Operations Management

TRICONEX TOPICAL REPORT

APPLICATION GUIDE

Document No.: 7286-545-1

Revision 4

Appendix B

TRICON TOPICAL REPORT

TABLE OF CONTENTS

SECTION **PAGE**

1.0 INTRODUCTION....4

2.0 SYSTEM CAPABILITIES....5
2.1 The Tricon Programmable Logic Controller....5
2.2 Key System Features....5

3.0 SYSTEM DESIGN GUIDANCE....7
3.1 Power....7
3.2 Connection to Plant Instrumentation and Controls....8
3.3 Tricon Chassis Configuration....9
3.4 Tricon Communications Interfaces....11
3.5 Failure Analysis and SAR Chapter 15....12
3.6 Diversity and Defense-in-Depth....14
3.6.1 Licensing Criteria....16
3.6.2 Defense-In-Depth and Diversity Requirements....17
3.6.3 Diversity Implementation....18
3.7 Setpoint Accuracy Calculations....22
3.8 Bypass and Indication....25
3.9 Self-Test Capabilities....26
3.10 Surveillance Capabilities....28
3.11 Operational Constraints....31
3.12 Error Reporting and Tracking....32

4.0 ENVIRONMENT AND LOCATION....33
4.1 Mounting....33
4.2 Temperature and Humidity....33
4.3 Heat Loads in Cabinets and Rooms....34
4.4 Seismic Acceleration Limits....34
4.5 Radiation Fields....37
4.6 EMI/RFI Compatibility....37
4.7 Electrical Fast Transient Testing....44
4.8 Surge Withstand Testing....44
4.9 Electrostatic Discharge (ESD) Testing....45

TRICON TOPICAL REPORT

TABLE OF CONTENTS

SECTION **PAGE**

4.10 Isolation Testing 46
4.11 Operability Testing 46

5.0 PROGRAMMING GUIDANCE 48
5.1 Cycle time 48
5.2 Software Quality Assurance Processes 49
5.3 Guidance for Application Programming 50
5.4 Loss of Power Fault Indication 54
5.5 Communication with External Systems 56
5.6 Peer-to-Peer Communication 56
5.7 Communication Application Safety Layer 58

6.0 INSTALLATION, COMMISSIONING, AND MAINTENANCE 60
6.1 Required testing 60
6.2 Operations Procedures 60
6.3 Maintenance Procedures 61
6.4 Application Program Maintenance Procedures 63
6.5 Maintenance and Bypass Capabilities 64

7.0 REFERENCES 67

1.0 INTRODUCTION

This report provides guidelines and qualification limitations for applying the Triconex Tricon Programmable Logic Controller (PLC) in nuclear power plant systems classified as Safety Related and Important to Safety. The guidance provided in this document is intended to simplify use and application of the Tricon by consolidating design requirements, operational limitations, and other important data derived from the generic qualification program. Additional requirements and limitations may apply to a plant-specific application.

Some of the guidance provided in this document is not necessarily specific to the Tricon PLC or TriStation 1131 Developer's Workstation. In these cases, the guidance provided is generic and should be applied to any installation involving digital equipment. Installation practices can create long term problems, which are often ascribed to software. Correct initial system installation will enhance reliable system operation. In that respect, the generic guidance provided should be considered appropriate for use with any PLC in a safety critical application.

Guidelines are provided for design, licensing, installation, operation, and maintenance of the system. Many of the guidelines in this document are interrelated. As an example, consider generation of fault alarms. The fault alarm has implications in design, operating and maintenance procedures, plant interface, main control room impacts, and several other seemingly unrelated topics, including system power supply. Therefore, the guidelines should be considered as a whole, rather than in separated, individual pieces.

In addition to the guidelines presented in this document, the standard manufacturer's recommendations provided by Triconex for application of the Tricon should be followed. These are documented in the Triconex Planning and Installation Guide (Reference 7.13).

2.0 SYSTEM CAPABILITIES

2.1 The Tricon Programmable Logic Controller

The Tricon Programmable Logic Controller (PLC) with the TriStation 1131 Development Workstation provides a suitable platform for implementation of safety-critical digital Instrumentation and Control systems. The Triple Modular Redundant design of the Tricon PLC has been shown to provide a high degree of reliability in addition to high availability. These characteristics make the Tricon platform particularly suited to nuclear safety-related applications. The TriStation 1131 Development Workstation, when used as described in this guide, provides a suitable means for developing and maintaining application software and configuring the Tricon system.

A detailed description of the Tricon PLC and TriStation 1131 is provided in Section 4.1 of the Qualification Summary Report (Reference 7.18).

Hardware type tests were performed with Version 10.2.1 of the Tricon system. However, the specific version of the Tricon system supplied for nuclear plant applications may be a later version. If versions later than Version 10.2.1 are supplied for nuclear safety-related applications, the qualification basis described in this report will be augmented with technical evaluations or additional testing based on the requirements established in Section 6.8 of IEEE Standard 323-1974.

2.2 Key System Features

This section provides an overview of the key features of the Tricon PLC.

The Tricon PLC is constructed of individual modules, installed in rack mount chassis. There are certain modules that are required, such as power supplies and Main Processors. The remaining modules, number of chassis required, and locations of the modules are configurable.

The Tricon PLC is designed as a Triple Modular Redundant (TMR) system and has been demonstrated to be resistant to single, active failure mechanisms. The power supplies are dual redundant, with each supply capable of providing all power requirements to the chassis in which it is installed. The backplane communication paths are triple redundant. The input and output modules are triple redundant internal to the module. Three separate Main Processor modules are required. Communication modules to external systems may be single train or dual redundant.

TRICON TOPICAL REPORT

The Tricon PLC was designed as a single division Emergency Shutdown System or Safety Instrumentation System. Industries other than nuclear make use of only a single division safety system. The Tricon will be used in the nuclear industry in a mode retaining the existing redundancy provided in separated channels, divisions, and trains.

The Tricon PLC provides conservative alarming of internal faults. Rather than fail to identify internal faults, the Tricon identifies possible faults for resolution by maintenance. The Tricon does not attempt a program-based determination of the safety consequences of a given fault condition.

Faults on a Tricon PLC are not indicators of system failure. Rather, the system continues to operate through faults, based on the TMR design. Faults are indicators that maintenance action is required to restore complete redundancy. There are no known, identified, active single points of failure within a Tricon PLC except Software Common Cause Failure. While the Tricon PLC can tolerate a single fault on every module and continue to implement the application program correctly, prompt repair decreases the already remote possibility of multiple faults combining into a failure. From review of the system, there is a large class of faults where multiple faults may exist on a single module with no adverse effect on system operability.

The Tricon PLC uses triplicated, isolated analog and digital inputs, sampled from a single input point. Each input is voted prior to use in the application software. The median analog value is selected for use. Faults on any single portion of the input circuit will be alarmed and that faulted input will not be used by the application software.

The Tricon PLC qualified digital outputs provide quad voting circuits on each output. Each output is voted from the three separate output channels. The supervised digital outputs check for current flow and appropriate voltage levels. Output voter diagnostics are performed to detect failures in the voter circuit and to detect shorts or opens on the expected field load to be driven by the output. Faults will be alarmed.

The Tricon PLC analog outputs provide three separate digital to analog conversion channels on each point. The current flow from each analog output is measured. Faults in a given digital to analog converter channel will be alarmed and the output module then copes with the fault.

A list of qualified Tricon hardware is provided in the main body of this Summary Report.

The Tricon PLC requires an installation design that separates and isolates the 24 V dc field power supplies to the discrete input/output (I/O) and analog I/O module circuits.

3.0 SYSTEM DESIGN GUIDANCE

The Triconex technical manuals, including the planning and installation guides, provide technical information on the application of the Tricon PLC; use of the TriStation 1131 Programmer's Development Workstation; and the operation and maintenance of the resulting system. This Application Guide supplements the requirement in those documents as appropriate for nuclear safety systems. In addition, certain TÜV Rheinland Restrictions and Requirements for all safety, Emergency Shutdown (ESD), and Fire and Gas systems have been modified to fit the expected applications in the nuclear power industry and are incorporated in this guidance document.

For applications in industries other than nuclear power, only one Tricon PLC is used to provide the safety system functionality. In the nuclear power industry, the Tricon PLC will be used as a replacement for the existing channels, divisions, and trains of safety systems, with one or more PLCs being used to replace a single channel, division, or train. Thus, each protection channel, division, or train will retain the high degree of independence required by IEEE Standard 603. This degree of redundancy results in lessened restrictions from those necessary in a single channel, division, or train safety system.

3.1 Power

Power supply design considerations that are specific to the Tricon system include the following:

A. Redundant chassis power supplies shall be installed in each chassis. Redundant input power must be provided to the redundant chassis power supplies installed in each chassis. With this configuration, failure of one logic power supply, or the power to that supply, does not affect system operation. The single failure of the power supply will be annunciated.

B. The 120 V ac chassis power supply has been validated to operate successfully over input ranges of 85 V ac to 140 V ac and 47 Hz to 63 Hz. The 230 V ac chassis power supply has been validated to operate successfully over input ranges of 185 V ac to 285 V ac and 47 Hz to 63 Hz. The 24 V dc chassis power supplies have been validated to operate successfully over input ranges of 22 V dc to 31 V dc.

C. The 120 V ac chassis power supplies provide hold-up times on power interrupt of at least 40 milliseconds when installed as the only chassis power supply or when installed in combination with a second chassis power supply. The 24 V dc chassis

power supplies provide no hold-up on power interruption. Note that with redundant power supplies, hold up time is important only for power interruptions with the redundant power source turned off.

D. Modules must be loaded into chassis in a manner that does not overload the chassis logic power supplies. Design methods and tables are provided in the Triconex Planning and Installation Guide for assuring proper, conservative power supply loading.

In addition to these Tricon-specific considerations, the field power supplies that are required to activate critical outputs and source safety-critical inputs must be redundant. These external supplies are separate from the Tricon chassis power supplies. The field power supply redundancy is based on the General Design Criteria requirement for single failure tolerance in nuclear safety related applications. Failure of a single, non-redundant supply would render most safety related applications of a single train inoperable.

3.2 Connection to Plant Instrumentation and Controls

Plant instrumentation and control wiring and interface design considerations that are specific to the Tricon system include the following:

A. The PLC must be wired and grounded according to the procedures defined in the Triconex Planning and Installation manuals, Triconex Part Number 9720077-012.

B. If redundant inputs are provided to a single Tricon, the inputs should not be terminated on a single standard Tricon External Termination Assembly (ETA) and thus read by a single input module. If redundant outputs are provided from a single Tricon, the outputs should not be terminated on a single ETA and thus driven by a single output module. The ETA and cable between the ETA and the Tricon chassis are not single failure tolerant.

C. The qualified module list, provided in the Qualification Summary Report, includes:

- Tricon Communications Module (TCM) providing ModBus and Peer-to-Peer capabilities.
- Digital input modules for 24, 48, and 115 volts ac and dc.
- Digital output modules for 24, 48, and 120 volts dc and 115 volts ac.

- A relay output module for interface to non-safety related systems such as annunciators.
- Analog input modules for 0-5 volt or -5 to +5 volt differential, 0-10 volt, and thermocouple input signals.
- Type J, K, T, and E thermocouples may be directly interfaced to thermocouple input modules, which provide cold junction compensated temperatures in Celsius or Fahrenheit.
- RTD input signals are processed through an external converter, which provides a 0-5 volt signals to a standard 0-5 volt analog input module.
- Thermocouples may be input to standard analog voltage input modules after conditioning through qualified signal conditioning modules.
- Analog output modules for 4-20 ma dc.
- A pulse input module optimized for use with non-amplified magnetic speed sensors common on rotating equipment such as turbines or compressors.

D. Qualified External Termination Assemblies with prefabricated interface cables are available for each module. The qualified version of the ETAs provides screw terminal mounting capabilities for field wiring.

E. Alarm contact outputs are provided on each chassis. These alarms, or a logical and fault tolerant equivalent, shall be wired to appropriate control room annunciation. Faults within the Tricon shall be annunciated to the Operations staff for resolution. The alarm contacts on the power supply modules provide a single summed output for system failure indication.

In addition, to these Tricon-specific considerations, all wiring supplied to the PLC must satisfy the requirements for protective separation according to applicable IEEE standards.

3.3 Tricon Chassis Configuration

A. The Tricon chassis is not explicitly protected against dust, corrosive atmospheres, or falling debris. The user must provide atmospheric and airborne particle protection by mounting the equipment inside an appropriate enclosure.

B. The Tricon must be installed in a mild environment. The Triconex Planning and Installation Guide provides additional installation specifications.

C. The Tricon can support from one to 15 chassis. Module locations and types are defined in the Triconex Planning and Installation Guide.

D. Three types of chassis are provided. Each of the chassis provides logical slots for Tricon modules.

1. Each system must include one Main Chassis for the Main Processors.

2. An Expansion Chassis is available for housing additional modules.

3. A pair of RXM Chassis is required at each end of the fiber optic links to house the triplicated Remote Extender Modules (RXM). The RXM may be used as a means to extend the distance between chassis locations or provide qualified isolation between 1E and non-1E equipment. **For configurations involving safety-related Primary RXM and nonsafety Remote RXMs, the application engineer will have to ensure the proper assignment of input/output (I/O) points so that the safety function will not be dependent upon the non-safety input. See Sections 5.0 and 6.0 for additional guidance on application program development.**

E. The Tricon chassis may be interconnected using either standard bus cables or fiber optic cables. In both cases, the connections made are triplicated. General guidelines for the number of chassis and the maximum lengths of standard interconnecting cabling are provided in the Triconex Tricon Planning and Installation Guide (Reference 7.13).

F. In order to minimize the possibility of total loss of communication, the triplicated chassis interconnection cabling should not be run together outside the cabinet. For maximum protection from failure, the chassis interconnection cabling should be run through diverse routes inside the cabinet as well, to the extent possible.

G. If the expansion chassis are connected with standard bus cables, the total length of cable installed to daisy chain up to 15 chassis together may be no longer than 30 meters or 100 feet.

H. If the expansion chassis are connected over fiber optic links, the minimum number of chassis required is three, because the fiber optic links cannot be installed in the Main Chassis. An RXM Chassis must be installed near the Main Chassis for the fiber optic link modules to communicate with the second RXM

Chassis. Up to 12 kilometers or 7.5 miles of fiber optic cable may be used between the two RXM chassis. The first RXM Chassis is connected to the Main Chassis using standard bus cables.

I. Triconex provides guidance on the application restrictions that exist for system configuration. These include module configuration to remain within chassis logic power supply limits, and locations where communication modules can be installed. The complete list of standard guidance and restrictions for system configuration is provided in the Triconex Planning and Installation Guide (Reference 7.13).

3.4 Tricon Communications Interfaces

Communication interface design considerations that are specific to the Tricon system include the following:

A. Communications interfaces can be installed only in the Main Chassis or in the first Expansion Chassis connected to the Main Chassis. If a second chassis is required, the second chassis must be an I/O Expansion Chassis or a Primary RXM Chassis.

B. The communication between the TriStation 1131 PC and the Tricon PLC shall be over a communication link using the IEEE Standard 802.3 protocol, to gain the protection of CRC checks on transmitted messages. In order to provide an 802.3 port, a TCM communication module must be installed.

C. Peer-to-peer communication is allowed between Tricon PLCs, as long as the restrictions provided in Section D, Peer-to-Peer Networking, of this guideline are incorporated in the design.

D. A local non-safety related display panel is recommended, located close to the Tricon. This panel is provided for technician and engineering use during calibration of external devices, diagnostics, and troubleshooting.

E. For communications between a Tricon controller(s) and a safety-related display unit(s), an application layer protocol is required to ensure end -to-end data integrity. The Safety Application Protocol (SAP) is an application layer protocol that allows safety-related communication between a Tricon system and a safety-related display unit. The Tricon controller application and the safety-related display unit use the SAP to exchange safety-critical data. The SAP utilizes a

NIST-published cryptographic algorithm, data keys, sequence numbers, etc., for detecting communication errors such as corrupted messages, duplicated messages, out-of-sequence messages, etc.

Additional guidance is provided in Section 5.7.

In addition, while it might be desirable under certain circumstances to perform all Tricon configuration activities with TriStation 1131 from a single communication network node, the separation and independence requirements established in IEEE Standard 384-1992 discourages cabling across protection channels, train divisions, cabling, or trains. The interconnections required to provide this functionality with TriStation 1131 would interconnect all Tricon PLCs in all divisions, channels, or trains to a single location, which is not acceptable. For network architectures involving interdivisional communications with non-safety devices (e.g., non-safety video display units), verified conformance to the guidance in Interim Staff Guidance DI&C-ISG-04, Highly Integrated Control Rooms – Communications Issues (Reference7.7), is strongly recommended. Conformance to DI&C-ISG-04 may require supplemental administrative and physical access controls at the installed location or site.

Therefore, to prevent inadvertent configuration changes, communications interfaces should be designed to preclude a TriStation 1131 PC from communicating simultaneously with more than one division, channel, or train of Tricon PLCs. Any network cabling should be implemented in a manner to assure that multiple division, channel, or train connections are not possible. This will help assure that only the desired division, channel, or train is modified. The network cabling for TriStation 1131 should not cross division, channel, or train boundaries.

3.5 Failure Analysis and SAR Chapter 15

A. A Failure Modes and Effects Analysis (FMEA) was performed as part of the qualification effort. Triconex Report 9600164-531 (Reference 7.21) provides the FMEA in tabular format. Results of this FEMA show that only a few vulnerabilities in the Triconex design. Proper system design, installation, and maintenance must address these vulnerabilities. These include the following:

- Loss of redundant power supplied to the Tricon, which is indicated by fail-safe operation of all outputs and of the alarm contacts on each power supply.

- Loss of external power for discrete or analog voltage inputs, which can be detected through system wiring (as a discrete or analog input wired to the required power and alarmed when off or outside user specified tolerances).

- Positioning the Main Chassis Control keyswitch to the STOP position. This will be disabled in the application software configuration.

- Internal shorts or opens on all logic power supply rails, all TriBUS serial links, or all I/O Bus serial communication links inside any of the chassis, or all RXM communication links between chassis, which will result in fail-safe operation of all Tricon outputs in and downstream of the affected chassis. The Main Chassis Power Module Alarm circuits will also be alarmed.

- Faults in all three Main Processor modules, which is indicated by fail-safe operation of all outputs and of the alarm contacts on each power supply.

- Opens or shorts in the cables between any chassis and an External Termination Assembly will result in loss of all signals input from or output to that ETA.

- Destructive loss of an ETA will result in loss of all signals input from or output to that ETA.

- Failures of an input point that are duplicated on more than one leg will result in loss of that input point.

- Multiple failures in an output voter circuit may result in forcing the output point on or off.

- Failure of all three separate, redundant communications processors on a single module will result in various actions, depending on the module type. If the failure occurs in a digital input module, the Main Processor will declare all digital inputs to be off. If the failure occurs on a digital output module, the module microprocessors will force all digital outputs to the fail-safe, de-energized state. If the failure occurs on an analog input module, the Main Processors will declare all inputs downscale. On a pulse input module, the Main Processors will declare all inputs downscale.

B. A reliability and availability analysis was performed as part of the qualification effort. A specific system configuration was subjected to an extensive Markov chain modeling process, using the reliability data provided by Triconex. Triconex Report 9600164-532 provides a Markov model for a given configuration

(Reference 7.22). The system models and data provided could be used to estimate the possibility of failure for other Tricon configurations.

- The Tricon offers a field proven reliability, with no failures to implement a required safety action, for over 500 million system operating hours. The likelihood of software common cause failure can thus be shown to be remote.

- From a licensing perspective, the results of the FMEA and Reliability/Availability reports should be incorporated into licensing analyses for each Tricon installation.

- Shorting common power supplies to ground is likely to result in a protective action. The short may result in forcing all inputs to zero, or the short may result in all outputs failing to the de-energized, fail-safe state.

3.6 Diversity and Defense-in-Depth

The main body of the Final Summary Report describes the generic qualification of the Tricon for nuclear safety-related applications based on compliance with hardware and software requirements. In addition to the requirements that relate specifically to the Tricon platform, other important requirements govern the implementation of the Tricon platform in nuclear facilities. This section is provided to address one of the important sets of system-specific requirements (as opposed to platform-specific requirements), namely defense-in-depth and diversity.

The philosophy of defense-in-depth is a multi-layered approach to safe plant operation. For example, in nuclear power plants it includes multiple physical boundaries between the fuel and environment, redundant paths and equipment to provide core cooling, and qualified control and monitoring systems for safe shutdown and long term cooling of the reactor.

When applied to instrumentation and control (I&C) systems, defense-in-depth refers to multiple means to trip the reactor and to initiate safeguards functions for nuclear power plants. It includes provisions for multiple back-up protection actions should the primary protective systems fail to perform. In the original design of nuclear power plants, this is achieved by the use of multiple, independent, and redundant trip channels, independent and redundant safeguards actuation trains, qualification of equipment for the intended service, and diverse means to perform selected protective actions.

Diversity is one aspect of defense-in-depth that is used to avoid equipment common mode failure. Diversity has been applied to nuclear facilities since the earliest designs to account for uncertainties in design and for common mode failure of equipment.

With the use of digital platforms to perform safety functions, the US NRC has placed a special emphasis on evaluation of the common mode failure of software. Though highly unlikely, current regulatory requirements for the design of digital safety-related systems require consideration of a scenario in which all equipment that share a common digital platform are assumed to fail in an unsafe state simultaneously. Alternate plant systems or manual operator actions must therefore be available to provide a means of shutting down the nuclear process to prevent adverse impacts on public health and safety and environmental damage. Due to the extremely low probability of software common mode failure, the alternate shutdown means need not be classified as safety related nor need it meet other safety system criteria such as redundancy, automatic action, etc.

Protection against common mode failure of software is achieved by establishing four "echelons" of defense against equipment failures:

- Control system – The control echelon consists of that non-safety equipment which routinely prevents facility excursions toward unsafe regimes of operation, and is used for normal operation of the facility.

- RTS – The Reactor Trip System (RTS) echelon consists of that safety equipment designed to reduce reactivity rapidly in response to an uncontrolled excursion.

- ESFAS – The Engineered Safety Features Actuation System (ESFAS) echelon consists of that safety equipment which removes heat or otherwise assists in maintaining the integrity of the three physical barriers to radioactive release (cladding, vessel, and containment). The RTS and ESFAS do not have to be diverse, but additional evaluations and equipment are required if they are not diverse.

- Monitoring and indicators – The monitoring and indication echelon consists of sensors, displays, data communication systems, and manual controls required for operators to respond to reactor events.

Within and between these echelons, a strategy of diversity is employed that includes:

- Diverse signals used to perform the same safety functions;

- Diverse equipment to perform the same safety function;

- Diverse platforms used for safety and non-safety related control and protection systems (i.e., diverse platforms for reactor trip and Anticipated Transient Without Scram mitigating systems);
- Diverse safety or nonsafety equipment installed to provide automatic protective actions when software common cause failure occurs; and
- Diverse indications and controls that allow manual operator action.

The common mode failure of software is considered to be less likely than a single hardware failure, but it is still considered to be a credible event and must be addressed.

3.6.1 Licensing Criteria

NUREG-0800 recognizes that digital I&C upgrades require additional design and qualification approaches than those which were typically employed for analog systems. Analog system performance can typically be predicted by the use of engineering models. Digital I&C systems are fundamentally different from analog I&C systems in that minor errors in design and implementation can cause them to exhibit unexpected behavior. Current design techniques for digital I&C systems do not have equivalent engineering models that can be used for system validation.

Consequently, the performance of digital systems over the entire range of input conditions cannot generally be inferred from testing at a sample of input conditions. The use of quality processes, including design, peer review, inspections, type testing, and acceptance testing of digital systems and components does not alone accomplish design qualification at high confidence levels. Also, in digital I&C systems, a design using shared data or code has the potential to propagate a common-cause failure. Greater commonality or sharing of hardware among functions within a channel increases the consequences of the failure of a single hardware module and reduces the amount of diversity available within a single safety channel.

The NRC's approach to the review of design qualification of digital systems focuses, to a large extent, upon confirming that the development process incorporated disciplined specification, implementation, verification, and validation of design requirements. Inspection and testing is used to verify correct implementation and to validate desired functionality of the *final product*, but confidence that isolated, discontinuous point failures will not occur derives from the discipline in the *development process*. The NRC's review of digital I&C systems, particularly reactor protection systems, also emphasizes quality, defense-in-depth, and diversity (D3) as protection against

propagation of common-mode failure within and between functions. The NRC's position on quality of software for safety system functions is stated in Branch Technical Position (BTP) 7-14, "Guidance on Software Reviews for Digital Computer-Based Instrumentation and Control Systems." The NRC's position on D3 is stated in BTP 7-19, "Guidance on Evaluation of Defense-in-Depth and Diversity in Digital Computer-Based Instrumentation and Control Systems."

3.6.2 Defense-In-Depth and Diversity Requirements

Requirements for establishing appropriate levels of defense-in-depth and diversity (D3) for control and instrumentation systems are described in BTP 7-19 for new designs of or changes to existing RTS and ESFAS systems. In particular, the following activities are required:

1. The applicant/licensee should assess the defense-in-depth and diversity of the proposed instrumentation and control system to demonstrate that vulnerabilities to common-mode failures have been adequately addressed.

2. In performing the assessment, the vendor or applicant/licensee shall analyze each postulated common-mode failure for each event that is evaluated in the accident analysis section of the safety analysis report (SAR) using best-estimate methods. The vendor or applicant/licensee shall demonstrate adequate diversity within the design for each of these events.

3. If a postulated common-mode failure could disable a safety function, then a diverse means, with a documented basis that the diverse means is unlikely to be subject to the same common-mode failure, should be required to perform either the same function or a different function. The diverse or different function may be performed by a non-safety system if the system is of sufficient quality to perform the necessary function under the associated event conditions.

4. A set of displays and controls located in the main control room should be provided for manual system-level actuation of critical safety functions and monitoring of parameters that support the safety functions. The displays and controls should be independent and diverse from the safety computer systems identified in items 1 and 3 above.

As required by BTP 7-19, each licensing basis event must be evaluated to determine if a postulated common-mode failure could disable a safety function that is required to respond to the design basis event being analyzed. If so, then a diverse means of

effective response is necessary. The diverse means may be a non-safety system, using either automatic or manual control, if the system is of sufficient quality to perform the necessary function under the associated event conditions and within the required time. For this evaluation, "best-estimate" methods and assumptions are allowed rather than the more conservative assumptions defined in 10 CFR 50, Appendix K for design basis accident analyses. The evaluation assumes that only the software common mode failure occurs in conjunction with an initiating event, thus not requiring operation of the diverse elements through a seismic event.

For existing nuclear facilities, it is expected that this evaluation would consider whether existing manual controls and indications and/or diverse automatic controls are sufficient to provide the necessary backup to the digital engineered safeguards actuation systems. It is expected that existing plant Emergency Operating Procedures or Emergency Response Guidelines could be used in this evaluation as appropriate. The manual controls and indications and/or diverse automatic controls required for backup would be required to be separate and isolated from the digital engineered safeguards actuation systems. In many existing plants, manual controls are already provided for manual actuation of safety-related equipment at the component level. Additional manual system level actuation may be required, based on the evaluation results.

3.6.3 Diversity Implementation

When the Tricon platform is used to perform RTS, ESFAS, or other protective functions in nuclear facilities, either in new facilities or to upgrade existing systems, the defense-in-depth and diversity analysis described above will need to be performed based on facility-specific accident conditions. The analysis will also need to consider facility-specific diverse indications and controls. One approach to implementing RTS and/or ESFAS functions in nuclear power plants using the Tricon platform is illustrated in Figure 3-1 and is discussed below.

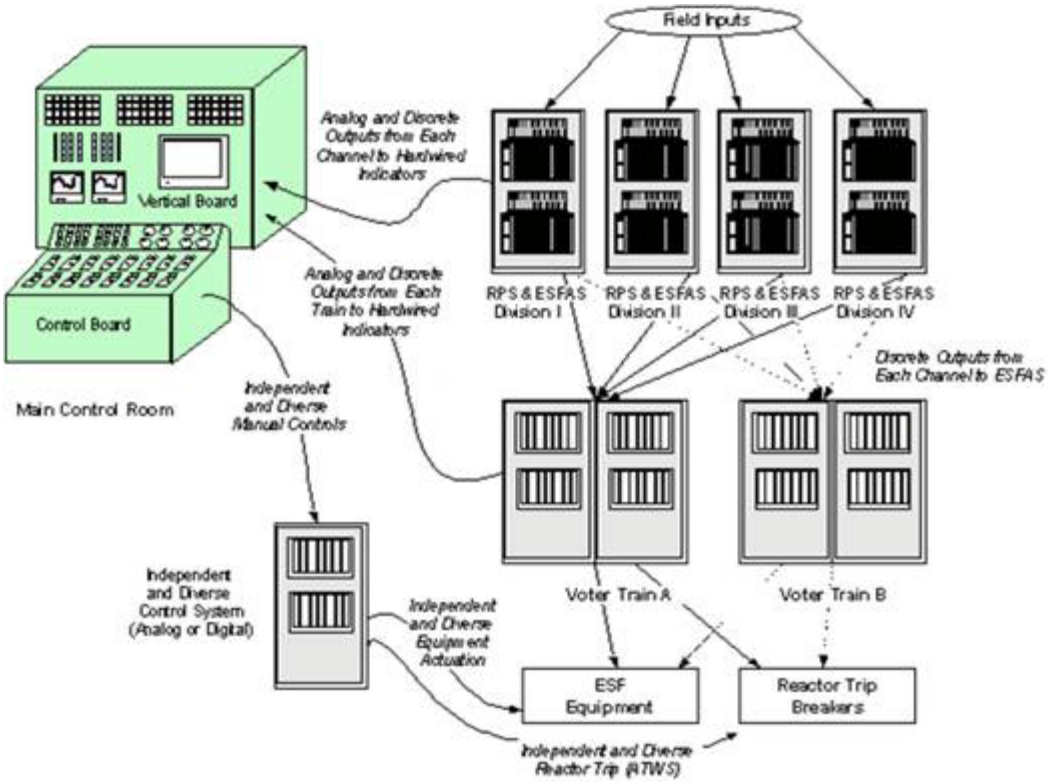


Figure 3-1 Tricon Reactor Protection System with Diversity

The figure illustrates use of the Tricon platform to implement reactor protection system functions using most of the traditional channel, division, and train approach. Such a system could be implemented as an upgrade to an existing plant. With this approach, four Tricon systems are installed to acquire data, perform bistable trip comparisons, and generate discrete outputs to the two trains of the RTS and ESFAS systems. Each of the four systems operates independently. Each of the four Tricon systems may also provide discrete or analog outputs to drive annunciator points or indicators in the main control room. The final reactor trip voting and ESFAS automatic equipment actuation is performed by the two independent trains.

The hypothetical configuration would combine RPS and ESFAS functions on a single platform, i.e., the V10 Tricon PLC. The Tricon, with its TMR architecture, is resilient against single failures and operating experience has shown it is highly reliable (more than 9,000 units in operation and over 500,000,000 hours without failure to perform on demand). Invensys understands there remains the very rare possibility of a software

common cause failure (CCF). Since digital system CCFs are not classified as single failures, postulated digital CCFs are not assumed to be a single random failure in design basis evaluations. The two design attributes sufficient to eliminate consideration of common cause failure – diversity and testability – would not be satisfied by the proposed architecture. Therefore, a diverse actuation system (DAS) would be required with the proposed combined RPS/ESFAS architecture, and is shown in the figure. Invensys recommends full design analysis following BTP 7-19 for partial or complete RPS/ESFAS upgrades or installations including best-estimate techniques to evaluate the effects of digital system CCFs coincident with design basis events. Upon support and approval by the licensee, Invensys will conduct D3 analysis of new and replacement RPS/ESFAS applications in conformance with NUREG/CR-6303, IEEE Std. 279-1971 or IEEE Standard 603-1991, Reg. Guide 1.152 Rev. 2 and BTP 7-19.

Because a CCF is not a design basis event, the alternate shutdown means need only be adequately robust consistent with 10 CFR 50.62. A specifically designed DAS to actuate RPS/ESFAS equipment must independently monitor plant process parameters, automatically initiate protective actions, and must be designed and manufactured in accordance with Generic Letter 85-06 "Quality Assurance Guidance for ATWS Equipment that is Not Safety-Related". When included in the design, the DAS, composed of diverse hardware and software, would independently monitor plant process parameters and automatically initiate protective actions, as shown in the figure. DAS designated components will be configured and programmed to automatically initiate reactor shutdown and activate cooling equipment when accident conditions are sensed.

The DAS will also provide independent and diverse plant information displays in support of manual initiation. As illustrated in the figure, manual operator action will be supported in all Invensys-designed RPS/ESFAS architectures. The operator will have the capability to view plant process information at independent displays – Safety Parameter Display Console (analog or digital display) and the Plant Process Computer and/or DCS VDUs. Manual safety initiation will be independent of both systems. The specific design and technology of the DAS is beyond the scope of this topical report, but at a minimum, the following would have to be analyzed as part of the D3 assessment:

- design architectures are diverse (including underlying technology, such as hardware and software)
- diverse power source(s)
- quality of the components in the diverse system

- actuation path for the diverse system (i.e., downstream of the Tricon-based RPS/ESFAS, as shown in the figure), and

- timing analysis for manual operator actions, if credited, as well as quality of the operator displays and switches.

The figure also shows that independent and diverse manual controls are also used to actuate reactor trip equipment. In addition to the manual controls, the Anticipated Transient Without Scram (ATWS) system provides independent and diverse automatic actuation of the reactor trip equipment separately.

As illustrated by Figure 3-1, the Tricon platform could be used in both the reactor protection system channels and the RTS and ESFAS trains. With this approach, four independent Tricon systems perform the reactor protection system functions described above, and two additional independent Tricon systems perform the RTS and ESFAS functions of trip logic and equipment actuation. Again, the interface between the four channels and the two RTS/ESFAS trains would typically be discrete signals. The Tricon peer-to-peer communication link could be used and would simplify wiring for new plants. However, this communication link is not triple redundant and therefore communications from one Tricon to another are vulnerable to a single failure if redundant communication paths were not provided. Use of discrete signals would reduce the risk of losing all inputs from one of the reactor protection system channels to the RTS/ESFAS systems.

Again, independent and diverse automatic and manual controls are used to actuate ESFAS equipment by a diverse control system, which would be likely be more extensive with RTS and ESFAS implemented on a common platform. The defense-in-depth and diversity analysis described above would be used to identify the specific equipment requiring diverse actuation capability. This analysis would also be used to establish whether sufficient time is available for manual operator actuation or if automatic actuation is required. The timing for manual actions would likely be verified by tests in a facility simulator. In addition, the analysis would establish whether component level actuation is sufficient, or whether certain diverse system-level actuations are necessary.

The diverse equipment actuation circuits would use priority logic modules to combine the credited safety system and the diverse automatic and manual actions into control outputs for the actuated equipment. Priority logic modules are not included in this topical report.

Additional protection from software common mode failures can also be obtained if the Tricon safety systems are installed in a plant with digital non-safety related control and information systems. For example, Invensys has developed a plant design in which TCM modules in each of the independent Tricon safety systems are interfaced to a Foxboro I/A distributed control system (DCS). As previously described, the TCM module can provide one-way communication to the Foxboro I/A system and is qualified as a 1E-to-non 1E isolator. The TCM module provides the DCS with the value of each parameter and the status of the Tricon system diagnostics. This allows the operator to monitor the status of the safety system using the advanced human system interface features available through the DCS. In addition, the DCS can be configured to emulate the safety system trip logic. If the DCS detects that the protection system has failed to respond to an upset condition, it will immediately provide this information to the operator so that he can take appropriate manual action or could provide an automatic trip function or automatic ESF functions, if the DCS is based upon an acceptable quality based design approach. With this approach, the DCS should also be configured to perform automatic and routine cross-comparisons of the data between each channel, division, and train of the Tricon protection system to identify possible field sensor failures.

3.7 Setpoint Accuracy Calculations

An analysis was performed to provide a single concise listing of the accuracy specifications of the Triconex Tricon control system. The specifications documented are those typically used by nuclear industry users for calculating instrument measurement uncertainties and establishing critical control setpoints.

The Triple-Modular Redundant architecture of the Tricon along with its continuous diagnostics and self-calibration features eliminates many of the typical error sources found in standard instrumentation. Component or module failure;, channel, division, or train failures;, or communication failures at the Input, Output, or Main Processor Module level will be corrected and/or compensated for by the Tricon system's ability to detect transient and steady state errors, and to take appropriate corrective actions online through the system's hardware and software voting mechanisms.

Tables 3-1 through 3-3 document the Reference Accuracy specifications for each of the analog I/O modules included in the Triconex Tricon PLC qualification program.

Table 3-1 - I/O Module Accuracy Specifications

I/O Module Type	Model Number	Reference Accuracy (Note 1)
0-10V Analog Input	3701	< 0.15% of FSR (Volts) 0° to 60° C (Note 2 & 3)
0-5V or 0-10V Analog Input (16 Inputs)	3703E	< 0.15% of FSR (Volts) 0° to 60° C (Note 2 & 3)
4-20 mA Analog Output	3805E	< 0.25% (in range of 4-20 mA) of FSR (0-22mA) 0° to 60° C
Thermocouple Input J, K, T, E	3708E	See Table 2
Pulse Input	3511	@ 1,000 Hz to 20,000 Hz – ±0.01% @ 100 Hz to 999 Hz – ±0.1% @ 20 Hz to 99 Hz – ±1.0%
0-5V Analog Input or -5 to +5V Differential	3721	< 0.15% of FSR 0° to 60° C (Notes 2 & 3)

1. Reference Accuracy includes all the components of accuracy (repeatability, hysteresis, non--linearity, and dead band). Triconex guarantees that the performance of the module meets specifications. This performance has been verified by testing performed on all modules during production. Typically, field application of the modules with respect to calibration accuracies is more stringent than the specified accuracy. Therefore, Reference Accuracy values are considered to be a 95% or better probability value with a 95% or better confidence level.

2. On current loop inputs, a 0.01% precision resistor is used on the input termination to convert the current signal to a voltage reading (250 ohm for 0 -5 VDC or 500 ohm for 0-10 VDC). The resistor accuracy This is not included in the specified module accuracy.

3. FSR = Full Scale Range

Table 3-2 - Reference Accuracy of Model #3708E Thermocouple Input Module

TC Type	Temperature Range	Reference Accuracy (Notes 1 and 2) @0-60°C (32-140°F)	
		T_a=25°C (77°F)	T_a=0-60°C (32-140°F)
		Typical	Maximum
J	-150 to 0°C (-238 to 32°F) 0 to 760°C (>32 to 1400°F)	±1.7°C (±3.0°F))	±5.0°C (±9.0°F) ±3.1°C (±5.5°F)
K	-150 to 0°C (-238 to 32°F) 0 to 1251.1°C (>32 to 2284°F)	±2.3°C (±4.0°F)	±4.5°C (±8.0°F) ±3.9°C (±7.0°F)
T	-161 to 0°C (-250 to 32°F) 0 to 400°C (>32 to 752°F)	±1.7°C (±3.0°F)	±4.8°C (±8.5°F) ±2.5°C (±4.5°F)
E	-200 to 0°C (-328 to 32°F) 0 to 999°C (>32 to 1830°F)	±1.7°C (±3.0°F)	±4.5°C (±8.0°F) ±2.8°C (±5.0°F)

1. Reference Accuracy includes all the components of accuracy (repeatability, hysteresis, non-linearity, and dead band). Triconex guarantees that the performance of the module meets specifications. This performance has been verified by testing performed on all modules during production Typically, field application of the modules with respect to calibration accuracies is more stringent than the specified accuracy. Therefore, Reference Accuracy values are considered to be a 95% or better probability value with a 95% or better confidence level.

2. Accuracy specifications account for errors related to reference-junction compensation but do not account for errors caused by temperature gradients between the temperature transducers and thermocouple terminations. The user is responsible for maintaining a uniform temperature across the thermocouple termination module.

Table 3-3 - Reference Accuracy of Analog Devices Signal Conditioners

Signal Conditioner Type	Model Number	Reference Accuracy (Note 1)
AD7B34CUSTOM, RTD Signal Converter, 200 ohm Pt., 0 – 600°C	1600083-600	+/- 0.11% span
AD7B34CUSTOM, RTD Signal Converter, 200 ohm Pt., 0 - 200°C	1600083-200	+/- 0.2% span
AD7B340401, RTD Signal Converter, 100 ohm Pt., 0 - 600°C	1600024-040	+/- 0.1% span
AD7B340301, RTD Signal Converter, 100 ohm Pt., 0 - 200°C	1600024-030	+/- 0.15% span
AD7B340201, RTD Signal Converter, 100 ohm Pt., 0 - 100°C	1600024-020	+/- 0.2% span
AD7B340101, RTD Signal Converter, 100 ohm Pt., -100 to +100°C	1600024-010	+/- 0.15% span
AD7B300201, RTD Signal Converter, 0 – 100 mV	1600082-001	+/- 0.1% span

1. Reference Accuracy includes all the components of accuracy (repeatability, hysteresis, and non-linearity).

3.8 Bypass and Indication

A. Any interface to the existing bypass and inoperable indication system should be incorporated into the new design, with any necessary outputs driven by the Tricon.

B. If the Tricon communicates with a Distributed Control System, Plant Computer, or other Historian, additional software and historian capabilities should be evaluated for diverse indication and alarming as well as retention of historical data for the control room.

3.9 Self-Test Capabilities

BTP 7-17 and other applicable IEEE standards describe requirements for self-test capabilities for digital systems. The design of the Tricon incorporates most of these features. Specific capabilities provided by the Tricon and considerations for application design are discussed below.

A. As required in BTP 7-17, the Tricon includes self-test features to confirm computer system operation upon system initialization. Additional tests and diagnostics are provided in the Tricon PLC beyond the minimal set identified in BTP HICB-17 and the referenced guidance documents. The Tricon PLC provides continuous self-testing, including monitoring memory and memory reference integrity, using watchdog timers, monitoring communication channels, monitoring central processing unit status, and checking data integrity.

B. Digital computer-based instrumentation and control systems are prone to different kinds of failures than traditional analog systems. Properly designed self-test, diagnostic, and watchdog timers reduce the time to detect and identify failures, but are not a guarantee of hardware or software error detection. Computer self-testing is most effective at detecting random hardware failures. The Tricon TMR PLC has been designed and validated by the vendor and by TÜV Rheinland to detect and identify failures. The system design goal was 100% detection of failures. Random hardware failures have been demonstrated by Triconex automated testing and by analysis at TÜV Rheinland to be unlikely to defeat the Tricon PLC triple redundancy. Therefore, the TMR design is likely to detect and annunciate these failures if the application software includes detection features and external equipment to annunciate the fault in the control room is provided.

C. The internal self-test functions are transparent to the application programmer and are an integral part of the base platform software. The application is provided self-test results through a simple, pre-designed, verified and validated interface. The platform software is pre-developed, standard, modular, and well structured. The improved ability to detect failures provided by the self-test features reduces the probability of failure associated with the self-test feature and has been demonstrated in certification as a safety critical system and by field experience in

similar safety critical applications. Faults and failures detected by hardware, software, and surveillance testing are consistent with the failure detection assumptions of the single-failure analysis and the failure modes and effects analysis. The TMR capabilities decrease the probability of system failure, as demonstrated in the Availability and Reliability Report. In addition, identification and alarming by the application software, as well as use of valid input data, further increases the overall system reliability in detection of previously undetected faults and failures internal to the existing systems.

D. The Tricon PLC system performs self-tests as well as validation of inputs and outputs on each module. The self-test capabilities of the Tricon and appropriate application software could be credited with some of the test and calibration functions for channels and devices currently provided by manual surveillance tests.

E. The Tricon TMR architecture provides continuous self-testing that will detect, tolerate, and alarm on single internal faults and failures. These self-tests include testing the operability of digital output points, which provide two out of four voting on each of the output points. Single failures in the output drive circuits do not cause inadvertent actuation or prevent necessary actuation of controlled field devices. The output drive voter is diagnosed by internal self-tests within the Tricon. Any faults in the output drive circuitry will be annunciated in the control room.

F. The Tricon platform also provides inherent capabilities for testing external devices. The output point can be diagnosed for appropriate current and voltage conditions. If the wiring or field device coil is open or shorted, the Tricon will alarm the loss of the field device for each output point.

G. The Tricon platform provides inherent capabilities for internal self-test and calibration that provide detection of faults in the analog input processing. This resolves issues with drift and calibration uncertainty, which are licensed as being required for the existing analog controls. The Tricon platform has the capability of continuously diagnosing the health of and appropriately adjusting the calibration of the analog to digital signal conversion modules. If the analog to digital conversion module has been significantly adjusted or is outside the limited automatic calibration limits, the module will be marked faulted and an alarm will be generated in the control room. The analog bistable calibrations required by the older, obsolete systems are not required for the Tricon platform.

H. Mechanisms for operator notification of detected failures should comply with the system status indication provisions of IEEE Standard 603 and should be consistent with, and support, plant technical specifications, operating procedures, and maintenance procedures. The Tricon system will provide more diagnostic and notification information than is required in IEEE Standard 603. The Tricon system is designed to support Operations, the safety analysis report, the Technical Specifications, and maintenance functions. New procedures and procedure changes will be incorporated into the design change to support the Tricon system and the staff in plant operation and maintenance.

3.10 Surveillance Capabilities

This section discusses considerations for changes to existing plant surveillance tests based on the design features incorporated in the Tricon system (including the self-test features discussed above). These considerations are provided here to assist plants in identifying areas in which use of the Tricon system will have a beneficial effect on the surveillance program.

A. Modifications to the existing surveillance tests and licensing commitments will be required, as is identified in BTP 7-17. Self tests and automatic analog input calibration could be used to reduce the surveillance testing requirements for the Tricon PLC. The self-test capabilities of the Tricon and appropriate application software could be credited with some of the test and calibration functions for channels and devices currently provided by manual surveillance tests. The application software would provide additional features to support the reduced surveillance testing requirements. The Tricon provides at least as much test coverage as the existing surveillance tests, through the fault tolerance, detection, and repair capabilities inherent in the Tricon PLC design.

B. Because of design and architectural differences between analog and digital systems, traditional surveillance test provisions for analog systems may not be adequate or appropriate for digital computer-based systems. The required surveillance test capabilities to be included in each system design will have to be evaluated to assure adequacy to fulfill the requirements and the intent of the surveillance tests.

C. The replacement system design should provide the ability to conduct periodic testing consistent with the modified technical specifications and plant procedures. The Tricon PLC application can be designed to provide these capabilities, in accordance with the requirements established in the regulatory guidance

referenced in BTP 7-17. There is nothing inherent in the Tricon or TriStation designs that do not comply with the requirements of IEEE Standard 603, as required in BTP 7-17. The Tricon has been successfully evaluated against the recommendations made in IEEE Std. 7-4.3.2 in the Critical Digital Reviews, References 7.19 and 7.20. The Tricon PLC provides capabilities in excess of the minimum criteria found in IEC Standard 880.

D. In order to reduce surveillance testing, an analysis of the Tricon PLC self-test features, single-failure analyses, failure mode and effect analyses, and application software would be required against the requirements established in the Technical Specifications and by the USNRC. The self-test and failure analysis capabilities are documented in the Software Qualification/Critical Digital Review, Availability/Reliability Study, and FMEA Reports from the qualification program. The application software would also require the capability to confirm that the automatic tests are still functional during plant operation.

E. The Tricon has been designed and would be incorporated into the facility design in a mode that should reduce the current manual maintenance and testing activities in existing systems, thus reducing the risks associated with performing these periodic tests. By invoking the self-checking capabilities inherent in the Tricon architecture, the protection systems assure that the lessened amount of maintenance and testing activities reduce the number of losses of protection functions from inadvertent maintenance or surveillance errors.

F. The actuation device testing specified in Reg. Guide 1.22 is still applicable. As a software-based device, the Tricon can be configured to perform any of the testing described in Reg. Guide 1.22, from complete function to judicious choice of components for several tests.

G. The minor software complexity associated with automating required surveillance testing is offset by the reduced risk associated with performance of such testing. Since the number of technician and engineering physical changes inside the protective systems is reduced, the chance for inadvertent modification is also reduced.

H. Reg. Guide 1.118 states in part that test procedures for periodic tests should not require makeshift test setups. For digital computer-based systems, makeshift test setups, including temporary modification of code or data that must be appropriately removed to restore the system to service, should be avoided or at least, designed into the on-line application software. The application software should be configured to incorporate design features to preclude the need for

temporary modifications to hardware or software, jumpers, and reconfiguration to perform periodic testing.

I. As required by ANSI/IEEE Standard 279, Section 4.13; IEEE Standard 603, Section 5.8.3; and RG 1.47, if the protective action of some part of a protection system is bypassed or deliberately rendered inoperative for testing, continued indication of that state shall be provided in the control room automatically. Provisions should also be made to allow operations staff to confirm that the system has been properly returned to service. Not only will the traditional bypass indication be provided, the amount of hardware and jumpers associated with testing a traditional analog system will not exist, since the "jumpers" and "reconfiguration" would be incorporated into the application software. Thus, the possibility of creating errors or faults through inadvertent system modifications is precluded by design. Since the testing is initiated and controlled by the Operations staff and built into the Tricon software, awareness of testing and test progress is maintained and further enhanced in the control room. Anything not restored to service would also be annunciated in the control room.

J. Hardware and software used to perform automatic self-testing are integral to the Tricon and are classified as safety related, having the same quality and reliability as the Tricon PLC. The Tricon PLC can be applied in a manner that maintains existing channel independence, maintains system integrity, and meets the single-failure criterion. The scope and extent of interfaces between software that performs protection functions and software for other functions such as testing has been designed to minimize the complexity of the software logic and data structures. The complexity resulting from TMR is controlled, and integral to the standard, field-proven base platform.

K. The design should have either the automatic or manual capability to take compensatory action upon detection of any failed or inoperable component. The design capability and plant technical specifications, operating procedures, and maintenance procedures should be consistent with each other. The design provides annunciation in the control room on detection of any fault within the Tricon or of any detectable failure in field sensors or actuators. If the Tricon stops operation, the outputs are driven to an OFF state. Faults in any single portion of the TMR Tricon result in that portion being removed from service and annunciated in the control room. Faulted or inoperable field inputs and outputs are detected and alarmed. Other actions could be built into application software as necessary to implement compensatory actions and annunciate the detected failures of external devices.

L. Plant procedures should specify manual compensatory actions and mechanisms for recovery from automatic compensatory actions.

M. Surveillance testing shall be designed to validate correct operation of the Tricon self-tests, to the extent practical. However, many of the self-test functions embedded in the Tricon are not easily tested outside of Triconex facilities and cannot be readily validated in the field.

N. Surveillance testing taken together with automatic self-testing should provide a mechanism for finding and annunciating all detectable failures. The characteristics of digital systems must be considered in the review of technical specification surveillance features. Architectural differences between digital and analog systems warrant careful consideration during the review of surveillance test provisions. Furthermore, the concepts used to determine test intervals for hardware-based systems do not directly apply to the software used in digital computer-based instrumentation and control systems. Therefore, previous reliability analysis used to establish test intervals may not apply. The reliability and availability analysis and the FMEA report indicate that the TMR controls exceed the availability targets of the analog hardware they replace, but that there is still a reliability enhancement from shortened surveillance testing. The 500 Million operating hours without a failure to implement a required protective action demonstrates the Tricon capabilities. There is thus no risk that the maintenance and calibration will have to be done more frequently than required with the existing system. The field hardware testing requirements remain unchanged. With the enhanced system reliability, data cross-checking, automatic analog input calibration, automatic output diagnostics, and automated support for the tests, the risk of undetected failures should be decreased.

3.11 Operational Constraints

Specific operational constraints that apply to the use of the Tricon system in nuclear safety-related applications include the following:

A. The Tricon keyswitch shall preferably be in the RUN, or alternatively in the REMOTE, position when the Tricon is not bypassed and thus performing safety related functions. If the Tricon is not in a bypassed state, alarms must occur in the control room if the keyswitch is in any position other than RUN or alternatively REMOTE.

B. The STOP position on the keylock switch shall be disabled in the system software configuration to preclude inadvertently stopping the program while performing software maintenance functions.

C. Repairs to the Tricon must be performed in an expeditious manner. Main Processors should not be left in a faulted state for extended periods. Operation in single Main Processor mode should be minimized and should not be longer than one day to minimize risk of masking other faults. The Tricon has limited diagnostic capabilities in dual processor mode. A second Tricon fault might cause the outputs to go to the safe, de-energized state. The length of time allowable for running in dual or single mode may be calculated using Markov modeling by pre-determination of the minimum acceptable probability to fail on demand. Invensys uses Markov models based on Tricon system states and individual Module data for a given Tricon system configuration. The calculations are based on Markov Models developed by the Instrument Society of America's SP84 committee during the development of the ISA's SP84 Technical Report S84.0.02.

Separate sections of this Application Guideline provide specific recommendations for Maintenance Overrides and Communication with External Systems.

3.12 Error Reporting and Tracking

Triconex has always had formal error tracking and recording systems for industrial safety critical issue notification. Errors are classified according to severity, with Product Alert Notices (PAN) being the most significant, and Technical Advisory Bulletins (TAB) and Technical Application Notes (TAN) being of lesser significance. Product Alert Notices document conditions that may affect the safety of the application. It is essential that all current PANs, TABs, and TANs be reviewed before starting application development, and that the system be kept up-to-date with any newly released PANs, TABs, or TANs as appropriate.

4.0 ENVIRONMENT AND LOCATION

Specific requirements pertaining to the environment in which a safety-related Tricon system is located are discussed in this section. These environment and location requirements are based on the manufacturer's recommendations in the Triconex Planning and Installation Guide (Reference 7.13), and the results of the qualification testing.

4.1 Mounting

A. The Tricon chassis is designed for mounting in 19-inch industry-standard racks. Mounting specifications for standard, non-seismic mounting are provided in the Triconex Technical Product Guide and in the Triconex Planning and Installation Guide

B. The seismic qualified Tricon chassis requires use of the standard mounting brackets on the front of the chassis as well as the additional standard mounting brackets at the rear of the chassis.

C. Seismic mounting details for all qualified Tricon hardware is provided on Triconex Drawing No. 9600164-102, "Seismic Test Equipment Configuration Detail." All fastener torque values are indicated on Triconex Drawing 9600164-102. The mounting uses standard Tricon front and rear chassis mounting brackets and fastener hardware, and standard Tricon External Termination Assembly (ETA) mounting plates.

D. Whether the chassis is rack mounted or panel-mounted, allow at least 5.25 inches (13.3 centimeters) between the outer panels of the Tricon chassis and the front, sides and top and bottom panels of the enclosure, in order to achieve sufficient convection cooling airflow. See the Triconex Planning and Installation Guide further details.

E. Any unused module slots shall be covered with module slot covers.

4.2 Temperature and Humidity

A. Environmental testing of the Tricon was performed in accordance with the requirements of EPRI TR-107330 and IEEE Standard 381-1977. The Tricon met all applicable performance requirements during and after application of the environmental test conditions. The environmental test included high temperatures of 140^{o} F and 95% relative humidity (RH) and low temperatures of 32^{o} F and 5% relatively humidity. The temperature and humidity profile applied during

environmental qualification testing of the Tricon PLC is shown in Figure 8-1 of the Environmental Test Report, Triconex Report Number 9600164-525 (Reference 7.25).

B. The specific Tricon hardware that was tested (chassis, power supplies, modules, external termination assemblies, and interconnecting cabling) is identified in the project Master Configuration List (Reference 7.30).

4.3 Heat Loads in Cabinets and Rooms

A. When mounting the Tricon chassis into enclosures, heat management calculations must be made to avoid exceeding the qualified ambient temperature ratings of the Tricon. For purposes of these calculations, all power consumed by the Tricon should be assumed to be dissipated inside the enclosure where the Tricon chassis is mounted.

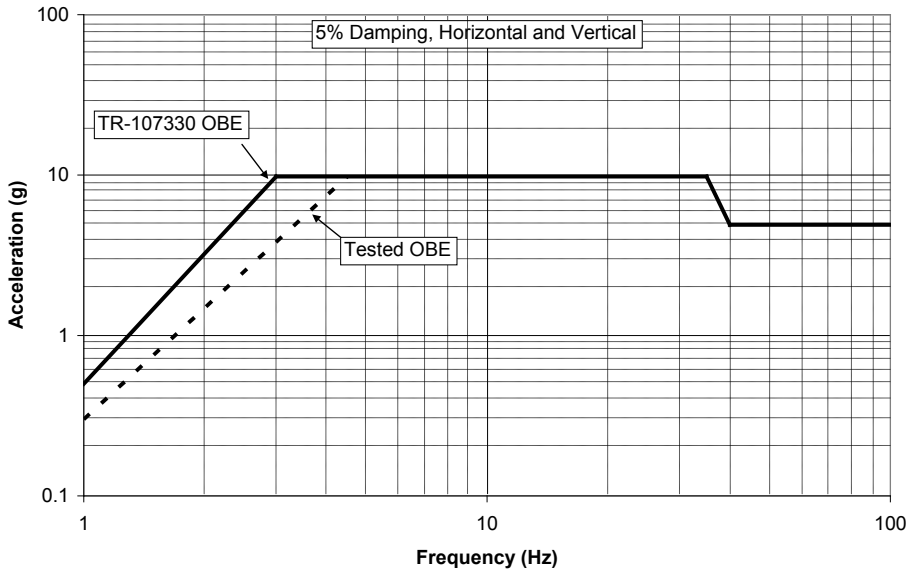
B. If the room temperature plus any heat rise within the cabinet exceeds the Tricon qualification envelope, additional provision must be made for temperature control.

C. The Tricon temperature range must be computed with cabinet doors open and closed.

D. The Triconex Planning and Installation Guide provides guidance on computing the heat load for a loaded chassis.

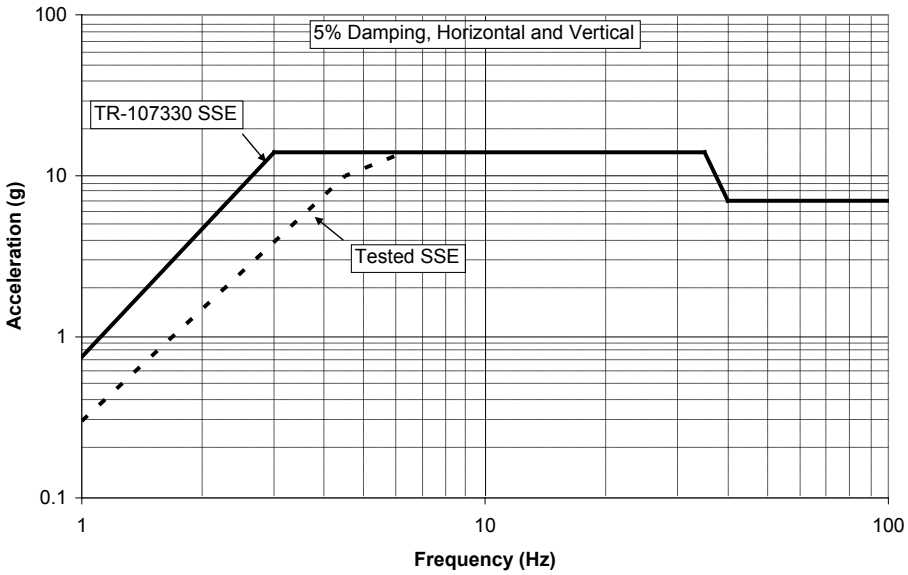
4.4 Seismic Acceleration Limits

Seismic testing was performed in accordance with the requirements of EPRI TR-107330, Section 4.3.9, and IEEE Standard 344.



Frequency	Tested Level	TR-107330 Level
1.0 Hz	0.3 g	0.5 g
3.0 Hz	4.0 g	9.8 g
4.5 Hz	9.8 g	9.8 g
35 Hz	9.8 g	9.8 g
40 Hz	4.9 g	4.9 g
100 Hz	4.9 g	4.9 g

Figure 4-1 Comparison of OBE Test Levels to EPRI TR-107330 OBE Requirements



Frequency	Tested Level	TR-107330 Level
1.0 Hz	0.3 g	0.75 g
3.0 Hz	4.0 g	14 g
4.5 Hz	10 g	14 g
6.3 Hz	14 g	14 g
35 Hz	14 g	14 g
40 Hz	7.0 g	7.0 g
100 Hz	7.0 g	7.0 g

Figure 4-2 Comparison of SSE Test Levels to EPRI TR-107330 OBE Requirements

A. Seismic testing demonstrates that the Tricon is qualified as a Category I seismic device within the test limits shown in Figures 4-1 and 4-2. A plant-specific evaluation will be needed to determine whether the as-tested limits bound the plant seismic acceleration requirements. If not, additional evaluation or seismic testing may be required.

B. Monitoring for chatter of the chassis alarm contacts during seismic testing was not done as a result of utilizing an interposing relay installed in the contact monitoring

circuit. Therefore these contacts are not seismically qualified and this contact output is not credited as performing safety functionality for the facility.

4.5 Radiation Fields

Radiation testing of the Tricon was performed in accordance with the requirements of EPRI TR-107330 and IEEE Standard 323-1974. The Tricon met all applicable performance requirements after application of the radiation test conditions. The radiation test included the withstand capability of the Tricon to a rapid dose of radiation that would be normally provided as a long term, low level 1000 rad gamma dose integrated over a 40 year period in a mild environment (Reference7.29)

4.6 EMI/RFI Compatibility

EMI/RFI Testing of the TUT was performed to the requirements of Sections 3 and 4 of NRC Regulatory Guide (RG) 1.180, Rev. 1 (Reference 7.6). Section 3 of NRC RG 1.180 addresses EMI/RFI emissions testing. Section 4 of NRC RG 1.180 addresses EMI/RFI susceptibility testing. Each section endorses both Military Standard MIL STD 461E series and International Electrotechnical Commission (IEC) 61000 series EMI/RFI test methods. Based on the RG, Triconex has the option to use either series of test methods. NRC RG 1.180, Rev. 1 stipulates that for emissions or susceptibility testing, the chosen series of test methods must be applied in its entirety (i.e., there should be no selective application or mixing of the MIL-STD and IEC test methods during susceptibility testing or during emissions testing).) The maximum frequency for emissions and susceptibility test was 1 GHz, since the maximum intentionally generated frequency of the Tricon is 100 MHz (Reference 7.6, Section 6 and Reference 7.26).

A. Test Methods

EMI/RFI emissions testing of the TUT included both radiated and conducted emissions testing done to the following MIL-STD-461E series test methods specified in Section 3 of NRC RG 1.180, Rev. 1:

- MIL-STD-461E, Test Method CE101, Conducted Emissions, Low Frequency (30 Hz to 10 kHz), AC and DC Power Leads
- MIL-STD-461E, Test Method CE102, Conducted Emissions, High Frequency (10 kHz to 2 MHz), AC and DC Power Leads

- MIL-STD-461E, Test Method RE101, Radiated Emissions, Magnetic Field (30 Hz to 100 kHz), TUT Surfaces and Leads
- MIL-STD-461E, Test Method RE102, Radiated Emissions, Electric Field (2 MHz to 1 GHz), Antenna Measurement

EMI/RFI susceptibility testing of the TUT included both radiated and conducted susceptibility testing done to the following IEC 61000 series test methods specified in Section 4 of NRC RG 1.180, Rev. 1:

- IEC 61000-4-3, Radiated Susceptibility, High Frequency (26 MHz to 1 GHz), Antenna Exposure
- IEC 61000-4-6, Conducted Susceptibility, Radio Frequency (150 kHz to 80 MHz), Power and Signal Leads
- IEC 61000-4-8, Radiated Susceptibility, Power Line Frequency (60 Hz) Magnetic Field, Helmholtz Coil Exposure
- IEC 61000-4-9, Radiated Susceptibility, Pulsed Magnetic Field, Helmholtz Coil Exposure
- IEC 61000-4-10, Radiated Susceptibility, Damped Oscillatory Magnetic Field (100 kHz and 1 MHz), Helmholtz Coil Exposure
- IEC 61000-4-13, Conducted Susceptibility, Harmonics and Interharmonics (16 Hz to 2.4 kHz), Power Leads
- IEC 61000-4-16, Conducted Susceptibility, Common-Mode Disturbances (15 Hz to 150 kHz), Power and Signal Leads

All testing was performed with the TUT energized and operating under control of the executing TSAP software.

B. Test Levels

The following lists the EMI/RFI Testing emissions acceptance levels or applied susceptibility test levels from the applicable figures and tables of NRC RG 1.180, Rev. 1.

EMI/RFI Emissions Test Method	NRC RG 1.180, Rev. 1 Acceptance Level
MIL-STD-461E, CE101	Figure 3.1
MIL-STD-461E, CE102	Figure 3.2
MIL-STD-461E, RE101	Figure 3.3
MIL-STD-461E, RE102	Figure 3.4

EMI/RFI Susceptibility Test Method	NRC RG 1.180, Rev. 1 Test Level	
IEC 61000-4-3	Sect. 4.3.3:	10 V/m
IEC 61000-4-6	Sect. 4.1.2:	Power Leads, 140 dBµV
IEC 61000-4-6	Table 15:	Signal Leads, 130 dBµV
IEC 61000-4-8	Table 19:	Continuous, 30 A/m
IEC 61000-4-8	Table 19:	Short Duration, 300 A/m
IEC 61000-4-9	Table 19:	300 A/m
IEC 61000-4-10	Table 19:	30 A/m
IEC 61000-4-13	Table 10:	See Table 10
IEC 61000-4-16	Table 11:	Power Leads, See Table 11
	Table 11:	Signal Leads: 3/10 of Power Leads

C. Emissions Testing

The EMI/RFI emissions test results demonstrate that the Triconex Tricon v10 PLC does fully comply with the allowable emissions levels of NRC RG 1.180, Rev. 1 for MIL-STD-461E in both RE101 and RE102 testing. The Triconex Tricon v10 PLC does not fully comply with the allowable emissions levels of NRC RG 1.180, Rev. 1 for MIL-STD-461E, CE101 and CE102.

D. Susceptibility Testing

The EMI/RFI susceptibility test results show that the Tricon v10 PLC system complies with the minimum susceptibility levels required by NRC RG 1.180, Rev. 1, as presented in Tables 4-1 and 4-2 with regard to the following system level operational criteria. The main processors continued to function correctly throughout testing as noted. The transfer of input and output data was not interrupted. There were no interruptions or inconsistencies in the operation of the system or the software.

The TUT main processor, chassis power supply, remote extender, and communication modules fully comply with the minimum susceptibility thresholds required by NRC RG 1.180, Rev. 1 for all of the EMI/RFI susceptibility tests listed in Subsection A.

The EMI/RFI susceptibility test results show that the following Tricon v10 PLC input/output hardware does not fully comply with the minimum susceptibility thresholds required by NRC RG 1.180, Rev. 1 for the listed susceptibility tests:

IEC 61000-4-3 Testing

- RTD Signal Conditioning Module 1600083-600 (threshold levels determined)
- RTD Signal Conditioning Module 1600083-200 (threshold levels determined)
- RTD Signal Conditioning Module 1600024-030 (threshold levels determined)
- RTD Signal Conditioning Module 1600024-020 (threshold levels determined)

IEC 61000-4-6 Testing

- RTD Signal Conditioning Module 1600081-001 (no threshold levels determined)
- Digital Output Module 3601T (115 VAC) w/ ETP 9663-610N (threshold levels determined)

Prior to installing the Tricon v10 PLC in a nuclear safety-related application, an evaluation of the input, output, and communication module susceptibilities should be performed. An evaluation of the module susceptibilities should also be performed for non-safety related applications if there is a potential for the PLC to impact plant reliability and availability. The Tricon v10 PLC EMI/RFI susceptibility testing documented in the EMI/RFI test report (Reference 7.26) provides the data required to perform such an evaluation..

Tables 4-1 and 4-2 included at the end of section 4.6 provide a summary of the EMI/RFI conducted and radiated susceptibility test results for each module installed in the TUT. The purpose of the table is to identify a set of modules that demonstrated acceptable susceptibility performance at the required NRC RG 1.180, Rev. 1 test levels.

The Tricon v10 PLC was tested without the benefit of a secondary enclosure, additional cable and wire shielding, or installed power line filtering. Mitigating

actions to address the non-compliances in measured emission levels should incorporate these common in-plant installation features.

The specific Tricon v10 PLC hardware which was tested (chassis, power supplies, modules, external termination assemblies, and interconnecting cabling) is identified in the Triconex Master Configuration List, Document No. 9600164-540 (Reference 7.30).

NOTE: The susceptibility test results given above are contingent on a Tricon v10 PLC installation design that separates and isolates the 24 V dc field power supplies to the discrete I/O and analog I/O module circuits.

TABLE 4-1: SUMMARY OF EMI/RFI CONDUCTED SUSCEPTIBILITY TEST RESULTS

Module Model No.	ETP Model No.	Module Type	IEC 61000-4-6 Radio Frequency 150 kHz - 80 MHz	IEC 61000-4-13 Harmonics and Interharmonics	IEC 61000-4-16 Common-Mode Disturbances
3008	- - -	Main Processor	Pass	Pass	Pass
8310	- - -	Power Supply, 115 VAC	Pass	Pass	Pass
8311	- - -	Power Supply, 230 VAC	Pass	Pass	Pass
8312	- - -	Power Supply, 24 VDC	Pass	Pass	Pass
4200	- - -	Remote Extender	Pass	Pass	Pass
4201	- - -	Remote Extender	Pass	Pass	Pass
4352A	- - -	Communication	Pass	Pass	Pass
3511	9794-110N	Pulse Input	Pass	Pass	Pass
3708E	9782-110N	Thermocouple Input	Pass	Pass	Pass
3501T	9561-810N	Digital Input, 115 VAC	Pass	Pass	Pass
	9561-110N	Digital Input, 115 VAC	Pass	Pass	Pass
3623T	9664-810N	Digital Output, 120 VDC	Pass	Pass	Pass
3603T	9664-810N	Digital Output, 120 VDC	Pass	Pass	Pass
3601T	9663-610N	Digital Output, 115 VAC	**Susceptible**	Pass	Pass
3503E	9563-810N	Digital Input, 24 VDC	Pass	Pass	Pass
3625	9662-810N	Digital Output, 24 VDC	Pass	Pass	Pass
	9662-610N	Digital Output, 24 VDC	Pass	Pass	Pass
3636T	9668-110N	Relay Output	Pass	Pass	Pass

TABLE 4-1: SUMMARY OF EMI/RFI CONDUCTED SUSCEPTIBILITY TEST RESULTS

Module Model No.	ETP Model No.	Module Type	IEC 61000-4-6 Radio Frequency 150 kHz - 80 MHz	IEC 61000-4-13 Harmonics and Interharmonics	IEC 61000-4-16 Common-Mode Disturbances
3607E	9667-810N	Digital Output, 48 VDC	Pass	Pass	Pass
3502E	9562-810N	Digital Input, 48 VDC	Pass	Pass	Pass
3701	9795-610N	Analog Input, 0-10 VDC	Pass	Pass	Pass
	9783-110N	Analog Input, 0-10 VDC	Pass	Pass	Pass
3703E	9790-610N	Analog Input, 0-10 VDC	Pass	Pass	Pass
	9783-110N	Analog Input, 0-10 VDC	Pass	Pass	Pass
3805E	9860-610N	Analog Output, 4-20 mA	Pass	Pass	Pass
3721	9764-310N	RTD, No. 1600083-600	Pass	Pass	Pass
		RTD, No. 1600083-200	Pass	Pass	Pass
		RTD, No. 1600024-040	Pass	Pass	Pass
		RTD, No. 1600024-030	Pass	Pass	Pass
		RTD, No. 1600024-020	Pass	Pass	Pass
		RTD, No. 1600024-010	Pass	Pass	Pass
		mV, No. 1600082-001	Pass	Pass	Pass
		RTD, No. 1600081-001	**Susceptible**	Pass	Pass
3721	9783-110N	Analog Input, 0-5 VDC	Pass	Pass	Pass
	9790-610N	Analog Input, 0-5 VDC	Pass	Pass	Pass
	9783-110N	Analog Input, 0-5 VDC	Pass	Pass	Pass

TABLE 4-2: SUMMARY OF EMI/RFI RADIATED SUSCEPTIBILITY TEST RESULTS

Module Model No.	ETP Model No.	Module Type	IEC 61000-4-3 High Frequency 26 MHz - 1 GHz	IEC 61000-4-8 60 Hz Magnetic Field	IEC 61000-4-9 Pulsed Magnetic Field	IEC 61000-4-10 Oscillatory Magnetic Field
3008	- - -	Main Processor	Pass	Pass	Pass	Pass
8310	- - -	Power Supply, 115 VAC	Pass	Pass	Pass	Pass
8311	- - -	Power Supply, 230 VAC	Pass	Pass	Pass	Pass
8312	- - -	Power Supply, 24 VDC	Pass	Pass	Pass	Pass
4200	- - -	Remote Extender	Pass	Pass	Pass	Pass

TABLE 4-2: SUMMARY OF EMI/RFI RADIATED SUSCEPTIBILITY TEST RESULTS

Module Model No.	ETP Model No.	Module Type	IEC 61000-4-3 High Frequency 26 MHz - 1 GHz	IEC 61000-4-8 60 Hz Magnetic Field	IEC 61000-4-9 Pulsed Magnetic Field	IEC 61000-4-10 Oscillatory Magnetic Field
4201	- - -	Remote Extender	Pass	Pass	Pass	Pass
4352A	- - -	Communication	Pass	Pass	Pass	Pass
3511	9794-110N	Pulse Input	Pass	Pass	Pass	Pass
3708E	9782-110N	Thermocouple Input	Pass	Pass	Pass	Pass
3501T	9561-810N	Digital Input, 115 VAC	Pass	Pass	Pass	Pass
	9561-110N	Digital Input, 115 VAC	Pass	Pass	Pass	Pass
3623T	9664-810N	Digital Output, 120 VDC	Pass	Pass	Pass	Pass
3603T	9664-810N	Digital Output, 120 VDC	Pass	Pass	Pass	Pass
3601T	9663-610N	Digital Output, 115 VAC	Pass	Pass	Pass	Pass
3503E	9563-810N	Digital Input, 24 VDC	Pass	Pass	Pass	Pass
3625	9662-810N	Digital Output, 24 VDC	Pass	Pass	Pass	Pass
3636T	9668-110N	Relay Output	Pass	Pass	Pass	Pass
3607E	9667-810N	Digital Output, 48 VDC	Pass	Pass	Pass	Pass
3502E	9562-810N	Digital Input, 48 VDC	Pass	Pass	Pass	Pass
3701	9795-610N	Analog Input, 0-10 VDC	Pass	Pass	Pass	Pass
	9783-110N	Analog Input, 0-10 VDC	Pass	Pass	Pass	Pass
3703E	9790-610N	Analog Input, 0-10 VDC	Pass	Pass	Pass	Pass
	9783-110N	Analog Input, 0-10 VDC	Pass	Pass	Pass	Pass
3805E	9860-610N	Analog Output, 4-20 mA	Pass	Pass	Pass	Pass
3721	9764-310N	RTD, No. 1600083-600	**Susceptible**	Pass	Pass	Pass
		RTD, No. 1600083-200	**Susceptible**	Pass	Pass	Pass
		RTD, No. 1600024-040	Pass	Pass	Pass	Pass
		RTD, No. 1600024-030	**Susceptible**	Pass	Pass	Pass
		RTD, No. 1600024-020	**Susceptible**	Pass	Pass	Pass
		RTD, No. 1600024-010	Pass	Pass	Pass	Pass
		mV, No. 1600082-001	Pass	Pass	Pass	Pass
		RTD, No. 1600081-001	Pass	Pass	Pass	Pass
3721	9783-110N	Analog Input, 0-5 VDC	Pass	Pass	Pass	Pass
	9790-610N	Analog Input, 0-5 VDC	Pass	Pass	Pass	Pass
	9783-110N	Analog Input, 0-5 VDC	Pass	Pass	Pass	Pass

4.7 Electrical Fast Transient Testing

EFT Testing of the TUT was performed in accordance with the applicable requirements of NRC Regulatory Guide 1.180, Rev. 1 and IEC 41000-4-4. The following EFT tests were performed (Reference 7.31):

- 120 VAC Chassis Power Supplies: ± 0.5 kV, ± 1.0 kV, ± 1.5 kV and ± 2.0 kV
- 230 VAC Chassis Power Supplies: ± 0.5 kV, ± 1.0 kV, ± 1.5 kV and ± 2.0 kV
- 24 VDC Chassis Power Supplies: ± 0.5 kV, ± 1.0 kV, ± 1.5 kV and ± 2.0 kV
- Peripheral Communications Cables: ± 0.5 kV and ± 1.0 kV
- ETP Input Power Wires: ± 0.5 kV and ± 1.0 kV
- Analog Input/Output Wires: ± 0.5 kV and ± 1.0 kV
- RTD, /T/C and Pulse Input Wires: ± 0.5 kV and ± 1.0 kV
- Discrete Input/Output Wires: ± 0.5 kV and ± 1.0 kV

A. The TUT met all applicable operational and performance requirements during and after each application of the EFT Test voltages.

B. The EFT Test results demonstrate that the Triconex Tricon v10 PLC will not experience operational failures or susceptibilities due to exposure to repetitive electrical fast transients on the power, communication and signal input/output leads.

4.8 Surge Withstand Testing

Surge withstand testing of the Tricon PLC was performed in accordance with the applicable requirements of the IEC 61000-4-5 and IEC 61000-4-12 test methods. The following surge withstand tests were performed (Reference 7.27):

- IEC 61000-4-5 Combination Wave: ± 2.0 kV (common mode and differential): Chassis Power Supplies
- IEC 61000-4-12 Ring Wave: ± 2.0 kV (common mode): Chassis Power Supplies
- IEC 61000-4-12 Ring Wave: ± 1.0 kV (differential mode): Chassis Power Supplies

- IEC 61000-4-12 Ring Wave, IEC 61000-4-5 Combination Wave: ± 0.5 kV (differential): AC and DC Rated Discrete Input/Output Modules, Analog Input/Output Modules, TCM Communication Modules, MODBUS Serial Ports
- IEC 61000-4-12 Ring Wave, IEC 61000-4-5 Combination Wave: ± 1.0 kV (common mode): AC and DC Rated Discrete Input/Output Modules, Analog Input/Output Modules, TCM Communication Modules, MODBUS Serial Ports

The specific Tricon hardware that was tested (chassis, power supplies, modules, external termination assemblies, and interconnecting cabling) is identified in the project Master Configuration List (Reference 7.307.29).

A. The TUT met all applicable operational and performance requirements during and after each application of the Surge Withstand Test voltages.

B. The Surge Withstand Test results demonstrate that the Triconex Tricon v10 PLC will not experience operational failures or susceptibilities that could result in a loss of the ability to generate a trip due to exposure to Ring Wave and Combination Wave electrical surges to the components listed above.

4.9 Electrostatic Discharge (ESD) Testing

ESD Testing of the TUT was performed in accordance with the applicable requirements of Appendix B, Section 3.5 of EPRI TR-102323-R1 and IEC 61000-4-2. The following ESD tests were performed:

ESD Direct Contact Discharges: ± 2 kV, ± 4 kV, ± 6 kV and ± 8 kV
ESD Direct Air Discharges: ± 2 kV, ± 4 kV, ± 8 kV and ± 15 kV
ESD Indirect Contact Discharges: ± 2 kV, ± 4 kV, ± 6 kV and ± 8 kV

The TUT met all applicable operational and performance requirements during and after each application of the ESD Test voltages.

The ESD Test results demonstrate that the Triconex Tricon v10 PLC will not experience operational failures or susceptibilities due to exposure to electrostatic discharges. The main processors continued to function. The transfer of I/O was not interrupted. The TCM Peer-to-Peer and MODBUS communication links continued to operate correctly.

4.10 Isolation Testing

Class 1E to Non-1E isolation testing of the Tricon was performed in accordance with the requirements of EPRI TR-107330 and IEEE Standard 384-1981.

A. The testing demonstrated electrical isolation capability of Model 4352A TCM Communication Module and the Model 3636T Relay Output Module. Note that since interposing relays were required to monitor chassis alarm contacts, the chassis alarms are not qualified for electrical isolation and will require interposing relays, especially if these contacts are to be wired to nonsafety annunciator systems.

B. The testing demonstrated electrical isolation capability of the TCM MODBUS serial communication ports to applied voltages of 250 V ac and 250 V dc, 10 amps maximum, for 30 seconds.

C. The testing demonstrated electrical isolation capability of the relay output points to applied voltages of 600 V ac, at 25 amps maximum, and 250 V dc, at 10 amps maximum.

D. The fiber optic cables are incapable of transmitting electrical faults from the remote Non-1E RXM module to the primary RXM module (which would be installed in the safety related Tricon chassis), and therefore meet IEEE Standard 384-1981 electrical isolation requirements.

4.11 Operability Testing

Operability testing involves exposing the TUT to various normal and abnormal conditions of input/output operation and source power. Operability Testing was performed in accordance with the requirements of Sections 5.3 and 6.4.3 of EPRI TR--107330 and the Invensys Triconex published specifications, to ensure that performance data for the TUT were achieved during and after being subjected to the various qualification tests. The following specific tests were performed:

- Analog Input/Output Accuracy Test
- Response Time Test
- Discrete Input Test
- Discrete Output Test
- Timer Test
- Failover Test

- Loss of Power/Failure to Complete Scan Detection Test
- Power Interruption Test
- Power Quality Tolerance Test

The Operability Tests successfully established performance data for the TUT in accordance with the Invensys Triconex published specifications and/or EPRI TR-107330 specifications and all acceptance criteria stated in the procedure were met.

The test results for the Pre-Qualification Operability Test and Performance Proof Operability Test were analyzed to determine for any degradation in the performance of the TUT. The analyses established that the TUT performed in accordance with Invensys Triconex published specifications and/or EPRI TR-107330 specifications before and, after Qualification Tests and no degradation in the performance of the TUT were identified.

5.0 PROGRAMMING GUIDANCE

This section provides guidance on development of safety-related application programs for the Tricon. Included is guidance on design of application programs, implementation of software quality assurance processes, and operator notification of Tricon system alarms. Some of the guidance provided on application program design and software quality assurance is not specific to the Tricon system, but is included to assist the plant with understanding applicable regulatory requirements.

5.1 Cycle time

A. The Tricon PLC input to output response times are a function of the actual hardware configuration of the PLC and the scan time of the application program loaded in the PLC. Invensys Triconex provides response time formulas for calculating the upper bound on response times for a particular hardware and application program configuration (Reference 7.32). The application specific maximum allowable response time shall be used to design the Tricon hardware and software configuration. The Triconex calculations do not include the time response of external devices, including the RTD to voltage converters.

B. The scan time of the Tricon must be set to meet the required response time of the process and also to provide adequate margin to allow adequate time to run the diagnostics. To do this, set the Tricon scan time below 50% of the required response time. This provides sufficient processing time to perform diagnostics. Less time may result in decreased diagnostic coverage, which is not acceptable. Any scan time significantly greater than the expected 50% of the target scan time shall result in an alarm to the operator, which would generate an annunciation in the control room. Engineering evaluation of the scan time fault should be performed and adjustments or repairs made if the error persists. These requirements are provided in the TÜV Rheinland restrictions for safety critical use of the Tricon. Further guidance on sampling and process response is found in NUREG-1709.

C. Based on the architecture of the Tricon PLC, consistent loop response times within ±20% are not possible. Rather, the system response time should be based on not exceeding the maximum calculated response time. Testing during the qualification has demonstrated that the measured input to output response times were less than the maximum expected values that were calculated based on equations provided by Invensys Triconex. The testing demonstrates that the response time formulas provide a reliable upper bound on maximum expected response times for a particular hardware and application program configuration.

In addition, the test results show no degradation in response time from initial pre-qualification testing throughout qualification and performance proof testing.

D. The Tricon PLC timer function accuracy is a function of the scan time of the application program loaded in the PLC. Specifying an absolute baseline timer function accuracy is therefore inconsistent with the architecture of the Tricon PLC. Instead, application timer function accuracy and the maximum scan time computation for the entire application will be considered in development of any actual application programming. Timers should operate in multiples of the Tricon scan interval to maximize accuracy. During qualification testing, timer functions were demonstrated to not expire any earlier than the required timing period and no later than three scan periods after the required timing period. Longer timers will thus provide increased accuracy. For extremely short timing functions where extreme accuracy is required, an external timing relay is recommended. The accuracy of the timers is dependent on the scan time used in the application. For the specific scan time used in baseline testing, a 1-minute timer function provided accuracy of 0.19%, and a 5-minute timer function accuracy provided accuracy of 0.093%.

E. The response time to an RTD input was not measured. However, the time response of the field installed RTD and the thermowell in which it is likely installed, will be known and the time response of the Analog Devices RTD to voltage converter is published. These values add to the time response determined for an analog voltage input for RTD inputs.

5.2 Software Quality Assurance Processes

General considerations relating to software quality assurance processes include the following:

A. The Triconex Product Alert Notices (PAN), Technical Advisory Bulletins (TAB), and Technical Application Notes (TAN) should be reviewed as they are released for applicability to the installed system. This requires the bulletins go to the engineer responsible for the system, rather than solely to licensing, procurement engineering, or maintenance.

B. The application must be created under a nuclear safety-related software quality assurance process. A process acceptable to the USNRC is outlined in the Standard Review Plan in Branch Technical Position 7- 14.

C. After commissioning, any changes to the application itself or the application program must be made under strict change-control procedures, similar to those required in BTP 7-14. All changes must be thoroughly verified and validated, as well as audited and approved by the plant safety change control committee or group. After an approved change is made, all appropriate software and documentation must be archived.

D. Configuration data shall be retained, including programs, system configuration, module configuration, input/output databases, and other Tricon and TriStation 1131 configuration items.

E. Since the user readable program is available only on the PC, retention of the PC configuration items is critical for long term maintenance. In addition to printed documentation of the application program, at least two electronic copies of the program must be archived in separate locations. This is necessary to comply with requirements for dual storage of safety related quality records.

F. The archival media must be write-protected after storage of the application program to avoid accidental changes. More robust media than diskettes are recommended, to include the longer-lived CD-R, CD-RW, or DVD.

5.3 Guidance for Application Programming

Specific guidance for development of application programs using the TriStation 1131 programming tool is discussed below. The guidance provided below is intended to: (1) minimize the chance for design errors built into application programs during the development process, (2) maximize the reliability of the process used to download application programs from the TriStation 1131 PC to the Tricon PLC, and (3) support required software quality assurance processes.

A. The PC used for developing, controlling, interfacing, and downloading to the Tricon shall have enabled Error Correcting Code (ECC) memory and shall be listed, at least when initially put into service, on the applicable Microsoft Windows Hardware Compatibility List. This PC should not be used for any other functions, to avoid uncontrolled and unintentional changes to the Windows environment or computer security risks.

B. The Tricon is programmed in one or more of the supported IEC 61131-3 languages. The functional diagrams shall be generated using the TriStation 1131 Developer's Workbench.

C. The TriStation 1131 Developer's Workbench generates printed output of the application software equivalent to the traditional I&C Logic Drawings. This output shall be used for independent verification and validation and application review. This printed output should be considered the primary reference to the application.

D. Programs shall be developed in accordance with TriStation 1131 User's Manuals, which provide guidelines for the programming of software written in Function Block Diagrams, Ladder Diagrams, Structured Text, and Cause Effect Matrix Programming Language. Modifications to certain TUV restrictions related to application programming are provided in this section.

E. Applications programs should be developed with guidance from various industry sources, including NUREG/CR-6463, "Review Guidelines on Software Languages for Use in Nuclear Power Plant Safety Systems."

F. Application programs shall be a product of a disciplined implementation process, providing the traceability necessary to associate source code with higher level design documents to enhance verification, validation, and other aspects of software quality assurance.

G. The programmer shall use methods to maximize structure and readability, including use of comments.

H. Application programs shall be designed to enhance the capability of the software to handle exception conditions, recover from internal failures, and prevent propagation of errors arising from unusual circumstances.

I. Application programs shall be designed to reduce the likelihood that faults will be introduced during adaptive or corrective software changes made after delivery.

J. Each variable shall be initialized. Variables may be set once in the first scan after startup, or in each scan, as required by the programmed function. Constant values shall be declared.

K. Constants, such as setpoints, that might require modification are to be defined as variables, to allow online changes to these variables without requiring a software download. TriStation 1131 can modify Tricon variables without having to download the complete application.

L. Comments shall be included in the program. Each network purpose shall be commented. Operations or series of operations shall be described in comments, to

maximize the ease of reading, understanding, and modifying networks. Comments shall be structured and placed in the network to minimize interface ambiguities and errors.

M. Application program comments should reference the higher-level design documentation, particularly for data type, variable, and constant declarations.

N. For any unusual or complex constructs as well as any deviations from normal programming practices, comment blocks shall be provided explaining the purpose and operation of the construct or the reason for the deviation.

O. Names for variables, procedures, functions, data types, constants, exceptions, objects, methods, labels, and other identifiers shall be descriptive, consistent, and traceable to higher-level (i.e., software design) documents. Naming conventions are an important part of the coding style and practices. Using the same name for multiple variables should be avoided unless obviously advantageous and, when employed, shall be accompanied by clear, consistent, and unambiguous notations in all locations where the variable is used.

P. The Tricon must detect open and short circuits in the wiring between the PLC and the critical field devices, as well as open or short circuits in the field devices. Detected faults shall be alarmed in the control room. An application should not use the OVDDISABLE function, which disables the output module short, open, and load validation self test functions for any supervised outputs.

Q. Existing Triconex-supplied functions and Structured Text can be used to create special purpose function blocks in the User Library for use in program generation.

R. Support for surveillance testing shall be provided in the basic Tricon application program. No program changes shall be necessary to implement any of the required periodic surveillance tests.

S. A Tricon normally does not contain any disabled points unless there is a specific reason for disabling them, such as initial testing. To disable points, the Tricon keyswitch must be in PROGRAM mode rather than RUN or REMOTE mode. If the system does contain one or more disabled variables, then an installed network should annunciate in the control room to indicate that disabled points are present. No disabled points should be present in an operating unit.

T. TÜV requires a safety application to include networks that will initiate a safe shutdown of the process being controlled if the Tricon goes to single processor

mode. In a nuclear environment, the expected divisional or channel redundancy in nuclear applications does not require this functionality. However, any of the faults identified below should be annunciated in the control room and should be repaired in an expeditious manner. The following system information variables, accessible as outputs of the TR_MP_STATUS function block, should be checked:

- **MPMAIN-**At least one Main Processor is out-of-sync or faulted.
- **IOMAIN-**MPMAIN is on, or at least one leg of one I/O module has faulted.
- **MPBAD-**Two Main Processors are out-of-sync or faulted (in single mode).
- **IOBAD-**MPBAD is on, or at least one I/O module is in single mode.

U. One condition that can energize the IOBAD variable is the presence of Bad Board errors on any two legs of an I/O module. Bad Board means that a fatal error has been reported by one of the legs of the I/O module, or communication to one of the legs has been lost. However, the IOBAD variable cannot distinguish between modules that are critical to the process and modules that are not critical. For example, an output module that interfaces to status lamps on a local panel is usually not critical to the process. Logic should be generated which provides a lower level annunciation of the detected fault for those modules that do not perform safety-related functions. This logic should consider whether reflash of the output is necessary as additional faults occur. With this additional logic, repair of the failed module is still required, but at a lower priority than repair of modules implementing safety critical functions.

V. The system mechanisms to detect failure to complete a scan (or watchdog timers) are checked during hardware diagnostics performed on power-up of the Tricon PLC. If a failure of a watchdog timer mechanism is detected, the PLC power-up will stop and the main processor fault indicators will turn on. Therefore, successful restart of the Tricon PLC on restoration of power indicates proper functioning of the watchdog timer mechanisms. Additionally, these watchdog timers are periodically tested during system operation.

W. **When using the RXM for 1E to non-1E isolation, the non-safety points must be treated the same as safety points during the development of the application program.**

5.4 Loss of Power Fault Indication

A. The Tricon PLC exhibits clear indications of power loss on chassis alarm relay outputs, analog outputs, and discrete outputs. All outputs are placed in a fail-safe, de-energized condition during power failure. The Tricon PLC also provides clear indication of power restoration through the same mechanisms.

B. On one occasion during qualification testing for the V9, a Tricon module did not restart on a momentary loss of power. Triconex Design Engineering indicates that, with one power source turned off and momentary glitches on the redundant power source, there is a remote possibility that the power fail/reset circuit on an individual module may not operate correctly. This fault was clearly indicated on the system and was resolved by recycling the system power supplies. Most electronic equipment cannot tolerate short duration, transient power losses.

C. During qualification testing loss of power tests were performed. The test results demonstrate a predictable and consistent response of the Tricon PLC to loss of power including:

(a) Chassis alarm relay circuits change state to indicate the loss of power condition.

(b) Analog output points go to a zero output value during the loss of power period.

(c) Discrete and relay output points held closed during application program execution open during the loss of power period.

(d) All communication links to peripheral devices are disabled during the loss of power period. The communication links that were monitored during testing include the TCM module connections to the TriStation Console and the Simulator Tricon PLC running the MODBUS protocol and Peer-to-Peer networking.

D. The loss of power test results also demonstrate a predictable and consistent response of the Tricon PLC to restoration of power including:

(a) Chassis alarm relay circuits change state to indicate restoration of power.

(b) Analog output points go to the value commanded by the application program on restoration of power.

(c) Discrete and relay output points held closed during application program execution re-close on restoration of power.

(d) All external communication links are restored on restoration of power.

5.5 Communication with External Systems

A. Communication with external systems must use the approved module.

B. There are no restrictions on incoming communication from external systems when operated in a mode where only date and time adjustments are allowed to the Tricon. Restrictions are provided and must be incorporated when the external systems are allowed to write data into the Tricon, as defined in Sections 5.5, D, and 6.5 of this report.

C. Under certain conditions, the Tricon may be run in a mode where an external computer or operator station can write to the Tricon PLC variables. This is normally done by means of a communication link. In this mode, serial communication must not be allowed to write directly to input or output variables. Restrictions and guidance for Maintenance and Override functions are provided in a separate section of the application guideline. These restrictions are based on guidance from the "Safety Considerations Guide for Tricon v9-–v10 Systems." The communication link and variables shall comply with the Maintenance and Override requirements provided in Section 6.5 of this Application Guide.

D. Nonsafety and safety communication links cannot be mixed on any communications module.

5.6 Peer-to-Peer Communication

A. The Tricon supports redundant physical peer-to-peer communication links and provides embedded support for the redundancy. Application programs can determine whether the peer-to-peer network is operating in single or redundant mode. If the peer-to-peer operation is critical, loss of redundancy should be alarmed in the control room.

B. Any use of the peer-to-peer communication shall be evaluated to determine if the delay between message initiation and message reception is acceptable for the given safety related application. The normal delay is up to 6 scan times.

C. The sending node must set the sendflag in the send call to one so that the sending node sends new data as soon as the acknowledgment for the last data is received from the receiving node.

D. Because safety systems tend to remain in a single state for extended periods, messages containing state values may not change regularly. The sending node must use the TR_USEND function block and include a diagnostic integer variable that gets incremented with each new message. The receiving node must check this variable for change every time it processes new data, because the message itself may not change.

E. The sending node should require no more than five TR_USEND functions in an application. The Tricon only initiates five TR_USEND functions per scan. In order to send data as fast as possible, the TR_USEND function must be initiated as soon as the acknowledgment for the last data is received from the receiving node. If maximum throughput is not required, more than five TR_USEND functions may be programmed. Evaluations should be performed to verify that the required safety functions occur within the maximum time interval possible for multiple communications failures on all transmitted messages.

F. The sending node must check the status of the TR_URCV and TR_PORT_STATUS functions to see if there is a network problem.

G. The receiving node's application must include logic to see whether new data is received within the specified maximum time-out limit. The maximum time-out limit is equal to half the process-tolerance time. If the receiving node does not get at least one sample of new data from the sending node within the maximum time-out limit, then the receiving node's program must take one or more of the following actions, depending on requirements for the safety functions being implemented:

- Use the last data received for safety-related decisions in the application.
- Use default values for safety-related decisions in the application
- Initiate the appropriate safety functions.

H. If new data is not received within the specified maximum time out limit, the receiving node's application must also check the status of the TR_URCV and TR_PORT_STATUS functions to see if there is a network problem that requires operator intervention.

I. In any case, this failure shall be annunciated in the control room, preferably from both Tricon PLCs, and appropriate maintenance action shall be implemented immediately. The specific actions that an application should take depend on the process safety requirements. The receiving node must check the diagnostic

integer variable every time it receives new data to see whether this variable has changed.

5.7 Communication Application Safety Layer

A. The Tricon supports redundant physical safety-related SAP communication links with qualified display units. If the communication is safety-related, loss of redundancy must be alarmed in the control room.

B. In the Tricon System, the communication subsystem cannot be used to provide measures and techniques to insure the integrity of communication. As with Peer to Peer (section 5.6), the application on each end is responsible for the end-to-end integrity of safety-critical communications.

C. The safety-related application code implementing the SAP must be functionally independent from the transmission code (i.e., the network stack).

D. Even when the messages are arriving in a correct (deterministic) manner the safety data still may be corrupted. As with Peer-to-Peer, the data integrity assurance is a fundamental component of the safety-related application code implementing the SAP to achieve the communication-link integrity requirements.

E. The communication channel (i.e., transmission protocols at the lower layers of the network stack) must not use the same hash function as the SAP.

F. All SAP-defined measures for data integrity assurance must be implemented within the SAP based safety application.

G. SAP communication error handling will be defined and implemented by the application program.

H. Any use of the SAP for communication must be evaluated to determine if the delay between message initiation and message reception is acceptable for the given safety-related application.

I. The application on each end shall implement a diagnostics message to detect loss of communication.

J. Detected communication failures shall be annunciated in the control room, from the Tricon PLC(s). The safety-related display unit shall program and display the alarm for the detected communications errors.

6.0 INSTALLATION, COMMISSIONING, AND MAINTENANCE

This section discusses considerations for installation, commissioning, and long term maintenance of safety-related Tricon systems. This guidance is intended to identify important considerations for these activities particularly for microprocessor-based safety systems. As such, much of the guidance is relatively generic in nature and is not specific only to the Tricon system.

6.1 Required testing

A. Functional testing must be performed to validate the correct design and operation of the user-written application program for commissioning and after any modification is implemented. The amount of validation after a change must be appropriate to the magnitude and safety criticality of the modification.

B. After a safety system is commissioned, no changes to the system software (operating system, I/O drivers, diagnostics, etc.) may be performed without re-commissioning the system. This requirement is provided in the TÜV Rheinland restrictions for safety critical use of the Tricon.

C. Periodic testing shall be performed to the requirements established in the Technical Specifications. Credit for self-tests can be used to reduce the requirement for surveillance testing, based on changes to the Technical Specifications. Guidance for applying the inherent and application program generated capabilities of the Tricon PLC for surveillance is provided in a separate section of this report.

6.2 Operations Procedures

A. Dependent on the level to which faults are displayed in the control room, abnormal operating and alarm response procedures will require modification. If, for example, the operator can query the status of individual Tricon modules, more detailed procedures and training will be required than if a multiple level failure and trouble alarm annunciation scheme is provided with Maintenance personnel providing troubleshooting and Technical Specification impact determination.

B. Operating procedures for the safety system being replaced will have to be modified to accommodate the Tricon. Procedures for new fault alarms will have to be created. Procedures for the unlikely software common cause failure will have to be validated. Procedures for entry, exit, and performance of maintenance

and surveillance testing procedures will have to be modified or enhanced for the differences between an older analog and a newer digital protection system.

6.3 Maintenance Procedures

Specific maintenance considerations for the Tricon system include the following:

A. The Tricon PLC Main Chassis requires two batteries for RAM backup of the application programs. These batteries provide backup power to maintain system programming in the unlikely event of total loss of the two independent power sources and chassis power supplies. When powered, the Tricon will alarm when the battery power falls to a point where it can no longer support system operation. Based on the shelf life limitations of lithium batteries, new batteries should be ordered when the battery life alarm occurs or every ten years, whichever comes first.

B. The Tricon PLC power supplies contain electrolytic capacitors for filtering. These power supplies should be replaced on a ten year cycle.

C. Section 5 of the Triconex Planning and Installation Manual contains recommendations for periodic testing of power supplies and toggling field points.

D. The maintenance procedures should be written with the guidance from the Triconex Planning and Installation Guide (Reference 7.13).

E. Logical pairs of locations exist for input and output module locations. For a given location, either of the two logical locations are equivalent. Procedures and documentation should be generated that allow the normal primary card to be installed in either of the logically paired locations in a chassis. Thus, the spare card referred to in this section could be either location in a logical pair of locations and the primary module could be in either location as well.

F. In order to assure timely access to known operable modules, it is recommended that spare modules be installed in the on-line Tricon PLCs. At least one hot spare of every type of I/O module should be installed in each division, channel, or train. This hot spare module should be installed as active, redundant cards. By keeping the modules in operation, any faults on the spare modules will be diagnosed by the Tricon, since the spare modules will be actively used in control. There are no identified life-limited failure mechanisms for these modules. By following this recommendation, the spare modules will be available for instant use by

maintenance personnel. When a faulted module is returned to Triconex for repair, additional spare modules exist in other divisions, channels, or trains.

Additional important maintenance considerations for digital systems that are not specific to the Tricon system include the following:

G. Procedures shall be developed to support normal maintenance functions. Since an installed spare is expected to be available in each division or channel, the procedures should be based on used of that spare module or a module from another division or channel, to replace the failed module. The industries currently using the Tricon for safety functions offer several lessons learned. This process is based on those lessons. The procedures for module replacement shall include appropriate instructions to 1) find, verify, and remove only the inactive spare card from the bypassed channel in preparation for replacing the faulted module, 2) insert the spare card at the faulted module logical paired location, 3) wait for the system to transfer control to the newly installed module, 4) remove the faulted module only after the Tricon has been confirmed to have transferred control to the new module, 5) repair the faulted module after diagnosis of the problem, and 6) reinstall the refurbished module as a hot spare somewhere in the channel, division, or train.

H. Modifications resulting from Maintenance procedures must be coordinated with Operations to minimize risk during performance of the Maintenance procedures, including surveillance testing.

6.4 Application Program Maintenance Procedures

Considerations for application program maintenance procedures that relate specifically to the Tricon system include the following:

A. Applications procedures should be created and implemented for configuration management.

B. A procedure shall be written for downloading a configuration to the Tricon. This procedure shall provide compensatory measures to disable the Tricon outputs during the download. A procedure is provided in the Triconex TriStation 1131 Developer's Workstation User's Guide for a Download All into a Tricon PLC, in the section labeled 'Downloading A Project.' Since this procedure requires removal of all three Main Processors to clear all of the application code from memory completely, all Tricon outputs will go to the fail-safe state, with all discrete outputs powered off and analog outputs set to 0 milliamperes. Operations and Engineering should be adequately prepared to avoid unnecessary challenges to other safety systems and the nuclear generating station.

C. Based on TÜV's evaluation and recommendations, when development and testing of the safety application is complete or after any modifications are performed, the Download All and Compare functions should be used to download and verify the success of the download of the final application to the Tricon. When the download is verified to be correct, the RUN or REMOTE function is used to start running the programs. Any required testing would be performed and the Tricon would be removed from bypass. Taking these steps guarantees that all of the variables in the safety application logic will be initialized properly in the Tricon's memory, and that only a valid downloaded program would be loaded in the Tricon. This also resolves the issues and concerns from multiple downloaded changes, including fragmentation and possible exhaustion of free memory in the Tricon.

D. Connecting a TriStation PC to an online Tricon is possible. With the keyswitch in the RUN position, the TriStation can not affect the program or variables. With the keyswitch in the RUN position, the TriStation cannot pause or halt the application program. There is also password security in the TriStation 1131 to lessen the chance of unauthorized access. For that reason, there are no restrictions to connecting a TriStation PC to a Tricon.

E. While not specific to the Tricon system, any changes to the application itself or the application program after commissioning must be made under strict change-control procedures, such as those required in BTP-14. Modifications to the application software shall be made with at least as rigorous a set of software quality assurance procedures, including independence of verification and validation activities, as were used during the initial program development. All changes must be thoroughly verified and validated, as well as audited and approved by the plant safety change control committee or group. After an approved change is made, it must be archived.

6.5 Maintenance and Bypass Capabilities

Existing safety-related systems in nuclear power plants typically include bypass capabilities for maintenance and testing. Implementation of these capabilities in a digital system requires particular attention to prevent undesired operation of the system. Generic guidance on the implementation of bypass capabilities is provided below.

A. Maintenance bypasses can be initiated either using special switches connected to PLC inputs, or overrides can be programmed into the Tricon to enable a remote

device to serially request the override. This allows the user to request bypassing a single sensor or all functions implemented in a Tricon PLC.

B. If special switches are used to initiate the bypass, these discrete inputs will be used to deactivate actuators and sensors under maintenance or to force safety functions to an enabled or disabled state. The maintenance bypass conditions are handled as part of the application program of the PLC. The switches would conform to the specifications and requirements for class 1E devices and circuits. This is equivalent to the process currently used in most US nuclear plants.

C. If bypasses are programmed into the Tricon, enabling a remote device to request the bypass over appropriate serial communication links to the PLC, the programming must be implemented in accordance with NRC regulatory guidance.

D. Connecting to the PLC over serial lines shall be performed using protocols with protection from garbled or corrupted communication packets. Any communication protocol used should include CRC, address check, and check of the communication time frame.

E. If no bypass functions are active, lost communication should lead to a warning to the operator. If bypass functions are active, lost communication shall be annunciated to the operator and at the Tricon. After loss of communication, the design safety evaluation should determine whether a time delayed automatic removal of the bypass is desirable. If this function is implemented, a warning should be provided to the operator prior to implementing the removal.

F. The external system shall provide individual action requests as integer values. Each action request shall be provided as separate integer values. If the integer were set to zero, the action request would be cancelled after the implement command contact changes state. The action request integer is required to change on no less than a one-second period. If the Tricon detects an unchanged input for an unacceptable period, the lost communication process described in this section shall be implemented. The commanded action request shall be valid as long as the action request integer value changes on a periodic basis.

G. The use of the maintenance bypass function should be documented on the external system and should be visible on the TriStation 1131, when connected. The data retained should include time stamps at the beginning and end of the bypass; the ID of the person who activated the bypass (if the information cannot be easily entered, it should be retained in the work permit); and the tag name of the signal or function being overridden.

H. The maintenance bypass function would not be performed by the TriStation 1131 engineering workstation.

I. If signal bypass is possible, the Tricon shall have a pre-defined table or code in the application program that defines the signals that may be bypassed and, implicitly, those that may not be bypassed. If simultaneous bypasses are possible for multiple signals, the Tricon shall have a pre-defined table or code in the application programs defining which combinations are acceptable.

J. Direct bypasses shall not be installed on inputs or outputs. Bypasses have to be checked and implemented in relation to the application. Multiple bypasses in a Tricon are allowed as long as only one bypass is used in a given safety related group.

K. An alarm shall exist for bypasses in the appropriate control room. It shall not be possible to override or disable the alarm.

L. The PLC shall alert the operator that a bypass condition exists. The warning shall exist until the bypass is removed. This alert may be used to confirm that the bypass condition has been installed or removed.

M. It may be desirable, from decisions made based on licensing and failure analysis, to have a second, backup, method to remove maintenance bypasses. Functions of this nature require extensive testing prior to being placed in service.

N. The external system and Tricon programs as well as programmatic guidance enforce a limited time span for the bypass to be in place. Typically, no more than one shift should be required or allowed. Hardwired indication should be considered in a location where the control room operator is reminded of the loss of that division or channel of protective functions. The number and location of lamps should be based on the plant license requirements.

O. The external system should check regularly that no discrepancies exist between its bypass command list and the Tricon PLC bypass accepted list.

7.0 REFERENCES

7.1 USNRC Standard Review Plan, Chapter 7, Revision 5

7.2 USNRC Standard Review Plan, NUREG-0800, Branch Technical Position 7-14, Revision 5, Guidance on Software Reviews for Digital Computer-Based I&C Systems

7.3 USNRC Standard Review Plan, NUREG-0800, Branch Technical Position 7-18, Revision 5, Guidance on the Use of Programmable Logic Controllers in Digital Computer-Based I&C Systems

7.4 USNRC Standard Review Plan, NUREG-0800, Branch Technical Position 7-17, Revision 5, Guidance on Self-Test and Surveillance Test Provisions

7.5 USNRC Standard Review Plan, NUREG-0800, Branch Technical Position 7-21, Revision 5, Guidance on Digital Computer Real-Time Performance

7.6 USNRC Regulatory Guide 1.180, Revision 1, "Guidelines for Evaluating Electromagnetic and Radio-Frequency Interference in Safety-Related Instrumentation and Control Systems," October 2003

7.7 USNRC Interim Staff Guidance DI&C-ISG-04, Highly Integrated Control Rooms – Communications Issues, Revision 0, September 28, 2007

7.8 EPRI TR-107330, Generic Requirements Specification for Qualifying a Commercially Available PLC for Safety-Related Applications in Nuclear Power Plants

7.9 EPRI TR-102323-R1, Guidelines for Electromagnetic Interference Testing in Power Plants

7.10 IEEE Standard 323-1974, IEEE Standard for Qualifying Class 1E Equipment for Nuclear Power Generating Stations

7.11 IEEE Standard 384-1992, IEEE Standard Criteria for Independence of Class 1E Equipment and Circuits

7.12 IEEE Standard 603-1991, IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations

TRICONEX DOCUMENTS

7.13 Triconex Planning and Installation Guide, Part Number 9720077-012

7.14 Triconex User's Manual for Field Terminations, Part Number 9700052-018

7.15 Triconex Technical Product Guide, Part Number 9791007-013

7.16 Triconex TriStation 1131 Developer's Workbench User's Guide, Part Number 9700100-003

7.17 Triconex Safety Considerations Guide for Tricon v9-v10 Systems, Part Number 9700097-007

TRICONEX NUCLEAR QUALIFICATION PROJECT DOCUMENTS

7.18 Qualification Summary Report, Triconex Report Number 9600164-545

7.19 Software Qualification Report, including the Critical Digital Review, Triconex Report Number 7286-535

7.20 Critical Digital Review of the Tricon V10.2.1, Triconex Report Number 9600164-539

7.21 Failure Modes and Effects Analysis, Triconex Report Number 9600164-531

7.22 Reliability/Availability Study, Triconex Report Number 9600164-532

7.23 Tricon System Accuracy Specifications, Triconex Report Number 9600164-534

7.24 Seismic Test Report, Triconex Report Number 9600164-526

7.25 Environmental Test Report, Triconex Report Number 9600164-525

7.26 EMI/RFI Test Report, Triconex Report Number 9600164-527

7.27 Surge Withstand Test Report, Triconex Report Number 9600164-528

7.28 Class 1E to non-1E Isolation Test Report, Triconex Report Number 9600164-529

7.29 Exposure Test Report, Triconex Report Number 9600164-533

7.30 Master Configuration List, Triconex Report Number 9600164-540

7.31 Electrical Fast Transient Test Report, Triconex Report Number 9600164-521

7.32 Response Time Calculation, Triconex Document Number 9600164-731