invensys
TRICONEX®

TRICONEX PRODUCTS – INVENSYS PROCESS SYSTEMS

Project:	**TRICON v10 NUCLEAR QUALIFICATION PROJECT**

Non -Proprietary copy per 10CFR2.390
- Areas of proprietary information have been redacted.
- Designation letter corresponds to Triconex proprietary policy categories (Ref. transmittal number NRC-V10-09-001, Affidavit, Section 4.)

SOFTWARE QUALIFICATION REPORT

Triconex Document No: 9600164-535

Revision 1

August 5, 2009

	Name	Signature	Title
Author:	Frank Kloer		Responsible Engineer
Reviewed by:	Gary McDonald		Independent Review Engineer
	Alan Sands		Project Quality Assurance Engineer
Approval:	Naresh Desai		Project Manager

invensys™
TRICONEX®

TRICONEX PRODUCTS – INVENSYS PROCESS SYSTEMS

Project:	**TRICON v10 NUCLEAR QUALIFICATION PROJECT**

SOFTWARE QUALIFICATION REPORT

Triconex Document No: 9600164-535

Revision 0

July 2007

MPR ASSOCIATES QUALITY ASSURANCE DOCUMENT

This document has been prepared, reviewed, and approved in accordance with the Quality Assurance requirements of 10 CFR 50, Appendix B, as specified in the MPR Quality Assurance Manual and in accordance with the requirements of Invensys Triconex Purchase Order No. 113803, dated March 23, 2006.

	Name	Signature	Title
Author:	David Herrell	David C Herrell	Supervisory Engineer, MPR Assoc.
Reviewer:	Chris Rice	Chris Rice	Lead Engineer, MPR Assoc.
Approval:	Eric Claude		ICT Group Manager, MPR Assoc.

Document Change History			
Revision	**Date**	**Change**	**Preparer**
0	July 19, 2007	Initial Issue	D. Herrell
1	08/05/2009	Revised to include missing Figure 7-1. Made typographical corrections and minor format changes.	F. Kloer

TABLE OF CONTENTS

Section **Page**

1.0 Executive Summary

This report documents the evaluation of the Triconex software and firmware for the TRICON Programmable Logic Controller (PLC), and TriStation 1131 Developer's Workbench. This evaluation is based on two main elements: the software development process, including Verification and Validation, and the design integrity of the system. Evaluation of the Triconex software development is based on the guidance provided in NUREG-0800, Chapter 7, BTP HICB-14, "Guidance on Software Reviews for Digital Computer-Based Instrumentation and Control Systems" (Reference 11). Evaluation of the system design integrity is based on the requirements established in IEEE Standard 7-4.3.2-2003, "IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generation Stations."

The design of the TRICON PLC has evolved into a mature product over more than 20 years. The software quality assurance program has also evolved and improved significantly over this period, especially in the period between the initial evaluation of TRICON Version 9.3.1 in 2000 and TRICON Version 10.2.1 in 2006. In the original evaluation, MPR concluded that the process met the intent of the requirements established by BTP HICB-14. MPR concludes that the process meets the regulatory expectations in both evaluations. The version of TriStation 1131 Developer's Workbench evaluated in the Version 9.3.1 qualification, used for engineering support and programming of the TRICON has been developed over the last 7 years, under a process compatible with the intent of BTP HICB-14. The version of TriStation 1131 evaluated in the Version 10.2.1 qualification evolved under a process meeting the expectations of BTP HICB-14.

The evaluation uncovered strengths in the development process, including the quality of the final product, design partitioning, product testing, error diagnosis and reporting, and change and configuration control. In the Version 9.3.1 evaluation, weaknesses were uncovered in maintenance of documentation of design bases and in documentation of review, or verification, of those documents. These weaknesses are adequately compensated for by reviews provided by a classically independent external agency (TÜV Rheinland) and in the quality of the work performed by the Triconex design and validation staff. Proof of the quality of their work is demonstrated in such statistics as 100 million operating hours, in safety critical functions, without a single failure to take a required protective action. These strengths and weaknesses are discussed and evaluated in this report and its appendix.

In the Version 10.2.1 evaluation, the previously identified weaknesses have been resolved. Processes for developing design documentation and performing internal reviews have been significantly improved. In addition, the classically independent external agency continues to review the design and coding of the TRICON PLC and TriStation software tools and the Triconex design and validation staff continues to do good, high quality work.

With the incorporation of the application guidelines provided in this report, the Triconex TRICON PLC and the TriStation 1131 software tools required for programming are acceptable for use in any safety related or high criticality application for nuclear power plants. The specific versions of the software and firmware considered in this qualification are provided in the Triconex Master Configuration List applicable to the Version 10.2.1 qualification project.

As long as Triconex uses their current development processes, or provides audited improvements, new versions of this software will be developed under a process which has been evaluated and accepted as compliant with the requirements established in 10 CFR 50 Appendix B. Therefore, these new versions would also be acceptable for use.

2.0 Introduction

This report, which has been prepared in support of the TRICON nuclear qualification, documents the basis for qualification of the software used in the TRICON version 10.2.1 system. This software includes the embedded real time operating system with its associated communication and input/output modules, and the PC-based system configuration software, TriStation 1131 Developer's Workstation, Version 4.1 Build 437, which Triconex also refers to as Version 4.1.437.

The approach used to develop the software qualification is based on the guidance provided in EPRI TR-107330, "Generic Requirements Specification for Qualifying a Commercially Available PLC for Safety-Related Applications in Nuclear Power Plants." EPRI TR-107330 states that qualification of software is to be performed using the guidance provided in EPRI TR-106439, "Guideline on Evaluation and Acceptance of Commercial Grade Digital Equipment for Nuclear Safety Applications." MPR also used EPRI TR-107339, "Generic Requirements Specification for Qualifying a Commercially Available PLC for Safety-Related Applications in Nuclear Power Plants," and EPRI Report 1011710, "Handbook for Evaluating Critical Digital Equipment and Systems," in preparing this report. Essentially, the approach involved evaluating the processes, procedures, and practices used to develop the software, assessing the history of the software itself and its associated documentation and operating experience, and analyzing the software architecture.

In the original report prepared for the Version 9.3.1 evaluation, the objective of this approach was to develop the confidence necessary to assure that the product being qualified is of at least the same quality as would be expected of a product developed under a nuclear quality assurance program, complying with the quality assurance requirements of 10 CFR 50, Appendix B. The approach allows the qualifier to compensate for shortcomings in the design, quality assurance, and verification and validation of the software by taking compensatory actions, including evaluating operating experience and performing “black box” testing.

For the Version 10.2.1 evaluation, Triconex has been operating under a 10 CFR 50 Appendix B program and the modifications have, for the most part, been made under that program. Some of the earlier work on the Main Processor was performed under the original program, using the same methods accepted in the original qualification, accepted by the NRC in their Safety Evaluation Report. However, the Main Processor design and development activities were completed under the 10 CFR 50 Appendix B program, with a clear path forward to bring the Main Processor documentation totally into compliance with the program.

2.1 Differences between the TRICON Version 9.3.1 and Version 10.2.1

The following points summarize the differences between the TRICON Version 9.3.1, which was evaluated in 2000, and the TRICON Version 10.2.1, which is the subject of the Version 10.2.1 evaluation.

- The TRICON Version 9.3.1 was a true commercial product. Version 9.3.1 was developed under a quality assurance program that was based on an ISO 9000 and 9001, quality assurance program and was not developed under a 10 CFR 50 Appendix B program. The evolving Triconex quality assurance program is explained in Section 5.0. Most new or redesigned components since that evaluation were developed under the updated Triconex program, which is compliant with 10 CFR 50 Appendix B. This includes the Model 3008 Main Processor (MP) executive, which used the Model 3006N MP as a basis but was significantly revised. The revision was performed mostly under the new Triconex program, but with modifications starting before the Appendix B program was in place.

- The Model 3006N MP in Version 9.3.1 is constructed of almost completely obsolete through-hole technology integrated circuits. It is because of this and other obsolescence issues that the Model 3008 MP was produced, which as of Version 10.2.1 is a modern design, widely used, and constructed of current technology including surface mount integrated circuits. The Model 3008 MP will become the basis for the Model 3008N nuclear qualified MP.

- The TRICON Version 10.2.1 includes the new TRICON Communication Module (TCM), based on surface mount technology, designed to replace communication modules evaluated in the Version 9.3.1 qualification. The TCM is equipped with two network ports and four serial ports, and was developed under the Triconex Appendix B program, but without unit testing. The TCM uses a commercial-off-the-shelf multi-tasking operating system. The TCM provides support for GPS time synchronization.

- The TRICON Version 10.2.1 includes the Next Generation Input and Output (NGIO) modules. Triconex has simplified development by creating a common, core architecture, featuring a new microprocessor. The common NGIO core forms the basis for two new modules evaluated for Version 10.2.1, the Next Generation Digital Output (NGDO) module and the Next Generation Differential Analog Input (NGAID) module. The Next Generation Single-ended Analog Input (NGAIS) module was evaluated in the Critical Digital Review (CDR), but not included in the qualification. The NGDO is a 24 volt dc supervised discrete output module with 32 outputs, with faster and more comprehensive diagnostics than previous discrete output modules. The NGAIS provides 64 channels of single ended analog voltage inputs. The NGAID provides 32 channels of true differential analog inputs. Both the NGAIS and NGAID provide faster conversion cycles (less than 10 milliseconds) than the older analog input modules.

- The TriStation 1131 software has been revised, primarily to support the new hardware. The Enhanced Diagnostic Monitor has been separated from the TriStation 1131 software to allow maintenance and troubleshooting without the possibility of inadvertently modifying a TRICON configuration.

2.2 Differences between EPRI TR-107330 and TRICON Qualification

EPRI TR-107330 provides requirements for functional evaluations and tests. There are two significant differences between the approach used in this qualification effort and the EPRI requirements. In each case, the differences result from a careful technical evaluation, and do not result from issues of schedule, budget, or cost. These differences, and the technical reasons for their acceptability, are defined in this section.

<u>Application Software Objects Acceptance (ASOA) Testing</u>

TR-107330 requires an Application Software Objects Acceptance test. This test is designed to verify that the software functions available for use in application programs have been adequately tested and perform as specified in the design basis documents. EPRI TR-107330 defines this as a mandatory test, without any regard or credit for the vendor's internal programs or other previous testing.

a, f

Use of TriStation 1131 and TriStation MSW

The Version 10.2.1 qualification used the current version of the TriStation 1131 tools.

The qualification testing used the Test Specimen Application Program (TSAP) during all tests. In Version 9.3.1, this program was generated with the TriStation Multi-System Workstation (MSW) development tool. This report provides an evaluation, contained in Section 7.3, of operational differences between the TriStation MSW and TriStation 1131 tools from the Version 9.3.1qualification. However, the MSW tool is now obsolete.

At the time the TSAP was initially developed for the Version 9.3.1 qualification, TriStation MSW was the most mature application development tool available. However, the MSW software was only available in a DOS-based environment. For the Version 9.3.1 qualification, the more recently developed TriStation 1131 is designed for a Windows NT environment. As of the Version 10.2.1 qualification, the TriStation 1131 tools have been migrated to the Windows XP environment.

In both the Version 9.3.1 and Version 10.2.1 qualifications, TriStation 1131 is judged to be a mature product, with a documented design basis and improved functionality. Since TriStation 1131 provides beneficial improvements and more commercial longevity, the justification for qualification of application development software focuses on TriStation 1131 and not on TriStation MSW.

2.3 Report Structure

This report contains the evaluation of the TRICON firmware and the TriStation 1131 Developer's Workbench software. The report is structured to protect the Triconex proprietary materials required to support this evaluation. The proprietary materials, including the detailed architectural and process evaluations, are contained in the CDR (Reference 1). An architectural overview is provided to support the conclusions and application guidance provided in this report.

The CDR, which consists of Triconex proprietary materials, is provided as a separate report (Reference 1). The CDR also contains an evaluation of design integrity based on the requirements established in IEEE Standard 603-1998, IEEE Standard 7-4.3.2-2003, Regulatory Guide 1.152 Revision 2, and selected sections of NUREG-0800, Chapter 7.

Application guidelines were developed while evaluating the software. These guidelines are intended to assure that plant-specific systems are implemented in a way that reduces, to the maximum extent possible, the likelihood of errors due to application of the TRICON. These guidelines were incorporated into the Version 9.3.1 Application Guideline Section of the Qualification Summary Report, Triconex Report Number 7286-545. Triconex will incorporate these requirements into the Version 10.2.1 report, Triconex Report Number 9600164-545.

The TÜV Rheinland evaluation of the TRICON and TriStation 1131 resulted in the restrictions and requirements for safety critical programs defined in Triconex documentation. During evaluation of the TRICON and TriStation 1131 for nuclear safety related use, the TÜV requirements were evaluated and modified for application to USNRC nuclear safety related requirements. Triconex will incorporate these restrictions and requirements in the Application Guideline Section of the Triconex Qualification Summary Report.

3.0 Architecture Overview

In order to evaluate design integrity, it is necessary to understand the TRICON architecture. This section of the report provides a brief description of the TRICON system and its operation. The intent is to describe the important functionality of the system and the relationship between the hardware and software.

3.1 System Overview

The TRICON, a Triple Modular Redundant (TMR) digital controller, is triple redundant from input terminal to output terminal, as shown in Figure 3-1. The TMR architecture is intended to allow continued system operation in the presence of any single point of failure within the system.

a, b

a, b

The TRICON is designed for nuclear mild environments, as defined in IEEE standards for Equipment Qualification. The electronics use many CMOS components, allowing the system **to** function in up to 60°C environments without cooling fans. Each system consists of one or more rack or panel mounted chassis. Each chassis is powered by two independent, redundant power supplies, each capable of providing the full power requirements of the chassis. Thus, the system can withstand a power supply failure without interruption.

The TMR architecture, shown in Figure 3-1, is also intended to allow the TRICON to detect and correct individual faults on-line, without interruption of the process under control. It will recover from such faults when the affected module is replaced; thus returning to fully triplicated status. It provides for on-line, hot replacement of any module, under power while the system is running, with no impact to the operation of the control application. In addition to its triplicated operation, it will operate in dual and single modes, depending on the failure encountered and the user-selected configuration. This 3 2 1-0 operational mode stabilizes operations by providing the user the option of continued process operation or controlled shutdown in the presence of one or two failed main processors, and then going to the safe state when all main processors fail. The TRICON can also be configured to operate in a 3-2-0 operational mode, where failure of two single Main Processors results in the TRICON outputs going to the safe state (discrete outputs off, analog outputs set to minimum current).

Figure 3-1 shows the arrangement of the input, Main Processor (MP), and output modules. As shown, each input and output module includes three separate and independent input or output circuits. These circuits communicate independently with the three main processor modules. The TRICON chassis includes provisions for a spare module, logically paired with a single input or output module. These spare modules are hot swapped into the system by removing the other module. Standard firmware is resident on the main processor modules for all three microprocessors as well as on the input and output modules and other communication modules.

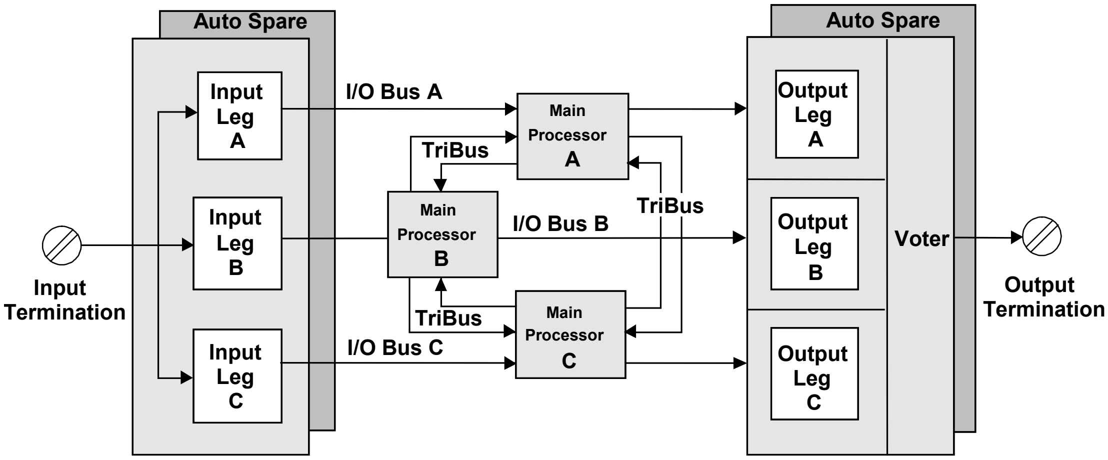

Figure 3-1. TRICON Triple Modular Redundant Architecture

3.2 Main Processor Modules

In the original qualification each Main Processor (MP) Model 3006N was designed around a thirty-two bit microprocessor (the National Semiconductor 32GX32) and two auxiliary 8-bit microprocessors used for communication. One of the auxiliary microprocessors interfaces with the eight bit microprocessors used on the input and output modules. The other auxiliary microprocessor interfaces with the eight bit microprocessors used for communication with external computing systems. The operating system, run-time library, and fault analysis for the MP is fully contained in read-only memory (ROM) on each module. The MPs communicate with one another through a proprietary, high speed, voting, bi-directional serial channel called TriBus. Each MP has an I/O channel for communicating with the triplicated I/O modules. Each MP has an independent clock circuit and selection mechanism that enables all three MPs to synchronize their operations periodically to allow voting of data and exchange of diagnostic information.

In the Version 10.2.1 qualification, each Main Processor (MP) Model 3008 uses two thirty-two bit microprocessors (the Freescale Semiconductor Model MPC860EN). One of the microprocessors runs the application software. The other microprocessor interfaces with the input, output, and communication modules. The operating system, run-time library, and fault analysis for the MP is fully contained in flash memory on each Main Processor Module. The MPs communicate with one another through a proprietary, high speed, voting, bi-directional serial channel called TriBus. Each MP has an I/O channel for communicating with the triplicated I/O modules. Each MP has an independent clock circuit and selection mechanism that enables all three MPs to synchronize their operations periodically to allow voting of data and exchange of diagnostic information. Each MP has a channel for communicating with the non-triplicated communication modules.

When a fault is detected on a main processor module, it is annunciated and voted out, and processing continues through the remaining two MPs. When the faulty main processor is replaced, it runs a self-diagnostic to determine its basic health. When the self-diagnostic successfully completes, the MP then begins the process of “re-education,” where the control program is transferred from each of the working units into the returning MP. All three Main Processors then resynchronize data and voting, and the replacement processor is allowed back in service.

During initial program loading, the application program is loaded into all three MPs simultaneously from the TriStation 1131 computer attached to a TRICON Communications Module.

The system firmware resident on the MP is designed in a modular manner. In the original Version 9.3.1 qualification, three sets of dedicated function microprocessor firmware exist on the Main Processor. The main 32-bit microprocessor had the TRICON System Executive (TSX) operating environment firmware. The two additional microprocessors (the I/O and communication interfaces) each have their own firmware.

In the Version 10.2.1 qualification, two sets of dedicated function microprocessor firmware exist on the Model 3008 MP. The main 32-bit microprocessor has the Enhanced TRICON System Executive (ETSX) operating environment firmware. The other microprocessor, interfacing to the input, output, and communication modules, has its own Input and Output Control and Communication (IOCCOM) firmware.

The main microprocessor firmware provides the intelligence to implement the extensive built-in self-diagnostics and triple redundancy functions.

The application program interfaces only with the main 32-bit microprocessor. The main microprocessor is configured with the application program from TriStation 1131. Some configuration data is provided to the I/O and communication microprocessors on the main processor board. A limited amount of communication module configuration data is passed from the main microprocessor to communication modules. All other microprocessors perform their dedicated functions based on fixed firmware programming.

3.3 I/O Modules

Each I/O module consists of three identical and independent circuits, all contained on a single printed circuit assembly. Input data is sampled continuously, in some modules compared and/or voted, and sent to the MPs. Each of the triplicated microprocessors communicates through a separate, hardwired input/output bus to a designated MP. In each Model 3006N MP qualified in Version 9.3.1, the I/O bus microprocessor on each MP reads the data and provides it to the MP microprocessor implementing the application logic through a dual port RAM interface. In each 3008 MP, the combined input, output, and communication (IOCCOM) microprocessor on each MP reads the data and provides the data to the MP microprocessor implementing the application logic through a dual port RAM interface. Each microprocessor implementing the application logic then transfers and votes on all data over the TriBus. The control algorithm is invoked only on known good data.

After the microprocessors implementing the application logic complete the control algorithm, each MP sends data to the output modules through the separate input/output module data busses to the output modules. The output modules vote on the data again at the final output point. Each solid state discrete output uses a unique, patented, power output voter circuit. Analog outputs use a switching arrangement tying the three legs of digital to analog converters to a single point. Outputs from the MPs are provided to the I/O bus microprocessors through dual port RAM. For the Version 9.3.1 qualification, the I/O bus microprocessors then transfer that data to the triplicated microprocessors on the output modules. For the Version 10.2.1 qualification, the IOCCOM microprocessors then transfer that data to the triplicated microprocessors on the output modules. The output modules then set the output hardware appropriately on each of the triplicated sections and vote on the appropriate state and/or verify correct operation.

If an I/O module channel fails to function, an alarm is raised to the MPs. If a redundant module is installed in the paired slot with the faulty module, and that module is deemed healthy by the MPs, the system automatically switches over to the standby unit and takes the faulty module off line. If no standby unit is in place, the faulty module continues to operate on two of the three legs and control is unaffected. The user obtains a replacement unit and plugs it into the paired slot associated with the failed module. This position is physically adjacent to and logically paired with the failed module’s location. When the MPs detect the presence of a replacement module, they initiate local health state diagnostics and, if the module is healthy, automatically switch over to the new module. The faulty module is then removed and returned to the factory for repair.

If redundant modules are installed and both are deemed healthy by the MPs, each of the modules will be exercised on a periodic basis. The MPs will swap control between the redundant modules. By periodically using the module, any faults will be detected, alarmed, and the failed module replaced while a redundant module is in place. This use of redundant modules does not cause process upsets.

The system firmware resident on the Input/Output modules is designed in a modular manner. For the original Version 9.3.1 qualification, the firmware was not designed on a common software base, and many different firmware sets exists. For the Version 10.2.1 qualification, the firmware is based around a hardware and software base. Specific customization is applied to fit the needs of the module and the data to be acquired. This customization includes the integral diagnostic capabilities. Each of the three microprocessors on a module runs exactly the same firmware. Each microprocessor interfaces to only one leg of the I/O bus, and thus to only one MP.

Since the original Version 9.3.1 qualification, many of the components on the Input/Output modules have become obsolete, and support for the varied firmware on the modules has become difficult. As a result, Triconex has been redesigning the Input/Output modules around a common hardware and software architecture. These new modules are referred to as the Next Generation Input/Output modules. For this qualification, only two of these new modules have been introduced, but software for three modules was evaluated. These Next Generation supervised Discrete Output (NGDO) and Next Generation Analog Input – Differential (NGAID) were part of the qualification project. The Next Generation Analog Input – Single Ended (NGAIS) software was evaluated, but the module was not included in the qualification. The software that runs on these new modules is evaluated in this report.

3.4 Communications Modules

The interconnection between Main Processors and Communication Modules is shown in Figure 3-2. There are similarities as well as significant differences between the design of communication modules and the input/output modules. Like the I/O modules, the communication modules have three separate communication busses and three separate communication bus interfaces, one for each of the three MPs.

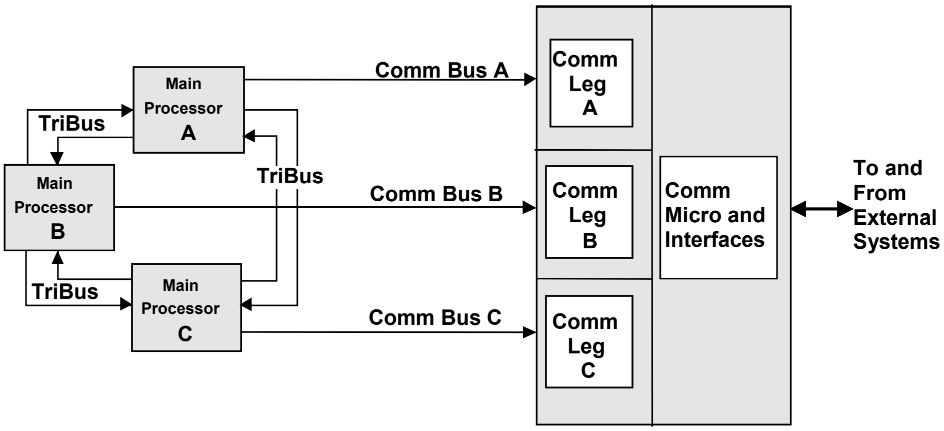

Figure 3.2. TRICON External Communication Architecture

Unlike the I/O modules, the three communication bus interfaces are merged into a single microprocessor.

In the original Version 9.3.1 qualification, three modules were evaluated, including the Advanced Communication Module (ACM), the Enhanced Intelligent Communication Module (EICM), and the Network Communication Module (NCM). In the ACM, the module's microprocessor votes on the communication messages from the three MPs and transfers only one of them to an attached external system. In the EICM and NCM modules, the most recent information is used without voting. For two-way communications, messages received from the attached external system are triplicated and provided to the three MPs.

In the Version 10.2.1 qualification, an additional communication module was evaluated, the TRICON Communication Module. In the TCM, the module microprocessor votes on the communication messages from the three MPs and transfers only one copy of the message to an attached external system if at least two agree. For messages received from external systems, the module triplicates the message and provides a copy to each of the three MPs.

The communication paths to external systems have appropriate levels of Cyclic Redundancy Checks (CRC), handshaking, and other protocol-based features. These protocol features are supported in hardware and firmware. For the original communication modules, theses features are core functionality common to the communication modules. For the Version 10.2.1 qualification, the TCM is intended to provide additional capabilities, which could be used to replace the original communication modules.

3.5 TriStation 1131 Software

One of the supported external protocols is communication with the external application programming and diagnostics tool. In the original qualification, application programming is generated and diagnostics are performed using the TriStation 1131 Developer's Workbench. In the Version 10.2.1 qualification, application programming is generated using the TriStation 1131 Developer's Workbench and diagnostics are performed using a separate Enhanced Diagnostics Monitor. The Enhanced Diagnostics Monitor was separated from the TriStation 1131 tools to reduce the risk of inadvertent changes during troubleshooting.

The TriStation 1131 software provides three IEC 61131-3 compliant languages, including Structured Text, Function Block Diagrams, and Ladder Diagrams, as well as a Triconex-defined Cause and Effect Matrix language, called CEMPLE. The TriStation 1131 software implements a Graphical User Interface comprising language editors, compilers, linkers, emulation, communication, and diagnostic capabilities for the TRICON. While the TRICON is performing safety critical functions, the TriStation 1131 PC would not normally be connected.

The TriStation 1131 software is the tool for developing an application program tailored to its field use and downloading that application to the TRICON PLC. When the original qualification was performed, TriStation 1131 was intended for use on an IBM compatible PC in a Windows NT environment. The current version of the TriStation 1131 software is intended for use on an IBM compatible PC in a Windows XP Professional environment. The software is constructed using current Microsoft Visual C++ and graphical user interface design techniques appropriate to Microsoft Foundation Classes.

4.0 Qualification Approach and Criteria

With an understanding of the platform and its architecture established in the earlier sections of this report, the basis for review can be established and findings discussed.

Ultimately, the basis for the qualification of the TRICON system software is the U.S. Nuclear Regulatory Commission Standard Review Plan (SRP), provided in NUREG-0800, Section 7, "Instrumentation and Controls." The approach used to demonstrate compliance with the requirements of the SRP is based on the guidance provided in various EPRI reports. This approach, including the activities performed as part of the software qualification effort and the acceptance criteria established for these activities, is described in this section.

4.1 Regulation and Industry Standards

The SRP (NUREG-0800) Chapter 7 (Reference 11) contains specific requirements for the digital aspects of instrumentation and control equipment. These requirements are contained in:

- NUREG-0800, Section 7.1, "Instrumentation and Controls – Introduction"
- NUREG-0800, Appendix 7.0-A, "Review Process for Digital Instrumentation and Control Systems"
- NUREG-0800, Branch Technical Position HICB-18, "Guidance on the Use of Programmable Logic Controllers in Digital Computer-Based Instrumentation and Control Systems"
- NUREG-0800, Branch Technical Position HICB-14, "Guidance on Software Reviews for Digital Computer-Based Instrumentation and Control Systems"
- NRC Regulatory Guide 1.152 Revision 2, which endorses IEEE Standard 7 4.3.2-2003 "IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generation Stations"
- IEEE Standard 7-4.3.2 provides a digital interpretation of IEEE Standard 603 1998, "IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations"
- Title 10 of the Code of Federal Regulations Part 50.55a(h) (10 CFR 50.55a(h)) endorses IEEE Standard 603-1991.

4.2 IEEE Standard 7-4.3.2-2003

IEEE Standard 7-4.3.2-2003 is primarily for the development of new computer systems and provides requirements for a complete system life cycle. Section 5.3.2 of this standard recognizes the need to qualify existing commercial computers. This standard does not go into any detail on the acceptance of pre-developed software, although the standard states that, after acceptance, future changes shall follow the IEEE Standard 7 4.3.2-2003 requirements.

The principal thrust of IEEE Standard 7 4.3.2-2003 is to address requirements for sufficient design integrity. Since the final proof of any Software Quality Assurance program is the quality of the final product, the TRICON and TriStation 1131 Developer's Workbench were evaluated to the design integrity requirements specified in this IEEE Standard. Detailed results from this evaluation are provided in the proprietary Critical Digital Review, (Reference 1).

4.3 NUREG-0800, Chapter 7, BTP HICB-18 and BTP HICB-14

An essential issue for acceptability is a defined, controlled development process. The requirements specified in IEEE Standard 1012-1986 provide an approach that is acceptable to the NRC staff for meeting the requirements of 10 CFR Part 50 and the guidance given in Regulatory Guide 1.152, “Criteria for Digital Computers in Safety Systems of Nuclear Power Plants.” NRC Regulatory Guide 1.168 endorses IEEE Standard 1012-1986 as an acceptable methodology for implementing the verification and validation of safety system software, subject to certain exceptions listed in that Regulatory Guide.

a, b, f

Referring to SRP Section 7.1, paragraph II, “Supplemental Guidance for Digital Computer-Based Safety Systems,” item 2.b discusses the use of existing PLCs as a means of implementing safety related instrumentation and controls. This item states that “BTP HICB-18 describes an acceptable process for applying the recommendations of this section to PLC implementations.”

BTP HICB-18 is based on review of licensee submittals and the analysis of PLC related issues documented in NUREG/CR-6090. The acceptance criteria of BTP HICB-18 discuss six areas of review. These are:

1. PLC hardware

2. Embedded and operating system software

3. Application software

4. Application software development tools

5. Real-time performance and testing

6. Program change configuration control

a, b, f

Certain areas of the PLC platform clearly map the base platform of the TRICON and the TriStation 1131 Developer's Workbench into the requirements established in NUREG-0800, Chapter 7, BTP HICB-14, "Guidance on Software Reviews for Digital Computer-Based Instrumentation and Control Systems." The platform and the application tools are clearly software written on a computer. The Critical Digital Review, provided as a separate report (Reference 1), provides a complete analysis of the PLC and the workstation tool for compliance with the requirements established in BTP HICB-14. The attributes provided in BTP HICB-14 are a means of evaluating the concerns associated with digital instrumentation and control (I&C) systems.

As expressed in SRP Appendix 7.0A, the use of digital I&C systems presents the concern that minor errors in design and implementation can cause digital devices to exhibit unexpected behavior. To minimize this potential problem the design qualification for digital systems needs to focus on a high quality development process that incorporates disciplined specification and implementation of design requirements. Potential common-mode failures caused by software errors are also a concern. One of the protection means against common-mode software failures is also accomplished by an emphasis on the quality process.

For Commercial-Off-The-Shelf (COTS) software, there needs to be a reasonable assurance that the equipment will perform its intended safety function and is deemed equivalent to an item designed and manufactured under a 10 CFR Part 50 Appendix B quality assurance program. To accomplish this, the SRP emphasizes the implementation of a life cycle process and an evaluation of the COTS software development process.

EPRI TR-107330, Section 8.7 lists the minimum documents that are needed to support software verification and validation and the related software quality processes. This list is based on NUREG/CR-6241, which NUREG-0800, Chapter 7, BTP HICB-18 (Reference 11) describes as an acceptable process for qualifying existing software, and ASME NQA-1-1994. The minimum documents are:

- Software quality assurance plan
- Software requirements specification

- Software design description
- Software V&V plan
- Software V&V report
- User documentation (Manuals)
- Software configuration management plan

This review establishes that there are sufficient documents, as well as sufficiently mature product, to accept the TRICON PLC and TriStation 1131 as acceptable for nuclear safety related use. f

4.4 Software Qualification Approach and Criteria

Table 4-1 below summarizes the critical characteristics of digital devices being evaluated for safety critical applications. The acceptance criteria used to qualify the TRICON and TriStation 1131 software and the methods used to evaluate compliance with these criteria are described in Table 4-1. Table 4-1 is based on Tables 4-1 and 4-2 of EPRI TR 106439. f

a, b, f

a, b, f

a, b, f

The results of these evaluations were then used to assess the overall quality of the TRICON software with respect to the level of quality expected for nuclear safety related systems. As shortcomings were found, compensatory actions were developed. The results from these compensatory measures are included in the CDR. The following items correspond to Table 4-1 and reflect conclusions developed and explained throughout the report and the appendices.

a, f

a, f

a, f

5.0 Process Evaluation

When the original review was performed, the TRICON software had been initially developed 15 years earlier, and had evolved into the Version 9.3.1 configuration. Within the original time frame, the product has matured to incorporate design enhancements. When the TRICON operating system and support software was conceived there was very little guidance in the way of industry standards to base the software development and design. Good programming practices were used based on the objective of producing a highly reliable safety system. When the Version 10.2.1 review was performed, the TRICON processes had grown significantly more mature than those reviewed in Version 9.3.1.

The evolution and history of the processes, practices, and procedures used to control the development of this software are summarized in this section. A more detailed description and evaluation of the development process is provided in the CDR (Reference 1).

5.1 Quality Assurance and Software Development Process

The basic software developed for the TRICON and TriStation originated around 1985. The development process demonstrates administrative and program controls which have evolved over time, becoming formally documented in departmental procedures.

The Triconex Quality Assurance Manual was first issued in June of 1986. The model for the QA program was ISO 9000 and 9001. As part of the Version 9.3.1 qualification, Triconex created an Appendix B program and added compliance to ASME NQA-1. The intent of ASME NQA-1 is to provide the nuclear industry with a standard for a Quality Assurance program that will meet the requirements of 10 CFR 50 Appendix B. Modifications to the software past the Version 9.3.1 qualification were performed in accordance with the guidance in that program and the guidance found in IEC 61508.

The Triconex Engineering Department Manual (EDM), first issued in 1986, formalized common practices with the following key procedures:

- EDM 20.00, Configuration Management
- EDM 40.10, **Software Specification Content and Format**
- EDM 40.51, Software Coding Practices **and Guidelines**

In 1991, the TRICON Version 6.2.3 received TÜV Rheinland certification for use as Class 5 safety equipment. As a result of the TÜV certification, new procedures were added and existing procedures reinforced to formalize the software development and configuration control process actually practiced in 1992. IEEE standards and other software development references available at that time were used as guides. New software development procedures included:

- EDM 24.00, Software Configuration and Change Control (based on IEEE Standard 1042)
- EDM 40.10, **Software Specification Content and Format** (based on IEEE Standards 830 and 1016)
- EDM 40.50, Software Development Guidelines (based on IEEE Standard 1012)
- EDM 40.51, Software Coding Practices **and Guidelines**

ASME NQA-1-1994 Subpart 2.7 addresses a software life cycle that is based on the model similar to IEEE 1012-1998, “IEEE Standard for Software Verification and Validation Plans.” It should be noted that these standards allow for alternate approaches and flexibility depending on the nature and complexity of the software. This is consistent with NUREG-0800, Chapter7, BTP HICB-14 which also acknowledges alternate approaches. In Table 5-1, a comparison of the major elements of the Triconex life cycle development process to ASME NQA-1-1994 and IEEE Standard 1012 is shown to illustrate similarities.

The QA program was updated in March of 1998 to be in full compliance with 10 CFR 50 Appendix B as well as ISO 9001-1994. The current QA program and departmental procedures satisfy the following:

- ISO 9001-1994 in the Version 9.3.1 qualification
- ISO 9001-2000 in the Version 10.2.1 qualification
- 10 CFR 50 Appendix B
- TÜV Certification for DIN V VDE 19250, resp. DIN V VDE 0801 Class 6 in the Version 9.3.1 qualification
- TÜV Certification for IEC 61508, Part 1-7:2000, IEC 61511-1:2004, EN 50156-1:2004, EN 61131-2:2005, EN 61000-6-2:2005, EN 61000-6-4:2001, EN 54-2:1997, NFPA 72:2002, NFPA 85:2001. TÜV concludes that the TRICON Version 10.2.1 system is suitable for safety related applications up to Safety Integrity Level (SIL) 3, based on their test report number 968/EZ 105.06/06, dated 2006-10-31.

The TRICON Version 10.2.1 and TriStation 1131 Version 4.1.437 being qualified started with the TRICON Version 9.3.1 and TriStation 1131 Version 2, which were modified and expanded under Triconex 10 CFR 50 Appendix B quality assurance program. Triconex also has upgraded their ISO compliant quality assurance program to ISO 9001:2000, which was applied. Triconex also works in compliance with IEC 61508 and 61511, which require documentation, verification, validation, peer review, and testing for safety critical SIL certification.

a, f

5.2 TÜV Certification

TÜV Rheinland is a German third party certification agency that validates equipment to existing international standards. In 1992, TÜV Rheinland first certified the TRICON Version 6.2 to meet standard DIN V VDE 19250, by meeting DIN V VDE 0801 requirements for safety equipment, class 5, as documented in TÜV Rheinland Test Report 945/EL 366/91.

Each new version has been tested by TÜV Rheinland, with Version 9.3 being certified in February of 1998 to class 5 and class 6 of the DIN standard (Test Report 945/EZ 102/98). The testing preformed by TÜV Rheinland examines both the hardware and the software. Both the system software (TSX and associated communication and I/O support modules) and the application development tools software (TriStation MSW 3.1 and 1131) are reviewed and tested with each new version.

When the Version 10.2.1 CDR was performed, Triconex had received the draft of the TÜV Rheinland report approving use of the TRICON Version 10.2 in applications up to SIL 3, in accordance with IEC 61508 and IEC 61511. This is documented in TÜV Rheinland Report-No.: 968/EZ105.05/06, dated October 31, 2006, approving use of TRICON Version 10.2 and TriStation 1131 Version 4.1 Build 437. For the Version 10.2.1 qualification, the system software (ETSX and associated communication and input/output modules) and the application development tool (TriStation 1131) continued to be reviewed and tested with each new version.

The three aspects of software review and testing by TÜV Rheinland are:

- Software analysis
- Software test
- Software and integration (software/hardware) test

<u>Software Analysis</u>

a, f

Software Test

The original TriStation MSW software (the application tools software) TÜV Rheinland testing consisted of three parts.

- User Program – The translation from the user program (ladder logic) to the final code for the Main Processors in the TRICON was checked. This was accomplished by disassembling the code the TriStation MSW software produced and then downloading the reassembled code to the TRICON using a TÜV program.
- User Interface – The programs developed for the hardware tests were used to validate the functionality of the ladder logic.
- Negative Testing – All the error message conditions (except Out of Space) were simulated and verified that the correct messages were produced.

In the original qualification, the TRICON software testing consisted of the following:

- Internal Fault Routines – Procedures such as the watchdog routines, CPU test, etc. were checked by watching the normal execution of these routines and by forcing execution of the routines by injecting faults.
- Noise on the Main Processor Module – A software module was developed to simulate noise on the processor by putting the CPU address pointer to arbitrary positions and verifying proper detection.
- TSX Functional Verification – Portions of the Triconex functional verification procedures were performed to verify software module performance and validity of Triconex test procedures.

For the latest version, the TRICON and TriStation 1131 software testing consisted of the following:

a, f

a, f

Software and Integration Testing

The function and purpose of the PLC is processing information based on instructions provided from the user application program. In addition, the PLC must have the ability to allow communication with the outside world and have the ability to detect and process hardware problems. These tests are designed to verify the interface between the PLC software and PLC hardware.

- Application Program – In the original qualification report, TÜV Rheinland tested the ability to process the user application program with the TriStation MSW software. TÜV Rheinland engineers have continued to verify that the TriStation 1131 software tools produce correct programs.

- System Test – In the original qualification report, the main processor operating system software (TSX) is tested by Triconex's Functional Verification procedure, which is intended to simulate a system environment. TÜV Rheinland performed selected portions of this procedure; particularly dealing with external inputs to the TRICON in addition to the TÜV Rheinland I/O malfunction test. For the Version 10.2.1 qualification, TÜV Rheinland engineers have continued to verify that the TRICON and TriStation 1131 software tools implement the user applications correctly.

5.3 Configuration Control

The TRICON contains several firmware sets, on several modules. A TRICON version is defined on a formally released, configuration controlled Software Release Definition. These documents define the unique compilation and linkage definition Meta number for each firmware set in a TRICON and TriStation 1131 release. The firmware defined in each Software Release Definition has been validated by both Triconex Product Assurance and by TÜV Rheinland before the release is announced. Unannounced releases can not be shipped to anyone other than TÜV Rheinland for testing.

It is important to recognize that the 2000 qualification effort evaluated and accepted the TRICON Version 9.3.1 and TriStation 1131 Version 2.0 as products acceptable for use in nuclear safety related applications.

a, f

Instead, both the Version 9.3.1 and Version 10.2.1reports accept the quality of the Triconex procedures and the TRICON and the corporate capability to maintain system quality. With a functional Quality Assurance program and acceptable software quality assurance procedures, the current version is acceptable for nuclear safety related use. The original report concluded that there were no issues with accepting a firmware enhancement in the ACM module, thus upgrading the TRICON to Version 9.4. With that upgrade, TriStation 1131 Version 2.0 is required. The Version 9.3.1 report concluded that both the TRICON Version 9.4 or later and TriStation 1131 Version 2.0 or later are acceptable for use in a nuclear safety related application. The Version 10.2.1report concludes that both the TRICON Version 10.2.1 and TriStation 1131 Version 4.1, Build 437, are acceptable for use in nuclear safety related applications.

A TRICON PLC and TriStation 1131 Developer's Workbench provides an acceptable platform on which applications can be built for safety related service. This qualification effort used a synthetic application program for testing, built under development, verification, and validation procedures in the Triconex EDM.

6.0 System History

The TRICON and the TriStation 1131 software are not new products. As mature products, they provide proven technology for safety related use. The TRICON and the TriStation 1131 are mature, evolutionary products, grown and enhanced through a continuous process of hardware, software, and firmware improvement. New versions reflect hardware or software improvements or corrections, not new directions. The development process leading up to the Version 9.3.1 qualification is reflected in Figure 6-1.

TRICON Version 6.2.3, released in 1991, is the first version to be certified by TÜV Rheinland for safety critical use. Figure 6-1 started at Version 6.0 to illustrate the development to Version 6.2.3, which is credited as the first version to have independent verification and validation from the classically independent certification agency, TÜV Rheinland.

In order to trace the development of the TRICON from that certification, the Product Release Notices and Software Release Definitions for the releases since Version 6.0 were reviewed. All Product Alert Notices for the entire system were reviewed. The Product Alert Notices are the Triconex commercial equivalent to the nuclear 10 CFR 21 notification process. The same process was followed to generate Figure 6-2, starting at the point where Figure 6-1 ended, with the original Version 9.3.1 qualification.

These version trees, provided as Figures 6-1 and 6-2, attempt to graphically summarize the resulting data. Time advances down the page. To provide some concept of the amount of time, Version 6.2.3 was released in 1991. Version 9.3.1 was released in April 1998. Version 9.4 was released in February 1999. Since the table was created, Version 9.5 has been released and is the current version that would be purchased and installed. Figure 6-2 starts with the Version 9.3.1 qualification and comes forward to the Version 10.2.1 qualified version.

Versions are numbered with a numbering system that provides the major, minor, and maintenance version data. Major versions on the figure are 6.0, 7.0, 8.0, and 9.0. Major releases require extensive hardware and/or software changes to upgrade. As an example, major Version 9.0 reflected a change in the system chassis, removing the terminations from plug-in modules with the Input/Output modules to Elco connectors on the top of the chassis. Thus, an upgrade to Version 9.0 would have required major hardware and field termination changes.

a, b

Upgrading to this release requires replacing the three Main Processors and recompiling the application.

Minor releases and maintenance releases generally require less effort to install. For these releases, software and/or firmware changes may be required. The minimum supported hardware, software, and firmware levels are defined in the Product Release Notice. These releases normally result from error corrections or product capability enhancements. Just because releases occur in a vertical line across the figure does not require or imply that there are errors common to the released versions. There are releases where the only commonality is the rough time of the release.

There is no fixed requirement to upgrade to the next release. As reflected in the table, Triconex continues to provide maintenance releases to older firmware versions. For instance, common issues in multiple versions were corrected with the Version 6.4.3, 8.2.3, 9.0.4, 9.1.3, and 9.3 releases. Triconex maintains support and availability of the products and related support services for a period of 10 years after Triconex has discontinued inclusion of such products on its standard Price List. While no new functionality will be provided for the older versions, the error detection, correction, and upgrade processes are performed across all active versions.

Figure 6-2 shows the Triconex history from the time of the original qualification of Version 9.3.1 to the 2006 qualification of Version 10.2.1.

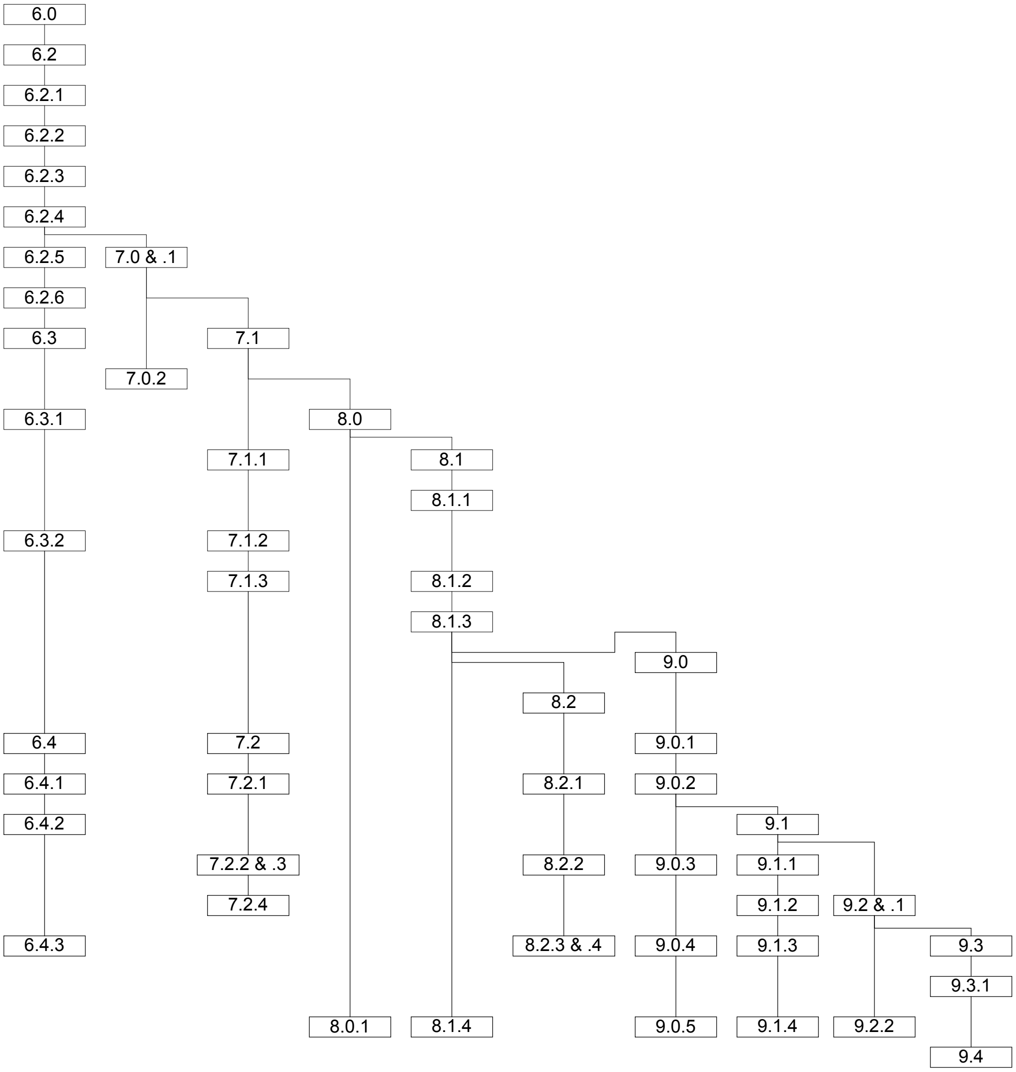

Figure 6-1. Development Tree of TRICON Versions

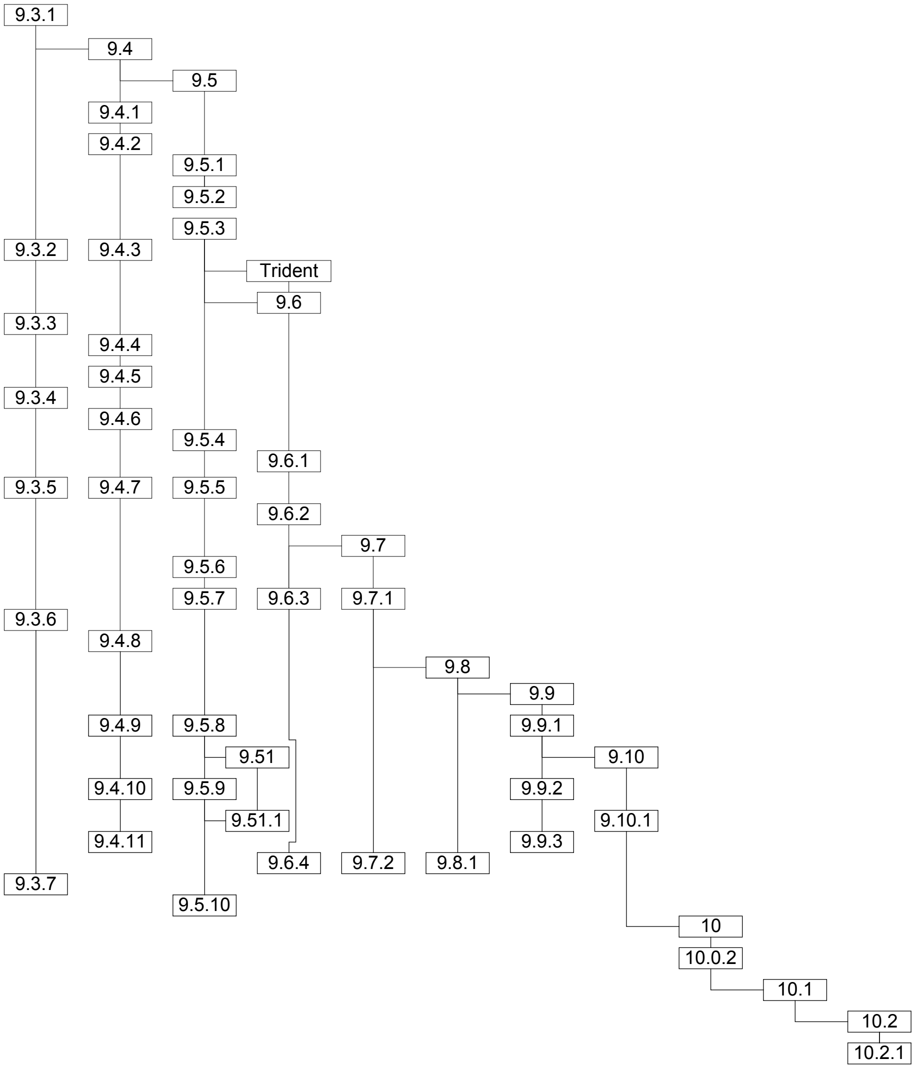

Figure 6-2. Development Tree for New TRICON Versions

7.0 Design Integrity

There is a great deal of guidance in the industry for evaluating the design integrity of newly developed systems. This guidance has been applied to this evaluation. However, one of the strongest proofs of design integrity is system operation. A sound history is available only for mature products and only if the manufacturer can keep extensive records. It is not cost effective for customers to discard faulted TRICON modules, so faulted modules are returned to Triconex for repair, rather than buying a new replacement. Thus, Triconex has extensive records of module failure mechanisms and can determine whether any given TRICON module is still being used.

One of the simplest measures of design integrity is evidenced in the fact that there have been no failures to take appropriate protective actions in more than 100 million operating hours. There are several possibilities for converting the 1E+8 system operating hours to failures per operating hour. The basic difficulty with such a conversion is that there are no failures during this period. If a statistically valid number of failures had occurred, one could divide the failure count by 1E+8 and determine a valid measured Mean Time Between Failures (MTBF). Since no failures exist, a different approach is required.

a

Further evaluations of architectural features to enhance or demonstrate design integrity are provided below.

7.1 Main Processor and Executive Firmware

The compiled application programs are downloaded to the TRICON from a TriStation 1131 Developer's Workbench. In order to minimize the resource requirements in the TRICON, the applications are translated into native machine code.

a

The program downloads include the necessary function and function block library entries necessary for each program segment. Thus, any possible library function errors are correctable by linking the program instances with new copies of the libraries.

a, f

a, f

As discussed earlier, the TriStation 1131 Developer's Workbench translates the various languages into native mode executable machine code. Intermediate steps are performed in the translation, and evaluated in the CDR. The Cause and Effect Matrix, Ladder Diagrams, and Function Block Diagrams are translated into Structured Text. The Structure Text is translated into an emulated code. The emulated code can then be translated into assembly language for the Main Processor. This is then assembled and linked with native mode code libraries to generate a program. Up to this point, all work can and should be performed off line, with no physical connection between the TriStation PC and the TRICON.

The TriStation 1131 Developer's Workbench also provides emulation capabilities for the TRICON. The tool provides a capability for running an intermediate language version of the program on the PC. Capabilities exist for manual input of program variables and observation of program outputs on the PC screen, with the inputs and output values merged and displayed with the program blocks. This simulation can be used as part of the validation process for new or modified application code.

a, b, f

Once the program download is complete, the user may and should request a comparison between the content of the TRICON and the data stored in the TriStation. Proprietary details of that comparison process are provided in the CDR. However, there is sufficient comparison between the stored and re-calculated TRICON data and the data stored in the TriStation to be confident that the application in the TRICON and the application last downloaded through the TriStation are identical. Comparison failures would indicate that the application in the TRICON and the content of the TriStation are no longer the same.

There are no issues with Y2K and the TRICON or TriStation.

a, b, f

7.2 Input, Output, and Communications Modules

The firmware used in these modules exhibits the recommendations from various NRC regulatory guides on high criticality software. The firmware is simple. The firmware does not use an operating system. The firmware performs a few functions and only those functions necessary for the operation of the board and the board's diagnostics. There is no dead code on the modules. Other evaluations performed, documented in the CDR, demonstrate that the dedicated function input, output, and communications module firmware is robustly designed to be used in high safety criticality applications.

7.3 TriStation 1131 and MSW

Triconex used the language and functions in IEC Standard 61131-3 as the technical design basis for the TriStation 1131 programming languages. The IEC standard defines the design basis and operation of most of the functions in the PLC. Additional Triconex documentation defines the operation of the TRICON specific functions, required to interface with diagnostics and TRICON implementation specific features. The operation of these functions has been exhaustively verified and validated by TÜV Rheinland. This independent agency has certified the TRICON since 1991.

a, f

The automated testing program was initially defined by Triconex. The program has been extended based on comments from TÜV Rheinland. As part of the qualification effort, Triconex evaluated the test case coverage and found it included almost all the functions. Those functions that can be exercised in an automated test were added to the test suite, based on the Triconex evaluation of test case coverage. Some functions can only be tested completely with manual tests, which are also included in the Triconex test program. The test cases validate operation at the numeric limits of integer and floating point mathematical functions.

The testing validates that a series of TRICON programs compile, fail to compile, run correctly, or produce defined error conditions. The testing has a set of predefined failure conditions that are validated to occur. Testing validates not only correct operation but correct identification of deliberately introduced errors. The testing system automatically downloads successful compilations into a TRICON and executes them. The pass/fail results of the program operation are returned to the PC used to automate this testing, evaluated for expected results, and stored. This process can continue for over two weeks, if all tests are performed.

In the original Version 9.3.1 qualification, the TS1131 Validation Test Coverage document, Triconex 9600066-001, revision 1, identified automated test suites containing 31,846 compiler tests, 3,218 standard library tests, and 37 TRICON library tests. There are additional manual tests performed for timing and error detection. Thus, more than 35,101 separate, distinct automated test cases exist, with additional manual tests. It should be pointed out that most of the test cases are collections of individual tests. For example, one of the test cases contains in excess of 1,600 individual tests. Triconex personnel have not counted the individual tests in most of the test cases. Additional validation tests have been added as the TriStation 1131 program has been augmented to support new modules and add features. Further proprietary data is contained in the CDR.

In the original Version 9.3.1 qualification, TriStation 1131 provided a secure, password protected environment, with a Windows NT look and feel, in which development is performed. In the Version 10.2.1 qualification, TriStation 1131 provides a secure, password protected environment, with a Windows XP look and feel, in which development is performed. Offline capabilities are provided for support of configuration control and documentation of changes.

a, f

The Version 9.3.1 qualification concluded that the more modern interface provided in TriStation 1131 should minimize inadvertent errors that might be made during program development and modification. From a human factors view, the TriStation 1131 tool is far superior to the older DOS-based TriStation MSW in minimizing human error. The TriStation 1131 tool also provides a common application language, familiar to most users of programmable logic controllers. In the Version 10.2.1 qualification, only the TriStation 1131 tool is available.

The TriStation 1131 tool provides additional functionality while connected to a TRICON over that provided in the older DOS-based tool. This additional functionality provides capabilities for verifying that the content of the PLC is the same as those on the PC from which the download occurred. The vulnerability associated with building programs in a nonsafety critical environment for SIL 3 applications has been further minimized in TriStation 1131 Version 4.1.437.

In the Version 9.3.1 qualification, the CDR evaluated TriStation 1131 Version 2.0, Service Pack 3. The Triconex Product Release Notice associated with TRICON Version 9.3.1 is TriStation 1131 Version 1.1. While Version 2.0 was not formally validated for use with TRICON 9.3.1 at the time of the Version 9.3.1 qualification, evaluation showed that the only significant differences were the inclusion of the high current analog output module (which was not included in the qualification) and a change to the ACM firmware. The TSX operating environment did not change. Desirable enhancements and software corrections were made in Version 2.0. These included the Cause and Effect Matrix Editor and internal corrections.

TriStation 1131 Version 4.1.437 has been formally validated for use with TRICON Version 10.2.1, and accepted by TÜV Rheinland.

In the Version 9.3.1 qualification, the TriStation 1131 software ran in a Windows NT. In the Version 10.2.1qualification, the TriStation 1131 software ran in a Windows XP Professional environment on a standard PC. Triconex recognized that a nonsafety critical environment, like Windows NT or Windows XP, is not acceptable for use in a safety system. However, the TRICON is acceptable for SIL 3 processing.

a, b, f

While acceptable in the Version 9.3.1 qualification, TriStation MSW is no longer supported by Triconex. The older TriStation MSW software operates in a DOS environment. This report evaluated TriStation MSW as part of the nuclear qualification and found that compensatory actions are required for its use in a nuclear safety related environment. While the program has been in use for several years, historical evidence coupled with extensive system testing is not sufficient for acceptance. Since design basis, verification, and validation documentation does not exist for TriStation MSW, compensatory actions are required for its use.

This compensatory action would include use of a Triconex tool to disassemble the executable image, interspersing the assembly language code into the appropriate relay ladder logic diagrams. The application engineer would then read the assembly language code and verify that the translation from relay ladder logic to assembly language was correct. This compensatory action is viewed as an excessive burden for nuclear safety related applications. Thus, TriStation MSW is not recommended for nuclear use.

While the TRICON is actively performing its safety related function, there are no significant differences between operation of programs developed under TriStation 1131 and TriStation MSW. Both use the Program Vector Table, described in Section 7.1 of this report, to dispatch functions. A minor difference is that TriStation MSW creates an entry in the Program Vector Table for each relay ladder segment, while TriStation 1131 creates an entry in this table for each program instance. The TRICON dispatches the functionality in the same manner, starting at the beginning of the table, and working through to the end. The results are the same. Since the TRICON successfully dispatched functions throughout qualification testing, it does not matter whether the functions were generated by TriStation 1131 or TriStation MSW.

The original Version 9.3.1 report recommends the use of the TriStation 1131 tool over TriStation MSW for the following reasons:

- The product is documented.
- The product operates in a language more familiar to utility engineers.
- The language used is an international standard.
- Triconex actively participates in the development of the IEC 61131-3 standard.
- Operation under code generated by the modern tool does not affect the qualification.
- TriStation 1131 will be supported and continue to be enhanced by Triconex. TriStation MSW will not.

Based on these reasons, TriStation 1131 is appropriate for use in a nuclear environment.

The Version 10.2.1 report also recommends the use of the TriStation 1131.

7.4 Application Software

The actual application programming for the TRICON is plant specific and is not evaluated as part of this report. However, the TriStation 1131 tools provide language features and functionality in keeping with the recommendations of USNRC guidance documents, such as NUREG/CR-6463, “Review Guidelines on Software Languages for Use in Nuclear Power Plant Safety Systems.”

Application software is developed from Structured Text, Ladder Diagrams, Function Blocks, or Cause and Effect Matrices, using the TriStation 1131 software. This software is loaded into the MPs using the TriStation 1131 software. The application software provides the functionality defined by the code and implements the desired monitoring and controls defined by the programmer for the specific nuclear safety application.

a, f

In addition to the support features offered by the TriStation 1131, the standardized language features will aid in development of safety critical functions. TriStation 1131 does not provide the complete implementation of all features in IEC 61131-3. The functions that are not offered are viewed as inappropriate for safety critical functions. The existing TriStation 1131 function subset does not allow such constructs as looping and GOTO that could inadvertently result in infinite program flow loops or at least in non-deterministic execution timing. This reduces the chance of bad programming constructs creating unexpected system hangs, further reducing the chance of system failures as well as software common cause failures.

8.0 Conclusions

Commercially, the TRICON is a proven and accepted means to implement high availability, high reliability, and safety critical systems. The evaluation of software quality assurance and design integrity demonstrates that the TRICON is acceptable for use in nuclear safety related applications. The TRICON is acceptable for use in systems such as Reactor Trip or Protection Systems, Engineered Safety Feature Systems, Safe Shutdown Systems, Information and Interlock Systems Important to Safety, and other safety critical control system applications. Other conclusions relating to the critical characteristics presented in Section 4.4 are presented in this section.

Detailed evaluations performed as part of the Critical Digital Review are provided in the CDR. The conclusions are provided below.

8.1 Process Controls and Software Quality Assurance

- The first revision of the Triconex QA Manual, dated 6/30/86, was developed based on the requirements of ISO 9000 and 9001, and specifies controls which essentially comply with the requirements of 10 CFR 50, Appendix B. When the Version 9.3.1 qualification was performed, the documentation for software development practices had become more formalized since 1986, although the basic processes have not been significantly changed. When the Version 10.2.1qualification was performed, both the documentation and the processes have been significantly more rigorous since the Version 9.3.1 evaluations, and meet the regulatory requirements. The current processes and procedures have been audited and shown to be in compliance with ISO-9001:2000 and 10 CFR 50, Appendix B. Based on this history, it is concluded that, from the earliest versions, the TRICON software has been developed in a controlled and structured environment, using industrial procedures that continue to improve.

- The TRICON and TriStation 1131 are not Legacy Software. Starting at TRICON Version 6.2.3, Triconex established a contract with an external, independent certification agency (TÜV Rheinland) to perform code review and testing for the product. TÜV assisted Triconex in establishing safety coding standards, which have been maintained and extended since. The TriStation 1131 software was developed under these standards. TRICON software changes since then have been documented and controlled. Based on the independent review performed by TÜV Rheinland, this report provides objective evidence in the CDR supporting a conclusion that the TRICON, after release 6.2.3, and TriStation 1131 have been developed and maintained under a controlled process. Further, this process is substantially compliant with NUREG-0800, Chapter 7, BTP HICB-14 and current industry standards.

- In the 2000 qualification, Version 9.3.1 of the TRICON software was extensively reviewed as part of the qualification effort. The software development, V&V, and test documentation was found to be in compliance both with Triconex procedural requirements as well as the intent of the current industry standards. This compliance provides high confidence that the software was developed and tested in a controlled and structured manner, which will tend to produce high quality software products. The 2007 CDR (Reference 1) reviewed the TRICON Version 10.2.1 software documentation, and found the documentation to be in compliance with Triconex procedures current when the software was designed and developed. MPR concludes that the results meet the regulatory expectations.

- In the Version 9.3.1 qualification, the software quality assurance program was generally found to be strong. The weakest link in software development was in documenting peer review (verification and validation) activities. This weakness was adequately compensated for by reviews provided by classically independent external agencies and in the quality of the work performed by Triconex design and validation staff. Significant improvement has been made since the initial TRICON development. Triconex has committed to compliance to IEC 61508. Additional improvement in documentation of verification activities is being implemented. Current procedures and practices comply with those provided in IEEE Standard 7 4.3.2. In the Version 10.2.1 qualification, the software quality assurance program is stronger than it was when evaluated during the Version 9.3.1 qualification, and peer reviews are now documented. The compensatory actions noted in the Version 9.3.1 review are still in place. MPR concludes that Triconex now complies with IEC 61508, documents verification and validation activities well, and complies with regulatory expectations.

8.2 Configuration Control

- Triconex has always had formal configuration and change control systems. Software and documents, once placed under configuration control, are retrievable and changes are controlled. Included in the configuration control system is a complete listing of each system and module, by serial number, defining where the module is, when it was installed, and any repairs at Triconex.

8.3 Error Tracking and Reporting

- Triconex has always had formal error tracking and recording systems. These systems are consistent with the requirements established in 10 CFR 21. Errors are classified according to severity, with Product Alert Notices (PAN) being the most significant. When the Version 9.3.1 qualification was performed, only five PANs had been issued against the

TRICON since the release of the system in 1985. When the Version 10.2.1 qualification was performed, PAN 15 was being released, and was included in the evaluation. All of the Product Alert Notices were evaluated as part of this qualification process. An extremely conservative approach to customer notification was found. Most of the Product Alert Notices affected only a very small subset of users. Instead of attempting to determine which customers might be at risk, Triconex chose to notify all customers. None of the notices affect this qualification effort, but some result in application cautions that are described in the CDR. In addition to this industrial safety critical issue notification system, other notification systems exist which are used to disseminate technical data. An earlier utility audit evaluated the 10 CFR 21 notification system and accepted it.

- Errors, once entered into the automated error tracking system, are retrievable, changes are controlled, appropriate resolutions are generated, and all data is available. After review for risk of implementation by the Quality Assurance Review Board (QARB), errors may be held for future implementation, released for immediate resolution, or indefinitely postponed. Customer notification is also addressed in this decision. Immediate customer notification will result if possible safety implications exist.

8.4 Reliability and Dependability

- There is a large base of experience with the TRICON system and its associated software. Triconex has an ongoing relationship with each customer. Knowledge is maintained about the system configuration and any customer concerns for those systems.

- The Version 9.3.1 qualification evaluated the operating experience. The operating experience with these systems demonstrates that the software is highly reliable. This operating experience is based on data sampled in early 1999 and provided in Table 8-1. Of the 812 Version 9 systems, 354 are Version 9.3.1. Assuming that just the Version 7, 8, and 9 systems remained in service and that no new systems were sold (which combine to a conservative evaluation), then these 1892 systems, operating 24 hours a day, 7 days a week, for the last year and a quarter added more than 20 million additional hours to the total provided in Table 8-1. Thus, there have been no failures to take the appropriate protective action in more than 100 million operating hours as of 1999. The Version 10.2.1 qualification did not update the operating experience hours.

Table 8-1 TRICON System Cumulative Operating Hours, Early 1999

Version	Number of Systems	Operating Hours
5	104	9,110,401
6	696	39,514,945
7	646	24,699,181
8	434	10,154,372
9	812	7,072,640
	Total	90,551,539

- Supplementary testing performed as part of the nuclear qualification effort provided further confidence in the quality and reliability of the TRICON software. In the Version 9.3.1 qualification, this supplementary testing included seismic, temperature, humidity, and electromagnetic compatibility. In the Version 10.2.1 qualification, radiation exposure was added to these tests. These tests impose significant challenges to the software-based system. Throughout these tests, a Test Specimen Application Program (TSAP) operated, ensuring that the system continued to operate in the presence of these challenges.

- There is no single action that can be taken to mitigate software common cause failure. However, there are many aspects to the TRICON that make software common cause failure less likely. The system is mature and widely used. The installed base has been operated for over a 100 million hours with no failures to take a required protective safety action. The system has been subjected to verification and validation by an independent group. Since common cause failure is not caused by random faults, the capability of the system to find and vote out single faults is not applicable. The assumption is that the failures would occur simultaneously in all TRICON PLCs. For a typical protection system, particularly in older units, none of the programs in the TRICON PLCs is likely to be identical, since many differences exist in sensor inputs to the divisions. All of these features and functions, taken as a group, tend to indicate that software common cause failure, resulting in failure to take a protective action, is highly unlikely to occur.

8.5 Quality of Design

- The design of the hardware and software evidences modularity, design partitioning, the concepts of information hiding which are now defined as object oriented programming, logical partitioning of functions between software and hardware, and other key evidence of a logical, thorough, well-designed system. During the evaluation, the samples of coding that were reviewed were logical, simple, well thought out, and commented. The code has been reviewed by TÜV Rheinland. Triconex based their coding standard on IEC standards. TÜV Rheinland uses the IEC and Triconex coding standards as guidelines for their evaluation. MPR evaluation shows that the Triconex coding complies with the precepts established in guidance documents such as NUREG/CR-6463, "Review Guidelines on Software Languages for Use in Nuclear Power Plant Safety Systems."

- The Triconex Design Engineering staff exhibits the safety conscious, safety critical attitudes that are consistent with those expected from nuclear industry personnel.

- The Triconex Design Engineering staff also demonstrates the ideas now codified in the Software Engineering Institute's Personal Software Process. Their successful processes are documented in the procedures, and are based on the actual activities and principles used by individual engineers at Triconex. The Triconex software design and development procedures are reflections of the methods used by the engineering staff. The procedures are updated to reflect the evolutionary improvements made by the engineering staff, over and above the requirements reflected in previous design and development procedures. Process improvements are driven by staff belief, not established by management decree. Thus, the intent of the quality assurance program is embodied in work product, since the staff using the procedures believes that the methods and processes used are appropriate and necessary to produce safe, high quality products. Since the Version 9.3.1 review, Triconex has updated their processes to generate the documentation expected by both industrial and nuclear users for safety critical equipment, in keeping with the guidance provided in IEC 61508.

a, b

a, b

8.6 Fault Management and Diagnostics

- The design of the software includes features to detect and mitigate system failures. These features include hardware and software based diagnostics. The diagnostic capabilities of the system are validated when hardware or software changes are made in any module. The validation requires that the stuck at zero, stuck at one, and contact noise from the automated fault injection system produce the pre-defined, expected diagnostic result. Failure to produce the correct result is evaluated and corrected exactly like a failure to produce any diagnostic result.

- The extensive diagnostics provided comply with the requirements established in NUREG-0800, Chapter7, BTP HICB-17, “Guidance on Self-Test and Surveillance Test Provisions” (Reference 11). The diagnostics are integrated into the base TRICON and require no special programming. In addition, data is made available to the application program concerning program operation, results of arithmetic operations, and other internal faults, consistent with the requirements of BTP HICB-17. The application program shall be designed to provide appropriate error recovery and annunciation of such faults. Use of several of the diagnostic data inputs are mandated in the application guidelines in the CDR and in the Triconex Application Guidelines.

- The diagnostics are not excessively complex. The diagnostics provide proven fault coverage, based on validated automated fault injection testing. Triconex performs automated tests that verify correct system behavior, fault detection, and the check for detection of the expected fault. Triconex also conservatively evaluates the diagnostic coverage for each module.

- Based on the quality and coverage of the internal diagnostics, surveillance testing requirements should be reduced by taking credit for the extensive system diagnostics.

9.0 References

The extensive list of proprietary Triconex documentation used in the development of this report is contained in the Critical Digital Review (Reference 1).

1. MPR Report with Triconex Report Number 9600164-539, "Critical Digital Review of the TRICON Version 10.2.1 System," July 2007

9.1 Regulatory Documents

2. United States of America, Title 10 of the Code of Federal Regulation, Part 50, "Domestic Licensing of Production and Utilization Facilities"

3. United States of America, Title 10 of the Code of Federal Regulation, Part 21, "Reporting of Defects and Noncompliance"

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

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

6. Regulatory Guide 1.169, Revision 0, "Configuration Management Plans for Digital Computer Software Used in Safety Systems of Nuclear Power Plants," September 1997

7. Regulatory Guide 1.170, Revision 0, "Software Test Documentation for Digital Computer Software Used in Safety Systems of Nuclear Power Plants," September 1997

8. Regulatory Guide 1.171, Revision 0, "Software Unit Testing for Digital Computer Software Used in Safety Systems of Nuclear Power Plants," September 1997

9. Regulatory Guide 1.172, Revision 0, "Software Requirements Specifications for Digital Computer Software Used in Safety Systems of Nuclear Power Plants," September 1997

10. Regulatory Guide 1.173, Revision 0, "Developing Software Life Cycle Processes for Digital Computer Software Used in Safety Systems of Nuclear Power Plants," September 1997

11. NUREG-0800, Revision 4, "Standard Review Plan," Section 7.0, "Instrumentation and Controls – Overview of Review Process," June 1997

12. NUREG/CR-6083, "Reviewing Real-Time Performance of Nuclear Reactor Safety Systems," May 28, 1993

13. NUREG/CR-6090, "The Programmable Logic Controller and Its Application in Nuclear Reactor Systems," June 30, 1993

14. NUREG/CR-6101, "Software Reliability and Safety in Nuclear Reactor Protection Systems," June 11, 1993

15. NUREG/CR-6241, "Using Commercial-Off-the-Shelf (COTS) Software in High-Consequence Safety Systems," November 10, 1995

16. NUREG/CR-6303, "Method for Performing Diversity and Defense-in-Depth Analysis of Reactor Protection Systems," December 1994

17. NUREG/CR-6463, "Review Guidelines on Software Languages for Use in Nuclear Power Plant Safety Systems," October 1997

9.2 Industry Standards and Guides

18. ASME NQA-1-1994, "Quality Assurance Program Requirements for Nuclear Facilities Applications," July 1994

19. IEEE Standard 7-4.3.2-1993, "IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations," September 1993

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

21. IEEE Standard 730-1989, "IEEE Standard for Software Quality Assurance Plans," August 1989

22. IEEE Standard 730-2002, "IEEE Standard for Software Quality Assurance Plans," September 2002

23. IEEE Standard 730.1-1989, "IEEE Guide for Software Quality Assurance Planning," October 1989

24. IEEE Standard 828-1990, “IEEE Standard for Software Configuration Management Plans,” September 1990

25. IEEE Standard 828-1998, “IEEE Standard for Software Configuration Management Plans,” June 1998

26. IEEE Standard 829-1983, “IEEE Standard for Software Test Documentation,” December 1982

27. IEEE Standard 829-1998, “IEEE Standard for Software Test Documentation,” September 1998

28. IEEE Standard 930-1993, “IEEE Recommended Practice for Software Requirements Specification,” December 1993

29. IEEE Standard 1008-1987, “IEEE Standard for Software Unit Testing,” December 1986, reaffirmed March 2003

30. IEEE Standard 1012-1998, “IEEE Standard for Software Verification and Validation Plans,” March 1998

31. IEEE Standard 1016-1987, “IEEE Recommended Practice for Software Design Descriptions,” March 1987

32. IEEE Standard 1016-1998, “IEEE Recommended Practice for Software Design Descriptions,” September 1998

33. IEEE Standard 1016.1-1993, “IEEE Guide to Software Design Descriptions,” March 1993

34. IEEE Standard 1028-1988, “IEEE Standard for Software Reviews and Audits,” June 1988, Corrected June 1989

35. IEEE Standard 1028-1997, “IEEE Standard for Software Reviews and Audits,” September 2002, reaffirmed December 1997

36. IEEE Standard 1042-1987, “IEEE Guide to Software Configuration Management,” September 1987, Reaffirmed December 1993

37. IEEE Standard 1058.1-1987, "IEEE Standard for Software Project Management Plans," December 1987, Reaffirmed December 1993

38. IEEE Standard 1058-1998, "IEEE Standard for Software Project Management Plans," December 1998

39. IEEE Standard 1059-1993, "EEE Guide for Software Verification and Validation Plans," December 1993

40. IEEE Standard 1074-1997, "IEEE Standard for Developing Software Life Cycle Processes," December 1997

41. ISO 9000-3:1991, "Quality management and quality assurance standards – Part 3: Guidelines for the application of ISO 9001 to the development, supply and maintenance of software," June 1991

42. ISO 9001:1994(E), "Quality systems – Model for quality assurance in design, development, production, installation and service," September 1994

43. ISO 9001:2000, "Quality Management Systems – Requirements," May 2005

9.3 Other

44. EPRI TR-102348, "Guideline on Licensing Digital Upgrades," December 1993

45. EPRI Report 1002833, "Guideline on Licensing Digital Upgrades, TR-102348 Revision 1, NEI 01-01, A Revision of EPRI TR-102348 to Reflect Changes to the 10 CFR 50.59 Rule" March 2002

46. EPRI TR-106439, "Guideline on Evaluation and Acceptance of Commercial Grade Digital Equipment for Nuclear Safety Applications," October 1996

47. EPRI TR-107330, "Generic Requirements Specification for Qualifying a Commercially Available PLC for Safety-Related Applications in Nuclear Power Plants," December 1996; with the April 24, 1998 revisions and the USNRC Safety Evaluation of July 30, 1998

48. EPRI Report 1011710, "Handbook for Evaluating Critical Digital Equipment and Systems," November 2005

49. EPRI TR-107339, "Generic Requirements Specification for Qualifying a Commercially Available PLC for Safety-Related Applications in Nuclear Power Plants," December 1996

50. EPRI Report 1011710, "Handbook for Evaluating Critical Digital Equipment and Systems," November 2005