invensys™
TRICONEX®
TRICONEX PRODUCTS – INVENSYS PROCESS SYSTEMS

TRICON v10
NUCLEAR QUALIFICATION PROJECT
SOFTWARE QUALITY ASSURANCE PLAN

Document No.: 9600164-537

Revision 0

07/24/06

	Name	Signature	Title
Author:	Hariprasad Parthasarathy		V&V Engineer
Reviewers:	Babu Krishnamurthy		QA Engineer
	Ted Porfilio		Project QA Engineer
Approval:	Jeff Larson		IPS Nuclear Quality Director

Revision History

Revision	Date	Description	Author
0	07/24/06	Initial Issue	Hariprasad Parthasarathy

Table of Contents

1 PURPOSE

1.1 Introduction

This Software Quality Assurance Plan (SQAP) defines the quality assurance measures to be applied to the software associated with the Tricon v10 Nuclear Qualification Project. This Project involves qualifying a typical Tricon v10 system, including hardware and associated software. This plan is intended to implement the requirements of EPRI TR-107330 and NQA-1-1994, Subpart 2.7. The primary objective of this process is to ensure the production of high quality software according to stated requirements and established standards.

1.2 Scope

The use of this plan will help ensure the following:

1) That software is developed and documented in accordance with the Invensys Triconex 10CFR50, Appendix B quality program and applicable nuclear qualification standards;
2) That the results of software quality reviews will be appropriately resolved;
3) That feedback is provided as to how well the development effort is conforming to various Tricon v10 Nuclear Qualification Project development standards; and
4) That software verification and validation (V&V) activities are conducted in accordance with applicable standards.

There are three types of software involved with the Tricon v10 Nuclear Qualification Project:

1) Embedded operating system firmware;
2) Application software development tools; and
3) Application software.

Embedded operating system firmware is delivered to the user in the same form as it received for incorporation into the system. As this firmware is not modified within the lifecycle of this Project, no testing is performed on it other than the functional checks conducted as part of system testing. This firmware is listed on the Master Configuration List (MCL) by name and version number. The verification and validation of this firmware is beyond the scope of this SQAP. The embedded operating system firmware used in the Tricon v10 system has been independently verified and validated by Invensys Triconex and certified by TUV under "Programmable Electronic Systems (PES, PLCs)".

The application software development tool is the Triconex TriStation 1131 Developer's Workbench, which is used to develop the Tricon v10 Nuclear Qualification Project Test Specimen Application Program (TSAP). As this software development tool is not modified within the lifecycle of this Project, no testing is performed on it other than for functional checks conducted as part of testing. This software is listed on the Master Configuration List (MCL) by name and version number. The verification and validation for this software is beyond the scope of this SQAP. The application software development tool has been independently verified and validated by Invensys Triconex and certified by TUV.

Application software is the Tricon v10 Nuclear Qualification Project TSAP. The TSAP, which will be generated as specified in EPRI TR-107330 and the TSAP Software Requirements Specification (SRS), is intended to demonstrate a Tricon application program which exercises the Tricon-Under-Test (TUT) functionality during all phases of qualification testing. The TSAP is being developed as test software and is not being qualified for a specific nuclear plant application. The TSAP developed for the Tricon v10 Nuclear Qualification Project shall be classified as Software Integrity Level 4 in accordance with IEEE Std. 1012-1998, Section 4. The TSAP to be developed during this Project will be controlled in accordance with Invensys Triconex 10CFR50, Appendix B quality procedures and as described within this Plan.

2 REFERENCE DOCUMENTS

2.1 Regulatory Documents

1) 10CFR50, Appendix B, Quality Assurance Criteria for Nuclear Power Plants & Fuel Reprocessing Plants, January 20, 1975
2) USNRC Regulatory Guide 1.168 – Verification, Validation, Reviews and Audits for Digital Computer Software Used in Safety Systems of Nuclear Power Plants, February 2004

2.2 Standards and Guides

1) ANSI/ASME NQA-1-1994 - Quality Assurance Program Requirements for Nuclear Facilities Applications
2) EPRI TR-107330 - Generic Requirements Specification for Qualifying a Commercially Available PLC for Safety-Related Applications in Nuclear Power Plants; December 1996
3) IEEE Std. 7-4.3.2-1993 - IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations
4) IEEE Std. 730-2002 - IEEE Standard for Software Quality Assurance Plans
5) ANSI/IEEE Std. 1012-1998 - IEEE Standard for Software Verification and Validation Plans

2.3 Invensys Triconex Documents

1) Quality Assurance Manual (QAM)
2) Engineering Department Manual (EDM)
3) Tricon v10 Nuclear Qualification Project Nuclear Qualification Quality Plan (NQQP)
4) Tricon v10 Nuclear Qualification Project Master Test Plan (MTP)
5) Tricon v10 Nuclear Qualification Project SRS
6) Tricon v10 Nuclear Qualification Project TSAP Software Verification and Validation Plan (SVVP)

3 MANAGEMENT

3.1 Organization

The organization of the Tricon v10 Nuclear Qualification Project shall have a separate team for Verification and Validation (V&V) activities. The most effective organization is a separate V&V team that is responsible to an independent organization rather than to the manager of the development organization. To ensure independence, the V&V team reports to the IPS Nuclear Quality Director through the Project Quality Assurance Engineer (PQAE).

Refer to Section 3.0, Project Organization, of the NQQP for the organizational structure of the Tricon v10 Nuclear Qualification Project.

3.2 Tasks and Responsibilities

The responsibilities are defined in Section 4.0, Responsibilities, of the NQQP.

3.2.1 Software Design Team

The organizational structure for this Project is established in the Section 3.0, Project Organization, of the NQQP. The NQQP establishes and describes the Project organizational elements, duties and responsibilities, including those affecting quality and V&V activities. The management organization for software design is adequately addressed in the NQQP and further delineated in Section 3.2.3, Software Design Responsibilities.

3.2.2 Software Design Tasks

The tasks and their associations are defined in the NQQP. The following life cycle activities are applicable for TSAP development:

1) Requirements
2) Design
3) Implementation
4) Test
5) Installation and Checkout
6) Operations and Maintenance; and
7) Retirement

The softwar e quality as surance requ irements applicable to these life cy cles activities are described in this SQAP, the SVVP and the NQQP.

3.2.3 Software Design Responsibilities

The Project Manager (PM) has final authorization on TSAP software design issues. The PM provides overall management and provides technical direction for the nuclear qualification activities. The responsibilities of the PM are detailed in Section 4.4, Project Manager, of the NQQP.

The IPS Nuclear Quality Director has responsibility for TSAP quality assurance, e.g., adhering to the appropriate standards and guidelines; documenting the software in accordance with the quality assurance procedures set forth by the Project; conducting applicable testing; and developing verification and validation test procedures. The IPS Nuclear Quality Director

delegates authority for these activities to the PQAE, but retains overall responsibility. The tasks and responsibilities of the PQAE are detailed in Section 4.11, Project Quality Assurance Engineer, of the NQQP.

The Project Engineer (PE) has responsibility for the development of the application software, which is the TSAP, by following the standards specified in EPRI TR-107330 for nuclear qualification of the safety related application software, the SRS and the MTP. The responsibilities of the PE are detailed in Section 4.5, Project Engineer, of the NQQP.

3.2.4 Software Test Responsibilities

The Verification and Validation (V&V) Team shall independently perform all verification and validation activities related to the Tricon v10 Nuclear Qualification Project TSAP. The V&V Team shall perform software verification; develop the validation test plan/specification and test procedure(s); provide review of Project TSAP software documents; and conduct validation testing. The responsibilities of V&V Team are detailed in Section 4.12, TSAP Verification and Validation Team, of the NQQP.

Tricon v10 Nuclear Qualification Project TSAP verification and validation testing activities will proceed with the TSAP under version control. During these activities, the V&V Team has responsibility for ensuring that the TSAP under test is uniquely identified. TSAP testing will be complete when the TSAP passes the System Validation Test as described in the SVVP.

4 DOCUMENTATION

Invensys Triconex has an existing 10CFR50, Appendix B Quality Program which applies to all product hardware and software. The applicable software related policies and procedures of the Invensys Triconex Quality Program constitute an overall Software Quality Assurance Plan. Procedures which govern software development address a software life cycle model meeting the intent of NQA-1-1994, Subpart 2.7. The objective is to ensure that all new software generated by Invensys Triconex and/or revisions to existing Invensys Triconex software will follow the proper quality procedures for a software life cycle.

For Tricon v10 Nuclear Qualification Project quality activities, an NQQP has been established, as required by the Invensys Triconex QAM. The NQQP invokes the existing Invensys Triconex Quality Program/procedures in the above-referenced Manuals, and provides additional project-specific instructions. The NQQP requires development of this SQAP for software quality assurance.

EPRI TR-107330, Section 8.7 lists the minimum documents that are needed to support the V&V and related software quality processes. This list is based on ASME NQA-1-1994. The minimum documents are:

1) Section 8.7A Software Quality Assurance Plan (SQAP)
2) Section 8.7B Software Requirements Specification (SRS)
3) Section 8.7C Software Design Description (SDD)
4) Section 8.7D Software Verification and Validation Plan (SVVP)
5) Section 8.7E Software Verification and Validation Report
6) Section 8.7F User Documentation (Manuals)
7) Section 8.7G Software Configuration Management Plan

This SQAP is intended to satisfy item (1) above. Items (2) to (5) above apply to software developed for this Project. Item (6) is satisfied by Invensys Triconex User Manuals which are provided separately. Item (7) is conducted in accordance with Section 10, Code Configuration Management and Control, of this plan.

4.1 Software Requirements Specification

The SRS is structured to capture all the software requirements (design inputs). The SRS will describe each input and its function and these will be defined such that their achievement can be verified during the verification and validation (V&V) process. The requirements for the preparation, review, approval and control of the SRS are established in Section 10.1.3, Software Design Documents, of the NQQP.

4.2 Software Design Description

The SDD is structured to satisfy the software requirements of the SRS. The SDD will describe the components and subcomponents of the software design, including databases and internal interfaces. The requirements for the preparation, review, approval and control of the SDD are established in Section 10.1.3, Software Design Documents, of the NQQP.

4.3 Software Verification and Validation Plan

The TSAP SVVP is structured to identify the methods, tools and criteria used to determine the quality of items listed under this SQAP. The SVVP shall clearly indicate the verification and validation tasks that shall be carried out during the various stages of the TSAP development life cycle. The requirements for the preparation, review, approval and control of the SVVP are established in Section 10.1.2, Software Verification and Validation Plan, of the NQQP.

4.4 TSAP Final Verification and Validation Report

The TSAP Final V&V Report is structured to identify the various activities performed as part of Verification and Validation process. The TSAP Final V&V Report shall summarize the verification test results, validation test results, anomalies reported and corrective actions taken during V&V activities and provide a conclusion regarding TSAP quality. The requirements for the preparation, review, approval and control of the TSAP Final V&V Report are established in Section 10.4.4, Final V&V Report, of the NQQP.

4.5 User Documentation

Invensys Triconex user documentation specifies the required instructions for installation, project administration, application development, communications, configurations, implementation, limitations and other activities or items necessary for use of the software. Error messages are identified and corrective actions described, and a method provided for communicating problems to the correct technical support organization. The requirements for the preparation, review, approval and control of the user documentation are not applicable to the TSAP and are beyond the scope of this SQAP.

5 STANDARDS, PRACTICES, CONVENTIONS AND METRICS

This section of the SQAP identifies the standards (mandatory requirements), practices (recommended approach) and conventions (accepted guidelines) to be applied to software development of the Tricon v10 Nuclear Qualification Project. The NQQP covers the standards, practices and conventions to be followed in the software development process during this Project. No metrics are planned for TSAP development as the TSAP is one-time usage test software and metrics would not enhance the overall V&V process.

The standards and guides delineated in Section 2.2, Standards and Guides, of this Plan will be applied during various phases of the software development cycle, which includes the requirements, design, implementation, test, installation and checkout, operations and maintenance, and retirement phases.

Matrices are used to trace the EPRI TR-107330 requirements from source document through design documents. The traceability matrices shall be prepared, maintained, controlled and documented sufficiently during this Project to allow a technically qualified individual to follow from requirements to implementation and/or satisfaction. The matrices used to analyze the technical requirements in this Project are listed below:

1) CTM – EPRI TR-107330 Requirements Compliance and Traceability Matrix
2) STA – Software Traceability Analysis

CTM - The PE shall prepare the CTM in matrix form applicable to the technical requirements analyses for this Project. The CTM shall be reviewed by the IRE and approved by the PM prior to the preparation of Equipment Qualification (EQ) Summary Report. The PE shall ensure that the approved CTM is listed in the MCL as per Section 7.0, Configuration Management and Document Control, of the NQQP.

STA - The STA used in this Nuclear Qualification Project is detailed in Section 6.1, Technical Reviews and Tests, of this plan.

6 REVIEWS AND AUDITS

The TSAP software developed during the software life cycle process shall be reviewed on a planned basis to determine the extent of progress and to evaluate the technical adequacy of the work and its conformance to software requirements and standards. Reviews shall be conducted to evaluate the status and quality of development effort. Completion of reviews provides assurance that design integrity is maintained, software anomalies are identified and necessary changes have been identified and implemented. In general, the TSAP shall be reviewed for the following:

1) The requirements, i.e., inputs of the SRS, used for development of the TSAP are correctly selected and incorporated;
2) The functionality of the TSAP is consistent with design requirements, i.e., verification of the TSAP code against the SDD;
3) The program functions as expected based on its intended application as defined by the SRS, SDD and Function Block Diagrams (FBD), i.e., validation of the TSAP; and

4) The configuration of the TSAP is properly documented and maintained throughout the applicable life cycles.

6.1 Technical Reviews and Tests

The TSAP software developed during this Project shall undergo technical reviews when an engineering development phase is to be verified for acceptance and/or satisfaction of the exit criteria of that phase. All technical reviews shall be performed and documented in accordance with the NQQP and the SVVP.

1) STA – The V&V Team shall prepare the STA in matrix form applicable to the technical requirements analysis for this Project. The STA shall be reviewed, as a minimum, by the PQAE and a technically qualified reviewer and it shall be approved by the IPS Nuclear Quality Director prior to qualification activities. The PM shall ensure that the approved STA is listed on the MCL as per Section 7.0, Configuration Management and Document Control, of the NQQP.

2) Emulation Tests – The V&V Team performs the offline tests of the TSAP using the Emulator Panel. The Emulator Panel, which forms part of TriStation 1131, is also a tool that will be used for developing the TSAP. Emulated tests are conducted with simulated inputs and parameters to exercise the logic and confirm outputs. Emulated tests ensure that individual programs perform their required functions and output the proper results and data.

The requirements for Technical Reviews, as stated above, shall only apply to the TSAP developed during the life cycle of this Project. No technical reviews are planned for the embedded operating system firmware and application program development tool as these are not modified within the lifecycle of this Project.

6.2 Document Inspection

The software documentation developed during this Project will be subject to periodic technical review in accordance with the NQQP. These documents include, but are not limited to:

1) Software Requirements Specification
2) Software Design Description
3) Software Quality Assurance Plan
4) Software Verification and Validation Plan
5) Software Verification and Validation Reports
6) Test Specimen Application Program
7) TSAP Verification and Validation Records and Reports

6.3 Quality Assurance Audits

The quality assurance (QA) audits are scheduled as deemed necessary by the IPS Nuclear Quality Director.

7 TEST

7.1 Software Verification Testing

Tricon v10 Nuclear Qualification Project TSAP verification testing is conducted in accordance with the SVVP. All software will be tested to ensure that the TSAP performs its required functions and outputs the proper results and data. Software verification testing shall ensure each requirement of the SDD is adequately and correctly implemented. The TSAP for this Project will be analyzed and its internal programs shall be tested. The verification tests shall be conducted with inputs and parameters to exercise the logic and confirm outputs.

Software anomalies identified during the TSAP verification process shall be documented on a Qualification Project Anomaly Report (QPAR). Software anomalies are resolved through implementation of the QPAR process, as defined in Section 10.4.3, Anomaly Reporting, of the NQQP.

The TSAP anomaly resolution shall include documentation of the corrective actions taken to eliminate the anomaly and retest requirements. The anomaly shall be corrected and the associated TSAP function shall be appropriately retested and evaluated. Testing interaction with any previously tested function(s) shall be evaluated and all related documentation shall be updated.

As the embedded operating system firmware and TriStation 1131 are not modified within the lifecycle of this Project, no testing will be performed other than the functional checks conducted as part of system testing. However, if anomalies are found with these items during the verification process, they shall be documented on a QPAR. The QPAR disposition must be approved, but the QPAR does not have to be closed, in order for testing to proceed within the limits specified by the QPAR disposition. Justification shall be provided for testing to proceed within the specified limits. The QPAR disposition process will include identification of corrective action for these items and specify any retest requirements related to the Project

7.2 Software Validation Testing

Tricon v10 Nuclear Qualification Project TSAP validation is conducted after successful completion of the verification process. The TSAP to be validated is downloaded to the TUT and tested according to the SVVP. The results are evaluated to confirm that all requirements of the application software are met. Validation testing is conducted in accordance to the SVVP and Section 9.0, Test Control, of the NQQP. Software anomalies found during validation testing shall be documented and controlled as per the NQQP. Validation testing for the application software is detailed in Section 5.5, Test Phase (Validation), of the SVVP.

As the embedded operating system firmware and application program development tools are not modified within the lifecycle of this Project, no validation testing is performed. Software anomalies related to these items identified during validation are addressed in Section 7.1.

8 PROBLEM REPORTING AND CORRECTIVE ACTION

The results of verification tests shall be documented, which will state whether the functionality has passed or the reasons for its failure(s). If a test fails and the Project V&V Team decides that

the underlying problem must be fixed, then it shall be fixed based on an assessment. The individual tests, and any associated reviews which may be required as a result of the assessment, will be repeated and the specific failure will be retested for compliance and any changes to the TSAP and/or Configuration shall be evaluated and appropriate V&V activities shall be performed in accordance with the SVVP.

The QPAR shall be used to document deficiencies of software, including failure to meet acceptance criteria. When an anomaly is detected during testing or analysis, the problem will be resolved by initiating a QPAR, as defined in Section 10.4.3, Anomaly Reporting, of the NQQP.

The actions to be taken relative to any given anomaly are determined on a case-by-case basis. After an anomaly is resolved, affected tests or analyses will be repeated, as necessary.

9 TOOLS, TECHNIQUES AND METHODOLOGIES

Software development activities shall be accomplished using the applicable procedures to ensure that the system meets the requirements. Software quality assurance tools aid in the evaluation or improvement of software quality. Techniques include review of the use of standards, software documentation reviews, requirements tracing, and requirements and design verification and validation.

Software quality assurance methodologies shall be well documented for accomplishing a task or activity and provide a description of the process. This Project uses various application software tools to support software development for Tricon v10 system. All such tools, techniques and methodologies are described in Section 4.4, Tools, Techniques and Methodologies, of the SVVP.

10 CODE CONFIGURATION MANAGEMENT AND CONTROL

Project Software Configuration Management requirements are defined in EPRI TR-107330, Paragraph 7.7.3. In accordance with this paragraph, configuration management is mandated for the embedded operating system firmware, the TSAP application software, the application software development tools and software user documentation. As addressed in Paragraph 5.3.5 of IEEE Std. 7-4.3.2, software configuration management is to be performed in accordance with NQA-1-1994, Subpart 2.7.

Software configuration management is a routine and predefined process for design and manufacturing activities and has been incorporated in the Invensys Triconex 10CFR50, Appendix B program. Standard Invensys Triconex procedures, which encompass the above-mentioned elements of NQA-1-1994, Subpart 2.7, will be followed on this Project.

The PM shall have the responsibility for overall configuration management for both hardware and software as described in Section 7.0, Configuration Management and Document Control, of the NQQP. Software code development is an activity in progress until the application program is considered to be fully functional and ready for verification. V&V of the TSAP occurs throughout its life cycle and falls under configuration management control as it is released for Verification and Validation activities.

TriStation 1131 creates a project file that is under password and revision level control. TriStation 1131 increments the revision level each time an activity is compiled and adds an associated comments field. This information is retained in the project file. Access to the TriStation 1131 project (.pt2) file is password protected and only the TriStation 1131 tool can be used to modify the software.

When the software is ready for Verification and Validation, the code will be placed under the software configuration management process described in the NQQP. The TSAP is developed using FBDs and internal databases and it is programmed per the User Manual. The Function Block Diagram printouts are placed under configuration management at the time the code is considered fully functional and ready for Verification and Validation activities. This will occur near the end of the design and implementation life cycle phase and continue through the nuclear qualification testing activities.

The PM shall create and maintain the MCL, which captures the specific configuration information for all the software for this Project. The MCL shall be reviewed by the PQAE and approved by the PM prior to the start of nuclear qualification testing. The PM shall record any changes to the software during Verification and Validation activities of this Project in the MCL, which will be controlled and documented in accordance with the NQQP.

11 MEDIA CONTROL

The PE shall keep the PM informed of the software's location, program filename and associated password(s).

The original code, or a copy thereof, will be maintained on a server accessible to management. Backup provisions will be provided in accordance with local protocols. The server shall be backed up and data stored offsite to minimize the risks of data loss or corruption in accordance with the Invensys Triconex IT procedures. Alternatively, a CD-R or equivalent storage media may be used to make copies of the software. Such copies shall be stored in dual storage at locations known to the PM. In all cases, the fundamental requirement of having a back up copy, which is retrievable by management, shall be maintained.

If control of the program code is transferred, for testing or otherwise, then it must be maintained independently and should be retrievable by Project Management. Servers used for storage of original code will have access control protocols and permissions enabled. After the software code has been validated, a CD-R or other equivalent semi-permanent records will be used to backup and labeled with the program name and revision level. The TSAP software code (.pt2) file is a quality assurance record for the v10 Nuclear Qualification Project and, as such, it shall be maintained in accordance with the requirements of the NQQP. After this Nuclear Qualification Project, records are controlled in accordance with Invensys Triconex 10CFR50, Appendix B program.

12 SUPPLIER CONTROL

This section is not applicable for the T ricon v10 Nuclear Qualifi cation Project as no externally purchased software is used in the TSAP developm ent process an d/or verification and valida tion testing.

13 RECORDS COLLECTION, MAINTENANCE AND RETENTION

The PM shall develop and maintain the MCL. The MCL shall identify all approved nuclear qualification documents including requirements, plans, procedures, reports, final configurations of the test system, approved project software, test logs, etc.

The Nuclear Qualification Document Package contains all approved software documents in their final revision, necessary to demonstrate qualified software, and includes:

1. Nuclear Qualification Quality Plan (NQQP)
2. Software Quality Assurance Plan (SQAP)
3. Software Verification and Validation Plan (SVVP)
4. Software Requirements Specification (SRS)
5. Software Design Description (SDD)
6. Test Specimen Application Program (TSAP)
7. TSAP Test Specifications and Plans
8. TSAP Verification and Validation Reports
9. TSAP V&V Anomaly Reports
10. Software Traceability Analysis (STA)
11. EPRI TR-107330 Requirements Compliance and Traceability Matrix (CTM)

As a minimum, all the documents mentioned above are considered Quality Records. These documents shall be controlled, collected, maintained and retained according to the NQQP. After this Nuclear Qualification Project, the document package is controlled in accordance with Invensys Triconex 10CFR50, Appendix B program.

14 TRAINING

All Project personnel shall be trained and qualified in accordance with the NQQP.

15 RISK MANAGEMENT

Risk Management is:

1) An integral part of Project Management.
2) The responsibility of everyone on the Project team.
3) A process that starts at design and development stage and continues throughout the life of the Project.
4) Concentration on risks with the most adverse impact on Project activities.
5) Common sense.
6) Easy to understand and implement.

The following risks associated with the TSAP have been identified and are listed below:

Type	Description	Mitigation Plan
Risk	TSAP development prior to the baselining of the SRS, which may result in rework.	Maintain visibility and ensure TSAP development after SRS baseline.

Type	Description	Mitigation Plan
Risk	TSAP development prior to the baselining of the SDD, which may result in rework.	Maintain visibility and ensure TSAP development after SDD baseline.
Risk	Key V&V Engineers may be overloaded due to Project resource allocation constraints.	Maintain management visibility into the Project status. Be able to allocate more resources to reduce the workload.

The Tricon v10 Nuclear Qualification Project PM and PE will evaluate all identified risks and determine the methods to be used in eliminating and/or mitigating their consequences.