Enclosure 3

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

Invensys Response to Request for Additional Information (RAI)

Ref: Letter dated December 8, 2010, NRC to Invensys

Attachment	RAI No.	Description
1	1	RXM Safety/Non-safety Interface versus Interim Staff Guidance (ISG)-4
2	2	Assignment of Safety-related and Non-safety I/O to RXM Chassis
3	3	Testing Related to RXM Chassis Failures
4	4	Document Listing for FPGA Development
5	5	Response Time Compliance with EPRI 107330
6	6	Determinism and Use of Interrupts

ATTACHMENT 1
INVENSYS RESPONSE TO RAI No. 1

RAI No. 1: RXM Safety/Non-safety Interface versus Interim Staff Guidance (ISG)-4

How does the safety/non-safety interface between primary and remote extender chassis RXM's meet the 20 staff positions regarding interdivisional communications in Interim Staff Guidance (ISG)-4?

RESPONSE:

In response to the staff's Request for Additional Information 1, Invensys has developed a DI&C-ISG-04 compliance matrix for the RXM Chassis, which has also been included in the new Appendix 2 to the revised NTX-SER-09-10 (Revision 2). This new Appendix provides a significant expansion of the discussion of the RXM issues previously provided in a Supplementary Information submittal (ref. IOM letter NRC-V10-10-005, dated August 5, 2010). RXM compliance with the 20 staff positions is addressed in this matrix. IOM document NTX-SER-09-10, Revision 2 is being provided with this submittal.

ATTACHMENT 2
INVENSYS RESPONSE TO RAI No.2

RAI No. 2: Assignment of Safety-related and Non-safety I/O to RXM Chassis

Invensys document NTX-SER-09-10 Rev 1, "Compliance with ISG-2 & ISG-4", Page 11, states that "The non-safety remote RXM chassis would not have any safety related I/O [input/output] assigned to it." Please explain the basis for this statement including what hard, soft, or administrative controls exist in for the Triconex product or the 1131 programming application, how those controls ensure adequate protection, and whether controls are generic or application specific.

RESPONSE:

Assignment of I/O is a design decision based on customer requirements specified in, for example, system-level functional requirements specifications. There are not any controls in TriStation 1131 for ensuring proper assignment of safety and non-safety I/O, because it is an engineering tool that the application engineer will use to program software for the Tricon. However, Invensys documentation, such as the 7286-545-1 Appendix B V10 Tricon Application Guide, contains guidance for the application engineer on programming of fault-handling algorithms for I/O faults. Specialized Tricon library function blocks are available specifically for ensuring proper operation of safety-critical I/O. The Application Guide also contains guidance for the application engineer on proper handling of both safety-critical and non-safety critical I/O in application programs. By adhering to the above Invensys guidance, the safety function of safety-related systems utilizing non-safety Remote RXM chassis will not depend upon the non-safety I/O points.

Invensys proposes to revise item D.3 in Section 3.3 of Appendix B of the Topical Report as follows (new text in **bold**):

"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."**

Invensys proposes to also revise Section 5.3 of Appendix B of the Topical Report to add new item W, as follows:

"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."

With regard to the specific Invensys statement cited in the RAI above, the statement appears in two places in Invensys document NTX-SER-09-10; first on page 11, and the second on page 76 of 122 in response to Staff Position 17 of ISG-4. Invensys proposes to revise NTX-SER-09-10 such that all discussion of the RXM conformance to ISG-04 is moved to a new Appendix 2, "Additional Details on the Operation of the V10 Tricon Remote Extender Chassis." Proposed revisions to pages 11 and 76 will be discussed in turn.

The first reference on page 11 of 122 will be replaced with a reference to a new Appendix 2 that contains additional technical detail on the operation of the V10 Tricon Remote Expansion Chassis. As stated in the Invensys response to RAI-1, the ISG-4 conformance table for the RXM chassis will be included in the new Appendix 2. Below is the proposed revised text on page 11 (new text in **bold**, deleted text per strikethrough):

> "The 4200 and 4201 RXM Modules convert the system I/O Bus to multi-mode fiber optic cable. No network communications are routed through the RXM Modules. As discussed in the EQSR, the 4200 and 4201 RXM Modules are qualified electrical isolation devices. ~~Therefore, it is possible to have a safety-related Main and Primary RXM chassis, and a non-safety remote RXM chassis[3]. The application software executed in the safety-related Main Chassis (i.e., the 3008N MPs mounted in the Main Chassis) would be developed and tested in accordance with NRC regulatory requirements for safety-related software. The non-safety remote RXM chassis would not have any safety-related I/O assigned to it. Furthermore, there are no I/O hardware or software failures that could occur in the non-safety remote RXM chassis that would prevent the safety function in the safety-related Main Chassis and primary RXM.~~ **The associated regulatory issues described in ISG-04 are addressed in Appendix 2, 'Additional Details on the Operation of the V10 Tricon Remote Extender Chassis.'"**

Note that the above change will delete footnote 3 on page 11 of NTX-SER-09-10. There is an associated change required on page 14, Section 2.1, V10 Tricon System Bus Architecture, under the discussion of the I/O Bus. The last sentence of the last paragraph will be revised to point the reader to the new Appendix 2, as shown below (new text in **bold**, deleted text per strikethrough):

> "The I/O Bus is a system bus that utilizes a low-level, serial master-slave protocol that does not involve network communications. If I/O modules or RXM chassis are added without using TriStation 1131 and performing a download to the 3008N MPs in the Main chassis, the newly inserted I/O module or the RXM chassis would be inoperative with no degradation on the system as designed. The I/O module and RXM would never reach an ACTIVE state, and the 3008N MPs will ignore the new I/O module and/or RXM chassis. Because the I/O Bus is strictly an internal bus between the IOCCOM and I/O modules, external hosts cannot affect the I/O Bus (i.e., attach to the bus). ~~Therefore the I/O Bus has not been specifically assessed in terms of conformance to ISG4.~~ **The associated regulatory issues described in ISG-04 are addressed in Appendix 2, 'Additional Details on the Operation of the V10 Tricon Remote Extender Chassis.'"**

The second reference is on page 76 of 122 in response to Staff Position 17 of ISG-4 regarding the medium used in a vital communications channel being qualified for the anticipated normal and post-accident environments pursuant to 10 C.F.R. § 50.49. The Invensys statement is out of context, because the Staff Position is concerned with equipment qualification. Therefore, because of the addition of the new Appendix 2, the last paragraph of the Invensys response will be will deleted as follows:

> "~~Section 2, Tricon Chassis Configuration, discusses the types of Tricon chassis available, i.e., Main, Expansion, and Remote Expansion Chassis (RXM). Figures 2 and 3 show the cable connectors on the chassis and possible configurations using the Main, Expansion, and RXM chassis. It is possible to have a safety-related Primary RXM connected to a nonsafety-related Remote RXM chassis via triplicated multi-mode fiber optic cables between the 4200/4201 RXM Modules. No network communications are routed through the RXM Modules. As discussed in the EQSR, the 4200 and 4201 RXM Modules are qualified electrical isolation devices, because the fiber optic cable is incapable of propagating electrical faults between the RXM chassis, therefore they meet the requirements of IEEE 384-1981 electrical isolation requirements for 1E-to-non1E isolation devices. The non-safety Remote RXM chassis would not have any safety-related I/O assigned to it. Furthermore, tThere are no I/O hardware or software failures that could occur in the non-safety Remote RXM chassis that would impact the functioning of the safety-related Main Chassis and Primary RXM.~~"

Revisions to IOM documents 7286-545-1 Appendix B V10 Tricon Application Guide and NTX-SER-09-10 (containing the above changed pages) are being provided with this submittal.

ATTACHMENT 3
INVENSYS RESPONSE TO RAI No. 3

RAI No. 3: Testing Related to RXM Chassis Failures

Invensys document NTX-SER-09-10 Revision 1, "Compliance with ISG-2 & ISG-4", Page 11, states that "…there are no I/O hardware or software failures that could occur in the non-safety remote RXM chassis that would prevent the safety function in the safety-related Main Chassis and primary RXM." The NRC staff recognizes the related Failure Modes and Effects Analysis supplied in the August 3, 2010, supplemental information. Please identify any actual tests performed to support these conclusions and provide a summary of the tests and their results for NRC staff review.

RESPONSE:

Tests were performed on both Primary and Remote RXM Chassis and modules as documented in Test Procedure 9600158-002, "Tricon System Functional Validation Procedure." Specifically, Test Section Identifiers: 6.6, 6.8, 6.9, 6.11, 6.15, 6.17, and 6.18.

These tests were most recently executed during the verification and validation (V&V) of Tricon V10.5. The test results were all recorded as PASSED in the "Tricon 10.5 Verification and Validation Report" dated 7/22/09. These tests verify that the behavior of the RXM modules has not changed since the first release of the RXM module firmware Meta#3310 in Tricon V6.3 on 6/16/1993.

The RXM firmware Meta#3310 released in Tricon V10.5.1, the release currently being reviewed by NRC, is identical to the RXM Firmware Meta#3310 released for Tricon V6.3.

The tests were also executed and reported as PASSED as part of the:

- Tricon V10.4 V&V activity reported in the Tricon V10.4 V&V Summary Report dated 4/16/2010
- Tricon V10.3 V&V activity reported in the Tricon V10.3 V&V Summary Report dated 5/11/2007
- Tricon V10.2.1 V&V activity reported in the Tricon V10.2.1 V&V Summary Report dated 10/25/2006

It should be noted that the above RXM tests were routinely executed on all major Tricon releases between V6.3 and V10.0.

A Failure Modes and Effects Analysis for the non-safety RXM Chassis was submitted by Invensys in the Supplementary Information package dated August 3, 2010, Selected Topic 1 (ref. IOM letter NRC-V10-10-007). The FMEA has been incorporated into NTX-SER-09-10, "Tricon Applications in Nuclear Reactor Protection Systems - Compliance with NRC ISG-2 & ISG-4," as Appendix 2, *Additional Details on the Operation of the V10 Tricon Remote Extender Chassis*. In response to the staff's Request for Additional Information 1, Invensys has developed a DI&C-ISG-04 compliance matrix for the RXM Chassis, which has also been included in the new Appendix 2 to the revised NTX-SER-09-10. Staff Position 12 postulates a number of communication failures that should be addressed. Table 1 below numbers the postulated failures (SP12.x, where *x* = 1 thru 12), and indicates whether the RXM Chassis FMEA addresses the postulated failure. Table 2 maps the postulated communication failures in Staff Position 12 of DI&C-ISG-04 to the RXM Chassis FMEA using the numbering system from Table 1.

Note that not all postulated failures in Staff Position 12 are addressed in the RXM Chassis FMEA, because the FMEA is considering worst-case failures of the non-safety RXM Chassis – catastrophic failure of the entire chassis (i.e., loss) due to fire, flood, missile(s), or software common mode failure. All other single failures are mitigated through the triple-modular redundant design of the Tricon, as explained in NTX-SER-09-10. Additionally, the system-level testing (V&V) identified above demonstrates that the RXM Chassis and modules satisfy the system-level requirements, thus ensuring:

1) Any single failure of the non-safety RXM does not impair the safety function of the Tricon (i.e., protects against the DI&C-ISG-04 postulated failures); and
2) Catastrophic failures analyzed in the RXM Chassis FMEA do not prevent the safety function of the Tricon.

Table 1. DI&C-ISG-04 Staff Position 12 Postulated Communication Failures

No.	Postulated Fault	Analysis[1]
SP12.1	Messages may be corrupted due to errors in communications processors, errors introduced in buffer interfaces, errors introduced in the transmission media, or from interference or electrical noise.	FMEA
SP12.2	Messages may be repeated at an incorrect point in time, due to errors, faults, or interference.	Appendix 2, Section 6.0
SP12.3	Messages may arrive out of order, in that message store and forward may send later messages before successfully transmitting older messages.	N/A[2]
SP12.4	Messages may be lost, which includes both failures to receive an uncorrupted message or to acknowledge receipt of a message.	FMEA
SP12.5	Messages may be delayed beyond their permitted arrival time window, such as errors in the transmission medium.	FMEA
SP12.6	Messages may be inserted into the communication medium from unexpected or unknown sources.	N/A[3]
SP12.7	Messages may be sent to the wrong destination, which could treat the message as a valid message.	Appendix 2, Section 6.0
SP12.8	Messages may be longer than the receiving buffer, resulting in buffer overflow and memory corruption.	Appendix 2, Section 6.0
SP12.9	Messages may contain data that is outside the expected range.	Appendix 2, Section 6.0
SP12.10	Messages may appear valid, but data may be placed in incorrect locations within the message.	Appendix 2, Section 6.0
SP12.11	Messages may occur at a high rate that degrades or causes the system to fail.	Appendix 2, Section 6.0
SP12.12	Message headers or addresses may be corrupted.	FMEA

[1]For postulated failures identified with "Appendix 2, Section 6.0", see Invensys document Section 6.0 in Appendix 2 to NTX-SER-09-10 for technical description of the V10 Tricon response to the identified postulated failure.

[2] The I/O Bus protocol is single-threaded by design, which means one command message is sent from the IOCCOM and no other until a valid response is received or the thread times out. There is no credible fault that can cause messages to be received out of order. See Invensys document Section 6.0 in Appendix 2 to NTX-SER-09-10 for technical details.

[3] The I/O Bus is a closed system utilizing a single-threaded, master-slave serial protocol. In order to inject a message onto the I/O Bus, physical access is required to insert a RXM or I/O module into the system. Before a RXM Chassis or I/O module will go active, the hardware configuration must first be modified and downloaded to the Tricon controller(s) using TriStation 1131. See Invensys document Section 6.0 in Appendix 2 to NTX-SER-09-10 for technical details.

DI&C-ISG-04 Staff Position 12 Failure	Affected Components	Failure Mode	Failure Mechanisms	Effect on PLC Inputs and Outputs	Effect on PLC Operability
NON-SAFETY REMOTE RXM MODULE-RELATED FAILURES					
SP12.1 SP12.2 SP12.5	1) Model 4201-3; Non-Safety Remote Extender Module (RXM), Multimode Fiber Optics (set of 3 modules)	Loss of all three non-safety RXM modules	Fire; flood; missiles; Software common mode failure	Input signals in affected non-safety RXM chassis will not be read. Non-safety analog and digital outputs fail low.	Safety-Related Main and Primary RXM Chassis continue to operate, with loss of non-safety I/O function in the failed non-safety Remote RXM chassis as noted, and all downstream non-safety chassis assemblies. Safety-Related 3008N MP diagnostics will detect and flag non-safety Remote RXM communications fault.
SP12.1 SP12.2 SP12.5 SP12.6	2) Model 4201-3; Non-Safety Remote Extender Module (RXM), Multimode Fiber Optics (set of 3 modules)	Loss of one or two non-safety RXM modules	Electronics or software failure	None	Safety-Related Main and Primary RXM Chassis continue to operate via intact non-safety Remote RXM module(s). Safety-Related 3008N MP diagnostics will detect and flag non-safety Remote RXM module fault.
NON-SAFETY REMOTE RXM CHASSIS POWER SUPPLY-RELATED FAILURES					
No impact	1) Non-Safety RXM Chassis power supply: Model 8310 – 120Vac/Vdc Model 8311 – 24Vdc Model 8312 – 230Vac	Loss of one non-safety power supply output	Electronic component or fuse failure	None	Safety-Related Main and Primary RXM Chassis continue operation. Non-Safety Remote RXM Chassis continues to operate via the redundant non-safety Remote RXM Chassis power supply. Safety-Related 3008N MP diagnostics will detect and flag board fault on the non-safety Remote RXM Chassis power supply. Fault alarm via safety-related Main Chassis Power Module alarm circuit.
SP12.1 SP12.2 SP12.5	2) Non-Safety RXM Chassis power supply: Model 8310 – 120Vac/Vdc Model 8311 – 24Vdc Model 8312 – 230Vac	Non-Safety power supply outputs fail (both non-safety power supplies fail)	Electronic component or fuse failure	All outputs fail low on all modules in affected non-safety Remote RXM Chassis.	Safety-Related Main and Primary RXM Chassis continue operation. Safety-Related 3008N MP diagnostics will detect and flag board fault in the non-safety Remote RXM Chassis. Fault alarm via safety-related Main Chassis Power Module alarm circuit.
NON-SAFETY REMOTE RXM CHASSIS-RELATED FAILURES					
SP12.1 SP12.2 SP12.5	1) Non-Safety Remote RXM Chassis power supply rails	Both rails fail open or short to ground	Electrical power transient; fire; flood; missiles	Non-Safety input signals will not be read. Non-Safety analog and digital outputs fail low for shorted rails, and fail low at and past the failure points for open rails.	Safety-Related Main and Primary RXM Chassis continue to operate, with loss of non-safety I/O function in the failed non-safety Remote RXM Chassis as noted, and all downstream non-safety chassis assemblies. Safety-Related 3008N MP diagnostics will detect and flag power rail fault in the non-safety Remote RXM Chassis. Fault alarm via safety-related Main Chassis Power Module alarm circuit.
No impact	2) Non-Safety Remote RXM Chassis power supply rails	One rail fails open or shorts to ground	Electrical power transient and/or Motherboard insulation failure	None	Safety-Related Main and Primary RXM Chassis continue operation. Non-Safety Remote RXM Chassis continues operation via the redundant non-safety Remote RXM Chassis power supply. Safety-Related 3008N MP diagnostics will detect and flag power rail fault in the non-safety Remote RXM Chassis. Fault alarm via the safety-related Main Chassis Power Module alarm circuit.

SP12.1 SP12.2 SP12.5	3) Non-Safety Remote RXM Chassis I/O Bus	All buses open or short to ground	Electrical power transient; fire; flood; missiles	Non-Safety input signals will not be read. Non-Safety analog and digital outputs fail low for shorted rails, and fail low at and past the failure points for open rails.	Safety-Related Main and Primary RXM Chassis continue to operate, with loss of non-safety I/O function in the failed non-safety Remote RXM Chassis as noted, and all downstream non-safety chassis assemblies. Safety-Related 3008N MP diagnostics will detect and flag power rail fault in the non-safety Remote RXM Chassis. Fault alarm via safety-related Main Chassis Power Module alarm circuit.
SP12.1 SP12.2 SP12.5 SP12.6	4) Non-Safety Remote RXM Chassis I/O Bus	One or two buses open or short to ground	Electrical power transient and/or motherboard insulation failure	None	Safety-Related Main and Primary RXM Chassis continue to operate via intact I/O bus(es). Safety-Related 3008N MP diagnostics will detect and flag I/O bus fault.
PLC CABLE-RELATED FAILURES					
SP12.1 SP12.2 SP12.5	3) Model 4200-3 to Model 4201-3; Safety-Related Primary RXM to Non-Safety Remote RXM, Multi-mode Fiber Optics (set of 6 fiber optic cables)	Loss of all three RXM transmit or receive cables	Fire; flood; missiles	Input signals in affected non-safety Remote RXM Chassis will not be read. Analog and digital outputs fail low.	Safety-Related Main and Primary RXM Chassis continue to operate, with loss of I/O function in the failed non-safety Remote RXM Chassis as noted. Safety-Related 3008N MP diagnostics will detect and flag non-safety Remote RXM communications fault.
SP12.1 SP12.2 SP12.5 SP12.6	4) Model 4200-3 to Model 4201-3; Safety-Related Primary RXM to Non-Safety Remote RXM, Multi-mode Fiber Optics (set of 6 fiber optic cables)	Loss of one or two RXM transmit or receive cables	Fire or cable cut	None	Safety-Related Main and Primary RXM Chassis continue to operate via intact RXM fiber optic cable(s). Safety-Related 3008N MP diagnostics will detect and flag non-safety Remote RXM communications fault.

ATTACHMENT 4
INVENSYS RESPONSE TO RAI No. 4

RAI No. 4: Document Listing for FPGA Development

Invensys states in the field programmable gate array whitepaper that the current process is not consistent with a software lifecycle development process and that a process update is forthcoming. Please identify a list of all documents used or related to the development of programmable logic since the approval of V9.5.3 in December 2001.

RESPONSE:

Clarification of this request was established by the NRC audit team December 17, 2010.

It was requested that an explanation of how field programmable gate array (FPGA) source code is controlled. For all legacy programmable logic devices (PLDs) approved for use in Nuclear applications the PLD source code is controlled in our configuration control database (Agile). Going forward, per our new PLD development process EDM 40.60, PLD source code, build environment and release builds will be controlled in our source control database (IBM Rational Synergy). This is the same database used for source/build control for Firmware/Software developed at Invensys/Triconex.

In response to a draft RAI and verbal instructions, Invensys/Triconex provided a binder containing all of the released TriBus FPGA design documentation. During the NRC audit, it was established that the RAI is requesting a list of information contained in the binder with an addition to the list of any other pertinent information related to the development of the Tribus FPGA that is now part of the release.

In assembling the aforementioned TriBus FPGA design documentation binder it was self discovered by Invensys/Triconex that there was some design collateral missing from the 1998 AGILE release. This missing collateral has been located and has been added to the release. Additionally ARR 861 has been assigned:

> During preparation for the NRC audit it was discovered that not all documentation is released as stated in document NTX-SER-09-06 for complex PLD's. Document states that "Both pre- and post-routing test benches exist in the release".

Below is a list of the documentation provided for review and other related files included in the Agile configuration control database:

Filename	Size	File Type	Date	Description	a, b

In AGILE release not included in binder

a, b

Files added to AGILE release after discovery of missing testbench

a, b

ATTACHMENT 5
INVENSYS RESPONSE TO RAI No. 5

RAI No. 5: Response Time Compliance with EPRI TR 107330

In Appendix A, Section 4.2.1.A, of the Triconex Topical Report Revision 3, Invensys document 7286-545-1, Invensys states that the product complies with stated response time requirements, but lists two test results that exceed the 100 millisecond requirement. Invensys qualifies compliance by stating the test was performed under more difficult conditions (more logic elements) than required by Electric Power Research Institute Topical Report 107330. Please provide data that demonstrates compliance with the requirement.

RESPONSE:

The design of the V10 Tricon is such that Tricon response time varies with system configuration and application program size. For more information, please see IOM response to Staff Position 20 in IOM document NTX-SER-09-10, Revision 1, "Tricon Applications in Nuclear Reactor Protection Systems – Compliance with NRC Interim Guidance ISG-2 & ISG-4." As stated in the IOM response, actual scan time, throughput, and data error rates will be measured and recorded during the plant-specific Factory Acceptance Tests (FATs).

Because the number of factors involved, Tricon response time and throughput cannot be exactly predicted for any given configuration. Therefore, IOM considers this an application-specific issue that warrants NRC staff review.

With regard to Appendix A, Section 4.2.1.A, of the Triconex Topical Report Revision 3, Invensys document 7286-545-1, IOM will revise the COMPLIANCE column from "Comply" to "Exception" as follows (proposed new text in bold, deleted text per strikethrough):

SECTION	SUMMARY OF EPRI TR-107330 REQUIREMENTS[1]	COMPLIANCE[2]	COMMENTS[3]
4.2.1.A	Response Time. The overall response time from an analog or discrete input exceeding its trip condition to the resulting discrete outputs being set shall be 100 milliseconds or less. Response time shall include time required for input filtering, input module signal conversion, main processor input data acquisition, two scan times of an application program containing 2000 simple logic elements, main processor output data transmission, digital output module signal conversion, and performance of self-diagnostics and redundancy implementation.	~~Comply~~ **Exception**	Ref 7, Section 4.0 gives a summary of calculated maximum response time. However, the as tested Maximum response times were 83.0 milliseconds (for a DI to DO loop), 119.0 milliseconds (for an AI to DO loop), and **126.5** milliseconds (for an AI to AO loop). See Ref. 53, Section 6. ~~The test specimen application program included 3946 simple logic elements, and 175 simple and complex logic elements, almost twice that required by the TR. This effectively resulted in almost double the scan time associated with 2000 elements.~~

A revision to IOM document 7286-545-1 Appendix A V10 Tricon Compliance Matrix containing the above changed page is being provided with this submittal.

ATTACHMENT 6
INVENSYS RESPONSE TO RAI No. 6

RAI No. 6 – Determinism and Use of Interrupts:

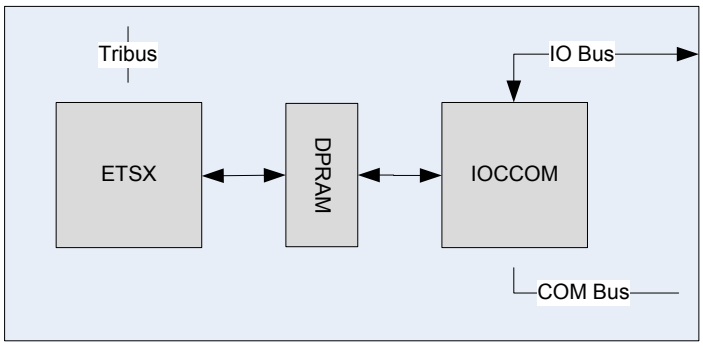
In Section 2.1.3.3 of the Triconex Topical Report Revision 3, Invensys document 7286-545-1, Invensys states that the TriStation 1131 function subset does not allow constructs that could lead to non-deterministic timing. However, there is no mention of the deterministic behavior of the Tricon design itself. Please provide a description of the deterministic behavior of the Tricon platform, including interrupt handling.

RESPONSE:

Additional information on the Tricon Main Processor architecture, scan protocol, and interrupt handling is provided below. Deterministic behavior is assured through the synchronizing of application scans, as described below, which guarantees that a new set of inputs and a new set of outputs for the I/O modules are established during every application scan.

Main Processor

The 3008N Main Processor module consists of three main subsystems as shown in the figure below:



Each subsystem consists of a microprocessor and memory subsystem. The ETSX (Enhanced Triconex System Executive) is responsible for running the user defined application program on the Application Processor. The IOCCOM Processor is responsible for communications with the I/O modules in the system and the Tricon communications modules (TCM). The DPRAM provides the interface between the ETSX and IOCCOM. The DPRAM is divided into several sections:

- Physical Inputs from Input Modules
- Physical Outputs for Output Modules
- Input message queue for I/O Modules
- Output message queue for I/O Modules
- Input message queue for communication modules
- Output message queue for communication modules
- Output Bins for communication modules

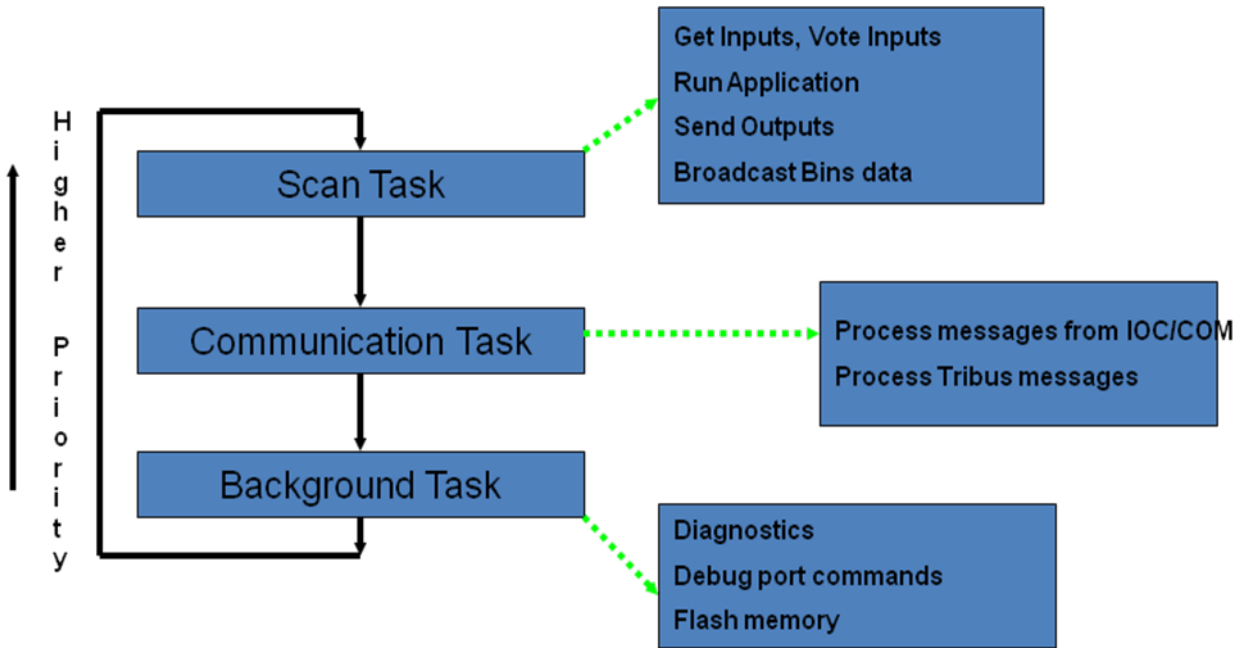
The structure of the DPRAM separates the queues for I/O modules and communication modules to provided isolation between the I/O modules and communication modules.

Determinism in the Main Processor

The three redundant 3008N main processor modules synchronize the application scan among the three Application Processors within 500 microseconds. The application scan start will not vary by more than 500 microseconds from scan to scan. The retrieving of inputs from the I/O modules in IOCCOM is synchronized with the application scan. This guarantees a new set of inputs for every application scan. Outputs for the I/O modules are guaranteed every application scan.

Enhanced Triconex System Executive

The ETSX is made up of three tasks:



A lower priority task cannot interrupt a higher priority task.

The above scan structure guarantees that the Tricon ETSX scan cycle is predictable and repeatable from scan to scan.

Scan Task

The scan task is entered periodically from the TriClock interrupt. This interrupt occurs at the scan rate of the application. The functions that are performed are:

- Reset Watchdog Timer
- Get clock calendar
- Get Inputs from IOCCOM Dual-Port RAM (DPRAM)
- TriBus transfer (Inputs, status, page of memory, outputs from last scan)
- Vote Inputs
- Execute Control Program (i.e., application program)
- Send Outputs (Copy outputs into DPRAM for later retrieval by the IOCCOM)
- Communication broadcast (fill data bins in DPRAM)
- End-Of-Scan sync

Once the functions are performed, the scan task exits and returns to the interrupted task (Communication task or background task). The Scan Task is the only task that resets the watchdog timer. If the scan task does not execute at least one every 512 milliseconds, the MP will be faulted and taken out of service.

Communication Task

The communications task is executed periodically off a timer interrupt every 10 milliseconds. This interrupt may be delayed by execution of the Scan Task. The functions the Communication Task performs are:

- Process communication messages from IOC/COM and Communication modules. These messages are received by the IOC/COM and put in the DPRAM
- Process Communication messages from TriBus

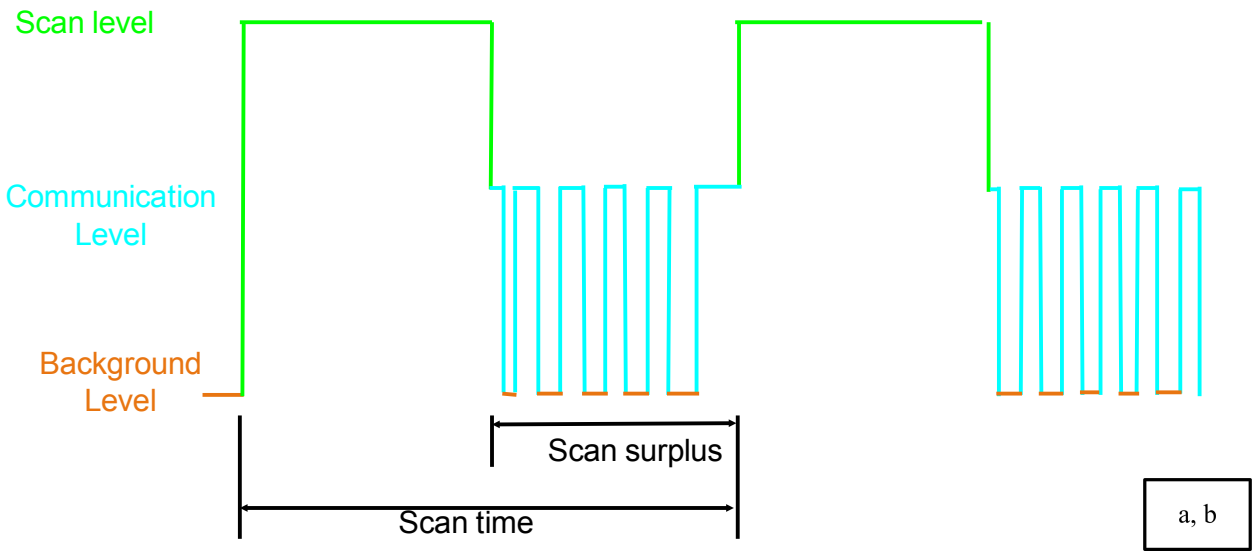
The minimum time that is reserved for this task by the Application Processor is five milliseconds.

Background Diagnostics

- Execute diagnostics
- Handle debug port commands
- Write information to flash memory during download

Task Scheduling

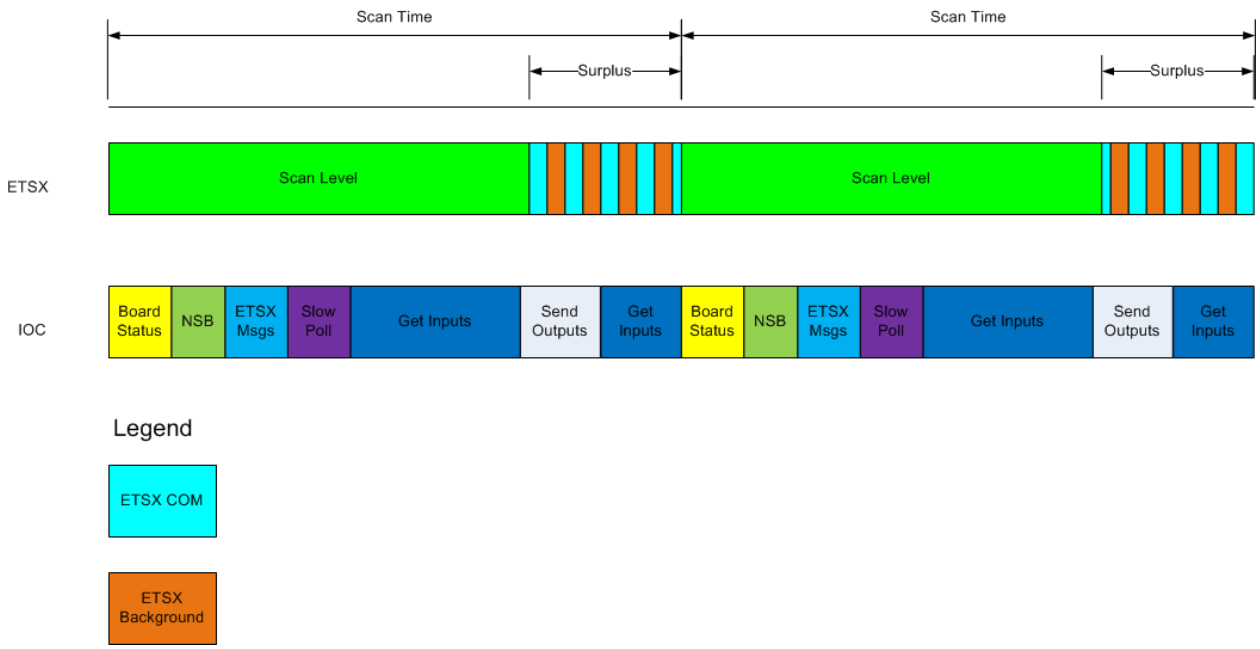
The following figure shows how the tasks would be scheduled for two application scans.



a, b

a, b

a, b


Scan Time
Scan Time
Surplus
Surplus
ETSX
Scan Level
Scan Level
IOC
Board Status
NSB
ETSX Msgs
Slow Poll
Get Inputs
Send Outputs
Get Inputs
Board Status
NSB
ETSX Msgs
Slow Poll
Get Inputs
Send Outputs
Get Inputs
Legend
ETSX COM
ETSX Background

a, b

a, b

Main Execution Loop

The main execution loop for Tricon I/O modules performs the following functions:

- Calculate Health
- Process I/O
- Diagnostics

Calculate Health

The calculate health function checks the health status of the module. It checks which of the three legs are healthy and determines the current voting mode.

Process I/O

The process I/O function performs the I/O-dependent processing for a module. For example, this function could read the analog to digital converter for an analog input module.

Diagnostics

The diagnostics function performs a slice of the diagnostics for the module. These diagnostics include module specific diagnostics and common diagnostics for 8031, RAM, etc.

a, b