application Software Testing with SIVAT", the last paragraph on page 11-3 states that "the goal of the project-specific simulation testing with SIVAT is to verify the correct implementation of *all the functions and requirements* specified in the SRS." It is apparent to the staff that some of the requirements that would be specified in an SRS would not be testable by SIVAT (e.g. time response functional requirements) due to the limitations of simulation listed in Section 3.6 of the TR. Please explain the meaning of this statement in relation to the intended use of the SIVAT tool considering the limitations of the tool.

19. The opening paragraph of Section 11.0 of the TR states that the limitations of simulation are discussed in the SIVAT Operations Plan; however, Section 11.2 "Limitations of Simulation" is a restatement of the list of limitations provided in Section 3.2, which includes only slight re-wording. Please provide a detailed discussion of the Limitations

of Simulation including an explanation of how and when each of these limitations will be tested through other means that are not reliant on the SIVAT tool.

20. Section 13.2 of the TR describes a behavioral difference that essentially renders Gateway processor functionality un-testable in SIVAT simulation. "Why is this Limitation of Simulation" not specifically listed in Section 3.6?

21. The SIVAT Configuration Management (CM) Plan Section 15.0 of the TR credits the CM process FAW-TXS-1.5 that was described in the TXS Topical report and evaluated by the NRC in 2000, however, Section 15.3 states that AREVA NP intends to use a different CM process. This section states that "... configuration management for SIVAT Tools used for U.S. TELEPERM XS projects will be controlled through the TELEPERM XS Application Software Configuration Management Plan described in Section 12 of the TELEPERM XS Software Program Manual." Please explain which of these Configuration Management Plans will in fact be used to maintain SIVAT configuration so that the staff can focus its evaluation on the appropriate process.

22. Figure 3-2 depicts a process labeled "Formal Verification" which apparently compares or verifies the generated C-Code against the Project Database. Two routines are referenced in this figure: "rediff" and "cmp_code." The definition of "rediff" in Section 2, however, states that "rediff" compares redundancies against each other and not code against the project database as is depicted in the figure. In addition, the definition of "cmp_code provided in Section 2 does not explain how this tool is used to perform "Formal Verification." Please provide additional information on the use of the software tools "rediff" and "cmp_code" and explain how and when these tools are used to perform "Formal Validation" of safety related application software.

AREVA

September 1, 2010
NRC:10:076

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

Request for Review and Approval of ANP-10303P, Revision 1, "SIVAT: TELEPERM XS™ Simulation Validation Test Tool Topical Report"

Ref. 1: Letter, Ronnie L. Gardner (AREVA NP Inc.) to Document Control Desk (NRC), "Request for Review and Approval of ANP-10303P, SIVAT: TELEPERM XS™ Simulation Validation Test Tool Topical Report," NRC:09:063, June 11, 2009.

Ref. 2: Letter, Stacey L. Rosenberg (NRC) to Ronnie L. Gardner (AREVA NP Inc.), "Acceptance for Review of AREVA NP, INC. SIVAT: TELEPERM XS™ Simulation Validation Test Tool Topical Report (TAC NO. ME1503)," December 28, 2009.

Ref. 3: Letter, Ronnie L. Gardner (AREVA NP Inc.) to Document Control Desk (NRC), "Review of ANP-10303PI SIVAT: TELEPERM XS™ Simulation Validation Test Tool Topical Report (TAC NO. ME1503)," NRC:10:001, January 4, 2010.

Ref. 4: Letter, Ronnie L. Gardner (AREVA NP Inc.) to Document Control Desk (NRC), "Response to Request for Additional Information Regarding ANP-10303, 'SIVAT: TELEPERM XS™ Simulation Validation Test Tool Topical Report' (TAC No. ME1503)," NRC:10:041, May 5, 2010.

Ref. 5: Letter, Ronnie L. Gardner (AREVA NP Inc.) to Document Control Desk (NRC), "Review of ANP-10303P, SIVAT: TELEPERM XSTM Simulation Validation Test Tool Topical Report (TAC NO. ME1503)," NRC:10:057, June 17, 2010.

Ref. 6: Letter, Ronnie L. Gardner (AREVA NP Inc.) to Document Control Desk (NRC), "Review of ANP-10303P, SIVAT: TELEPERM XSTM Simulation Validation Test Tool Topical Report (TAC NO. ME1503)," NRC:10:067, July 20, 2010.

AREVA NP Inc. (AREVA NP) requested the NRC's review and approval of ANP-10303P, Revision 0, "SIVAT: TELEPERM XS™ Simulation Validation Test Tool Topical Report, in Reference 1. The NRC documented its acceptance review of ANP-10303P in Reference 2.

The acceptance review letter also documented AREVA NP's commitment to provide translation of the relevant portion of the following SIVAT development documents made during a telephone conference call on October 22, 2009. The requested information was provided by AREVA in Reference 3.

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

AREVA NP and the NRC participated in a teleconference on March 17, 2010 to discuss a draft RAI. A formal version of the RAI was never issued. The AREVA NP response to the RAI discussed on the teleconference was provided in Reference 4. In that letter, AREVA NP noted that the RAI response identified areas where ANP-10303P would be clarified. AREVA NP also indicated that a draft revision of the topical report to incorporate the clarification had been prepared.

During the March 17, 2010 teleconference, the NRC discussed their intention to conduct an implementation audit to support the preparation of the safety evaluation for ANP-10303P. A draft copy of the audit plan was provided to AREVA NP by email on April 16, 2010; however, the audit plan was never formally issued by the NRC. During this teleconference, the NRC also requested an informal copy of the draft revision of the topical report to facilitate preparation for the audit. AREVA NP provided the requested information by e-mail on May 12, 2010.

The NRC conducted an audit in Alpharetta, GA on June 8-10, 2010. The audit was performed to provide additional support for the safety evaluation for ANP-10303P. No formal audit report has been issued by the NRC. AREVA NP provided the audit follow-up information requested by NRC is References 5 and 6.

In Reference 4 AREVA NP stated its intention to submit Revision 1 to the topical report after the implementation audit. This schedule allowed for the incorporation of any additional clarifications resulting from the audit. NRC requested no additional clarifications to the topical report resulting from the audit during the exit meeting or subsequent telephone discussions. The enclosure to this letter provides Revision 1 to ANP-10303P.

AREVA NP considers some of the material contained in the topical report 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 topical report are enclosed.

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

Sincerely,

Ronnie L. Gardner, Manager
Corporate Regulatory Affairs
AREVA NP Inc.

Enclosures

cc: H. D. Cruz
Project 728

AFFIDAVIT

COMMONWEALTH OF VIRGINIA)
) ss.
CITY OF LYNCHBURG)

1. My name is Mark J. Burzynski. I am Manager, Product Licensing, for AREVA NP Inc. 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 report ANP-10303P, Revision 1, "SIVAT: TELEPERM XS™ Simulation Validation Test Tool Topical Report" and referred to herein as the "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 this Document is considered proprietary for the reasons set forth in paragraphs 6(b), 6(c) and 6(d) above.

7. In accordance with AREVA NP's policies governing the protection and control of information, proprietary information contained in this Document has 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.

Mark J Burzynski

SUBSCRIBED before me on this 31st

day of August, 2010.

Sherry L. McFaden
NOTARY PUBLIC, COMMONWEALTH OF VIRGINIA
MY COMMISSION EXPIRES: 10/31/2010
Registration # 7079129

SHERRY L. MCFADEN
Notary Public
Commonwealth of Virginia
7079129
My Commission Expires Oct 31, 2010

AREVA

July 20, 2010
NRC:10:067

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

Review of ANP-10303P, "SIVAT: TELEPERM XS™ Simulation Validation Test Tool Topical Report," (TAC NO. ME1503)

Ref. 1: Letter, Ronnie L. Gardner (AREVA NP Inc.) to Document Control Desk (NRC), "Request for Review and Approval of ANP-10303P, SIVAT: TELEPERM XS™ Simulation Validation Test Tool Topical Report," NRC:09:063, June 11, 2009.

Ref. 2: Letter, Ronnie L. Gardner (AREVA NP Inc.) to Document Control Desk (NRC), "Review of ANP-10303P, SIVAT: TELEPERM XS™ Simulation Validation Test Tool Topical Report (TAC NO. ME1503)," NRC:10:001, January 4, 2010.

Ref. 3: Letter, Ronnie L. Gardner (AREVA NP Inc.) to Document Control Desk (NRC), "Review of ANP-10303P, SIVAT: TELEPERM XS™ Simulation Validation Test Tool Topical Report (TAC NO. ME1503)," NRC:10:057, June 17, 2010.

AREVA NP Inc. (AREVA NP) submitted ANP-10303P, Revision 0, "SIVAT: TELEPERM XS™ Simulation Validation Test Tool Topical Report," for review and approval in Reference 1. The NRC conducted an audit in Alpharetta, GA. The audit was performed to provide additional support for the safety evaluation for ANP-10303P. One of the objectives of the audit was an evaluation of the software development and configuration management control processes that were used for the SIVAT software development. The NRC also reviewed the following documents as part of that audit objective:

- Rahmenlastenheft: TXS-Simulator (KWU NLL4/98/042)
  (translated title: General requirements specification: TXS simulator)
- Lastenheft SIMM (KWU NLL4/98/068)
  (translated title: Requirements specification: SIMM)
- TXS-Pflichtenheft, Version 01.21: Generator CATS-SDE für die TXS-Simulationsumgebung (KWU NLLZ ST/99/023b)
  (translated title: TXS design specification, version 01.21: Generator CATS-SDE for the TXS simulation environment)
- Lastenheft: Simulation Development Environment (KWU NLL4/98/049)
  (translated title: Requirements Specification: Simulation Development Environment)

The NRC requested that additional portions of these documents be translated and added to AREVA NP document NLTC-G/2009/en/0069 A, "TELEPERM XS Simulation tools - translation of selected chapters from requirements and design specification documents from the initial

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

development," which was previously provided by Reference 2. AREVA NP committed to provide this information by July 23, 2010 in Reference 3.

The requested translations are provided in an enclosure to this letter in AREVA NP document NLTC-G/2009/en/0069 B, TELEPERM XS Simulation tools - translation of selected chapters from requirements and design specification documents from the initial development, dated July 9, 2010. A cross reference between the requirements traced in the audit and the translated documents is provided in a separate enclosure.

AREVA NP considers some of the material contained in AREVA NP document NLTC-G/2009/en/0069 B 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 document are enclosed.

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

Sincerely,

Alan B. Meginnis For

Ronnie L. Gardner, Manager
Corporate Regulatory Affairs
AREVA NP Inc.

Enclosures

cc: H. D. Cruz
R. Stattel
Project 728

AFFIDAVIT

STATE OF WASHINGTON)
) ss.
COUNTY OF BENTON)

1. My name is Alan B. Meginnis. I am Manager, Product Licensing, for AREVA NP Inc. 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 NLTC-G/2009/en/0069 B, TELEPERM XS Simulation tools - translation of selected chapters from requirements and design specification documents from the initial development, dated July 9, 2010 and referred to herein as the "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 this Document is considered proprietary for the reasons set forth in paragraphs 6(b), 6(c) and 6(d) above.

7. In accordance with AREVA NP's policies governing the protection and control of information, proprietary information contained in this Document has 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 on this 20th day of July, 2010.

Susan K. McCoy
NOTARY PUBLIC, STATE OF WASHINGTON
MY COMMISSION EXPIRES: 1/10/12

SUSAN K. MCCOY
COMMISSION EXPIRES
NOTARY
PUBLIC
01-10-12
STATE OF WASHINGTON

AREVA NP RESPONSE to REQUIREMENTS TRACING THREAD AUDIT

ANP-10303, "SIVAT: TELEPERM XS™ SIMULATION VALIDATION TEST TOOL

TOPICAL REPORT" (TAC NO. ME1503)

1. Code Generation related requirements (based on TELEPERM XS SIVAT-TXS Simulation Based Validation Tool User Manual Section 4, "Creating and Configuring the TXS Simulator")

   a. When the Code Generator is called from the Welcome mask, the systems hardware information is retrieved from the Space Project database.

      This requirement is implemented as part of the graphical user interface (GUI). The CATS-SDE tool passes the selected system hardware via command line options to the TXS code generators which check if that specified hardware is available to selections. The list of systems hardware in the GUI permits the user to specify the hardware without typing in these strings. In the event unavailable system hardware is selected, the TELEPERM XS code generators abort the code generation with an associated error message, which causes CATS-SDE to abort the SIVAT code generation/adaptation as well.

   b. The Working Directory path is assigned based upon the project and cannot be changed by the user.

      The CATS-SDE tool allows specifying the target directory of a SIVAT code generation via the option "-into <dir>". The GUI does not allow changing this path so that users store their simulators in a well defined path. This path is deduced from the directory structure for TELEPERM XS projects. The requirement about how and where the generated simulator should be stored is described in:

      - Rahmenlastenheft: TXS-Simulator (KWU NLL4/98/042)
        - A general note in section (second list item) about the places, where the projects data is stored on TELEPERM XS service unit or engineering server.
        - Figure 6 in Section 2.2.4 shows a directory structure in principle on how the generated files should be stored.

      - Lastenheft SIMM (KWU NLL4/98/068)
        - A reference to figure 6 of Rahmenlastenheft: TXS-Simulator in the last list item of Section 2.2.1, Item 1 "Selecting of Files".

      - TXS-Pflichtenheft, Version 01.21: Generator CATS-SDE für die TXS-Simulationsumgebung (KWU NLLZ ST/99/023b)
        - The Design description for CATS-SDE describes the option "-into" which allows the user to define the target directory for the generation of the SIVAT simulator in Section 2.2.1.4.1, Item 1 and the text after the list, including figure 7).

c. When the "Make Interface Model check box is selected, two models are created from the data in the interface file for signal conversion and are linked to the simulator.

   Two models are one for input signals and one for output signals. These models can be used for two tasks.

   i. Conversion from physical signal values to electrical signals values as done by the measuring or actuating periphery.

      Usually, analog input signals that hold electrical values used by the input boards are converted into physical units inside the function diagrams. So called MRC function blocks can be used for this conversion. They allow a linear conversion for analog signals. The following logic in the function diagram is implemented using these physical units.

      So when just simulating the TELEPERM XS CPUs the input signals would have to be set using electrical values. This might be inconvenient because the requirements for the TELEPERM XS application might be defined using physical units. So these models can be used to simulate the inverse conversion of signals that is done by the MRC function blocks.

      For the generation of these models, the user can choose to whether use the inverse conversion which is determined from the parameterization of the MRC blocks or the user can define such a conversion manually by specifying a gain and an offset for the linear conversion.

   ii. Connection to process models using the input and output signals of the TELEPERM XS system.

      This is done by assignments between the TELEPERM XS input/output signals and signals of the process models. This assignment has to be defined by the user.

   Documents:

   - Lastenheft SIMM (KWU NLL4/98/068)
     - Section 2.2.1, item 7 "Coupling of interface signals" describes the coupling of process models via input/output signals by using the interface models.

   - TXS-Pflichtenheft, Version 01.21: Generator CATS-SDE für die TXS-Simulationsumgebung (KWU NLLZ ST/99/023b)
     - Section 2.1.3, in the end of the section, states a generation requirement for a conversion from electrical to physical values and vice versa.
     - Section 2.2.1.8 describes the generation of the interface models in depth.

d. When the "No Voter" check box is selected, the effects of two voter subsystems in the event of a fault are suppressed.

This option allows disabling the separate simulation of a second voter subunit. This was introduced for performance reasons because simulating both voter subunits does not have a functional effect (since no malfunctions are assumed).

This is not a requirements requested in the requirements documents. It was analyzed and described in the design specification CATS-SDE.

- TXS-Pflichtenheft, Version 01.21: Generator CATS-SDE für die TXS-Simulationsumgebung (KWU NLLZ ST/99/023b)
  - Chapter 2.2.1.4.1, list item 10 describes the option –no_voter
  - Chapter 2.2.1.5.1, "Analyzing the runtime environment," third paragraph, describes the difference between voters and single CPUs and how signals and messages are handled by a voter. It also describes that (and why) variables have to be renamed if both voter subunits are simulated.

2. Simulation Related Requirements (based on TELEPERM XS SIVAT-TXS Simulation Based Validation Tool User Manual Section 5, "Simulation")

   Background

   The simulation control system SDE is a third party product that was developed by the company SimPower for the use on HP-UX workstations. Some documentation was provided by SimPower regarding the SDE tools DBE, DBB and SimEx and a user manual for the SDE product in the whole. When the TXS tools were ported to the Linux operating system the right on the SDE product was purchased by AREVA and the tool was ported to Linux. No functional changes were done to the product at that time. It was integrated into the TXS configuration management and change procedure. SDE provides the basic SCS functionalities for SIVAT, like processing the simulation models (run/stop), saving and restoring ICs (initial conditions), accessing (read/write) the simulation variables, and so on. SDE provides an interface to extend the basic user interface by providing a GUI and Tcl/Tk commands that are processed by the simulator shell. Actually, the GUI is also some script that is processed by the simulator shell. The GUI and some convenience functions were added by AREVA.

   Requirements for the SCS (SDE) are described in the document Lastenheft SDE (KWU NLL4/98/049). Most of the requirements were implemented by SimPower in the basic SDE tools. Some requirements were implemented by using the interface for extensions.

   a. When the "Go For" button is pressed on the user interface window, the simulation runs for the duration specified in the text entry box to the right of the button. When the time elapses, the simulator is set to the FREEZE state.

      This requirement is defined in Lastenheft SDE (KWU NLL4/98/049) Section 2.2.1.3, Item 2, list item 4. As stated right below the list, the command names are just suggestions that might be subject to changes, but the described functionality must be implemented.

   b. When the Save IC button is selected, the Save IC window opens which allows the operator to save the state of all values at a specific point in time to a file.

Initial Conditions (ICs) are saved by dumping the complete simulation memory (simulation database) into a file. The requirement is defined in Lastenheft SDE (KWU NLL4/98/049) Section 2.2.1.3, Item 2, list items 6 and 7.

c. The monitoring window contains an option to allow the operator to change the status or value of any variable being monitored.

The requirement to read and write any simulation variable is described in:

- Rahmenlastenheft: TXS-Simulator (KWU NLL4/98/042)
  - Section 2.2.1.2, end of the section, list item 2 and 3

- Lastenheft SDE (KWU NLL4/98/049)
  - Section 2.2.1, end of the section, first bullet item is described that this feature was developed in cooperation of SimPower and AREVA.
  - The second bullet in the list describes, that is must be possible to read and write the simulation variables for supporting display functions.

d. During simulation, the values of all variables specified with plot are written to the file in the plot-open command.

The requirement is listed in:

- Rahmenlastenheft: TXS-Simulator (KWU NLL4/98/042)
  - Section 2.2.1.2, end of the section, list item 2

- Lastenheft SDE (KWU NLL4/98/049)
  - Section 2.2.1.3, item 3, list items 7, 8 and 9

Implementation was done by AREVA using the extension interface of SDE.

e. Command line requirement: Ramp function description. Process for ramping a signal.

The requirement is listed in:

- Rahmenlastenheft: TXS-Simulator (KWU NLL4/98/042)
  - Section 2.2.1.2, end of the section, list item 2

- Lastenheft SDE (KWU NLL4/98/049)
  - Section 2.2.1.3, item 3, list item 4

Implementation was done by AREVA using the extension interface of SDE.

May 05, 2010
NRC:10:041

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

Response to Request for Additional Information Regarding ANP-10303, "SIVAT: TELEPERM XS™ Simulation Validation Test Tool Topical Report" (TAC No. ME1503)

Ref. 1: Letter, Ronnie L. Gardner (AREVA NP Inc.) to Document Control Desk (NRC), "Request for Review and Approval of ANP-10303P, 'SIVAT: TELEPERM XS™ Simulation Validation Test Tool Topical Report'," NRC:09:063, June 11, 2009.

Ref. 2: Letter, Stacey L. Rosenberg (NRC) to Ronnie L. Gardner (AREVA NP Inc.), "Acceptance for Review of AREVA NP Inc. 'SIVAT: TELEPERM XS™ Simulation Validation Test Tool Topical Report'," December 28, 2009.

AREVA NP Inc. (AREVA NP) requested the NRC's review and approval of topical report ANP-10303P, Revision 0, "SIVAT: TELEPERM XS™ Simulation Validation Test Tool Topical Report," in Reference 1. The NRC's acceptance letter (Reference 2) states that NRC expected to issue a request for additional information (RAI) by January 31, 2010, and issue its draft safety evaluation by June 30, 2010.

AREVA NP and the NRC participated in a teleconference to discuss a draft RAI on March 17, 2010. A formal version of the RAIs was never issued. The response to the RAI discussed on the teleconference is provided in the enclosure to this letter.

During the same teleconference, the NRC discussed their intention to conduct an implementation audit to evaluate the usage of the SIVAT tool in conjunction with the verification and validation processes that are being used to qualify safety related applications for use in nuclear power plants. A draft copy of the audit plan was provided to AREVA NP by email on April 16, 2010. AREVA NP has no comments on the audit plan. AREVA NP recommends the first week of June (week of June 7) for the SIVAT implementation audit. Please advise AREVA NP of the confirmed audit date to allow for travel of audit support personnel from the Erlangen, Germany office.

The RAI response identifies areas where ANP-10303 will be clarified. AREVA NP has prepared a draft revision incorporating the clarifications and plans to submit Revision 1 to the topical report after the implementation audit. This schedule allows for the incorporation of any additional clarifications resulting from the audit.

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

If you have any questions related to this submittal, please contact Mark J. Burzynski, Regulatory Affairs. He may be reached by telephone at 434-832-4695 or by e-mail at mark.burzynski@areva.com.

Sincerely,

Ronnie L. Gardner

Ronnie L. Gardner, Manager
Corporate Regulatory Affairs
AREVA NP Inc.

Enclosure

cc: H. Cruz
R. Stattel
Project No. 728

AREVA NP RESPONSE to REQUEST FOR ADDITIONAL INFORMATION (RAI)

ANP-10303, "SIVAT: TELEPERM XS™ SIMULATION VALIDATION TEST TOOL

TOPICAL REPORT" (TAC NO. ME1503)

RAI 1 Question: In Section 3.0 of the topical report (TR), the statement is made that "... the I&C functionality represented in the TXS [(TELEPERM XS)] Application Software can be *completely verified* with SIVAT [(Simulation Validation Test Tool)]". However, Section 3.6 of the TR lists a series of limitations of the simulation, several of which could impact the ability of the tool to verify the I&C functionality of a TXS application. Please define what is meant by this statement and explain how the limitations of simulation listed in Section 3.6 do not invalidate this statement.

AREVA NP Response to RAI 1: The SIVAT Tool is designed to support testing of the TELEPERM XS Application Software. The I&C functionality that is testable with the SIVAT Tool consists of the software logic represented in the Function Diagrams (FDs) and the signal connections established between Function Diagrams created with the TELEPERM XS Specification and Coding Environment (SPACE) Engineering Tool. This I&C functionality is defined in the TELEPERM XS Application Software layer. The limitations described in Section 3.6 of the SIVAT Topical Report are related to the dynamic effects of asynchronous processor operations and the hardware/software interfaces. This clarification will be added to Section 3.0 in Revision 1 of the SIVAT Topical Report.

RAI 2 Question: In Section 3.2 of the TR, the Specification and Coding Environment (SPACE) code generator is described as being qualified. Please explain what is meant by this. Though the SPACE tool was described in the reference TXS topical report as well as the safety evaluation performed by the NRC, there is no mention of a qualification level achieved by these efforts.

The TXS SE concluded that " ... SPACE (specification and coding environment) tool for designing and assembling safety-related applications has the capability and safeguards to ensure that the implementation of the application programs can be successfully accomplished on a plant-specific basis.

The staffs understanding is that the SPACE tool has not been qualified as being Safety Related nor was it developed to the equivalent standards necessary for Software Integrity Level (SIL) 4 software. Please confirm that the qualification level stated in this TR is consistent with the conclusions made in the referenced TXS safety evaluation.

AREVA NP Response to RAI 2: The description of the SPACE Tool as qualified was meant to convey that the SPACE Engineering Tool was approved as part of the TELEPERM XS Topical Report. In the Safety Evaluation Report NRC concluded "that the SPACE Tool has the capability and safeguards to ensure that the implementation of the application programs can be successfully accomplished on a plant-specific basis."

The SPACE Automatic Code Generators are developed by AREVA NP and qualified by the independent German safety authorities in the same manner as the safety-related TELEPERM XS System Software and Function Block Library, which are considered appropriate for SIL 4 software. This clarification will be added to Sections 3.2 and 3.4 in Revision 1 of the SIVAT Topical Report.

RAI 3 Question: In Section 3.3 of the TR "Objectives for the SIVAT tool", the first listed objective makes reference to "... the original TELEPERM XS Application Software C code ..." and states that this same code is used for the SIVAT tool. It is evident that the SIVAT application is very different from the TXS application Software code as the objectives for each have little in common. How is it possible that the same code can be used to accomplish the objectives for the TXS application and the SIVAT tool programs?

AREVA NP Response to RAI 3: One of the key objectives of the SIVAT Tool is to utilize the project-specific TELEPERM XS Application Software C code for simulation by making minor adaptations to run the software in the simulation environment rather than on the target processor. This clarification will be added to Section 3.3 in Revision 1 of the SIVAT Topical Report.

RAI 4 Question: In Section 3.3 of the TR "Objectives for the SIVAT tool", the second feature of the SIVAT tool listed states that "No *functional modifications* of the TELEPERM XS Application Software C code" are made. However the staff understands that some changes are made to the application code prior to it being executed within the simulator. Section 16.1 describes the changes made to the TXS code as; "The code is slightly adapted in order to use the centrally managed memory of the simulator instead of the memory of the online systems". Please clarify what is meant by a *functional modification* within this context and explain why the changes that are made to the application code are not considered to be *functional modifications.*

AREVA NP Response to RAI 4: A key feature of the SIVAT Tool is the process for making the minor adaptations to the Application Software. In this process, no functional modifications are made to the Application Software (i.e., no changes to the FD logic or FD signal connections). This clarification will be added to Section 3.3 in Revision 1 of the SIVAT Topical Report. Also, see response to RAI 1.

RAI 5 Question: In Section 3.4 "TELEPERM XS Simulation Methodology, the second paragraph states that "... the Model provides an exact representation of the Original Application Software". Because non-functional modifications are being made to the application software code prior to it being executed within the simulator, this statement appears to be inconsistent. The following paragraphs' statement that this code is adapted accordingly also seems to conflict with this exact representation statement. This statement appears to be contradictory. Please provide clarification of this statement and justification for this claim.

AREVA NP Response to RAI 5: The model provides an exact representation of the I&C functionality in the project-specific Application Software. This clarification will be added to Section 3.4 in Revision 1 of the SIVAT Topical Report. Also, see response to RAI 1.

RAI 6 Question: The third paragraph of Section 3.5 "Simulation of communication" states that the MicroNET network system which is relied upon by the TXS for communication of messages between processors by the runtime environment is hardware based and is not simulated. The section also goes on to explain that message transfer functions are *implemented in a simplified manner.* This appears to be a significant limitation of the simulation environment because TXS applications are heavily reliant on communications between the various modules of the system yet there is no mention of this in Section 3.6 "Limitations of Simulation". Please explain why AREVA does not consider the simplified manner in which system communications are being implemented within the simulator to be a Limitation of Simulation.

AREVA NP Response to RAI 6: The SIVAT Tool is designed to support testing of the TELEPERM XS Application Software. The TELEPERM XS System Software layer and the TELEPERM XS hardware (including L2 Firmware) handle the communication features noted in RAI 6. The SIVAT Tool tests the Application Software signal connections established between FDs. The SIVAT Tool does not simulate the processing of the messages through the System Software or hardware. The simplification of the communication process made by the SIVAT Tool is to represent simply the logical signal connections in the simulation environment memory adaptation.

The communication features of the TELEPERM XS platform have been qualified as part of the generic platform qualification described in the TELEPERM XS Topical Report, as noted in the discussion of limitations in Section 3.6. The project-specific hardware and software interfaces are tested as part of the Hardware and Software Integration Testing, described in Section 13 of the TELEPERM XS Software Program Manual Topical Report. The limitations described in Section 3.6 of the SIVAT Topical Report address the project-specific dynamic effects of the communication protocol due to asynchronous processor operation and the hardware/software interfaces.

RAI 7 Question: Section 3.5.5 "TELEPERM XS Malfunctions" lists three types of functions used to simulate malfunctions. These three malfunction types do not appear to be capable of simulating all failures that can occur to a TXS system. Malfunctions such as the following are not described:

a. Memory errors,
b. Specific communication link faults,
c. Signal faults,
d. Power Degradation,
e. Faults associated with specific Function Block or a Function Block
f. Partial failure or degraded operation of a TXS central processing Unit (CPU).

Please explain how TXS malfunctions that are not within the three types described in this section would be accounted for.

AREVA NP Response to RAI 7: The SIVAT Tool is designed to support testing of the TELEPERM XS Application Software. As such, the malfunction simulation capability provided in the SIVAT Tool simulates malfunctions from the Application Software perspective. The Application Software communicates via messages, which can be lost through various system malfunctions (e.g., corrupted messages, loss of input/output (I/O) devices, or loss of TELEPERM XS processors). The SIVAT Tool does not attempt to model the cause of malfunctions; instead, it models the symptoms of these malfunctions as they affect the Application Software signals.

This clarification will be added to Sections 3.5.5 and 11.1 in Revision 1 of the SIVAT Topical Report.

The malfunctions listed in RAI 7 can be mapped to one or more of the SIVAT Tool malfunctions:

Memory errors – Memory errors that corrupt a single message are equivalent to the 'failure of a message' malfunction. Memory errors that affect processor operation are equivalent to the 'failure of a complete TELEPERM XS CPU' malfunction. Memory checks are part of the TELEPERM XS cyclic self-monitoring function.

Specific communication link faults – Communication link faults affect a single communication device connection, which is equivalent to the 'failure of a message' malfunction.

Signal faults – Signal faults are equivalent to the 'failure of an I/O module' malfunction or failure of an individual signal malfunction (i.e., by setting the status of individual signals as faulted").

Power Degradation – Power degradation faults can affect I/O modules or TELEPERM XS processors. These faults are equivalent to the failure of an I/O module,' and 'failure of a complete TELEPERM XS CPU' malfunctions.

Faults associated with specific Function Block or a Function Block – The Function Block Library and the Application Software that use the Function Blocks are developed as safety-related software to SIL 4 requirements. Credible failures associated with Function Blocks are associated with memory errors that affect parameterization or corruption of the software on a single TELEPERM XS processor. Memory checks and software integrity checks are part of the TELEPERM XS cyclic self-monitoring function.

Partial failure or degraded operation of a TXS central processing Unit – Degradation of a TELEPERM XS processor can result in the loss of messages or the loss of a processor. These problems are equivalent to the 'failure of a message,' and 'failure of a complete TELEPERM XS CPU' malfunctions. Other failure modes of the TELEPERM XS processor are addressed as described in Section 10.3.6 of the TELEPERM XS Software Program Manual Topical Report.

RAI 8 Question: The description of the three types of functions used to simulate malfunctions listed in Section 3.5.5 does not explain how these failures are to be applied to an application under simulation.

For example; what message would the "Failure of a message" function be applied to? Can this function be applied to all, some or just one specific message within the application? Can specific input or output (I/O) modules or selected signals within an I/O module be selected for the "Failure of an I/O module" functions or would the function being switched on just fail all of the systems I/O modules?

Please provide a more detailed description of these functions to help the staff to understand exactly what system malfunctions can be tested during simulation and to identify what additional malfunction types would need to be tested when the application is loaded onto TXS hardware.

AREVA NP Response to RAI 8: The SIVAT Tool has a malfunction for every individual generated message that sets the status in the specific message header to *error*. As a result, the receiving CPU provides all signals in the message with the error status. To simulate the failure of a network connection, the malfunction flags of all messages that are sent via this connection must be activated. The SIVAT Tool also has a malfunction for every individual I/O module that sets the statuses of all signals of this module to *error* after the corresponding flags have been activated. Additionally, the status of an individual input signal can be set to *error*. This corresponds to the system behavior when a specific I/O module or input channel fails. This clarification will be added to Section 3.5.5 in Revision 1 of the SIVAT Topical Report.

The SIVAT Tool is designed to support testing of the TELEPERM XS Application Software. As such, the malfunction simulation capability provided in the SIVAT Tool simulates malfunctions from the Application Software perspective. The Application Software communicates via signals, which can be lost through various system malfunctions (e.g., corrupted messages, loss of input/output (I/O) devices, or loss of TELEPERM XS processors).

As noted in Section 11 of the SIVAT Topical Report, SIVAT has the capability to support both white box and black box testing of the TELEPERM XS Application Software. The following tests should be carried out using SIVAT:

- Validation of the I&C functions against the software requirements
- Testing of the specified I&C functionality as defined in the Software Design Description
- Simulated system behavior and failure response

The SIVAT Tool malfunctions are used to support failure response testing by checking the response of the Application Software to failures of I/O modules, TELEPERM XS processors, or data messages. The acceptance criteria for these tests are correct performance at FD boundaries and output interfaces under error conditions. This clarification will be added to Section 11.1 in Revision 1 of the SIVAT Topical Report.

RAI 9 Question: In Section 3.5.5, the symptoms of a failed CPU are described and activation of the "Failure of a complete "TELEPERM XS CPU" function would simulate these symptoms. This implies that there is only one mode of failure for the TXS CPU. If this is not the case, then would it also be possible to simulate the symptoms for CPU failure modes other than the one described in this section?

Please provide additional information on the postulated failure modes for a TXS CPU and explain how simulation tests performed using SIVAT would provide an adequate means of ensuring that the safety system would be able to complete the required safety functions in the event of such a failure. If SIVAT testing cannot be used to test this level of system functionality, then this additional Limit of Simulation should be included in Section 3.6 of the TR.

AREVA NP Response to RAI 9: The SIVAT Tool is designed to support testing of the TELEPERM XS Application Software. As such, the malfunction simulation capability provided in the SIVAT Tool simulates malfunctions from the Application Software perspective. The Application Software communicates via messages, which can be lost through various system malfunctions (e.g., corrupted messages, loss of input/output (I/O) devices, or loss of TELEPERM

XS processors). The SIVAT Tool does not attempt to model the cause of malfunctions; instead, it models the symptoms of these malfunctions as they affect the Application Software signals.

Partial failure or degradation of a TELEPERM XS processor can result in the loss of messages or the loss of a processor. These problems are equivalent to the 'failure of a message,' and 'failure of a complete TELEPERM XS CPU' malfunctions. The 'loss of CPU' malfunction represents 'fatal' errors within the CPU or errors detected by self checking resulting in a reset or shutdown of the CPU. Other failure modes of the TELEPERM XS processor are addressed as part of the project-specific system design, as described in Section 10.3.6 of the TELEPERM XS Software Program Manual Topical Report.

The limitations in Section 3.6 of the SIVAT Topical Report describe limitations on the testing of TELEPERM XS Application Software, not limitations of the SIVAT Tool for testing a complete TELEPERM XS system. The full range of project-specific testing for a TELEPERM XS system is described in Section 13 of the TELEPERM XS Software Program Manual Topical Report.

RAI 10 Question: Section 3.5.7 of the TR describes the Test Principles used for implementing SIVAT tests and it provides an example of how test cases would be formulated and run on an application using the SIVAT tool. The section does not, however, discuss the methods or processes that would be used to generate these test cases. Please provide a description of exactly how the test specification is developed and explain the criteria that would be used to develop test cases which are to be run on SIVAT. Also, explain what criteria would be used to determine which test cases can be run on SIVAT verses test cases that would need to be run on TXS hardware due to the limitations of simulation described in Section 3.6.

AREVA NP Response to RAI 10: The overall process to conduct validation testing for TELEPERM XS projects is described in Section 11.9 of the TELEPERM XS Software Program Manual Topical Report. The specific testing is further elaborated in Section 13 of that Topical Report. Additional information on testing performed with the SIVAT Tool can be found in Section 11 of the SIVAT Topical Report.

The SIVAT Tool can be used to conduct all of the Application Software Integration Testing described in Section 13.3 of the Software Program Manual. The SIVAT Tool can also be used to conduct a portion of the Application Software System and Acceptance Testing described in Section 13.5 of the Software Program Manual. Specifically, the SIVAT Tool can be used to validate those system requirements that are fully implemented within the Application Software layer. For example, a two-out-of-four trip logic can be tested with the SIVAT Tool; whereas, the response time of the trip feature cannot be validated with the SIVAT Tool. Similarly, simple process control loop logics can be tested with the SIVAT Tool; whereas, the overall dynamic performance (final tuning) cannot be validated with the SIVAT Tool. The validation tests that can be performed with the SIVAT Tool are the tests required by Software Program Manual Sections 13.5.1.1, 13.5.1.2, and 13.5.1.5. The Hardware and Software Integration Testing described in Section 13.4 of the Software Program Manual and the Application Software System and Acceptance Testing that cannot be tested with the SIVAT Tool (due to tool limitations or hardware/software interfaces) are always performed in the test field.

As noted in Section 13.5.1 of the Software Program Manual, representative test cases of the test scope of the simulation tests are selected and to be carried out with the same simulation test scripts (converted to the test field syntax) in the test field. The selection criteria for representative test cases are:

- Each TELEPERM XS processor has to be covered by at least one test case,
- Test cases with specific hardware dependencies (e.g. time-related correlation of measuring signals like neutron flux measurement and the appropriate measuring range),
- Selected test cases containing functions which are spread out across several TELEPERM XS processors (due to the asynchronous working method of the TELEPERM XS processors), and
- Selected test cases with more complex functions.

This overlap of testing establishes a degree of congruence between tests conducted in simulation environment and those conducted in the test field.

This clarification will be added to Sections 11.4 and 11.5 in Revision 1 of the SIVAT Topical Report.

RAI 11 Question: Since the TELEPERM XS analysis tool, "cpuload," referenced in Section 3.6 has not been evaluated or approved for use as a qualified V&V tool by the NRC, it cannot be used as a sole means of ensuring that CPU load requirements are met. Therefore, test field verification should be a required activity for all applications developed using the TXS platform. Please explain how the requirements for CPU Load testing will be met for TXS applications.

AREVA NP Response to RAI 11: Field testing is used to verify the actual CPU load when the calculated CPU load using the ***cpuload*** tool is within 10 percent of the maximum target load of 50 percent. The target CPU load allows time for processing self-monitoring tests and service requests. This clarification will be added to Sections 3.6 and 11.2 in Revision 1 of the SIVAT Topical Report.

RAI 12 Question: The CPU restart Limit of Simulation is described in Section 3.6 as having been performed as part of the TELEPERM XS generic qualification process. Since this process was completed for the TXS platform, the test results should be available. Please provide a description of these tests and a summary of the test results. (Optionally, the NRC staff could review these records during a future audit).

AREVA NP Response to RAI 12: The original TELEPERM XS platform plant-independent system test documentation is described in Section 8.1.1 of the TELEPERM XS Topical Report.

The TELEPERM XS System Software was subjected to an external qualification test by the German Institute for Safety Technology (ISTec) and the German Technical Inspection Agency (TÜV). The following system characteristic relative to CPU start-up was confirmed during the external qualification testing:

- The Runtime Environment behaves in the operating modes start-up, operation, parameterization, functional test, and diagnosis as specified. It changes between operating modes according to the specification.

The most recent testing is documented by ISTec-TÜV Certificate No.: TXS-AUST-1006-03, TELEPERM XS integration test (AUST-II), which documents that the TELEPERM XS system met the criteria listed above.

RAI 13 Question: Section 3.7 of the TR describes Simulation in the Test Field using ERBUS[1]. ERBUS testing is described as testing that is performed following the manufacture of the cabinet in the test field. Figure 3-13 also illustrates ERBUS testing as testing that is performed independently from the use of Validation by SIVAT. Please explain the relevance of ERBUS in relation to the Validation Testing activities associated with SIVAT. This section appears to be informative in nature and not necessarily relevant to the qualification of SIVAT as a Verification and Validation (V&V) tool.

AREVA NP Response to RAI 13: 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.

RAI 14 Question: In the last paragraph of Section 3.7.3, a limitation to ERBUS Test field simulation is described and a conclusion that "... no response time measurements can be done using this system" is made yet no other field test program is mentioned in the TR. Since response time testing is listed as a limitation for both the SIVAT simulation and the ERBUS field test simulator, please explain how time response testing will then be accomplished for a TXS application.

AREVA NP Response to RAI 14: Response time testing is performed in the test field, as described in Section 13.5.1 of the Software Program Manual. The response time tests verify the response time of each trip function of the TELEPERM XS System on a channel-by-channel basis. The response time test is performed by simulating each input to the trip function and monitoring that input as well as monitoring the corresponding trip relay outputs. The time between the change in the input and the change of the output is the response time. That response time will be evaluated against the response time requirements. The response time is measured using fast response recording devices (as noted in Section 13.8 of the Software Program Manual)

RAI 15 Question: In regard to SIVAT compliance to BTP 7-14 in Section 4.11 of the TR, the statement; "system characteristics not tested by SIVAT are either tested during the TXS generic qualification testing process, verified with other TXS analysis tools, or *validated during system validation testing...*" presents a circular argument since the SIVAT tool itself is being used to support TXS software validation. Please explain how characteristics which are not tested by SIVAT such as those listed in Section 3.6 will be subsequently tested during system validation testing when SIVAT itself is being used to perform system validation testing.

AREVA NP Response to RAI 15: The system characteristics not tested by SIVAT are either tested during the TELEPERM XS generic qualification process, verified with other TELEPERM XS analysis tools, or validated during system validation testing in the test field, as described in Section 11.2 of the SIVAT Topical Report. This clarification will be added to Section 4.11 in Revision 1 of the SIVAT Topical Report.

---

1 The name of a computer-assisted test system for TELEPERM XS test field application (test field simulator).

RAI 16 Question: In Section 5.4 "Problem Reporting" of the SDP, the first paragraph describes the scope of problem reporting as "... discrepancies regarding the use of the TELEPERM XS SIVAT tool for validation testing of Application Software developed by AREVA NP for use in safety-related I&C applications deployed in the U.S.". It is un-clear to the staff as to whether this scope applies to problems associated with the SIVAT tool, problems associated with TXS application software, or problems associated with both types of application. Please explain the intended scope for Problem Reporting within the context of the SIVAT SDP Section 5 of the TR. Include a description of how errors associated with the SIVAT tool will be identified, processed, and resolved.

AREVA NP Response to RAI 16: Section 5.4 of the SIVAT Topical Report defines the AREVA NP (Inc) responsibilities and requirements for identifying, processing, and resolving problems and discrepancies identified with the SIVAT Tool during validation testing of Application Software developed by AREVA NP (Inc). AREVA NP (Inc) forwards problems identified with the SIVAT Tool to AREVA NP GmbH for evaluation and resolution. AREVA NP (Inc) notified customers of any SIVAT Tool problems affecting installed TELEPERM XS Application Software. This clarification will be added to Section 5.4 in Revision 1 of the SIVAT Topical Report.

RAI 17 Question: Section 7.1 "SIVAT Quality Assurance Plan" states that "SIVAT was developed under the same QA program and software lifecycle development process as described in the TELEPERM XS Topical Report". That topical report evaluated the procedures FAW 3.4, 3.5, and 3.6 and sited these procedures as basis for its safety conclusion. Please explain why it is acceptable to credit the Lifecycle development process described in the TXS topical report when the FAW 3.6 procedure that was used as a basis for the safety evaluation was determined to be *not applicable to the development of SIVAT Software* in Section 6.1.2 of the SIVAT TR. Please also explain why the procedures FAW 3.4, and 3.5 are not referenced in the SIVAT TR and describe how the processes covered by these procedures are being otherwise performed in an acceptable manner for SIVAT.

AREVA NP Response to RAI 17: Section 6 describes the TELEPERM XS Phase Model, which was used for development of the SIVAT Tool. The Phase Model describes a graded approach to software development. Classes A and B represent software that performs safety functions. The software development controls for these classes of software is appropriate for SIL 4 software. The groups of procedures (FAW-TXS-3.3 through FAW-TXS-3.6) provide specific guidance to create the Appendix B safety-related design basis documentation. These same controls are also applied to Class C software associated with the SPACE Code Generators.

The graded Phase Model described in FAW-TXS-1.5 applies the configuration management requirements of FAW-TXS-1.5, the documentation requirements of FAW-TXS-2.2, the system integration requirements of FAW-TXS-4.1, and the review guidelines of FAW-TXS-4.2 to the development of the SIVAT Tool. In addition, the specific verification and validation activities described in Section 14 of the SIVAT Topical Report were applied to the development of the SIVAT Tool. The controls are the appropriate 10 CFR Part 50 Appendix B controls for the SIVAT Tool, since TELEPERM XS Application Software characteristics not tested by the SIVAT Tool are either tested during the TELEPERM XS generic qualification process, verified with other TELEPERM XS analysis tools, or validated during system validation testing in the test field.

RAI 18 Question: In Section 11.1 "Application software testing with SIVAT", the last paragraph on page 11-3 states that "*the goal of the project-specific simulation testing with SIVAT is to verify* the correct implementation of *all the functions and requirements* specified in the SRS". It is apparent to the staff that some of the requirements that would be specified in an SRS would not be testable by SIVAT (e.g. time response functional requirements) due to the limitations of simulation listed in Section 3.6 of the TR. Please explain the meaning of this statement in relation to the intended use of the SIVAT tool considering the limitations of the tool.

AREVA NP Response to RAI 18: The goal of the project-specific simulation testing with SIVAT is to verify the correct implementation of the I&C functionality that is testable with the SIVAT Tool and the associated requirements specified in the Software Requirements Specification. The I&C functionality that is testable with the SIVAT Tool includes the software logic represented in the FDs and the signal connections established between FDs created with the SPACE Engineering Tool. This clarification will be added to Section 11.1 in Revision 1 of the SIVAT Topical Report.

RAI 19 Question: The opening paragraph of Section 11.0 of the TR states that the limitations of simulation are discussed in the SIVAT Operations Plan; however, Section 11.2 "Limitations of Simulation" is a restatement of the list of Limitations provided in Section 3.6 which includes only slight re-wording. Please provide a detailed discussion of the Limitations of Simulation including an explanation of how and when each of these limitations will be tested through other means that are not reliant on the SIVAT tool.

AREVA NP Response to RAI 19: The project-specific hardware interface to the TELEPERM XS platform is validated during the project-specific Hardware and Software Integration Test. This testing checks the project-specific interface to Runtime Environment, correct operation of the project-specific network, and correct operation of CPU startup and restart. These tests are described in Section 13.4 and 13.5 of the TELEPERM XS Software Program Manual. Also, see the responses to RAIs 11 and 20. This clarification will be added to Sections 3.6 and 11.2 in Revision 1 of the SIVAT Topical Report.

RAI 20 Question: Section 13.2 of the TR describes a behavioral difference that essentially renders Gateway processor functionality un-testable in SIVAT simulation. Why is this, "Limitation of Simulation" not specifically listed in Section 3.6?

AREVA NP Response to RAI 20: The Function Blocks used on a real TELEPERM XS Gateway, write/read the export/import signals to/from the secondary side of the gateway, using a shared memory. Inside the SIVAT simulation the input and output signals are not processed by the FBs because there is no secondary Gateway side with which to communicate. Gateway operation is validated during system validation testing, as described in TELEPERM XS Software Program Manual Section 13.5.1.4. This clarification will be added to Sections 3.6 and 11.2 in Revision 1 of the SIVAT Topical Report.

RAI 21 Question: The SIVAT Configuration Management (CM) Plan Section 15.0 of the TR credits the CM process FAW-TXS-1.5 that was described in the TXS Topical report and evaluated by the NRC in 2000, however, Section 15.3 states that AREVA NP intends to use a different CM process. This section states that "... configuration management for SIVAT Tools used for U.S. TELEPERM XS projects will be controlled through the TELEPERM XS Application Software Configuration Management Plan described in Section 12 of the TELEPERM XS

Software Program Manual". Please explain which of these Configuration Management Plans will in fact be used to maintain SIVAT configuration so that the staff can focus its evaluation on the appropriate process.

AREVA NP Response to RAI 21: Section 15 of the SIVAT Topical Report describes two methods of configuration management: during SIVAT Tool development in Germany and during SIVAT Tool use for project-specific validation testing in the U.S. The configuration management plan described in the TELEPERM XS Topical Report is used for the development of the SIVAT Tool. The configuration management plan described in the TELEPERM XS Software Program Manual Topical Report is used for project-specific SIVAT Tool use in the U.S. This clarification will be added to Section 15 in Revision 1 of the SIVAT Topical Report.

RAI 22 Question: Figure 3-2 depicts a process labeled "Formal Verification" which apparently compares or verifies the generated C-Code against the Project Database. Two routines are referenced in this figure; "rediff", and "cmp_code". The definition of "rediff" in Section 2, however, states that "rediff" compares redundancies against each other and not code against the project database as is depicted in the figure. In addition the definition of "cmp_code provided in Section 2 does not explain how this tool is used to perform "Formal Verification". Please provide additional information on the use of the software tools "rediff" and "cmp_code" and explain how and when these tools are used to perform "Formal Validation" of safety related application software.

AREVA NP Response to RAI 22: The development of the TELEPERM XS Application Software is described in the TELEPERM XS Software Program Manual Topical Report. Figures 3-2 and 3-13 will be revised to remove the extraneous information in Revision 1 of the SIVAT Topical Report.

AREVA

January 4, 2010
NRC:10:001

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

Review of ANP-10303P, "SIVAT: TELEPERM XS™ Simulation Validation Test Tool Topical Report," (TAC NO. ME1503)

Ref. 1: Letter, Ronnie L. Gardner (AREVA NP Inc.) to Document Control Desk (NRC), "Request for Review and Approval of ANP-10303P, 'SIVAT: TELEPERM XS™ Simulation Validation Test Tool Topical Report'," NRC:09:063, June 11, 2009.

Ref. 2: Letter, Stacey L. Rosenberg (NRC) to Ronnie L. Gardner (AREVA NP Inc.), "Acceptance for Review of AREVA NP, INC. SIVAT: TELEPERM XS™ Simulation Validation Test Tool Topical Report (TAC NO. ME1503)," December 28, 2009.

AREVA NP Inc. (AREVA NP) submitted ANP-10303P, Revision 0, "SIVAT: TELEPERM XS™ Simulation Validation Test Tool Topical Report," for review and approval in Reference 1.

The NRC documented its acceptance review of ANP-10303P in Reference 2. The acceptance review letter also documented AREVA NP's commitment to provide translation of the relevant portion of the following SIVAT development documents made during a telephone conference call on October 22, 2009:

- Requirements specification: SIMM
  (original title: Lastenheft SIMM (KWU NLL4/98/068))
- TXS design specification, version 01.21: Generator CATS-SDE for the TXS simulation environment
  (original title: TXS-Pflichtenheft, Version 01.21: Generator CATS-SDE für die TXS-Simulationsumgebung (KWU NLLZ ST/99/023b))
- General requirements specification: TXS simulator
  (original title: Rahmenlastenheft: TXS-Simulator (KWU NLL4/98/042))

The requested translations are provided in an enclosure to this letter in AREVA NP document NLTC-G/2009/en/0069 A, TELEPERM XS Simulation tools - translation of selected chapters from requirements and design specification documents from the initial development, dated November 30, 2009.

AREVA NP INC.
An AREVA and Siemens company

3315 Old Forest Road, P.O. Box 10935, Lynchburg, VA 24506-0935
Tel.: 434 832 3000 - Fax: 434 832 3840 - www.areva.com

AREVA NP considers some of the material contained in AREVA NP document NLTC-G/2009/en/0069 A to be proprietary. As required by 10 CFR 2.390(b), an affidavit is enclosed lo support the withholding of the information from public disclosure. Proprietary and non-proprietary versions of the document are provided. .

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

Sincerely,

Ronnie L. Gardner

Ronnie L. Gardner, Manager
Corporate Regulatory Affairs
AREVA NP Inc.

Enclosures

cc: H.D. Cruz
Project 728

AFFIDAVIT

COMMONWEALTH OF VIRGINIA)
) ss.
CITY OF LYNCHBURG)

1. My name is Mark J. Burzynski. I am Manager, Product Licensing, for AREVA NP Inc. 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 NLTC-G/2009/en/0069 A, TELEPERM XS Simulation tools - translation of selected chapters from requirements and design specification documents from the initial development, dated November 30, 2009 and referred to herein as the "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 this Document is considered proprietary for the reasons set forth in paragraphs 6(b), 6(c) and 6(d) above.

7. In accordance with AREVA NP's policies governing the protection and control of information, proprietary information contained in this Document has 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.

Mark J. Burzynski

SUBSCRIBED before me on this 4th

day of January, 2010.

S McFaden

Sherry L. McFaden
NOTARY PUBLIC, COMMONWEALTH OF VIRGINIA
MY COMMISSION EXPIRES: 10/31/2010
Registration # 7079129

SHERRY L. MCFADEN
Notary Public
Commonwealth of Virginia
7079129
My Commission Expires Oct 31, 2010

UNITED STATES
NUCLEAR REGULATORY COMMISSION
WASHINGTON, D.C. 20555-0001

December 28, 2009

Mr. Ronnie L. Gardner, Manager
Site Operations and Regulatory Affairs
AREVA NP Inc.
3315 Old Forest Road
Lynchburg, VA 24501

SUBJECT: ACCEPTANCE FOR REVIEW OF AREVA NP, INC. "SIVAT: TELEPERM XS™ SIMULATION VALIDATION TEST TOOL TOPICAL REPORT" (TAC NO. ME1503)

Dear Mr. Gardner:

By letter dated June 11, 2009 (Agencywide Documents Access and Management System (ADAMS) ML091680619), AREVA submitted for U.S. Nuclear Regulatory Commission (NRC) staff review Topical Report (TR) ANP-10303P, "SIVAT: TELEPERM XS™ Simulation Validation Test Tool Topical Report," that would allow the use of SIVAT as a software validation tool for the development of safety related applications for the Teleperm XS system.

The NRC staff has performed an acceptance review of TR ANP-10303P. The NRC staff has determined that in order for the NRC to complete a comprehensive Safety Evaluation for this TR, the following additional supporting documentation will be required. Areva has agreed to provide the required documentation on or before before December 31, 2009.

- KWU NLL4/98/042 Frame Requirement Specification
- KWU NLL4/98/068, Requirement Specification
- KWU NLLZ ST/99/023b, Functional Specification

Based on AREVA providing high quality supporting documentation that reasonably conforms to regulatory guidance and the associated industry standards, the NRC staff expects to issue its request for additional information by January 31, 2010, and issue its draft safety evaluation by June 30, 2010. The NRC staff estimates that the review will require approximately 1000 staff hours including project management time. The review schedule milestones and estimated review costs were discussed and agreed upon in a telephone conference between Mark Burzynski, AREVA Licensing Manager, and the NRC staff on October 22, 2009.

Section 170.21 of Title 10 of the *Code of Federal Regulations* requires that TRs are subject to fees based on the full cost of the review. You did not request a fee waiver; therefore, NRC staff hours will be billed accordingly.

If you have any questions regarding this matter, please contact Holly D. Cruz at (301) 415-1053.

Sincerely,

Eric Bowman for

Stacey L. Rosenberg, Chief
Special Projects Branch
Division of Policy and Rulemaking
Office of Nuclear Reactor Regulation

Project No. 728

AREVA

June 11, 2009
NRC:09:063

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

Request for Review and Approval of ANP-10303P, "SIVAT: TELEPERM XS™ Simulation Validation Test Tool Topical Report"

Ref. 1: Letter, Sandra M. Sloan (AREVA NP Inc.) to Document Control Desk (NRC), "U.S. EPR Instrumentation and Controls Topical Reports," NRC: 09:004, January 23, 2009.

Ref. 2 Letter, Ronnie L. Gardner (AREVA NP Inc.) to Document Control Desk (NRC), "AREVA NP Response to Review Status of the ANP-10272, 'Software Program Manual For TELEPERM XS Safety Systems Topical Report' (TAC No. MD3971)," NRC:09:035, April 7, 2009.

AREVA NP Inc. (AREVA NP) requests the NRC's review and approval of the enclosure, ANP-10303P, Revision 0, "SIVAT: TELEPERM XS™ Simulation Validation Test Tool Topical Report." AREVA NP notified NRC of its intention to submit this report in Reference 1.

This topical report describes the Simulation Validation Test Tool (called SIVAT) developed by AREVA NP to support the development of project-related TELEPERM XS Application Software. This report describes:

- The concept of TELEPERM XS simulation and the principles of operation for the SIVAT Tool and;
- The high quality development process used to develop the SIVAT Tool.

The use of a NRC-approved simulation validation tool has been described in AREVA NP document ANP-10272, Draft Revision 1, Software Program Manual for TELEPERM XS™ Safety Systems Topical Report, which was submitted to NRC in Reference 2. The use of the SIVAT Tool to support TELEPERM XS Application Software validation has important benefits. The early detection of Application Software faults through validation testing with SIVAT serves to reduce project risks earlier in the development process.

AREVA NP requests that the NRC issue a Safety Evaluation Report that approves ANP-10303P. AREVA NP intends to use the SIVAT Tool to support validation testing of TELEPERM XS Application Software developed in accordance with the TELEPERM XS Software Program Manual. AREVA NP requests that the NRC complete its review of the enclosed report and issue the SER by June 2010.

AREVA NP INC.
An AREVA and Siemens company

3315 Old Forest Road, P.O. Box 10935, Lynchburg, VA 24506-0935
Tel.: 434 832 3000 - Fax: 434 832 3840 - www.areva.com

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

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

Sincerely,

Ronnie L. Gardner, Manager
Corporate Regulatory Affairs
AREVA NP Inc.

Enclosures

cc: H. D. Cruz
R. Subbaratnam
Project 728

AFFIDAVIT

COMMONWEALTH OF VIRGINIA	)	
	)	ss.
CITY OF LYNCHBURG	)	

1. My name is Mark J. Burzynski. I am Manager, Product Licensing, for AREVA NP Inc. 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 report ANP-10303P, Revision 0, "SIVAT: TELEPERM XS™ Simulation Validation Test Tool Topical Report" and referred to herein as the "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 this Document is considered proprietary for the reasons set forth in paragraphs 6(b), 6(c) and 6(d) above.

7. In accordance with AREVA NP's policies governing the protection and control of information, proprietary information contained in this Document has 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.

Mark J Burzynski

SUBSCRIBED before me on this 8th

day of June, 2009.

S. McFaden

Sherry L. McFaden
NOTARY PUBLIC, COMMONWEALTH OF VIRGINIA
MY COMMISSION EXPIRES: 10/31/2010
Registration # 7079129

SHERRY L. MCFADEN
Notary Public
Commonwealth of Virginia
7079129
My Commission Expires Oct 31, 2010

ANP-10303NP
Revision 1

SIVAT: TELEPERM XS™ Simulation Validation Test Tool

Topical Report

August 2010

AREVA NP Inc.

Non-Proprietary

ABSTRACT

This Topical Report describes the Simulation Validation Test Tool (called SIVAT) developed by AREVA NP to support the development of project-related TELEPERM XS Application Software. This report describes:

- The TELEPERM XS simulation concept and SIVAT principles of operation and
- The high quality development process used to develop the SIVAT Tool.

The SIVAT software package allows the engineered I&C functionality to be tested by simulation. SIVAT uses the NRC-approved TELEPERM XS SPACE Code Generator for generating simulation-capable code from the engineering data stored in the project database. This report shows that the I&C functionality represented in the Application Software can be effectively tested with the SIVAT Tool.

The objective is to prove that the functional requirements established by the process engineers have been translated into Function Diagrams (FDs) without errors, and that the software automatically generated from these FDs provides the functionality required in terms of input and output response. Process models can also be linked into the simulator to perform closed-loop tests.

Running pre-programmed test scripts ensures that simulation runs are traceable and repeatable. Test results are recorded in log files and plots for further evaluation. Additionally, simulation tests with SIVAT have shown to be an indispensable advantage when systems already in operation in the power plant need to be modified. In this case, simulation results prior to and after modification can be compared to verify that no inadvertent changes have been introduced to the I&C functions.

The use of the SIVAT Tool to support TELEPERM XS Application Software verification and validation has important benefits such as the early detection of Application Software faults that serves to reduce project risks earlier in the development process.

Nature of Changes

Revision	Section(s) or Page(s	Description and Justification
0	All	Initial issue.
1	Section 1	Removed revision levels from topical report references
	Section 3	Modified to add clarifications resulting from NRC request for additional information (RAIs)
	Section 4	Modified to add clarifications resulting from NRC RAIs
	Section 5	Modified to add clarifications resulting from NRC RAIs
	Section 11	Modified to add clarifications resulting from NRC RAIs
	Section 13	Modified to add clarifications resulting from NRC RAIs
	Section 15	Modified to add clarifications resulting from NRC RAIs
	Section 17	Removed revision levels from topical report references
	Section 18	Updated revision levels for topical report references

Contents

List of Tables

List of Figures

Nomenclature

Acronym	Definition
ASC	Assembling Center
BTP	Branch Technical Position
CAD	Computer Aided Design
CATS-SDE	Code Adaptation Tool for Simulator SDE
CCB	Change Control Board
CD-ROM	Compact Disc – Read Only Memory
CFR	Code of Federal Regulations
CoA	Configuration Administrator
CoM	Configuration Manager
CPU	Central Processing Unit
CR	Change Request
CRC	Cyclic Redundancy Checksum
DBB	Database Binder
DBE	Database Editor
DIN	Deutsches Institut für Normung (German Institute for Standardization)
EN	European Committee for Standardization
ERBUS	TELEPERM XS computer-assisted test system for TELEPERM XS test field application (test field simulator)
EUB	Expert User Board
FAT	Factory Acceptance Test
FB	Function Block
FD	Function Diagram
FDE	Function Diagram Editor
FDG	Function Diagram Group
FDGM	Function Diagram Group Module
GUI	Graphical User Interface
I&C	Instrumentation and Control
I/O	Input/Output
IC	Initial Condition
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronic Engineers
ISO	International Organization for Standardization
ITZ	Integration and Test Center
NRC	Nuclear Regulatory Commission

Acronym	Definition
NUPIC	Nuclear Procurement Issues Committee
QA	Quality Assurance
RTE	Runtime Environment
SCM	Software Configuration Management
SCU	Simulator Control Unit
SDE	Simulation Development Environment
SER	Safety Evaluation Report
SimDB	Simulator Database
SimEx	Simulator Executive
SIVAT	Simulation Validation Test Tool
SME	Subject Matter Expert
SMS	Service Monitor Server
SPACE	Specification and Coding Environment
SU	Service Unit
Tcl/Tk	Tool Command Language and associate toolkit
TXS	TELEPERM XS

1.0 INTRODUCTION

This Topical Report describes the Simulation Validation Test Tool (called SIVAT) developed by AREVA NP to support the development of project-related TELEPERM XS Application Software. This report describes:

- The concept of TELEPERM XS simulation and the principles of operation for the SIVAT Tool and
- The high quality development process used to develop the SIVAT Tool.

The SIVAT software package allows the engineered instrumentation and control (I&C) functionality to be tested by simulation. SIVAT uses the NRC-approved TELEPERM XS Specification and Coding Environment (SPACE) Tool Code Generator for generating simulation-capable code from the engineering data stored in the project database.

The objective is to prove that the functional requirements established by the process engineers have been translated into Function Diagrams (FDs) without errors, and that the software automatically generated from these FDs provides the functionality required in terms of input and output response. Process models can also be linked into the simulator to perform closed-loop tests.

Running pre-programmed test scripts ensures that simulation runs are traceable and repeatable. Test results are recorded in log files and plots for further evaluation. Simulation tests with SIVAT have shown to be an indispensable advantage when systems already in operation in the power plant need to be modified. In this case, simulation results prior to and after modification can be compared to verify that no inadvertent changes have been introduced to the I&C functions.

This topical report describes the concept of the TELEPERM XS simulation and the principle of operation of the SIVAT. This report shows that the I&C functionality represented in the Application Software can be effectively tested with the SIVAT Tool. The use of a NRC-approved simulation validation tool has been described in AREVA

NP document ANP-10272, Software Program Manual for TELEPERM XS™ Safety Systems Topical Report (Reference 29), which is referred to as the TELEPERM XS Software Program Manual.

The use of the SIVAT Tool to support TELEPERM XS Application Software validation has important benefits. The early detection of Application Software faults through validation testing with SIVAT serves to reduce project risks earlier in the development process.

AREVA NP requests that the NRC issue a Safety Evaluation Report that approves ANP-10303P, SIVAT: TELEPERM XS™ Simulation Validation Test Tool Topical Report. AREVA NP intends to use the SIVAT Tool to support validation testing of TELEPERM XS Application Software developed in accordance with the TELEPERM XS Software Program Manual.

2.0 DEFINITIONS

ADD File

Text file containing commands for entering models and variables into the simulator database; serves as input file for the database tool of the simulator control system.

AREVA NP GmbH

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.

AREVA NP (Inc)

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.

Application Software [ ]

Software designed to fulfill specific needs of a user. For TELEPERM XS systems the Application Software reflects the plant specific functionality of the TELEPERM XS I&C system. It is generated and documented by the TELEPERM XS SPACE tool.

Code [ ]

Computer instructions and data definitions expressed in a programming language or in a form output by an assembler, compiler, or another translator.

cmp_code

TELEPERM XS tool used for verification of the scope of a modification in Application Software code generated after implementing a specification change in the SPACE project database.

Component [ ]

One of the parts that make up a system. A component may be hardware or software and may be subdivided into other components.

Configuration [ ]

The arrangement of a computer system or component as defined by the number, nature, and interconnections of its constituent parts. In configuration management, the functional and physical characteristics of hardware or software as set forth in technical documentation or achieved in a product.

Configuration Control [ ]

An element of configuration management, consisting of the evaluation, coordination, approval or disapproval, and implementation of changes to configuration items after formal establishment of their configuration identification.

Configuration Control Board [ ]

A group of people responsible for evaluating and approving or disapproving proposed changes to configuration items, and for ensuring implementation of approved changes.

Configuration Identification [ ]

An element of configuration management, consisting of selecting the configuration items for a system and recording their functional and physical characteristics in technical documentation.

The current approved technical documentation for a configuration item as set forth in specifications, drawings, associated lists, and documents referenced therein.

Configuration Item [ ]

An aggregation of hardware, software, or both, that is designated for configuration management and treated as a single entity in the configuration management process.

Configuration Management [ ]

A discipline applying technical and administrative direction and surveillance to:

- Identify and document the functional and physical characteristics of a configuration item
- Control changes to those characteristics
- Record and report change processing and implementation status
- Verify compliance with specified requirements

Coverage

Method and indicators to assess that the functional features of the software have been comprehensively validated.

cpuload

TELEPERM XS load analysis tool used to analyze the loading on the central processor units.

Cyclic Redundancy Checksum (CRC)

Method applied for identification of data files using industry standard functions to produce a unique checksum. This checksum is used to identify and detect alteration of data during usage, transmission, or storage.

Discrepancies

During the software development life cycle, any difference or perceived difference discovered by various organizations in the later documents or code with the earlier requirements specified in other design documents. These discrepancies are initially documented on the Open Item list and are evaluated for further action.

H1

TELEPERM XS Ethernet network used for communication with TELEPERM XS Gateway and Service Unit (SU).

Interface [ ]

1. A shared boundary across which information is passed. This boundary includes design interfaces between design organizations (as interpreted by Regulatory Guide 1.169).
2. A hardware or software component that connects two or more other components for the purpose of passing information from one to the other.
3. To connect two or more components for the purpose of passing information from one to the other.
4. To serve as a connecting or connected component as in 2 above.

Interface Control [ ]

In configuration management, the process of:

- Identifying functional and physical characteristics relevant to the interfacing of two or more configuration items provided by one or more organizations
- Ensuring that proposed changes to these characteristics are evaluated and approved prior to implementation

K32

TELEPERM XS backplane bus used for communication inside TELEPERM XS computer units.

L2

TELEPERM XS PROFIBUS network used for communication between TELEPERM XS computer units.

Level 3

Functional requirements definition for the safety I&C technology to be implemented in TELEPERM XS. These requirements are defined in the Software Requirements Specification.

Level 4

Instrumentation and control requirements definition for TELEPERM XS. These requirements are defined in the Software Design Description.

Malfunction

Malfunction that is evoked in a simulated model.

MIC File

Machine language loadable code file.

netload

TELEPERM XS load analysis tool used to analyze the loading on the network connections.

Open Item

Any item which constitutes an error or anomaly from the required status or condition of a properly completed project. Each Open Item is given an identifier that is unique to the project and unit, as well as a record in a database. The entry contains information to track the life cycle of the item from initiation to final resolution.

rediff

TELEPERM XS tool used to detect differences in the functionality of Application Software in the redundant divisions of an I&C system. The tool performs an analysis of logics and parameter data specified for redundant system trains and identifies differences in functionality. The differences must be evaluated by an engineer to determine whether the differences are planned (engineered differences) or unplanned (errors).

reflist

A software program that creates CRC sums recursively for the subdirectories and files within a directory and outputs them in a list, including the date of the last change for the file. This method is used for identification of the TELEPERM XS system software, for project specific additions, for the Application Software implemented on an engineering platform (engineering workstation), and for software downloaded into the I&C system.

Regression Testing [ ]

Selective retesting of a system or component to verify that modifications have not caused unintended effects and that the system or component still complies with its specified requirements.

scanmic

'scanmic' is a TELEPERM XS software authentication tool. It analyzes the software configuration of loadable code (called MIC files). 'scanmic' is used to read the version strings of the Application Software components contained in a loadable MIC file from the MIC file itself, and calculate the CRC checksum for each software segment in the MIC file as well as the CRC checksum for the entire MIC file.

This information can be output to a list which serves to document the generated software version. Differences in the software configuration between the old version and the new version can be determined from these lists and then verified.

Software [ ]

Computer programs, procedures, and in some cases, associated documentation and data pertaining to the operation of a computer system.

Software Design Description [ ]

A representation of software created to facilitate analysis, planning, implementation, and decision making. The software design description is used as a medium for communicating software design information, and may be thought of as a blueprint model of the system.

Software Hazard [ ]

A software design error that could lead to an unintended operation or failure to operate when required.

Software Life Cycle [ ]

The period of time that begins when a software product is conceived and ends when the software is no longer available for use.

SPACE

The SPACE engineering system comprises the tools used for the engineering and maintenance of the TELEPERM XS I&C Application Software. In this context, engineering refers to the overall process of creating and testing the Application Software:

- Specification of the I&C functions and hardware topology
- Automatic code generation
- Software authentication, using ***reflist*** and ***scanmic***
- Software loading
- Load analysis tool
- Database administration

System Software [ ]

Software designed for a specific computer system or family of computer systems to facilitate the operation and maintenance of the computer system and associated programs such as operating systems, compilers, and utilities.

Test Plan [ ]

A document describing the scope, approach, resources, and schedule of intended test activities. It identifies test items, the features to be tested, the testing tasks, who will do each task, and any risks requiring contingency planning.

Unit [ ]

1. A separately testable element specified in the design of a computer software component.
2. A logically separable part of a computer program.
3. A software component that is not subdivided into other components.

Validation [ ]

The process of evaluating a system or component during or at the end of the development process to determine whether it satisfies specified requirements. *Contrast with:* verification.

Verification [ ]

The process of evaluating a system or component to determine whether the products of a given development phase satisfy the conditions imposed at the start of that phase. *Contrast with:* validation.

Version [ ]

An initial release or re-release of a computer software configuration item that is associated with a complete compilation or recompilation of the computer software configuration item.

Verification and Validation [ ]

The process of determining whether the requirements for a system or component are complete and correct, the products of each development phase fulfill the requirements or conditions imposed by the previous phase, and the final system or component complies with specified requirements.

3.0 TELEPERM XS SIMULATION WITH SIVAT

This section describes the concept of TELEPERM XS simulation and the principle of operation of the SIVAT Tool. The SIVAT Tool is designed to support testing of the TELEPERM XS Application Software. The I&C functionality that is testable with the SIVAT Tool consists of the software logic represented in the FDs and the signal connections established between FDs created with the SPACE Engineering Tool. This I&C functionality is completely described in the TELEPERM XS Application Software layer. The section describes how the I&C functionality represented in TELEPERM XS Application Software can be completely verified with SIVAT.

3.1 Fundamentals of Simulation

The basic principle of TELEPERM XS simulation is relatively simple. One or more models are used to define the process or system to be simulated as realistically as possible. The Simulator Control System is used to implement the following tasks:

The TELEPERM XS simulation concept is shown in Figure 3-1.

The accuracy of the simulation results depends on how well the process or system is represented by the model or models. SIVAT models the TELEPERM XS system running project-specific Application Software. A model with regard to the simulation is a software function which was generally written in a higher-level programming language (C or FORTRAN) or generated using special CAD tools. The simulator control system can be compared to a very user-friendly, task-specific debugger that permits successive execution of the program code while simultaneously enabling the visualization and modification of program variables.

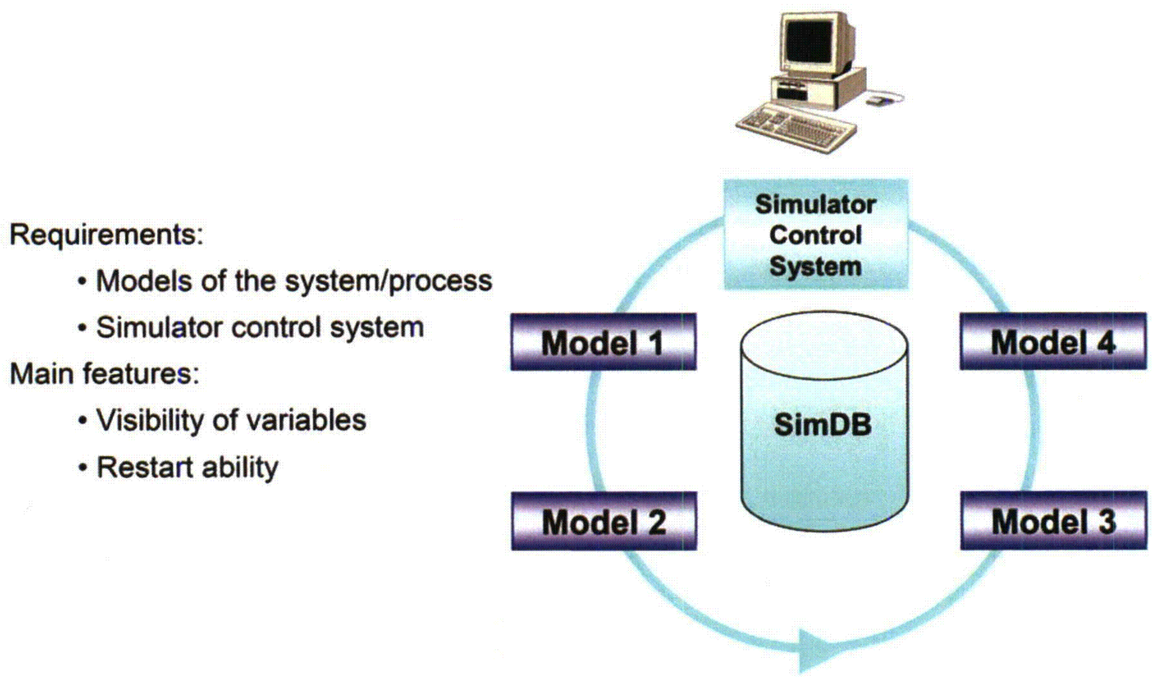

Figure 3-1 - TELEPERM XS Simulation Concept

3.2 SIVAT in the Application Software Development Process

The TELEPERM XS Application Software development process (shown in Figure 3-2) begins with the definition of the Software Requirements Specification (Level 3) for the I&C tasks which have to be implemented. This task definition is converted into the Software Design Description Function Diagrams (Level 4). The Software Design Description forms the basis for specifying the TELEPERM XS instrumentation and control system using the SPACE Function Diagram Editor (FDE). All data regarding the specified I&C functionality is stored in a project database. Thus the complete data set is available from one single source (single source principle). This project database is controlled by the Application Software Configuration Management Plan. The SPACE Code Generators are used for automatic code generation. The SPACE Engineering Tool was approved as part of the TELEPERM XS Topical Report. In the Safety Evaluation Report NRC concluded "that the SPACE Tool has the capability and safeguards to ensure that the implementation of the application programs can be successfully accomplished on a plant-specific basis." The SPACE Code Generators create the Application Software C Code, which is subsequently compiled and uploaded to the TELEPERM XS safety processors. The SIVAT Tool is used to support validation testing of the Application Software in a simulation environment. The Application Software development process is fully described in TELEPERM XS Software Program Manual.

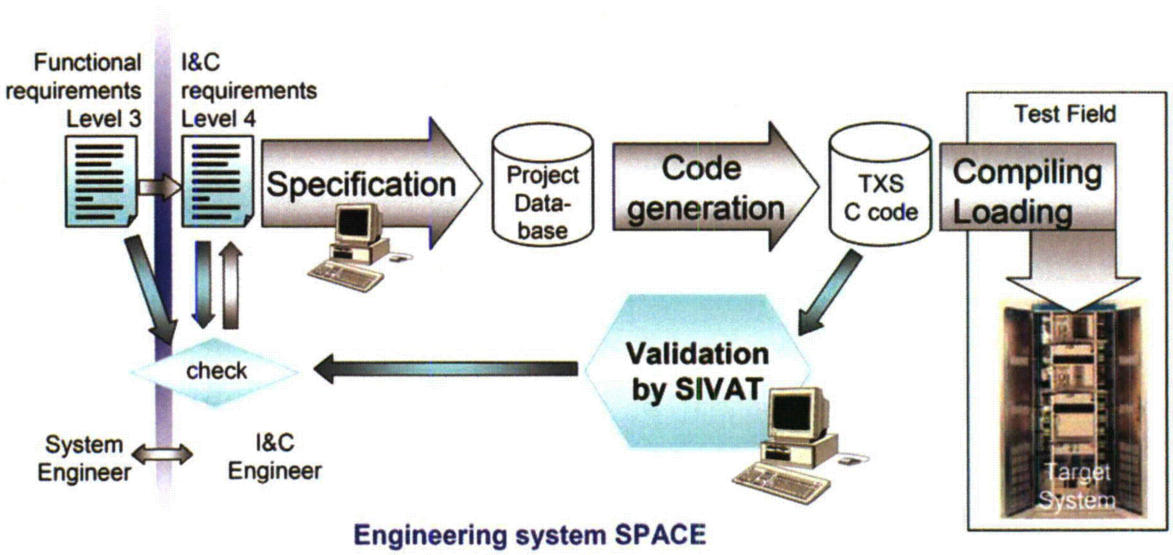

Figure 3-2 - SIVAT in the Application Software Development Process

3.3 Objectives for the SIVAT Tool

The SIVAT Tool is used to achieve the following objectives:

- Reproduce events in the simulator that occurred in installed TELEPERM XS systems.

To attain these goals, the SIVAT Tool has the following features:

- Utilization of a modern simulator control system (visualization of up to 400,000 signals/variables, restart ability).

- Restart capability using Initial Conditions (ICs).

- Easy integration of other models (e.g. process models).

- No real-time limitation (i.e., the simulation can run as fast as possible or can be run in slower time to support visual monitoring).

- Graphical user interface for easy handling of the automatic generation and user friendly interface with the simulation tool.

- Run on a LINUX workstation or a personal computer.

- Short time for generation of the simulator models.

3.4 TELEPERM XS Simulation Methodology

The I&C functionality of a TELEPERM XS System is achieved by interconnecting qualified Function Blocks (FBs). These FBs are stored for the target system in a precompiled library. The correct interconnection of FBs (assigning FB output and input signals) is implemented in the generated FD and Function Diagram Group (FDG) modules that are generated as C functions by the NRC-approved SPACE Code Generator.

The initialization of the Application Software is done in exactly the same way as in the real I&C system. The initialization is done by setting one global variable that is processed by the FBs. The original FB code is used for the initialization itself; thus, the following software modules are executing in the simulator:

The TELEPERM XS Simulation Components are shown in Figure 3-3.

A small part of the Runtime Environment (messages between TELEPERM XS CPUs and call of the FDGs), the FDGs, the Function Diagram modules, and the FBs contain the complete I&C functionality of a TELEPERM XS CPU. For a TELEPERM XS CPU model, these components are simulated in SIVAT.

Figure 3-3 - TELEPERM XS Simulation Components

3.5 TELEPERM XS Simulation Environment

3.5.1 SIVAT Components

SIVAT consists of three components:

- The simulator control system Simulation Development Environment (SDE),
- The Code Adaptation Tool for Simulator (CATS-SDE), which generates the TELEPERM XS models and controls the complete automatic generation process of the simulator, and
- A graphical user interface (GUI) specific to the TELEPERM XS simulation.

The SDE simulator control system used is made up of three components:

- The database administration program Database Editor (DBE),
- The database preprocessor Database Binder (DBB), and
- The control system Simulator Executive (SimEx).

The SIVAT components are shown in Figure 3-4.

3.5.2 SIVAT Simulation Modeling

Each TELEPERM XS CPU is represented by a model in the simulation environment, ensuring that all internal signals and variables of a CPU model are stored in the simulator database. This is achieved by generating the corresponding ADD files for the simulator control system with the help of CATS-SDE.

The CPU models are called by the control system according to their configured cycle time. SDE is able to process models with different cycle times. Models with shorter cycle times are called more frequently. Furthermore, CATS-SDE can generate an input and an output model. These models are used as a model for the measuring and actuating periphery of the TELEPERM XS System, by converting physical values into electrical values of analog signals and vice versa. This means that it is possible to simulate analog inputs with physical values. Furthermore, these models link external models (e.g., process models) with the TELEPERM XS models (see also Section 3.5.6).

There are various possibilities to simulate the input signals. Their values can be overwritten and are thus directly set in the SimDB. Or, transients can be specified by applying the ramp functionality. As another option, the values can be read in and assigned cyclically from data files, or the input values for TELEPERM XS can also be the output values of a process model. The SIVAT simulation environment is shown in Figure 3-5.

Figure 3-5 - SIVAT Simulation Environment

Just like all other signal and variable values, the values of the TELEPERM XS output signals are listed in the SimDB and can thus be visualized whenever required. Plot functions which support the writing of current signal or variable values in data files are also available.

Figure 3-6 - FDE Animation Mode

3.5.3 Simulator Database

All required signals and variables of the TELEPERM XS CPU models are stored in the SimDB. This enables the two main simulator features of signals and variables: visibility and overwritability. For this purpose, ADD files are generated by CATS-SDE, which list all variables used by the simulated TELEPERM XS CPUs. These files are then processed by the SDE tool DBE. The result is a database file that contains all TELEPERM XS model signals and variables (up to several hundred thousands).

By means of the ADD files, the respective required data structures are created in the size specified by the code generators. To be able to access the individual signals within these structures (pointers), links with the corresponding signal or variable name and the calculated offset relative to the beginning of the structure are created.

CATS-SDE ensures that all signals and variables that are calculated cyclically by the TELEPERM XS model are integrated in the database and thus stored at an IC. This guarantees that the simulation can be stopped at any time and an IC can be saved. By loading such an IC, it is possible to continue simulation at any time with the stored state.

Figure 3-7 - Data Structure in the Simulator Database

3.5.4 Simulation of Communication

Communication between the individual TELEPERM XS CPUs is implemented via messages that are generated by the SPACE Code Generator. The SPACE Code Generator specifies the message structure as well as the transmission path. Three paths are available for transmission depending on the network topology:

- The K32 backplane bus if the TELEPERM XS CPUs are arranged in the same subrack,
- The TELEPERM XS Profibus (L2) bus if there is an L2 network connection between the subracks, and
- The TELEPERM XS Ethernet (H1) bus if there is an H1 network connection between the subracks.

However, for simulation with SIVAT the transmission medium is irrelevant, since only the message structures are created. In the TELEPERM XS System, this structure is present in the sending, as well as in the receiving TELEPERM XS CPU. In the simulator it exists only once.

In the TELEPERM XS System, the Runtime Environment transfers the messages by utilizing functions of the MicroNET network system. These components are hardware-specific and are not simulated.

This form of communications simulation is completely sufficient for testing the specified I&C functionality. To examine the effects of failed communications links, the simulation of malfunctions is described in Section 3.5.5.

3.5.5 TELEPERM XS Malfunctions

To verify the effects of certain malfunctions on the specified I&C function, CATS-SDE generates three types of functions to simulate malfunctions that can be switched on or off via the corresponding flags in the SimDB:

3.5.6 Model Interfacing

The integration of the TELEPERM XS Application Software in SIVAT creates an open-loop simulation (i.e., the TELEPERM XS inputs can be stimulated by setting the corresponding signal values and by specifying transients). The behavior of the TELEPERM XS outputs can be recorded by generating data files and subsequently displayed as a graphic representation. The required response of the I&C to certain input signal modifications can thus be analyzed.

If a realistic feedback loop from the process or from one or several aggregates is required in order to evaluate the I&C behavior, separate models can be linked easily via a specified interface. This enables a partial or complete closed-loop simulation, and realistic events and disturbances can be simulated.

A simple example for an aggregate model is a valve model that is controlled by TELEPERM XS with an OPEN and CLOSE command and feeds the checkback signals and the current valve position back to TELEPERM XS. Such a model can be implemented with just a few lines of C or FORTRAN code and be integrated in SIVAT.

Principally, any number of separate models can be linked to the SIVAT simulator. Preconditions are that the models are available as C or FORTRAN functions, the model variables were stored in a simulator database using the SDE tool DBE, and the object code was compiled by the SDE-Tool DBB and the respective compiler. The object code is then available in a model library.

The open-loop / closed-loop simulation capability is shown in Figure 3-9.

The link between TELEPERM XS CPU models and the process model (or other models) is implemented via the TELEPERM XS input or output model. Loose links to process models are also possible. This procedure is preferable if the overhead is too high for completely integrating a complex process model in SIVAT or if the models are not available with source code. In this case, however, more overhead is generated in the synchronization of the models and the complete simulator cannot be restarted.

3.5.7 SIVAT Test Principles

The basic procedure for implementing SIVAT tests is described below using a simple example. Although there are many possibilities to control the simulation interactively three SDE tools DBE, DBB, and SimEx is provided as Tcl/Tk commands and is especially adapted to the simulation of I&C functions.

The typical process for SIVAT tests is shown in Figure 3-10. The test cases are formulated in test scripts based on a test specification in which the test objectives, the basic test conditions, and the structure of the test cases are described.

Figure 3-10 - SIVAT Test Process

The simple example below demonstrates the procedure for testing a limitation monitor (COMP MIN). The set point value is 7.5 kV and the hysteresis is 0.1 kV. Each test case is divided into three parts:

1. Initialization: The simulation time is set to an initial value (typically 0.0 seconds) to consistently obtain the same time reference in the data file (plot file). Furthermore, the start conditions for the input signals are set (in this example to 8.0 kV for the input signal). For more complex test objects, the initialization is usually implemented by loading an IC that serves as the base for several test cases (e.g. 100% reactor power, failure-free condition).

2. Plot Definition: The signals to be saved in the data file are specified by means of a ***plot***-command and added to the plot list. After the plot list has been defined, the data file is generated (command ***plot-open***).

3. Test Execution: The individual test steps are now executed in succession. In this example, a ramp is executed from 8.0 kV to 7.0 kV in 5 seconds to trigger the limit value. Then a ramp is executed again, this time back to 8.0 kV in 10 seconds, to check the hysteresis. Finally the plot file is closed.

A SIVAT test script example is shown in Figure 3-11.

The result of the test case is now listed in the plot file (in this example voltage_limit.dat) and can, for example, be visualized with the SIVAT plot tool based on ***gnuplot***. The result can be displayed on a monitor or printed out.

The result of the test case is now listed in the plot file (in this example voltage_limit.dat) and can, for example, be visualized with the SIVAT plot tool based on ***gnuplot***. The result can be displayed on a monitor or printed out.

An extract from a SIVAT plot file is shown in Figure 3-12. For each cycle (typically every 0.05 second), the plot function writes one line with the time stamp and the current values of the signals from the plot list to the plot file. The graphic representation of this plot file is shown next to the extract from the plot file. The results are evaluated manually based on the graphic outputs. Plot files can be consulted in cases of doubt.

3.6 Limitations of Simulation

As already mentioned in Section 3.1, the accuracy of the simulation depends on how well the models represent the systems. In Sections 3.2 through 3.5, the principles of SIVAT simulation were explained and it was demonstrated that the TELEPERM XS simulation is based on the original code of the Application Software (i.e., the simulation reflects the actual behavior of the specified I&C functions). Nevertheless, even TELEPERM XS simulations with SIVAT have their limitations that distinguish the verifying the I&C specification (analysis tools) independently of the simulation. The following system characteristics are not tested by SIVAT:

3.7 Simulation in the Test Field with ERBUS TELEPERM XS

3.7.1 Concept of the Test Field Simulator

The development of the ERBUS TELEPERM XS test field simulator system was based on existing and proven components. The following objectives were defined:

- Universal test system with a modular design that can be flexibly adapted to the respective requirements.

- Control via the network.

- Use of the simulator control system SDE already tried and tested with SIVAT.

The use of ERBUS in simulation testing with SIVAT is shown in Figure 3-13.

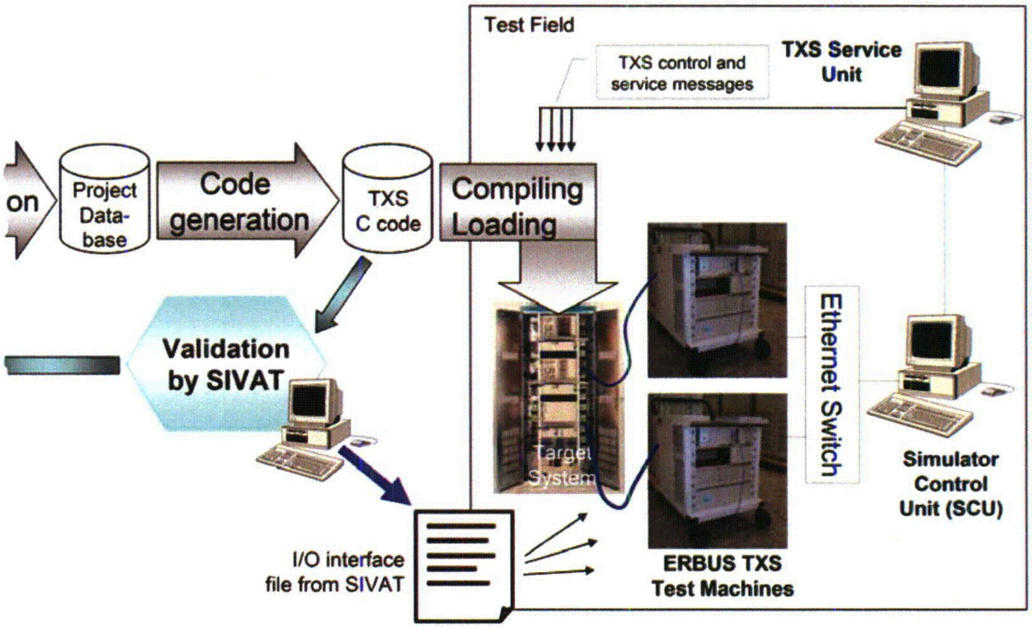

Figure 3-13 - ERBUS TELEPERM XS Concept

Following the manufacture of the cabinet, the TELEPERM XS system is set up in the test field. The objective is to commission the overall system and to test it. To do this, the TELEPERM XS Application Software is loaded onto the CPU modules in the TELEPERM XS cabinets and the TELEPERM XS inputs and outputs are linked with the ERBUS TELEPERM XS test machine outputs and inputs.

All test machines are connected to a central computer, the Simulator Control Unit (SCU). The SCU is the main component of the test field simulator. The same simulator control system that is used for SIVAT also runs on the SCU. Using a list of I/O signals that contains an assignment of the TELEPERM XS signals to the ERBUS TELEPERM XS channels, a simulator is generated. The SimDB contains a map of all TELEPERM XS I/O signals. There is one communications model for each connected test machine and Service Unit in the simulator. These models send or receive the respective assigned signals.

With the simulator in operation, the TELEPERM XS inputs are cyclically stimulated with the values in the SimDB via the ERBUS outputs, and the values at the TELEPERM XS outputs are cyclically entered into the SimDB.

Furthermore, the TELEPERM XS Service Unit (SU) can be linked with the SCU. In this case, the triggering of the TELEPERM XS inputs and outputs can also be implemented at the SU using the SMS.

The main task of the test field simulator is to stimulate and measure all inputs and outputs of a TELEPERM XS system. Depending on the size of the system, this can involve several hundred or even several thousand signals.

3.7.2 Model Interfacing

Due to the utilization of SDE as control system for ERBUS TELEPERM XS, the method of integrating process models could be adopted from SIVAT. The model interface is completely identical (i.e., the process models that were used for the simulation with SIVAT can also be used one-to-one for the test field simulation).

This possibility also permits a closed-loop simulation in the test field with minimum overhead and without time-consuming project-specific proprietary developments or additional hardware.

3.7.3 Limitations of Simulation with ERBUS TELEPERM XS

Unlike SIVAT, the ERBUS TELEPERM XS test field simulator does not model TELEPERM XS I&C. It only implements a hardware-based control of the inputs and outputs of the actual TELEPERM XS system using the communication models. If other models are integrated, they respond in exactly the same way as in the SIVAT simulator due to the same control system and interface.

The only limitation of the simulation with the ERBUS TELEPERM XS test field simulator results from the dynamic response of the overall system. The simulator, as well as the software on the test machines, operates with a fixed cycle time of 50 milliseconds. Like the TELEPERM XS CPUs, they are not synchronized. This results in system dependent signal propagation delays between setting the value in the SimDB and outputting the corresponding hardware signal. The same applies to reading of hardware signals.

The delay between setting the signal value in the SimDB and triggering the corresponding value with a suitable short-circuited ERBUS output-input is approximately 250 milliseconds. Thus, no response time measurements can be done using this system.

4.0 APPLICABLE REGULATORY GUIDANCE

The applicable regulatory guidance documents are identified and addressed below.

4.1 Regulatory Guide 1.173 - Software Life Cycle Processes

Regulatory Guide 1.173 (Reference 9) endorses IEEE Std 1074-1995 (Reference 23). NRC reviewed the TELEPERM XS software life cycle process as part of the review of the TELEPERM XS Topical Report (Reference 28). NRC approved the TELEPERM XS Topical Report in a safety evaluation report (SER) issued in May 2000 (Reference 25). NRC made the following conclusion in the SER:

> 2.2.2.2 Software Management Plan
>
> The software management plan for development of a Siemens digital safety system is the same procedure as used for all Siemens safety-critical software development projects. The software management plan is incorporated into Siemens Engineering Procedure FAW-1.1, "Software Life-Cycle Processes." FAW-1.1 specifies the management structure and the processes to be used in the project. This procedure is compatible to IEEE-1074, "Developing Life Cycle Process," and is, therefore, acceptable.

This conclusion is applicable to the SIVAT software, since the software was developed in accordance with the TELEPERM XS software development process described in Section 6.0.

4.2 Regulatory Guide 1.169 - Software Configuration Management,"

Regulatory Guide 1.169 (Reference 5) endorses IEEE Std 828-1990 (Reference 16) and IEEE Std 1042-1987 (Reference 22). NRC reviewed the TELEPERM XS software configuration management process as part of the review of the TELEPERM XS Topical Report. NRC made the following conclusions in the SER:

2.2.2.5 Software Configuration Management Plan

Configuration management activities are controlled by Siemens Engineering Procedure FAW-1.5, "Configuration Management," which outlines the procedures and tools for creating and implementing the configuration management structure and procedures. This procedure is compatible to IEEE-828, "Software Configuration Management Plan," and is, therefore, acceptable.

and

2.2.4 Configuration Management

The staff found that the configuration management procedure FAW-1.5 is compatible to IEEE-1042, "IEEE Guide to Software Configuration Management," and is, therefore, acceptable.

Theses conclusions are applicable to the SIVAT software, since the software was developed in accordance with the TELEPERM XS software configuration management process described in Section 15.0.

4.3 Regulatory Guide 1.168 - Software Verification and Validation

Regulatory Guide 1.168 (Reference 4) endorses IEEE Std 1012-1998 (Reference 20) and IEEE Std 1028-1997 (Reference 21). NRC reviewed the TELEPERM XS software verification and validation process as part of the review of the TELEPERM XS Topical Report. NRC made the following conclusions in the SER:

2.2.2.14 Software Verification and Validation Plan (SVVP)

The processes for conducting software verification and validation (V&V) activities are described in Siemens Engineering Procedure FAW-1.6, "Verification and Validation Plan." FAW-1.6 specifies the areas of application, the organizational responsibilities, requirements for IV&V

activities, and requirements for documentation. This procedure is compatible to IEEE-1012, "Software Verification and Validation Plans," and is, therefore, acceptable. The requirements for V&V are described in IEC-880-1986, "Software for safety Systems in Nuclear Power Stations," which Siemens has followed throughout the life cycle. IEC-880 is compatible to IEEE-7-4.3.2, "IEEE Standard for Digital Computers in Safety Systems of Nuclear Power Generating Stations," and is, therefore, acceptable.

NRC also documented in SER Sections 2.2.2.8, 2.2.2.10, and 2.2.2.12 that the TELEPERM XS software review process

described in Siemens Engineering Procedure FAW-4.2, "Reviews." This procedure describes the software review process, including responsibilities, review methods, the review processes, and activities to be performed after the review is completed. This procedure is compatible to IEEE-1028, "Software Review and Audit," and is, therefore, acceptable.

And, the TELEPERM XS software verification and validation process was further evaluated:

2.2.3 Development and V&V Organization and Process

The V&V processes are defined in Siemens Engineering Procedure FAW-1.6, "Verification and Validation Plan." This plan specifies all activities performed during the safety system development process. The responsibility for V&V activities is with the person responsible for the system or module development. This procedure is compatible to IEEE-1012, "Software Verification and Validation Plans," and is, therefore, acceptable. Siemens internal V&V processes were performed by members of the same development team, a member of another team within the digital I&C organization, or by employees outside the digital I&C organization. The person performing the internal V&V activity was not the same

> person who generated the product to be reviewed. External IV&V activities were performed by TÜV organizations and iSTec.

This conclusion is applicable to the SIVAT software, since the software was developed in accordance with the TELEPERM XS software development process described in Section 6.0.

4.4 Regulatory Guide 1.171 - Software Unit Testing

Regulatory Guide 1.171 (Reference 7) endorses IEEE Std 1008-1987 (Reference 19). NRC reviewed the TELEPERM XS software test process as part of the review of the TELEPERM XS Topical Report. NRC made the following conclusion in the SER:

> 2.2.3 Development and V&V Organization and Process
>
> Validation activities include testing the application to ensure it performs according to the system requirements. These activities are controlled by Siemens Engineering Procedure FAW-4.1, "Testing." Testing includes specifying the test requirements, performing the tests, and producing the test report. Testing includes module testing, component testing, and system testing in a simulated and real environment. This procedure is compatible to IEEE-1008, "Software Unit Testing," and is, therefore, acceptable.

This conclusion is applicable to the SIVAT software, since the software was developed in accordance with the TELEPERM XS software development process described in Section 6.0 and the test documentation requirements defined for the use of SIVAT in Section 11.3.

4.5 Regulatory Guide 1.170 - Software Test Documentation

Regulatory Guide 1.170 (Reference 6) endorses IEEE Std 829-1983 (Reference 17). NRC reviewed the TELEPERM XS software test documentation process as part of the review of the TELEPERM XS Topical Report. NRC made the following conclusion in the SER:

> 2.2.2 Software Documentation
>
> This section summarizes the software documentation associated with the TXS system development. The type tests of the TXS software components were performed in accordance with German standard KTA-Standard 3503. The principles of type testing and the test activities were defined from this standard. These were applied to the following areas: separation in the theoretical and practical tests, institutions to be involved in type tests, roles of these institutions in type tests, and documentation of type tests.
>
> The content of the theoretical and practical tests is defined by the software standard DIN IEC-880. KTA standards also require that the present state-of-the-art be taken into account during the qualification. In addition to KTA-1401, which defines criteria for quality assurance systems, the following software standards were applied and verified:
>
> - IS0-9000-3, "Management for Quality and Requirements of Quality Assurance,"
> - IEEE-830, "Software Requirement Specifications,"
> - IEEE-828, "Software Configuration Management Plan,"
> - IEEE-1012, "Software Verification and Validation Plans,"
> - IEEE-829, "Software Test Documentation,"
> - IEEE-1008, "Software Unit Testing,"
> - IEEE-1028, "Software Reviews and Audits," and

- ANSI/ANS-10.4, "Verification and Validation of Scientific Engineering Programs for the Nuclear Industry."

This conclusion is applicable to the SIVAT software, since the software was developed in accordance with the TELEPERM XS software development process described in Section 6.0 and the test documentation requirements defined for the use of SIVAT in Section 11.3.

4.6 Regulatory Guide 1.172 - Software Requirements Specifications

Regulatory Guide 1.172 (Reference 8) endorses IEEE Std 830-1993 (Reference 18). NRC reviewed the TELEPERM XS software requirements development process as part of the review of the TELEPERM XS Topical Report. NRC made the following conclusion in the SER:

> 2.2.2.6 Hardware and Software Specification
>
> The procedure for controlling the hardware and software specifications is Siemens Engineering Procedure FAW-3.3, "Organization of the General Specification for SW and HW Components." This procedure governs the organization of the specifications for the digital safety systems created under this set of tools and processes. This procedure is compatible to IEEE-830, "Software Requirement Specifications," and is, therefore, acceptable.

4.7 Alignment with IEEE Std 1012-1998 Testing Activities

IEEE Std 1012-1998 describes four testing activities:

> Component Testing: Testing conducted to verify the correct implementation of the design and compliance with program requirements for one software element (e.g., unit, module) or a collection of software elements. (Clause 3.1.3)

Integration Testing: An orderly progression of testing of incremental pieces of the software program in which software elements, hardware elements, or both are: combined and tested until the entire system has been integrated to show compliance with the program design, and capabilities and requirements of the system. (Clause 3.1.10)

System Testing: The activities of testing an integrated hardware and software system to verify and validate whether the system meets its original objectives. (Clause 3.1.26)

Acceptance Testing: Testing conducted in an operational environment to determine whether a system satisfies its acceptance criteria (i.e., initial requirements and current needs of its user) and to enable the customer to determine whether to accept the system. (Clause 3.1.1)

IEEE Std 1012-1998 Figure 2 shows a progression of test activities (i.e., component, integration, system, and acceptance testing) occurring during the development process (i.e., design, implementation, and test activities).

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 4-1.

AREVA NP intends to use of the SIVAT Tool to support validation testing of TELEPERM XS Application Software as shown by the blue-shaded box shown in Table 4-1.

The decision to use the SIVAT Tool for validation testing requires that the SIVAT Tool development process conformance with clause 5.3.2 of IEEE Std 7-4.3.2-2003 (Reference 14).

Table 4-1 - Alignment with IEEE Std 1012-1998 Testing Activities

<table>
<tr><th>IEEE Std 1012-1998 Testing Activity</th><th>Generic TELEPERM XS Testing</th><th>Project-Specific Testing</th></tr>
<tr><td>Component Testing</td><td>X
(hardware and software type tests, including Function Blocks)</td><td>Not Applicable
(based on use of qualified hardware and software modules)</td></tr>
<tr><td rowspan="2">Integration Testing</td><td rowspan="2">X</td><td>Application Software: SIVAT for integration of Function Block modules
Optional X
(see Note 1)</td></tr>
<tr><td>System Components: Pre-Factory Acceptance Test (FAT) prerequisites and procedure dry runs (manufacturing tests)</td></tr>
<tr><td>System Testing</td><td>X</td><td rowspan="2">X
(integrated in system testing, including FAT, based on use of qualified system components and development tools)</td></tr>
<tr><td>Acceptance Testing</td><td>Not Applicable</td></tr>
</table>

Legend: X indicates alignment with IEEE Std 1012-1998 testing.

Note 1 – Additional Application Software integration and functional test cases to validate engineering I&C functionality are added to the scope of system validation testing for the case where SIVAT testing is not used for Application Software integration and functional testing to satisfy IEEE Std 1012-1998 validation requirements. Validation testing with SIVAT is performed as an IEEE Std 1012-1998 Implementation Activity task.

4.8 Conformance with IEEE Std 7-4.3.2-2003

IEEE Std 7-4.3.2-2003 contains the following guidance for software tools used to support software development processes and verification and validation processes:

5.3.2 Software tools

Software tools used to support software development processes and verification and validation (V&V) processes shall be controlled under configuration management.

One or both of the following methods shall be used to confirm the software tools are suitable for use:

a) A test tool validation program shall be developed to provide confidence that the necessary features of the software tool function as required.

b) The software tool shall be used in a manner such that defects not detected by the software tool will be detected by V&V activities.

Tool operating experience may be used to provide additional confidence in the suitability of a tool, particularly when evaluating the potential for undetected defects.

IEEE Std 7-4.3.2-2003 has been endorsed by NRC in NRC Regulatory Guide 1.152 (Reference 3).

SIVAT conforms to the guidance in clause 5.3.2 of IEEE Std 7-4.3.2-2003. SIVAT was developed and is maintained within the TELEPERM XS configuration management process, described in Sections 4.2 and 15.0.

SIVAT was validated against test field data from the TELEPERM XS I&C modernization projects at the Unterweser and Philippsburg 1 nuclear power plants, as described in Section 14.1.

The limitations of SIVAT are clearly identified and understood, as described in Section 3.6. The system characteristics not tested by SIVAT are either tested during the TELEPERM XS generic qualification process, verified with other TELEPERM XS analysis tools, or validated during system validation testing, as described in Section 11.2. It must also be understood that validation testing with SIVAT is just one component of the overall verification and validation program used for Application Software development, as described in the TELEPERM XS Software Program Manual.

AREVA NP has operating experience with the use of SIVAT for more than 20 project specific applications, as described in Section 14.3.

In addition, the SIVAT software was developed with a high quality development process as described in Sections 5.0 through 16.0 that were performed in accordance with the AREVA NP quality assurance (QA) program.

4.9 Consistency with IEEE Std 1008-1987

The benefit of Application Software validation testing with SIVAT is the early detection of faults. A balance is drawn between performing Application Software validation testing during the FAT later in the development process and performing Application Software validation testing with SIVAT earlier in the process. IEEE Std 1008-1987 recognizes that:

> There are significant economic benefits in the early detection of faults. This implies that test set development should start as soon as practical following availability of the unit requirements documentation because of the resulting requirements verification and validation. It also implies that as much as practical should be tested at the unit level. (Paragraph B2.4)

The early detection of Application Software faults through validation testing with SIVAT serves to reduce project risks earlier in the development process.

The SPACE-generated code should be validated in a testing environment by means of the SIVAT simulation tool. The purpose of the simulation is to test the generated TELEPERM XS Application Software with regard to the way the process engineering tasks and/or the I&C function specification are implemented in the I&C. This is to identify any Application Software errors as soon as possible, and prove the fulfillment of the requirements.

4.10 Alignment with IEC 60880 Requirements for Tools

IEC 60880 (Reference 12) contains requirements for the development and use of software tools. This standard was used by AREVA NP in the development of the SIVAT Tool. The relevant sections of IEC 60880 related to software tools are discussed below.

IEC 60880 Section 8.2.3.2.2 suggests that software written in application-oriented languages shall be verified to be functionally correct and consistent, for example by manual inspection or by the use of automated tools which allow simulated running of the software in a debug environment. SIVAT is the TELEPERM XS tool that supports the verification and validation of Application Software in a simulation environment.

IEC 60880 Section 8.2.3.2.5 requires that software tools used for verification or validation shall be qualified as required by Clause 14. The elements of Clause 14 are addressed separately below.

IEC 60880 Section 14.1.1 states that software tools are most powerful when they are defined to work co-operatively with each other. It also notes that care should be taken not to require tools to undertake tasks beyond their capability, for example, they cannot replace humans when judgment is involved. It goes on to state that when selecting a tool, the benefits and risk of using a tool must be balanced against the benefits and risk of not using a tool. And finally, it suggest that the important principle is to choose tools that limit the opportunity for making errors and introducing faults, but maximize the opportunity for detecting faults.

SIVAT was developed specifically as part of the TELEPERM XS technology system as described in Section 3.0 of this report. The limitations of SIVAT are clearly identified and understood, as described in Section 3.6. The system characteristics not tested by SIVAT are either tested during the TELEPERM XS generic qualification process, verified with other TELEPERM XS analysis tools, or validated during system validation testing, as described in Section 11.2. The benefits testing with SIVAT are described in Section 11.0 of this report and are contrasted with the potential risk described in Section 13.0.

IEC 60880 Section 14.2 discusses the selection of tools and specifies that tools shall be selected to support the software engineering process. It states that the limits of applicability of all tools shall be identified and documented. It also states that tools shall have sufficient reliability to ensure that they do not jeopardize the reliability of the end product.

SIVAT has been specifically developed to support the TELEPERM XS Application Software development process, as described in Section 3.2 of this report. The limitations of SIVAT are clearly identified and understood, as described in Section 3.6. SIVAT was developed to have high reliability, as described in Section 4.8.

IEC 60880 Section 14.3.1 addresses the software engineering environment for tools. The SIVAT engineering process is described in Section 6.0 of this report. The results of the SIVAT development process are described Section 3.0.

IEC 60880 Section 14.3.2 addresses tool qualification. The qualification of the SIVAT Tool is described in Section 14.0 of this report.

IEC 60880 Section 14.3.3 addresses tool configuration management. Configuration management for the SIVAT Tool is discussed in Section 15.0 of this report.

IEC 60880 Section 14.3.4 addresses translators and compilers and is not applicable to the SIVAT Tool, since it is not a translator or compiler. The SPACE tool is the TELEPERM XS translator and compiler.

IEC 60880 Section 14.3.5 addresses application data tools and is not applicable to the SIVAT Tool, since it is not an application data tool.

IEC 60880 Section 14.3.6 discussed automation of testing and is not applicable to the SIVAT Tool. The use of the SIVAT Tool to support Application Software verification and validation activities is described in Section 11.0 of this report. The Independent Verification and Validation Group designs test specifications, test cases, and test procedures to achieve the required coverage. The Independent Verification and Validation Group also analyzes the test results to established acceptance criteria. These aspects of testing with the SIVAT Tool are not automated.

Figure 5-1 in this report aligns with the lifecycle for application orientated software engineering shown in Figure C-1 shown in IEC 60880.

4.11 Alignment with Branch Technical Position 7-14

NRC Branch Technical Position 7-14 (Reference 10) addresses software tools at several points.

> **B.3.1 Acceptance Criteria for Planning**
>
> <u>**Acceptance Criteria for Resources Characteristics of Planning Documents**</u>
>
> Methods/tools - It is important to remember that if the output of any tool can not be proven to be correct, such as may occur if the tool produces machine language software code, the tool itself should be developed or dedicated as safety-related, with all the attendant requirements.

SIVAT is not used to produce machine language software code. The SPACE Tool Code Generator is used for this purpose and is classified as safety-related.

B.3.1.2.3 Resource Characteristics of the SDP

Methods/tools involves a description of the software development methods, techniques and tools to be used. The approach to be followed for reusing software should be described. The SDP should identify suitable facilities, tools and aids to facilitate the production, management and publication of appropriate and consistent documentation and for the development of the software. It should describe the software development environment, including software design aids, compilers, loaders, and subroutine libraries. 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. Methods, techniques and tools that produce results that cannot be verified or that are not compatible with safety requirements should be prohibited, unless analysis shows that the alternative would be less safe.

SIVAT conforms to the guidance in clause 5.3.2 of IEEE Std 7-4.3.2-2003, which ensures that it is qualified with the degree of rigor and level of detail appropriate for a validation tool for safety-related software.

B.3.1.2.4 Review Guidance for the SDP

Under the Resource Characteristics, the methods and tools to be used should be evaluated. Of particular interest is the method by which the output of software tools, such as compilers or assemblers, will be verified to be correct. The criteria from IEEE Std 7-4.3.2-2003 is that software tools should be used in a manner such that defects not detected by the software tool will be detected by V&V activities. If this is not possible, the tool itself should be safety-related.

SIVAT conforms to the guidance in clause 5.3.2 of IEEE Std 7-4.3.2-2003, which ensures that it is qualified with the degree of rigor and level of detail appropriate for a validation tool. The limitations of SIVAT are clearly identified and understood, as described in Section 3.6 of this report. The system characteristics not tested by SIVAT are either tested during the TELEPERM XS generic qualification process, verified with other TELEPERM XS analysis tools, or validated during system validation testing in the test field, as described in Section 11.2. It must also be understood that validation testing with SIVAT is just one component of the overall verification and validation program used for Application Software development, as described in the TELEPERM XS Software Program Manual.

B.3.1.4.3 Resource Characteristics of the SIntP

Methods/tools refers to a description of the methods, techniques and tools that will be used to accomplish the integration function. The SIntP should require that integration tools be qualified with a degree of rigor and level of detail appropriate to the safety significance of the software which is to be created using the tools.

SIVAT is not used to produce or integrate software code. SIVAT conforms to the guidance in clause 5.3.2 of IEEE Std 7-4.3.2-2003, which ensures that it is qualified with the degree of rigor and level of detail appropriate for a validation tool.

B.3.1.5.3 Resource Characteristics of the SInstP

Methods/tools involves a description of the methods, techniques and tools that will be used to accomplish the installation function. The SInstP should require that installation tools be qualified with a degree of rigor and level of detail appropriate to the safety significance of the software which is to be installed using the tools.

SIVAT is not used to install software code. SIVAT conforms to the guidance in clause 5.3.2 of IEEE Std 7-4.3.2-2003, which ensures that it is qualified with the degree of rigor and level of detail appropriate for a validation tool.

B.3.1.10.3 Resource Characteristics for the SVVP

Methods/tools involves a description of the methods, equipment, instrumentation and tools used to carry out each V&V task. Test methods should be specified for unit, integration, validation, installation and regression testing. The SVVP should specify a process for selecting tools. The hardware and software environment within which the V&V tools are to be applied and any necessary controls should be described.

AREVA NP intends to use of the SIVAT Tool to support validation testing of TELEPERM XS Application Software. SIVAT conforms to the guidance in clause 5.3.2 of IEEE Std 7-4.3.2-2003, which ensures that it is qualified with the degree of rigor and level of detail appropriate for a validation tool.

5.0 SIVAT MANAGEMENT PLAN

SIVAT was originally developed during the years 1998-1999 to provide a simulation-based test environment to support the development of project-related TELEPERM XS Application Software.

5.1 Use of SIVAT within TELEPERM XS Technology

The TELEPERM XS Topical Report describes the simulator-based validation process for TELEPERM XS Application Software in Section 2.4.3.3.2. The simulator-based validation tool described in the report is SIVAT. The role of the simulator-based validation tool in the standard AREVA NP engineering process for TELEPERM XS project implementation is shown in Figure 5-1 (TELEPERM XS Topical Report Figure 2.8). The correctness of TELEPERM XS code generation in the course of application projects is covered by validation activities (i.e., software validation testing with SIVAT or during system testing).

TELEPERM XS Application Software is developed using the SPACE tool FDE. This tool is used to develop FDs and Network Diagrams. FDs specify the signal processing requirements for the system. Network Diagrams define the hardware components of the system and their logical interconnections. Software code is automatically generated from the FDs and Network Diagrams by the SPACE code generators. The project-specific TELEPERM XS System is developed from qualified hardware and software modules using the NRC-approved development tools. Logical 'software integration' occurs at this stage.

SIVAT was designed to be used to support validation testing of the Application Software prior to installation into the target hardware. The validation test cases are created on the basis of the functional requirements defined for the Application Software. These validation activities serve to validate the detailed software engineering performed with the SPACE tool.

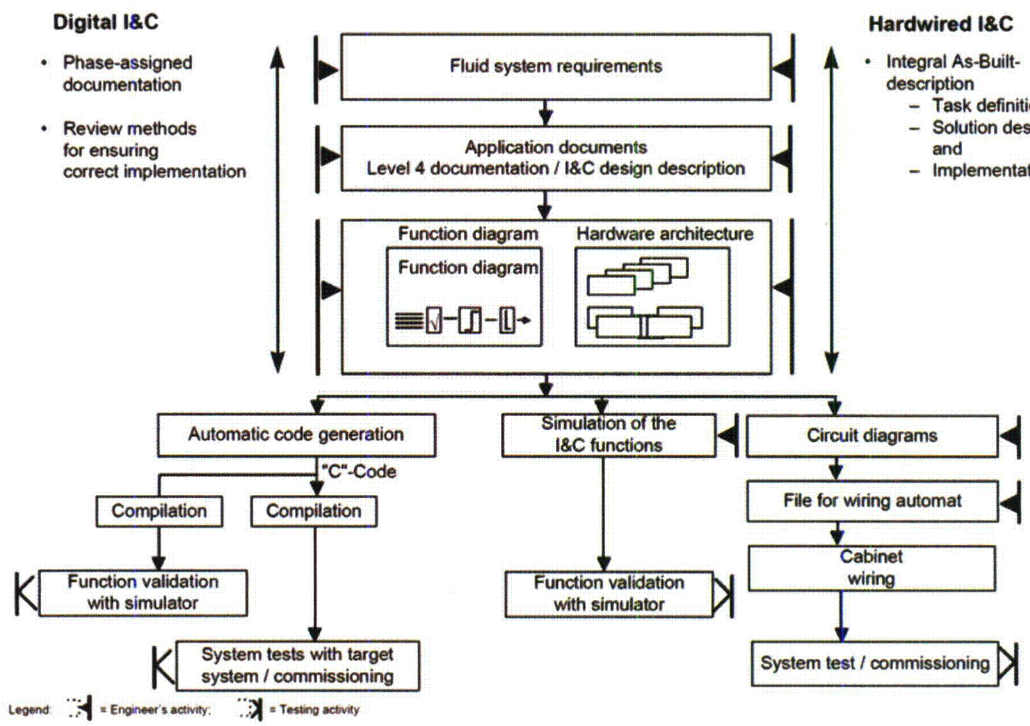

Figure 5-1 - Procedure for Designing Hardwired and Digital I&C Systems

The TELEPERM XS System Software development process is described in Section 3.2 of the TELEPERM XS Topical Report. The associated development process implementing procedures are summarized in Section 5 of the TELEPERM XS Topical Report.

5.2 Key Interfaces

The processes to develop and use the SIVAT Tool have key interfaces with other TELEPERM XS Topical Reports and the AREVA NP QA programs. Section 5.2.1 describes the interface with the TELEPERM XS Topical Report. Section 5.2.2 describes the interface with the TELEPERM XS Software Program Manual. Section 5.2.3 describes the interface with the AREVA NP QA programs.

5.2.1 Interface with the TELEPERM XS Topical Report

The TELEPERM XS Topical Report describes the generic development and qualification process for the TELEPERM XS digital I&C system.

SIVAT was developed under the same QA program and software lifecycle development process and procedures as described in the TELEPERM XS Topical Report. The SIVAT development environment is governed by the AREVA NP GmbH information security program. SIVAT was developed in accordance with the following AREVA NP GmbH procedures:

- Engineering Procedure FAW-TXS-1.1, Phase Model for the Development of Software Components for TELEPERM XS (Reference 31)

  SIVAT was developed based on a requirements specification and technical specification document. The results of the SIVAT development process are described in Section 3.0 of this Topical Report.

- Engineering Procedure FAW-TXS-1.5, Configuration Management Plan for the TELEPERM XS System Platform (Reference 32)

  Changes to the SIVAT Tool are controlled via FAW-TXS-1.5, which establishes requirements to ensure that changes are controlled, documented, and tested. The configuration management plan is described in Section 15.0 of this report.

- Engineering Procedure FAW-TXS-1.6, Software Verification and Validation Plan (Reference 33)

  The validation of the product was performed with tests of a real TELEPERM XS application (data from a test) and the results of a SIVAT simulation of the same application. The verification and validation process for SIVAT is described in Section 14.0 of this report.

NRC reviewed these and other procedures as well as the QA program as part of the review of the TELEPERM XS Topical Report (see References 26 and 27). NRC approved the TELEPERM XS Topical Report in a safety evaluation report issued in May 2000.

Engineering Procedures FAW-TXS-1.1 and FAW-TXS-1.6 have not changed since the TELEPERM XS Topical Report was issued.

Engineering Procedure FAW-TXS-1.5 has evolved since the TELEPERM XS Topical Report was issued. The changes include the addition of a change control board to the configuration management process and the inclusion of additional detail describing configuration management tasks (e.g., more precise configuration identification).

Section 6.0 of this Topical Report describes the development plan for the SIVAT Tool. Section 7.0 of this Topical Report describes the quality assurance plan for the SIVAT Tool. Section 14.0 of this Topical Report describes the verification and validation plan for the SIVAT Tool. Section 15.1 of this Topical Report describes the configuration management plan for the development of the SIVAT Tool. Section 16.0 of this Topical Report describes the test plan for changes to the SIVAT Tool.

5.2.2 Interface with the TELEPERM XS Software Program Manual

The TELEPERM XS Software Program Manual describes the overall lifecycle development process used for the development of project-specific TELEPERM XS Application Software.

AREVA NP intends to use the SIVAT Tool to support project-specific validation testing of TELEPERM XS Application Software developed in accordance with the TELEPERM XS Software Program Manual.

Section 11.0 of this Topical Report describes the use of for the SIVAT Tool for project-specific validation testing. Section 12.0 of this Topical Report describes the training plan for the use of the SIVAT Tool. Section 15.3 describes the software configuration management plan that would be used to control the SIVAT software obtained from AREVA NP GmbH for use on for TELEPERM XS projects.

5.2.3 Interface with AREVA NP Quality Assurance Programs

All design work, products, and services provided for a TELEPERM XS project in the U.S. are performed to the requirements of the AREVA NP Quality Management Manual (Reference 30), which implements the requirements of 10 CFR Part 50 Appendix B (Reference 2).

AREVA NP's implementation of the Quality Management Manual is periodically audited by the Nuclear Procurement Issues Committee (NUPIC). The NUPIC program evaluates suppliers furnishing safety-related components and services and commercial grade items to nuclear utilities. In addition, NRC periodically conducts inspections of AREVA NP (including AREVA NP GmbH) as part of the supplier inspection program.

AREVA NP purchases TELEPERM XS System Software (including the SIVAT Tool) that is developed by AREVA NP GmbH under its QA program. AREVA NP GmbH is an approved supplier per AREVA NP's approved supplier list.

5.3 Organization

The TELEPERM XS software development organization (AREVA NP GmbH) is organized in accordance with responsibility and authorities for the generic platform software lifecycle activities. This organization is also responsible for SIVAT Tool development. The organizational structure is shown in Figure 5-2.

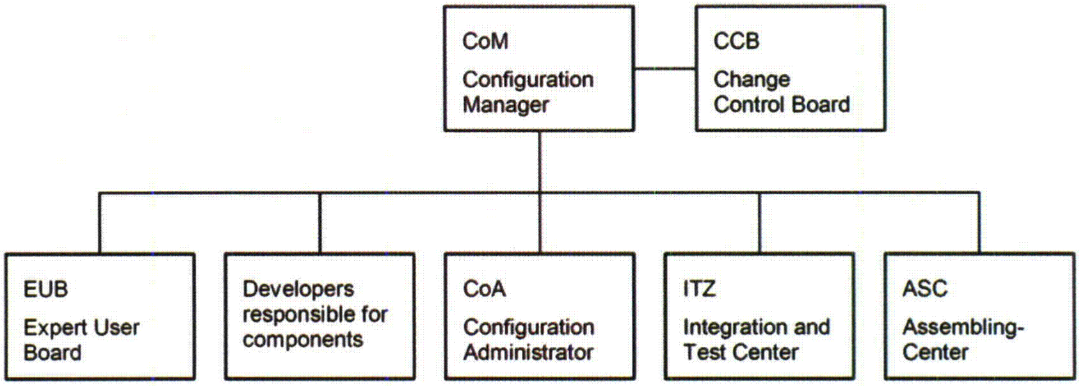

Figure 5-2 - Organizational Structure

5.3.1 Roles and Responsibilities

The following roles and responsibilities are defined for the TELEPERM XS platform software and software tool development activities.

- CCB: Change Control Board

  The CCB is a body comprising personnel from management, marketing, project development (TELEPERM XS users), and system support that controls important changes and the further development of the TELEPERM XS system platform from a strategic and business viewpoint as well as from the user's viewpoint.

  The CoM is appointed by the CCB and reports back to them at regular intervals.

- CoM: Configuration Manager

  The CoM defines the product structure, determines the configuration planning, initiates and monitors all activities in the CM and decides on

  - Content of a change plan
  - Scope, implementation and approval of change requests (CRs)

- Release of components and packages

- Content and release of Product Information documents

The CoM is supported by the CoA.

- CoA: Configuration Administrator

  The CoA is responsible for the activities of the change and release procedures and for continuous recording of the configuration documents, which also includes the generation of Product Information documents.

  The CoA is appointed by the CoM.

- EUB: Expert User Board

  The EUB is a body of experienced TELEPERM XS users, TELEPERM XS developers, the CoA and the CoM (CoM only when required). The composition of this body varies in accordance with the problem under discussion. The CoM is responsible for selection of the members. The CoA is responsible for its organization, the preparation of statements and reporting of results.

  The tasks of the body are:

  - To assess CRs that affect important aspects of the concept of the TELEPERM XS system platform

  - Development of strategies for individual components of the TELEPERM XS system platform and specification of the individual steps for following a strategy

  - Development of a long-term product strategy and determining the individual steps in its implementation

- Developers Responsible for Components

These persons are responsible for maintenance and further development of those configuration items (software or hardware components) within their responsibility, as well as for documenting implemented changes in the development documentation and in the change and release procedures. The area of responsibility also includes compliance with the development specifications and application of the relevant QA procedures including the CM activities.

- ITZ: Integration and Test Center

  The ITZ integrates new configurations into packages and checks the mutual interface compatibility of configuration items and packages, as well as the proper functioning of commonly used software and hardware configurations.

- ASC: Assembling Center

  The ASC supplies packages in traceable form to external and internal customers and performs software installation on customer's computers in accordance with the installation guidelines.

The activities of the software development organization are periodically audited by the Quality Assurance organization.

5.4 Problem Reporting

This section defines the AREVA NP (Inc) responsibilities and requirements for identifying, processing, and resolving problems and discrepancies identified with the TELEPERM XS SIVAT Tool during validation testing of Application Software developed by AREVA NP (Inc). The AREVA NP (Inc) problem reporting process handles hardware and software component problems, nonconformances, verification and validation and testing anomalies, reporting of defects and noncompliance in accordance with 10 CFR Part 21 (Reference 1), as well as user suggestions and potential product improvements.

AREVA NP (Inc) employees working on TELEPERM XS projects or using the TELEPERM XS software are responsible for following the methods and principles described in this section. Each employee who identifies a discrepancy, potential for improvement, a nonconformance, or a potential safety concern related to the SIVAT Tool must ensure that this deficiency or problem is clearly identified and reported, such as by recording error messages, producing screen shot copies, or creating a memory dump.

5.4.1 Corrective Action Program

The AREVA NP (Inc) Corrective Action Program (Reference 34) establishes the process for promptly identifying and correcting conditions adverse to safety and quality in addition to providing the means for customer notification of these conditions. The Corrective Action Program also establishes the means for the identification and resolution of near miss problems, customer identified problems, and complaints. The condition report process implements a graded approach to managing adverse conditions. Condition report process actions are based on the significance, that is, Levels 1, 2, 3, or 4, associated with the adverse condition. An evaluation is performed and documented in the Corrective Action Program to determine if previous similar projects and customers are affected by the problem identified with the SIVAT Tool. AREVA NP (Inc) will assign actions to AREVA NP GmbH for evaluation and resolution of any problems identified with the SIVAT Tool.

Items from the Open Items list (discussed in Section 5.4.2) are reviewed for conditions adverse to quality and safety, which are entered into the Corrective Action Program. Additionally, problems identified after delivery (see Section 5.4.4) are entered into the Corrective Action Program. The NRC reporting requirements of 10 CFR Part 21 are then evaluated. If required, a report is made in accordance with the AREVA NP (Inc) procedures and affected customers are notified of any SIVAT Tool problems affecting installed TELEPERM XS Application Software.

5.4.2 Open Items Process

Identified issues or Open Items are documented, and the organization responsible for the design evaluates and resolves them. Open Items are collected in a project-specific database as they are identified. AREVA NP (Inc) forwards Open Items associated with the SIVAT Tool to AREVA NP GmbH for evaluation and resolution. Open Items that involve conditions adverse to quality and safety are entered into the Corrective Action Program.

For each Open Item, a brief description and a reference that describes the origin and the reason for the Open Item is documented in the database.

Although the Open Items database is the tool by which the Open Items are processed and managed, it does not satisfy the record keeping requirements of Appendix B of 10 CFR Part 50. Therefore, individual Open Item forms for project Open Items are stored in the AREVA NP Records Management System at the end of the project as a part of final documentation.

5.4.3 Discrepancies Identified by Testing

Discrepancies identified by AREVA NP (Inc) during testing are first recorded in a test discrepancy log and evaluated with the Software Design Group to determine if the problem resolution lies in revising the test plan or procedures or if the discrepancy is a software problem that may result in a modification. AREVA NP (Inc) will forward problems identified with the SIVAT Tool to AREVA NP GmbH for evaluation and resolution.

5.4.4 Discrepancies Identified after Release to the Customer

Discrepancies identified with the SIVAT tool by either AREVA NP (Inc) or AREVA NP GmbH after TELEPERM XS Software release to the customer are to be handled in accordance with the Quality Management Manual and the Corrective Action Program. The NRC reporting requirements of 10 CFR Part 21 are evaluated. If required, a report is made in accordance with AREVA NP procedures and affected customers are notified.

6.0 SIVAT DEVELOPMENT PLAN

The Software Development Plan describes the life cycle activities for TELEPERM XS SIVAT Tool software development.

6.1 Use of TELEPERM XS Phase Model for SIVAT Development

The TELEPERM XS Topical Report describes the generic development and qualification process for the TELEPERM XS digital I&C system.

SIVAT was developed under the same QA program and software lifecycle development process as described in the TELEPERM XS Topical Report. SIVAT was developed in accordance with AREVA NP GmbH Engineering Procedure FAW-TXS-1.1, Phase Model for the Development of Software Components for TELEPERM XS.

SIVAT was developed based on a requirements specification and technical specification document. The results of the SIVAT development process are described in Section 3.0 of this Topical Report.

NRC reviewed this procedure and the QA program as part of the review of the TELEPERM XS Topical Report. NRC approved the TELEPERM XS Topical Report in a safety evaluation report issued in May 2000.

6.1.1 TELEPERM XS Software Application Classes

The TELEPERM XS software components are assigned to application classes, which serve to standardize various requirements on the development process and the verification and validation. The classes used in TELEPERM XS are shown in Table 6-1.

Table 6-1 - TELEPERM XS Software Application Classes

TELEPERM XS Software Application Classes:	
A = Safety Function	For safety functions, including Category A of IEC 61226 (Reference 11) (e.g., online software MICROS and Runtime Environment)
B = Safety Related Function	For signaling functions, other graded safety classes
C = Code Generation for Safety Function	Tools for generating software of classes A and B e.g. code generator for Function Diagram Groups (FDGCG) and Runtime Environment (RTECG)
D = Engineering and Service	Tools and software solutions without safety functions (e.g. FBs not in Class A (FB add-on), Gateway, simulator (SIVAT), service tools, internal tools, etc.)

The SIVAT software has been classified as Class D.

6.1.2 Phase Model for the Software Lifecycle

The phase model structures the process for manufacturing and maintaining software in a sequence of connected tasks and activities which when performed successively, results in completion and verification and validation that the software is fit for its purpose. Development of every TELEPERM XS software component, including the SIVAT Tool, is performed according to the requirements of the standard phase model.

The TELEPERM XS phase model is shown in Figure 6-1.

There are two alternative phase paths:

- "Original phase path": Support and modifications for all TELEPERM XS software components that were available in 2005
- Phase path "2006": Software or firmware newly developed from 2006 onwards.

Procedures FAW-TXS-1.1, FAW-TXS-1.5, FAW-TXS-2.2, FAW-TXS-4.1, and FAW-TXS-4.2 always apply. As such they are applicable to the development of the SIVAT software.

Procedures FAW-TXS-1.6, FAW-TXS-2.1, FAW-TXS-3.3 to FAW-TXS-3.6 apply to modifications to all software components of TELEPERM XS Software Application Classes A to C that existed at the end of 2005. As such they are not applicable to the development of the SIVAT software, since it is Class D software.

Software developments for Application Classes A and C must be submitted to an external assessor for software qualification during development. Creation and internal / external checking of the development results is performed as specified by FAW-TXS-1.6. For software development for Application Class B, it must be determined on a case-by-case basis whether external assessment is necessary. SIVAT software is classified as Class D software, based on the requirements in FAW-TXS-1.1; consequently, no software type-testing, including third party assessment was required.

6.2 SIVAT Development Documentation

The following documents were created for the initial development of SIVAT:

- KWU NLL4/98/042, Rahmenlastenheft TELEPERM XS-Simulator (Frame Requirement Specification)
- KWU NLL4/98/068, Lastenheft SIMM (Requirement Specification)

- KWU NLLZ ST/99/023b, TELEPERM XS Pflichtenheft, Version 01.21: Generator CATS-SDE für die TELEPERM XS-Simulationsumgebung (Functional Specification)
- KWU NLL4/1998/180a, Vergleich der Ergebnisse des Prüffeldes (n-cpu) und der Offline (1-cpu) Simulationsumgebung (Test Results NPPs Unterweser and Emsland)
- KWU NLL4/2000/032, Auswertung der SIVAT Tests der LT-Funktionen (Test Results NPP Philippsburg)

7.0 SIVAT QUALITY ASSURANCE PLAN

The Software Quality Assurance Plan describes the necessary processes that ensure that the software attains a level of quality commensurate with its importance to safety.

7.1 Use of TELEPERM XS Quality Assurance Process for SIVAT Development

SIVAT was developed under the same QA program and software lifecycle development process as described in the TELEPERM XS Topical Report. NRC reviewed this procedure and the QA program as part of the review of the TELEPERM XS Topical Report. NRC approved the TELEPERM XS Topical Report in a safety evaluation report issued in May 2000. NRC made the following conclusions in the SER:

> 2.2.2 Software Documentation
>
> This section summarizes the software documentation associated with the TXS system development. The type tests of the TXS software components were performed in accordance with German standard KTA-Standard 3503. The principles of type testing and the test activities were defined from this standard. These were applied to the following areas: separation in the theoretical and practical tests, institutions to be involved in type tests, roles of these institutions in type tests, and documentation of type tests.
>
> The content of the theoretical and practical tests is defined by the software standard DIN IEC-880.
>
> KTA standards also require that the present state-of-the-art be taken into account during the qualification. In addition to KTA-1401, which defines criteria for quality assurance systems, the following software standards were applied and verified:

- IS0-9000-3, "Management for Quality and Requirements of Quality Assurance,"
- IEEE-830, "Software Requirement Specifications,"
- IEEE-828, "Software Configuration Management Plan,"
- IEEE-1012, "Software Verification and Validation Plans,"
- IEEE-829, "Software Test Documentation,"
- IEEE-1008, "Software Unit Testing,"
- IEEE-1028, "Software Reviews and Audits," and
- ANSI/ANS-10.4, "Verification and Validation of Scientific/Engineering Programs for the Nuclear Industry."

Among the standards referenced in the Standard Review Plan and the Branch Technical Positions, IEEE-7-4.3.2 gives specific requirements concerning software development. Most of these requirements are given by reference to the standards ASME NQA-10.4, IEEE-730, IEEE-828, IEEE-1012, and IEC-880. The requirements of ASME NQA-10.4 are covered by KTA -401, and the requirements of IEEE-730 are covered by ISO-9000-3. All other standards were directly applied in the development and evaluated in the type tests.

The key elements of the SIVAT software quality assurance process include the software management process described in Section 5.0, the software development process described in Section 6.0, the verification and validation process described in Section 14.0, the configuration management process described in Section 15.0, and the test plan described in Section 16.0.

8.0 SIVAT SOFTWARE INTEGRATION PLAN

The purpose of a Software Integration Plan is to provide a general description of the software integration process, the hardware/software integration process, and the goals of those processes.

The issue of SIVAT Tool integration with the corresponding SPACE tool issue is central to the SIVAT life cycle activities described in Sections 15.2 and 16.2.

The release documentation for each version of the SIVAT software provides information on the required prerequisite TELEPERM XS Software (e.g., SPACE tool, database management systems, and LINUX operating systems) and supported versions to support installation, as noted in Section 9.0.

9.0 SIVAT SOFTWARE INSTALLATION PLAN

The SIVAT Users Manual provides general instructions for loading the SIVAT software.

The SIVAT software is delivered on a CD-ROM. The installation process is controlled by an installation script and can only be performed by a system administrator.

The release documentation for each version of the SIVAT software provides a listing of the software files, including file size and CRC checksum. The release documentation also provides information on the required prerequisite TELEPERM XS Software (e.g., SPACE tool, database management systems, and LINUX operating systems) and supported versions.

10.0 SIVAT SOFTWARE MAINTENANCE PLAN

The purpose of a Software Maintenance Plan is to provide a general description of the software maintenance process and the goals of that process. In particular, the Software Maintenance Plan should list the general functions that the software maintenance organization will be expected to perform, and provide general information on obtaining field trouble reports. Maintenance should be limited to the process of modifying a software design output to repair nonconforming items or to implement pre-planned actions necessary to maintain performance. Modifications to improve performance or other attributes, or to adapt the design outputs to a modified environment, should be considered design changes.

The Software Maintenance Plan is not directly applicable to the SIVAT software, since no maintenance is performed on the SIVAT software by AREVA NP Inc. Section 5.4 describes the problem reporting process used by AREVA NP (Inc) for identifying problems and discrepancies identified with the TELEPERM XS SIVAT Tool. The user organization (AREVA NP Inc) does not make changes to the TELEPERM XS SIVAT Tool to correct problems.

User suggestions for potential product improvements are forwarded to the TELEPERM XS software development organization (AREVA NP GmbH) for consideration. Changes to the SIVAT software are controlled by the TELEPERM XS software development organization. The configuration management process, including change control, is described in Section 15.0.

11.0 SIVAT OPERATIONS PLAN

The SIVAT Operations Plan provides a general description of the operation of SIVAT. The use of SIVAT to perform TELEPERM XS Application Software testing of I&C functionality and validation of system requirements is also described. The capability to simulate various TELEPERM XS malfunctions is described. In addition, the limitations of simulation are discussed.

SIVAT is used to support validation testing of TELEPERM XS Application Software developed in accordance with the TELEPERM XS Software Program Manual.

11.1 Application Software Testing with SIVAT

SIVAT can be used to perform Application Software integration and functional testing. Application software validation through SIVAT testing is one of the layers of validation testing that is used to ensure Application Software quality. It can also simulate certain

[ ]

response to these faults is as intended. SIVAT enables the independent verification and validation engineer to compare the validation results to the software requirements specification. The Independent Verification and Validation Group uses the software requirements traceability matrix to ensure that software requirements have been tested.

The benefit of Application Software validation testing with SIVAT is the early detection of faults. A balance is drawn between performing Application Software validation testing during the FAT later in the development process and performing Application Software validation testing with SIVAT earlier in the process. IEEE Std 1008-1987 recognizes that:

> There are significant economic benefits in the early detection of faults. This implies that test set development should start as soon as practical following availability of the unit requirements documentation because of

> the resulting requirements verification and validation. It also implies that as much as practical should be tested at the unit level. (Paragraph B2.4)

The early detection of Application Software faults through validation testing with the SIVAT Tool serves to reduce project risks earlier in the development process.

The SPACE-generated code should be validated in a simulation test environment by means of the SIVAT Tool. The purpose of the simulation is to test the generated TELEPERM XS program modules with regard to the way the process engineering tasks and/or the I&C function specification are implemented in the I&C. This testing is performed to identify any Application Software errors as soon as possible and prove the fulfillment of the requirements.

The Independent Verification and Validation Group personnel should be independent from the Software Design Group according to NRC Regulatory Guide 1.171:

> Criterion III, "Design Control," imposes an independence requirement for the verification and checking of the adequacy of the design, requiring that those persons who verify and check be different from those who accomplish the design. Therefore, independence is an additional requirement for software unit testing. Either those persons who establish the requirements-based elements for a software unit test must be different from those who designed or coded the software, or there must be independent review of the establishment of the requirements-based elements. The guidance in section A7 of Appendix A to IEEE Std 1008-1987 provides acceptable ways to meet this requirement for software unit testing. These independent persons must be sufficiently competent in software engineering to ensure that software unit testing is adequately implemented.

Application Software integration and functional testing with SIVAT can be used to validate engineering I&C functionality and satisfy IEEE Std 1012-1998 validation requirements for Application Software integration testing. This Application Software integration testing using SIVAT is performed under the direction of the Independent Verification and Validation Group. The test plans, specifications, procedures, and reports are prepared in accordance with the Application Software verification and validation plan and 10 CFR Part 50 Appendix B requirements.

The functions of the TELEPERM XS Application Software can be tested module by module for each TELEPERM XS processor and can also be tested as an integrated software system. SIVAT can also be used in conjunction with system models to test the TELEPERM XS Application Software in a closed-loop test.

SIVAT has the capability to support both white box and black box testing of the TELEPERM XS Application Software. The following tests should be carried out using SIVAT:

- Validation of the I&C functions against the software requirements
- Testing of the specified I&C functionality as defined in the Software Design Description
- Simulated system behavior and failure response

The simulation in SIVAT is based on the code of the FDs and FDGs generated by means of the SPACE Code Generators. The tests cover the correct choice, integration, and parameterization of function modules. The SIVAT Tool malfunctions are used to support failure response testing by checking the response of the Application Software to failures of I/O modules, TELEPERM XS processors, or data messages.

The goal of the project-specific simulation testing with SIVAT is to verify the correct implementation of the I&C functionality that is testable with the SIVAT Tool and the associated requirements specified in the Software Requirements Specification. The I&C functionality that is testable with the SIVAT Tool includes the software logic represented in the FDs and the signal connections established between FDs created with the SPACE Engineering Tool.

Additionally, simulation testing with SIVAT will verify that Application Software functionality, specified in the Software Design Description, is tested to validate that the software elements correctly implement software requirements. As a minimum the criteria for this determination are:

- Compliance with functional requirements.
- Correct performance at FD boundaries, output interfaces under normal operation and error conditions.

The proper functionality of the project-specific Application Software is tested to validate the following standard TELEPERM XS characteristics:

- Test results must be verified from start of test until the completion of the test in order to ensure that no unexpected intermediate results are present.
- Signals must be handled in a manner to ensure spurious alarms are not generated by the software.
- Correct setting of FB parameters must be checked against software requirements.

11.1.1 Test of the Required I&C Functionality

The aim of the Functional tests is to validate the correspondence of the FDs developed with SPACE against the I&C requirements (Software Requirements Specification and Software Design Description). Inputs, outputs, and/or internal signals are simulated in the SIVAT test environment (e.g., by using scripts, signal generators, etc.). The signals and the system responses are recorded and compared to those stated in the test specification. The result of the comparison is documented.

The correct processing of FDs, the parameter settings of function blocks, the signal exchange between redundant channels, the correct generation of output, status, and alarm signals are all tested.

The test cases are adjusted to the modular structure of the FDs. Separate test cases are developed for each I&C function. The test cases can be subdivided for ease of testing. Each I&C function is validated. In the scope of function tests, all input and output signals as well as the signal paths (logic connections in the FD) are covered by tests. Functions which are not validated in the scope of this phase of testing are identified for later validation in the test field.

For integration testing of the TELEPERM XS Application Software, the tests are preferably carried out in steps by starting with the inspection of small units, incrementing up to the inspection of larger units, such as:

- Tests of partial functions (e.g., of a sub-module)
- Test of the overall module
- Test of complete I&C functions

The tests to be carried out using SIVAT are designed such that they can be repeated to support validation of future revisions to the TELEPERM XS Application Software.

11.1.2 System Level Simulation Tests

The aim of this phase is the validation of the I&C functionality at the simulation system level. The test cases are derived from the design basis event protection requirements and test the system response as a whole. Interactions between I&C functions and redundancies are included in the test. Tests of control functions whose dynamic behavior is not significantly affected by the feedback of the system can be carried out as open loop tests. If significant dynamic feedback from the target system needs to be considered, as in case of standard functions, closed loop tests are used. If closed loop tests are required the availability of dynamic plant models is preferred; otherwise, simplified models can be used.

11.1.3 TELEPERM XS Malfunctions Simulation

The software is tested with regard to the requirement specification for postulated errors. The cases to be checked are analyzed and the checks defined according to requirements. The test program is defined together with the customer.

In the plant-specific tests, the effects of failures to the I&C functions are tested. The test cases include computer and communication failures. The effects of the tested errors are analyzed. Alarm and status signal processing are also tested. Tests cases can be developed to check the system behavior involving cross channel communications and function interaction of signals exchanged between redundancies and any failures associated with these signal exchanges. Functional tests under error conditions are performed.

Communication between the individual TELEPERM XS CPUs is implemented via messages that are generated by the SPACE Code Generator. The SPACE Code Generator specifies the message structure as well as the transmission path. Three paths are available for transmission depending on the network topology:

- The K32 backplane bus if the TELEPERM XS CPUs are mounted in the same subrack,
- The L2 bus if there is an L2 network connection between the subracks, and
- The H1 bus if there is an H1 network connection between the subracks.

communications simulation is completely sufficient for testing the specified I&C functionality. The effects of failed communications links on the I&C functionality are tested.

To verify the effects of certain malfunctions on the specified I&C function, SIVAT generates three types of faults to simulate malfunctions that can be inserted or removed:

11.2 Limitations of Simulation

TELEPERM XS simulation by SIVAT is based on the original code of the Application Software (i.e., the simulation reflects the actual behavior of the specified I&C functions). Nevertheless, even TELEPERM XS simulations with SIVAT have their limitations that distinguish the simulation environment from the actual TELEPERM XS system. Some of these limitations can only be overcome at great expense, others are resolved by formally verifying the I&C specification (analysis tools) independently of the simulation.

The following system characteristics are not tested by SIVAT:

11.3 SIVAT Test Documentation

Test Specifications are prepared for each Test Case. Test Specifications incorporate the Test-Design Specification and Test-Case Specification into a single document and conform to IEEE Std 829-1983 and IEEE Std 1008-1987.

Test Procedures are prepared for each Test Case. The Test Procedures contain test scripts that implement the test cases defined in the Test Specifications. The Test Procedure verifies that the correct versions of the project-specific TELEPERM XS application software, SIVAT, and test scripts are used for the testing. The Test Procedures conform to IEEE Std 829-1983 and IEEE Std 1008-1987.

The Independent Verification and Validation Group verifies the SIVAT Test results by reviewing the Test Log, Test Incident Report, and Test Summary Report to ensure that they demonstrate that the system satisfies the criteria of the SIVAT Test Plan and Test Procedures. The Independent Verification and Validation Group verifies the correct versions of software were used in the SIVAT Test.

The Test Case is considered failed if the test script has a syntax error that prevents the script from running or if the test script, the Test Specification, or Test Procedure are found to be in error (i.e., the results of the test do not match the predicted results described in the Test Procedure).

Any errors encountered while performing the test will be documented in the Test Log and Test Incident Report.

The suspension criteria and resumption requirements used for software validation testing are:

- If a discrepancy is found during test execution, the discrepancy is documented in the Test Log and the Test Incident Report and, if warranted, the testing resumes.
- A disposition of the discrepancies logged will determine if the discrepancy affects the Test Specification, Test Procedures, Software Requirements Specification, or the project-specific Application Software.
- If a discrepancy is found while comparing the plot data to the expected results, the discrepancy is recorded, evaluated, and resolved. The discrepancy is recorded in the Test Incident Report and the review of test results continues.
- When a discrepancy is detected that affects the affected design documents or the project-specific Application Software, an Open Item is created and the discrepancy is resolved.

- During review of the test results, all discrepancies are recorded in the Test Incident Report.

- Test reruns may start after required changes to the affected design documents and project-specific Application Software have been implemented and the Test Specifications and Test Procedures have been updated to the new design.

- Test reruns are performed on all sections of the Test Specification determined necessary and recorded in the Test Incident Report.

The pass/fail criteria used for system/software validation testing are:

- A Test Item is considered successfully passed when the results of the test match the expected results described in the Test Procedure with no unexpected intermediate results.

- A test Item containing unexpected results may be considered to be successfully passed if the evaluation of the unexpected result concludes that the TELEPERM XS Application Software is functioning correctly. Disposition of the item is documented and preserved in the Test Incident Report. Under these conditions, a retest of the item will not be necessary.

- A Test Item is considered failed if the test script has a syntax error that prevents the script from running or if the test script, the Test Specification, or the Test Procedure are found to be in error (i.e., the results of the test do not match the predicted results described in the Test Procedure).

The Open Items process, as described in Section 5.4.2, is used to document any discrepancies identified during software validation testing. The project verification and validation report lists any verification and validation discrepancies or problems discovered during the software validation tests, and associated anomaly evaluations.

11.4 Summary of Application Software Integration Testing with SIVAT

Testing with SIVAT is optional but it is the preferred approach to TELEPERM XS Application Software Integration testing. This approach is preferred because it leads to early detection and correction of Application Software faults, which serves to reduce project risks earlier in the development process. The SIVAT Tool can be used to conduct all of the Application Software Integration Testing.

Testing with SIVAT can serve as module or unit testing (i.e., FD or FDG testing). It can also serve as integration testing of the TELEPERM XS Application Software (i.e., testing of the Application Software for all TELEPERM XS modules working together) within the limitations of simulation. Additional testing is performed as part of the manufacturing tests to address the limitations of simulation testing.

The SIVAT test cases are designed such that they can be repeated to support validation of future revisions to the TELEPERM XS Application Software.

11.5 Summary of Application Software System Testing with SIVAT

The SIVAT Tool can also be used to conduct a portion of the Application Software System and Acceptance Testing. Specifically, the SIVAT Tool can be used to validate those system requirements that are fully implemented within the Application Software layer. For example, a two-out-of-four trip logic can be tested with the SIVAT Tool; whereas, the response time of the trip feature cannot be validated with the SIVAT Tool. Similarly, simple process control loop logics can be tested with the SIVAT Tool; whereas, the overall dynamic performance (final tuning) cannot be validated with the SIVAT Tool.

Representative test cases of the test scope of the simulation tests are selected and to be carried out with the same simulation test scripts (converted to the test field syntax) in the test field. The selection criteria for representative test cases are:

- Each TELEPERM XS processor has to be covered by at least one test case,

- Test cases with specific hardware dependencies (e.g. time-related correlation of measuring signals like neutron flux measurement and the appropriate measuring range),
- Selected test cases containing functions which are spread out across several TELEPERM XS processors (due to the asynchronous working method of the TELEPERM XS processors), and
- Selected test cases with more complex functions.

This overlap of testing establishes a degree of congruence between tests conducted in simulation environment and those conducted in the test field.

12.0 SIVAT TRAINING PLAN

The Training Plan describes the method of ensuring that training needs for the use of the SIVAT Tool for TELEPERM XS Application Software testing are achieved. The Training Plan provides a general description of the training organization and the basic training responsibilities. It also describes the basic training methods and primary training resources. The specific training requirements for use of the SIVAT Tool are defined.

12.1 Training Organization and Responsibilities

The AREVA NP (Inc) Training Group is responsible for conducting employee training on the use of the SIVAT Tool. The AREVA NP (Inc) Training Group reports to the AREVA NP (Inc) department manager. The AREVA NP (Inc) Manager has the overall ownership of training within the AREVA NP (Inc) department. The AREVA NP (Inc) Training supervisor is responsible for oversight and implementation of the AREVA NP (Inc) training program.

The training process is modular in nature and supports delivery of specific training for the needs of the various groups within the AREVA NP (Inc) department. The training is provided in accordance with AREVA NP administrative requirements

12.2 Training Methods

Training is normally implemented using one or more of the following forms of delivery:

- Instructor led - Instructors are either formally trained in instructional techniques, or SMEs under the guidance of the training supervisor. Instructor led training is presented in a classroom format using slides, overheads, or other media along with a student handout.
- Hands on - Hands on training is provided using hardware, software, and tools/equipment similar to those used on the job. Hands-on training is structured.

- Self-study - Self study is performed by the trainees, using formal materials or company/project documents as a guide.

- On-the-Job - On-the-Job training (also called mentoring) is performed under the cognizance of a qualified person. The qualified person maintains adequate oversight of the trainee to ensure the correct performance of the task.

Personnel mastery of the course materials is evaluated as required.

- If required by the curriculum, students are evaluated to determine mastery of the topics.

- Successful completion of hands-on tasks may be used to demonstrate mastery.

- Oral questioning techniques may be used to demonstrate mastery.

The method of evaluation is selected according to the following criteria:

- The difficulty of the task/job requirement

- The frequency of the task/job requirement

- The criticality of the task to nuclear safety

Training related records are submitted to the AREVA NP (Inc) Training supervisor and maintained electronically.

12.3 Training Resources

The SIVAT Tool and the associated SIVAT-TXS Simulation Based Validation Tool User Manual are the primary training resources.

12.4 Training Requirements

All Design Group personnel shall be qualified on the use of the SIVAT Tool prior to performing debugging of the Application Software with the tool.

All Independent Verification and Validation Group personnel shall be qualified on the use of the SIVAT Tool prior to performing validation testing of the Application Software with the tool.

13.0 SOFTWARE SAFETY PLAN

The SIVAT Tool utilizes the C Code generated by the SPACE Code Generators used to generate the code for the target system. The code is modified to run as a model in the SIVAT environment, but the code functionality is unaffected. The simulation process is described in more detail in Section 3.0. The C Code is compiled using two widely used compilers: one for the target processors (Intel iC 86) and one for the simulation environment (GNU Compiler Collection - GCC).

13.1 Effect of SIVAT on Target System Code

The SIVAT Tool does not produce code that is run on the TELEPERM XS safety processors. In fact, the code produced for simulation could not run on the safety processors due to differences in compilation and the alterations to memory mapping to support messaging simulation. The SIVAT Tool does not modify the Application Software code that is loaded on the TELEPERM XS safety processors. SIVAT has no effect on the Application Software and cannot create a safety hazard affecting safety functions.

13.2 Fidelity of SIVAT Simulation

SIVAT generates a separate CPU model in C Code for each processing module from the project-specific SPACE database. The Application Software code for FDs and FDGs is included in the respective CPU models. The CPU models also include a partial emulation of the TELEPERM XS Runtime Environment that satisfies the requirements of the simulation control system. The cycle time of the runtime environment is based on the design determined cycle time.

[ ]

The source codes of most FBs do not change for the simulator, as the code is designed with the requirement that the FBs can be used in the simulator. There are some exceptions to this rule for two hardware/software interfaces:

The interface of these FBs is the same in the simulator as in the actual I&C, but the behavior of these FBs in the simulator differs from the behavior in the actual TELEPERM XS I&C system hardware.

The limitations of SIVAT simulation are well known, as described in Sections 3.6. Other means of Application Software verification or validation are described in Section 11.2 to address these limitations. As such, the safety hazards not detected because of the limitations of SIVAT simulation can be identified by other verification or validation activities.

13.3 Transparency of SIVAT Code Generation

The C Code created by the SPACE Code Generator and the C Code modified for simulation can be readily compared using standard code difference identification tools. The differences can be checked at any time since the code files are archived in the software libraries. This capability allows internal auditors, customer representatives, external assessors, and regulatory authorities the capability to provide any degree of oversight. This capability also supports investigation of anomalous behavior observed during SIVAT use. This capability has been demonstrated to NRC on several occasions (meetings and audits related to TELEPERM XS projects). As such, suspected safety hazards can be readily investigated and corrected if substantiated.

14.0 SIVAT VERIFICATION AND VALIDATION PLAN

The SIVAT Verification and Validation Plan describes the methods used to ensure correctness of the SIVAT Tool software.

14.1 SIVAT Tool Verification and Validation Activities

The verification activities for the SIVAT software are performed in accordance with FAW-TXS-1.6. All software development lifecycle documents that are created for SIVAT are reviewed. The review process is conducted and documented according to FAW TXS-2.2 using review checklists. The verification process of the phase results is documented in the review protocol and the checklist for each phase of a software component.

All changes that are introduced to the SIVAT source codes are reviewed in accordance with the requirements of FAW TXS-1.5, as described in Section 15.0. The majority of the CRs address the controlling interface (e.g. changes to the graphical user interface or commands) of SIVAT. The simulated behavior of the TELEPERM XS Application Software depends directly on the SPACE Tool Code Generators, which are controlled in accordance with the lifecycle process described in the TELEPERM XS Topical Report.

All changes made to the SIVAT software are validated with an Integration and CR test performed by qualified personnel on dedicated test machines. The Integration and CR test is performed for each SIVAT release, as described in Sections 15.0 and 16.0. The testing includes tests for CRs that were introduced in the software release.

The validation results are stored together with the test report inside the document management system. The SIVAT source code is stored in the software configuration management system.

14.2 Initial SIVAT Tool Validation Activities

The I&C system at the Unterweser nuclear power plant was retrofitted with TELEPERM XS in 1996. At that time, all tests in the test field were still implemented with the real

TELEPERM XS system and a linked process model. The test cases were also verified with a UNISYS test arrangement and a Konvoi system simulator. UNISYS was the simulator control system that was used for TELEPERM XS simulations prior to SIVAT. The results of this simulation were compared with the test field results and concordance was verified.

No test field was available for upgrading the TELEPERM XS I&C system at the Unterweser plant in 2000, since the TELEPERM XS system was installed in the plant. Planned changes could only be tested through validation with SIVAT, which has been available as a TELEPERM XS V&V tool since 1998. For this purpose, first the test cases from the old simulation environment (UNISYS) and the test field were recalculated with SIVAT. Since the results matched, the verification of the modified I&C functionality was also implemented with SIVAT.

In addition, a closed-loop system test (load shedding from 71% reactor power down to house load) was recalculated by SIVAT and the process model (i.e., system model NLOOP Unterweser). The very high concordance between the actual system behavior and the simulation results lead to the authorization for installing the modified SIVAT-validated TELEPERM XS I&C. Authorization to install the modified TELEPERM XS application functions was given based on the very high concordance between the actual system behavior and the SIVAT validation. Plant commissioning took place without findings concerning the new I&C application functions.

A number of test field tests were verified with SIVAT as part of the TELEPERM XS retrofitting for the Philippsburg 1 nuclear power plant. The very high concordance made it possible to implement individual changes in the TELEPERM XS configuration even after the test field tests. These modifications were verified and validated exclusively with SIVAT.

14.3 Operating Experience with SIVAT

Since the first SIVAT version was introduced in 1999, this tool has been applied in all TELEPERM XS I&C projects. AREVA NP has operating experience with the use of SIVAT for more than 20 project specific applications. No instances have been reported where a system tested using SIVAT did not perform as expected after installation. The projects that have been verified and validated with SIVAT through 2005 are listed in Table 14-1.

Table 14-1 - TELEPERM XS Projects Verified and Validated with SIVAT

Plant/nuclear power plant	TELEPERM XS system
Unterweser (Germany)	Reactor control and limitation
Neckarwestheim 1 (Germany)	Reactor control and limitation
Bohunice V1 (Slovakia)	Reactor safety system
Bohunice V2 (Slovakia)	Reactor safety system
Philippsburg 1 (Germany)	Emergency system, local nuclear monitoring
Research reactor FRM2 (Germany)	Complete safety I&C
Beznau 1 and 2 (Switzerland)	Reactor safety system and control
Tianwan 1 and 2 (China)	Complete safety I&C
Research reactor AKR2 (Germany)	Complete safety I&C
Biblis B (Germany)	Reactor control and limitation
Biblis A and B (Germany)	Emergency supply steam generator (secondary)
Paks 1-4 (Hungary)	Reactor safety system
Forsmark (Sweden)	Rod control
Oskarsham 1-3 (Sweden)	Neutron flux
Atucha (Argentina)	Reactor safety (second heat sink)
Diverse systems (Germany)	I&C for turbine-generator set
Emsland (Germany)	Reactor control
Kozloduy (Bulgaria)	Diesel control, coolant pressure monitoring
Grohnde (Germany)	Power distribution monitoring

14.4 Independent Review of SIVAT

In 2006, the Institut für Sicherheitstechnologie (Institute for Safety Technology known as ISTec), issued an assessment report about the TELEPERM XS tools, which also includes a third party statement about the purpose and suitability of SIVAT. The discussions regarding SIVAT are reproduced below.

6 VALIDATION TOOL SIVAT

6.1 Concept of the SIVAT

The Simulation and Validation Tool (SIVAT) provides capabilities to test and validate the original SPACE generated code of I&C functions against the specification. The application code is compiled and operated on the simulator workstation with no need to access the tar-get hardware. The consequences of particular hardware malfunction of I&C functions can be simulated and analyzed. After the installation of the target system in the plant, there is a software test environment available to evaluate the effects of later modifications on the system. The SIVAT tool provides also the possibility to connect a process model in a closed loop configuration. The SIVAT tool CATS-SDE (Code Adaptation Tool for Simulator SDE) controls the automatic generation of the SIVAT simulator and the simulator environment. The generated code (function diagrams and the Run Time Environment[1] (RTE) as C code) serves as the input of the simulation.

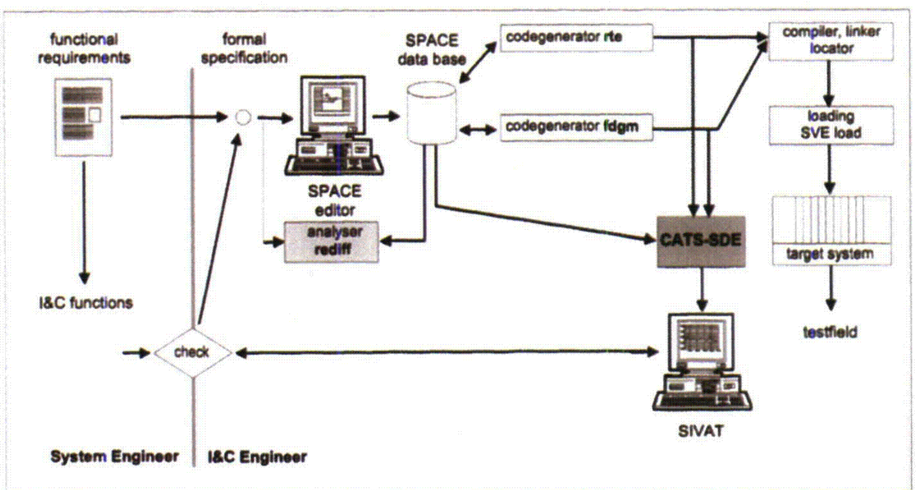

Fig: 3: Software validation using SIVAT

[1] That means the generated part of the RTE that is the interface of the RTE to the FD/FDG modules. Most of the RTE code is fix.

The main objectives of the SIVAT are to bring evidence that

- the correct FBs have been used,
- the FBs are correctly connected,
- the parameters of the blocks are correct,
- the I&C functions implement the specified behavior concerning the signal values as well as the signal status.

The availability of the SIVAT environment is independent of the availability of the target hardware. Therefore, SIVAT tests can be performed prior to test field tests, but also after the tests in the test field have been finished.

The validation of the I&C functionality of the application code is feasible in SIVAT because

- the functionality is contained in the function diagrams. From the function diagrams the C source code is generated automatically by the code generators of SPACE. This hardware independent C code is the source for the compiler for the target system of TXS and is also compiled and operated on the SIVAT environment. Therefore, the code of the application software used in the SIVAT environment is the original code used in the target sys-tem with few insignificant adaptations to the SIVAT simulator database. The project related application software is separated from the TXS platform system software by a clearly defined interface. The SIVAT environment provides this interface to the application software, too. The functional behaviour of the application software in the SIVAT environment and in the target system is the same (for insignificant differences see /3/, /4/).
- the system behaviour for assumed failures of components (I/O boards, CPUs, communication buses etc.) and systematic failures can be simulated
- safety set points and safety criteria can be tested
- signals and variables can be visualised
- partial functions and modules can be tested

The SIVAT tool has been successfully used in several validation procedures (see table 1).

Table 1: Major application of the SIVAT simulation environment

Project	Plant	Country
Control and limitation system	NPP Unterweser	Germany
RPS	NPP Bohunice V1	Slovakia
EKU emergency safety system	NPP Philippsburg 1	Germany
LKU-system for local core surveillance	NPP Philippsburg 1	Germany
Safety I&C	FRM-2	Germany
RPS, reactor control	NPP Beznau	Switzerland
RPS, reactor control and limitation system	NPP Tianwan	China

Especially the reports on the application of SIVAT in KKU (NPP Unterweser) and KKP-1 EKU (/3/, /4/) document the same functional results of the SIVAT tests and the corresponding tests in the test field. Differences have been discussed and justified.

The simulated run of I&C functions on the workstation is performed cyclically and synchronised, but not in real time. The real time aspect is not important, due to the fact that there is no time management in the system software. Time conditions are mapped to numbers of computation cycles. The sequence of the computation of the function diagrams in the simulation environment is only one special sequence of the computation of the function diagrams in the target system. Since the concept of the TELEPERM XS is based on an asynchronous behaviour of the different processing units, the simulated run of I&C functions will have no significant deviations from the functional behaviour of the target system.

7 SUMMARY

The TELEPERM XS platform and its environment comprise several software tools for development, documentation, analysis, verification and validation. Dependent on their role in the life cycle and the different safety significance of their outputs these tools are differently qualified.

The code generators that are specific for the TELEPERM XS platform are type tested following the same procedures applied to the on-line software, because their outputs are the C code of the application specific on-line software.

Compiler, linker, and locator are widespread used tool. Long time operational experience is available. Known bugs of these tools do not come to effect in TXS projects. During the type test of the TXS platform the usability of these tools were assessed by independent third party expert organizations with positive result.

The SPACE editor directly modifies the content of the specification database. From the data-base graphical representations of the project specification data are created. Thus, the results of the inputs can be verified. Additionally the independent documentation tool "fdprint" produces the paper documentation that can be used for verification. Until now, no functional failures have been detected.

The specification is stored in the standard data base system ORACLE that is used in a very large number of applications, also in safety relevant ones.

Documentation and analysis tools are used during project planning. They have no direct safety significance. Thus, these tools are designed and implemented based on the quality assurance procedures of the supplier. Third party assessment was not identified as necessary.

The verification tool "scanmic" is a simple tool to extract strings from MIC files and to calculate CRC check sums. It has no impact on the on-line software and no direct safety significance. It was designed and implemented using the internal quality assurance procedures of the supplier. Third party assessment was not identified as necessary.

The verification tool RETRANS was designed and implemented completely independent from the development of SPACE. This tool was validated by several different applications. It generates various text files that list potential inconsistencies. The decision about fault or planned deviation must be made by the assessor, a human being.

The validation tool SIVAT is suitable for validation of the functional behavior of the TXS application software. It was validated by several applications. The validation of SIVAT demonstrated the equivalence of the functional behaviour of the application software in the SIVAT environment and in the target system.

It should be noted that the SIVAT software is classified as Class D software, based on the requirements in FAW-TXS-1.1; consequently, no software type-testing, including third party assessment was required. SIVAT has been accepted for its mission by Technischer Überwachungs-Verein (German Technical Inspection Agency known as TÜV) in the course of the project-specific licensing for the German projects.

15.0 SIVAT CONFIGURATION MANAGEMENT PLAN

The SIVAT Configuration Management Plan describes two methods that maintain the SIVAT Tool software in a controlled configuration: during SIVAT Tool development in Germany and during SIVAT Tool use for project-specific validation testing in the U.S.

15.1 Use of TELEPERM XS Configuration Management Plan

The configuration management plan described in the TELEPERM XS Topical Report is used for the development of the SIVAT Tool. The TELEPERM XS Topical Report describes the generic development and qualification process for the TELEPERM XS digital I&C system. SIVAT was developed in accordance with the AREVA NP GmbH Engineering Procedure FAW-TXS-1.5, Configuration Management Plan for the TELEPERM XS System Platform. NRC reviewed this procedure as part of the review of the TELEPERM XS Topical Report. NRC approved the TELEPERM XS Topical Report in a safety evaluation report issued in May 2000.

SIVAT was originally developed during the years 1998-1999 to provide a simulation-based test environment to support the development of project-related TELEPERM XS Application Software. The TELEPERM XS configuration management process described in Engineering Procedure FAW-TXS-1.5 has evolved since the TELEPERM XS Topical Report was issued. A process change was made to add a change control board to the configuration management process. The process was enhanced to include additional detail describing configuration management tasks (e.g., introduction of a tracing sheet for each CR and more precise definition of the handling status of CRs). Specifically, there is an enhanced description of the platform configuration structure, unique component identifiers, version control, change control, release process, and documentation, with consideration of DIN EN ISO 10007 (Reference 11). This engineering procedure also addresses the requirements of the type tests for the TELEPERM XS system platform which covers the recommendations of relevant parts of DIN EN ISO 10007 and IEEE Std 828-1998.

SIVAT software, as is the case for all TELEPERM XS software, is managed using the Clearcase software configuration management system.

Changes to the SIVAT Tool are controlled via FAW-TXS-1.5, which establishes requirements to ensure that changes are controlled, documented, and tested. An overview of the TELEPERM XS software configuration management process is shown in Figure 15-1.

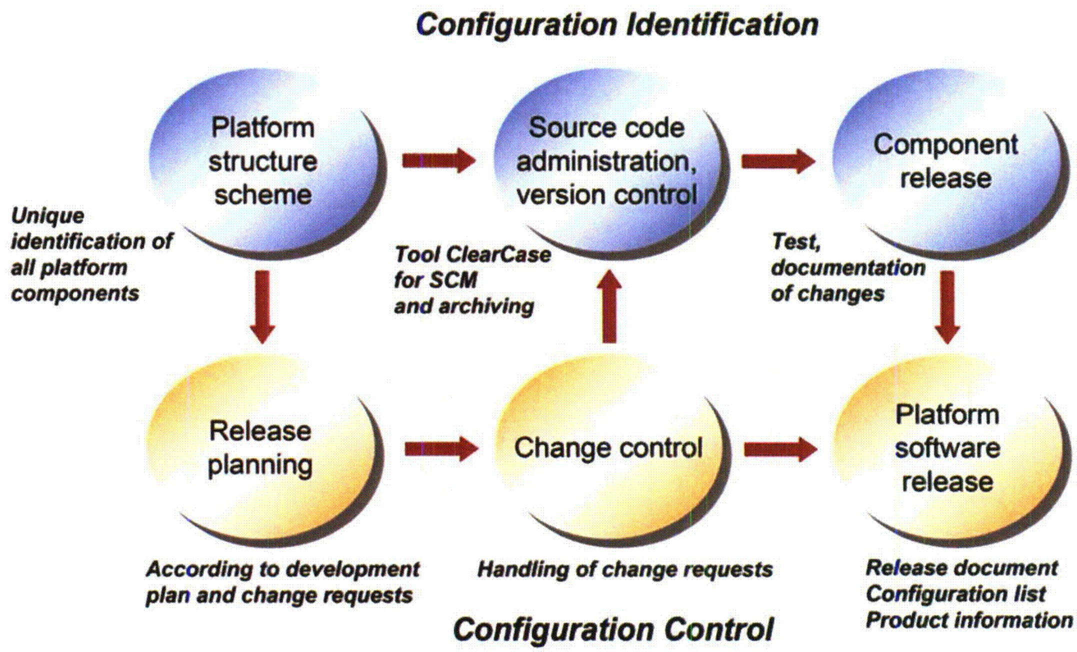

Figure 15-1 – Configuration Management Process Overview

15.2 SIVAT Life Cycle

The SIVAT Tool has been in use for many years. At this point, changes to the SIVAT Tool result from new user requirements, improvements based on operating experience feedback from the users, resolution of identified errors, and necessary adaptations due to changes in related components. The life cycle of the SIVAT Tool is shown in Figure 15-2.

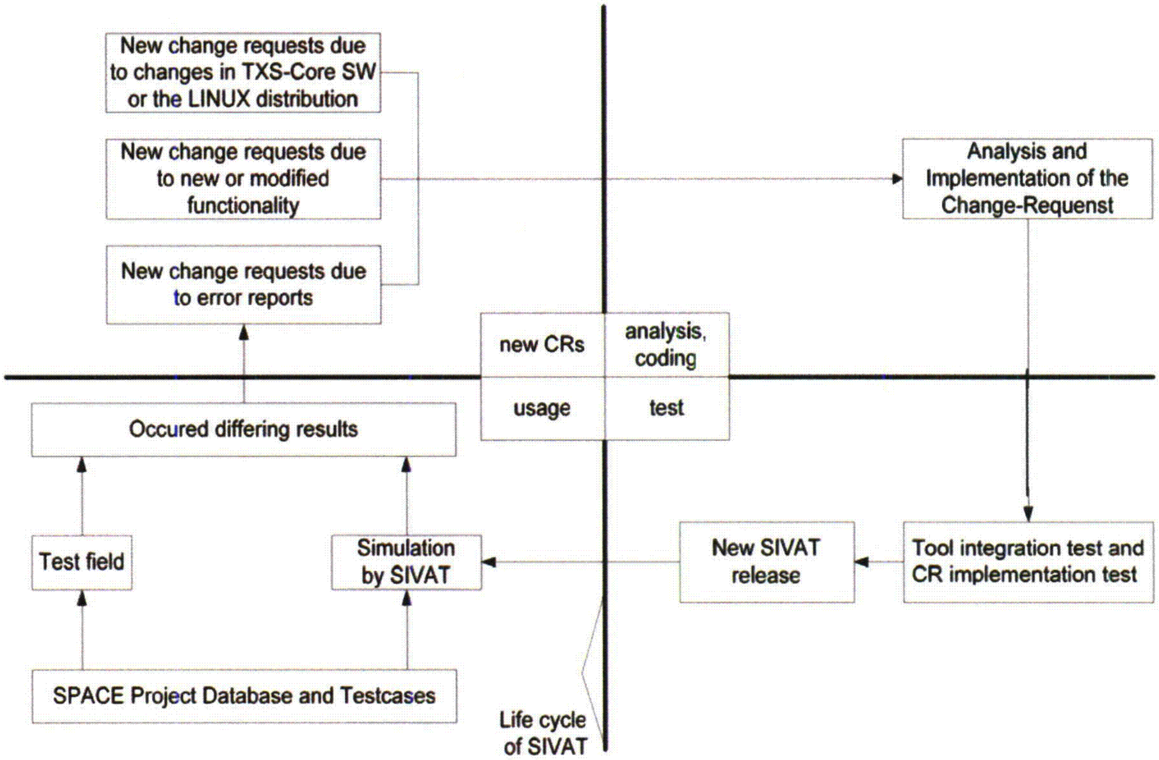

Figure 15-2 – SIVAT Life Cycle

CRs for the SIVAT Tool are analyzed and commissioned, if necessary, through the software configuration management process described above. The changes are implemented and the correct implementation of the changes is validated through testing (i.e., in the Integration and CR Implementation test). A new SIVAT version is released after successful completion of the specified testing.

15.3 Use of Software Program Manual Configuration Management Plan

The configuration management plan described in the TELEPERM XS Software Program Manual Topical Report is used for project-specific SIVAT Tool use in the U.S. AREVA

NP intends to use of the SIVAT Tool to support validation testing of TELEPERM XS Application Software developed in accordance with the TELEPERM XS Software Program Manual. As such, configuration management for SIVAT Tools used for U.S. TELEPERM XS projects will be controlled through the TELEPERM XS Application Software Configuration Management Plan described in Section 12 of the TELEPERM XS Software Program Manual.

The SIVAT software and associated documentation are classified as configuration items for the TELEPERM XS projects where they are used for Application Software testing. The versions of SIVAT Tool used on each release of the Application Software are controlled and recorded.

16.0 SIVAT TEST PLAN

SIVAT was developed in order to validate the Application Software functionality of I&C systems. After deployment, the results of a SIVAT simulation were compared with the results of the online system for certain project applications. It was shown that both systems show the same functional behavior. The same behavior of simulation and online system on functional level was shown for SIVAT release 1.2.4, as described in Section 14.0. The equivalence of the results must be shown for further releases of SIVAT. The SIVAT Test Plan outlines the methods to be used to test future releases of SIVAT.

16.1 Background Information

The SIVAT Tool was developed in order to replace existing simulator solutions such as UNISYS. It was intended that SIVAT simulates the functional behavior of TELEPERM XS I&C systems (called online systems below) on the level of I&C application functions. The simulation models are generated from the original TELEPERM XS Application Source Code which is obtained from the SPACE Code Generators. The code is slightly adapted in order to use the centrally managed memory of the simulator instead of the memory of the online systems. SIVAT Release 1.2.4 was tested against a set of input, output, and state data which were measured during factory acceptance tests of online systems in the test field. The online systems which provided the data were delivered to the NPPs Unterweser (KKU) and Emsland (KKE). As a result of the SIVAT tests, it can be stated that the release 1.2.4 shows the same functional behavior as the online system in the test field, as described in Section 14.0.

16.2 Scope of Testing

In general, the tests of the SIVAT Tool can be separated into a CR Implementation test component and a Tool Integration component.

16.2.1 Change Request Implementation Testing

CR Implementation testing is designed to validate that the modified SIVAT software meets the new or modified requirements established for the CR.

The CR Implementation test is designed by a different person than the developer who made the SIVAT software changes. The test developer is familiar with the functionality of SIVAT and the changes which were made. The test developer considers the effects of the CR and establishes the test cases, considering possible side effects of the change.

16.2.2 Tool Integration Testing

The Tool Integration test validates the following attributes:

- SIVAT can be installed on an engineering work station,
- All installed tools and configuration files are correctly installed,
- All tools can be called on an actual TELEPERM XS database, and
- A simulator that works can be generated in conjunction with the SPACE Tool Code Generators.

The test performer is familiar with the operation and use of SIVAT.

16.3 Test Documentation

Both, the CR Implementation and Tool Integration tests are documented in a single test specification. The test cases are established by the test developer. The test cases are documented in the test specification. The test specification is reviewed by another person (usually a developer of SIVAT). The review is documented in the review protocol.

The test cases are carried out on dedicated test machines, which have the same installation as the machines used for TELEPERM XS Application Software simulation testing. The test results are documented in a single test report.

All test findings are resolved or reconciled prior to the release of the modified SIVAT software.

17.0 CONCLUSIONS

This Topical Report described the Simulation Validation Test Tool (called SIVAT) developed by AREVA NP to support the development of project-related TELEPERM XS Application Software. This report described:

- The concept of TELEPERM XS simulation and the principle of operation of the SIVAT and
- The high quality development process used to develop SIVAT.

This topical report described the concept of the TELEPERM XS simulation and the principle of operation of the SIVAT. This report showed that the I&C functionality represented in the Application Software can be effectively validated with the SIVAT Tool. The use of a NRC-approved simulation validation tools has been described in AREVA NP document ANP-10272, Software Program Manual for TELEPERM XS™ Safety Systems Topical Report, which is referred to as the TELEPERM XS Software Program Manual.

The use of the SIVAT Tool to support TELEPERM XS Application Software verification and validation has important benefits. The early detection of Application Software faults through validation testing with SIVAT serves to reduce project risks earlier in the development process.

AREVA NP requests that the NRC issue a Safety Evaluation Report that approves ANP-10303P, SIVAT: TELEPERM XS™ Simulation Validation Test Tool Topical Report. AREVA NP intends to use the SIVAT Tool to support validation testing of TELEPERM XS Application Software developed in accordance with the TELEPERM XS Software Program Manual.

18.0 REFERENCES

18.1 U.S. Regulations

1. 10 CFR Part 21, "Reporting of Defects and Noncompliance."

2. 10 CFR Part 50, Appendix B, "Quality Assurance Criteria for Nuclear Power Plants and Fuel Reprocessing Plants."

18.2 U.S. Regulatory Guidance

3. Regulatory Guide 1.152, Revision 2, January 2006, "Criteria for Digital Computers in Safety Systems of Nuclear Power Plants."

4. Regulatory Guide 1.168, Revision 1, February 2004, "Verification, Validation, Reviews, and Audits for Digital Computer Software Used in Safety Systems of Nuclear Power Plants."

5. Regulatory Guide 1.169, September 1997, "Configuration Management Plans for Digital Computer Software Used in Safety Systems of Nuclear Power Plants."

6. Regulatory Guide 1.170, September 1997, "Software Test Documentation for Digital Computer Software Used in Safety Systems of Nuclear Power Plants."

7. Regulatory Guide 1.171, September 1997, "Software Unit Testing for Digital Computer Software Used in Safety Systems of Nuclear Power Plants.

8. Regulatory Guide 1.172, September 1997, "Software Requirements Specifications for Digital Computer Software Used In Safety Systems of Nuclear Power Plants."

9. Regulatory Guide 1.173, September 1997, "Developing Software Life Cycle Processes for Digital Computer Software Used in Safety Systems of Nuclear Power Plants."

10. NUREG-0800, Standard Review Plan, Chapter 7, Branch Technical Position 7-14, "Guidance on Software Review for Digital Computer-Based Instrumentation and Control Systems."

18.3 International Standards

11. DIN EN ISO 10007, "Quality management, guidelines for configuration management"

12. IEC 60880, Nuclear Power Plant Instrumentation and Control Systems Important to Safety: Software Aspects for Computer-Based Systems Performing Category A Functions, May 2006

13. IEC 61226, "Nuclear Power Plant Instrumentation and Control Systems Important to Safety: Classification of Instrumentation and Control Functions," 2005

18.4 U.S. Industry Standards

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

15. IEEE Std 610.12-1990, "Software Engineering Terminology."

16. IEEE Std 828-1990, "Standard for Software Configuration Management Plans."

17. IEEE Std 829-1983, "Standard for Software Test Documentation."

18. IEEE Std 830-1993, "Recommended Practice for Software Requirements Specifications."

19. IEEE Std 1008-1987, "IEEE Standard for Software Unit Testing."

20. IEEE Std 1012-1998, "Standard for Software Verification and Validation.

21. IEEE Std 1028-1997, "Standard for Software Reviews."

22. IEEE Std 1042-1987, "Guide to Software Configuration Management."

23. IEEE Std 1074-1995, "IEEE Standard for Developing Software Life Cycle Processes."

24. IEEE Std 1228-1994, "IEEE Standard for Software Safety Plans"

18.5 Regulatory Review Precedents

25. NRC Safety Evaluation Report for Siemens Topical Report EMF-2110(NP), Revision 1, "TELEPERM XS: A Digital Reactor Protection System," May 5, 2000.

26. Siemens letter from James F. Mallay to NRC dated September 1, 1999, Supporting Documentation for Review of EMF-2110(NP) Revision 1, "TELEPERM XS: A Digital Reactor Protection System," NRC:99:037.

27. Siemens letter from James F. Mallay to NRC dated December 16, 1999, EPRI and QA Documentation Supporting Review of EMF-2110(NP) Revision 1, "TELEPERM XS: A Digital Reactor Protection System," NRC:99:052.

18.6 AREVA NP Documents

28. Siemens Topical Report EMF-2110, Revision 1, "TELEPERM XS: A Digital Reactor Protection System," September 1, 1999.

29. ANP-10272, Revision 2, Software Program Manual for TELEPERM XS™ Safety Systems Topical Report

30. AREVA NP Document No. 56-5015885, "Quality Management Manual."

31. AREVA NP GmbH Engineering Procedure FAW-TXS-1.1, Phase Model for the Development of Software Components for TELEPERM XS

32. AREVA NP GmbH Engineering Procedure FAW-TXS-1.5, Configuration Management Plan for the TELEPERM XS System Platform

33. AREVA NP GmbH Engineering Procedure FAW-TXS-1.6, Software Verification and Validation Plan

34. AREVA NP Administrative Procedure 1717-06, "Corrective Action Program (WebCAP)."