invensys

NUCLEAR QUALIFIED PRODUCTS

TRICON APPLICATIONS IN NUCLEAR REACTOR PROTECTION SYSTEMS

COMPLIANCE WITH NRC INTERIM GUIDANCE ISG-2 & ISG-4

Document No.: NTX-SER-09-10

Revision: 0

Issue Date: August 31, 2009

TABLE OF CONTENTS

	TITLE	Page
1.0	**INTRODUCTION**	4
2.0	**DI&C-ISG-02 "DIVERSITY AND DEFENSE-IN-DEPTH ISSUES"**	8
	#1 Adequate Diversity	8
	#2 Manual Operator Actions	9
	#3 BTP 7-19 Position 4 Challenges	10
	#4 Effects of Common Cause Failures	10
	#5 Common Cause Failure Applicability	10
	#6 Echelons of Defense	10
	#7 Single Failure	10
3.0	**DI&C-ISG-04 "Highly-Integrated Control Rooms – Communications Issues"**	12
	#1 Interdivisional Communications	12
	Staff Position 1 Channel Independence	12
	Staff Position 2 Protection From Outside the Division	12
	Staff Position 3 Design Complexity	13
	Staff Position 4 Communication Processor Separation	13
	Staff Position 5 Cycle Time	13
	Staff Position 6 Function Processor Communication Protocol	14
	Staff Position 7 Message Format	14
	Staff Position 8 Division Data Exchange	14
	Staff Position 9 Message Memory Separation	15
	Staff Position 10 Program Change Restriction	15
	Staff Position 11 Safety Function Processor Independence	16
	Staff Position 12 Communication Fault	16
	Staff Position 13 Communication Fault Mitigation	18
	Staff Position 14 Point-to-Point Communications	19
	Staff Position 15 Data Communication Frequency	19
	Staff Position 16 Network Communication Functionality	19
	Staff Position 17 Communication Media Robustness	19
	Staff Position 18 Communication Hazards Analysis	20
	Staff Position 19 Data Communication Link Capacity	20
	Staff Position 20 Worst Case Response Time	20

TABLE OF CONTENTS

	TITLE		Page
#2	**Command Prioritization**		20
	Staff Position 1	Priority Module Requirements	20
	Staff Position 2	Diverse Actuation Independence	21
	Staff Position 3	Command Priority	21
	Staff Position 4	Multiple Component Control	21
	Staff Position 5	Priority Module Communication Isolation	21
	Staff Position 6	Developmental Software Quality	21
	Staff Position 7	Priority Module Software	22
	Staff Position 8	Proof-of-Design Testing	22
	Staff Position 9	Priority Module Automatic Testing	22
	Staff Position 10	Completion of Protective Action	22
#3	**Multidivisional Control and Display Stations**		22
	Staff Position 3.1.1	Non-safety Stations to Safety Division Communications	23
	Staff Position 3.1.2	Safety-Related Stations to Other Station Communications	23
	Staff Position 3.1.3	Non-safety Station Control of Safety-Related Equipment	23
	Staff Position 3.1.4	Safety-Related Stations Controlling Other Safety-Related Divisions	24
	Staff Position 3.1.5	Malfunctions and Spurious Actuations	25
	Staff Position 3.2	Human Factors Considerations	25
	Staff Position 3.3	Diversity and Defense-in-Depth Considerations	26
4.0	**REFERENCES**		28
	APPENDIX 1	Non-Safety to Safety Communication Recommendation	29

1.0 INTRODUCTION

The purpose of this attachment is to address the Invensys position in regard to NRC Interim Staff Guidance (ISG) ISG-02 (Reference 1) and ISG-04 (Reference 2) and other related regulatory standards and guidance.

The philosophy of Diversity and Defense-in-Depth (D3) analysis is a multi-layered approach to safe plant operation. 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, as defined in Nuclear Regulatory Commission (NRC) Branch Technical Position (BTP)-7-19 (Reference 3), with additional details and clarifications provided in ISG-02.

The Tricon is a mature, flexible, robust and fault tolerant controller and as such, is ideally suited for critical control and safety-related applications in the hydrocarbon process industries, transportation – rail and shipboard, power and now with the endorsement of the NRC by Safety Evaluation Report (SER), dated December 12, 2001 (Reference 4), nuclear power and processing plants subject to NRC licensing. The Invensys Tricon V10 Equipment Qualification (EQ) Report (Reference 5) demonstrates that the Tricon is sufficiently robust, and the quality of manufacturing hardware and operating software is acceptable for use in Nuclear Power Plant (NPP) safety-related systems.

Applicable systems include, but are not limited to:

Safety Systems	Systems Important to Safety
◆ Reactor Protection ◆ Reactor Trip Logic ◆ Safeguards Actuation ◆ Diesel Generator ◆ Heating Ventilation Air Conditioning ◆ Post-Accident Monitoring	◆ Saturation Margin Monitoring ◆ Reactor Vessel Level Indicating ◆ Inadequate Core Cooling ◆ Safety Parameter Display System ◆ Accident Mitigation System Actuation Circuit

This attachment describes how Invensys develops and applies Tricon systems in safety-related systems in nuclear industries in the USA in accordance with NRC regulations and guidelines. It is intended to be generic in the application of Tricons in safety-related applications. It does not include site specific acceptance, pre-operation, or surveillance testing requirements; nor site-specific life cycle hardware and software configuration management, nor quality assurance activities following installation. These topics are addressed in site specific submittals.

To create a site specific application, the licensee must identify differences between Tricon application guides and each unique application. It is expected that the licensee will add, delete,

modify or confirm requirements to support the system licensing basis. It is also expected that the licensee will oversee the development and approval of;

- the functional requirements for the application,
- design specific defense-in-depth and diversity approach (with license topical reports if Reactor Protection System (RPS) and/or Engineered Safety Features Actuation System (ESFAS),
- selection of Tricon power supplies, communication and I/O modules;
- the application software quality control;
- system assembly and Factory Acceptance Testing;
- installation and Site Acceptance Testing;
- and addressing NRC regulatory requirements and guidelines specific to the application.

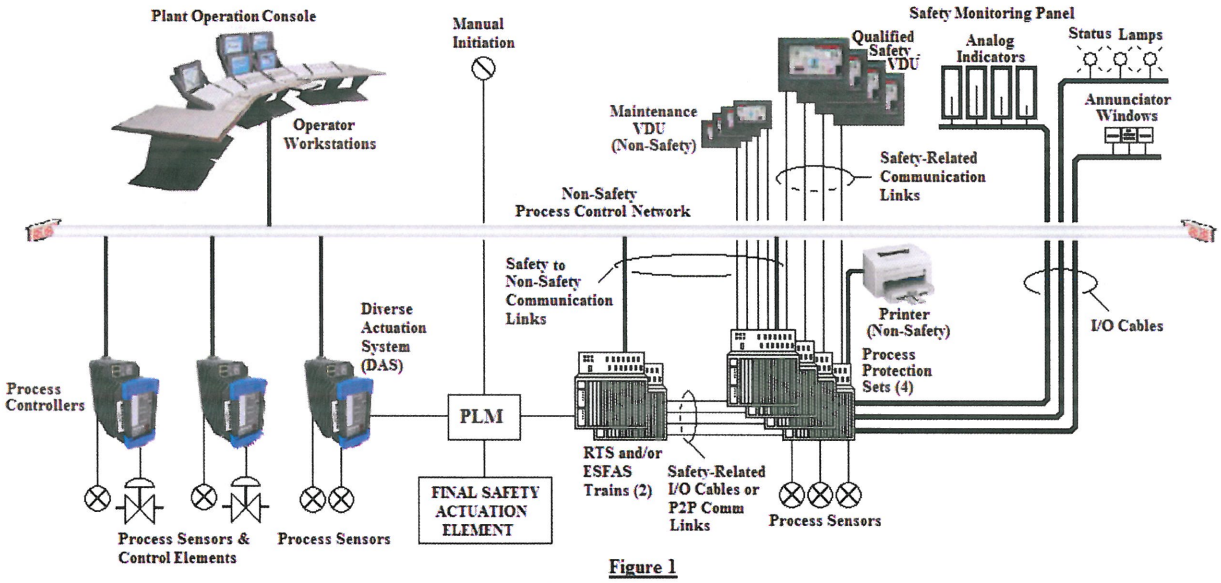

Figure 1

RPS - ESFAS Composite Architecture

While the Tricon platform is qualified for safety-related applications, how it is applied has a major bearing on plant safety. Figure 1 illustrates the flexibility and many of the features of Tricons configured for RPS and/or ESFAS applications. The figure is not proposed for any specific plant architecture, but is presented for discussion purposes of how Tricons may be applied in reactor protection applications in compliance with regulatory requirements and to industry standards.

As illustrated in Figure 1, a Distributed Control System (DCS) composed of Process Controllers and Operator Workstations, all communicating via a Process Control Network is installed in new

plants and may be retrofitted into legacy plants. One or more Plant Operation Consoles support control room operator tasks of monitoring primary and secondary plant process parameters (pressures, temperatures, levels, flows, positions, etc.) and the manipulation of various final control elements (valves, motors, circuit breakers, etc.) The Operator Workstations present information in several formats including text, bar graphs, status indicators, graphics and alarm windows. All components within the DCS are classified non-safety.

A small subset of plant process parameters are monitored and automatically manipulated by the RPS and ESFAS to halt the fission process and initiate cooling of the reactor during all anticipated accident scenarios. Typically four independent Process Protection Sets (PPS), each composed of Tricon components in separate cabinet(s), monitor critical plant process sensors. The Tricons convert the signals to engineering units; test against specified setpoints (bistable function); setting/clearing discrete memory variables depending on results of the test. Depending on the specific plant architecture, the discrete memory variables are passed to the other channel Tricons, or the Reactor Trip System (RTS), and the ESFAS via discrete I/O wiring, or high speed, redundant Peer-to-Peer (P2P) safety-related communication networks. The PPS and RTS (elements of the RPS) and ESFAS activate protective action upon receiving two or more signals from the four channels.

Maintaining the concept of Defense-in-Depth, the architecture also incorporates an automatic Diverse Actuation System (DAS) and supports manual initiation of protective actions. Since the DCS utilizes diverse digital technology and independent sensors to monitor the same critical parameters, one or more Process Controllers are dedicated to DAS functionality as shown in Figure 1. At their option, licensees may prefer other diverse technologies (PLCs, Field Programmable Gate Arrays (FPGA), etc.) which are of satisfactory quality to serve the DAS function. Arbitration of the safety initiation via the Tricon, DAS or operator manual action is accomplished via a Priority Logic Module (PLM).

Critical process parameters are displayed in the control room at optional individual analog indicators, status lamps and the setting of annunciator alarms. Each is controlled by Tricon output modules. In plants where the indicators, lamps and alarms are classified non-1E, those modules are mounted in remote chassis, which provide electrical isolation and separation .

The Tricon supports optional qualified Safety Visual Display Units (SVDU) or Safety Human-Machine Interfaces (SHMI). Each SVDU executes read/write messages with Tricons via safety communication links. The SVDUs are configured and programmed to display the critical process parameters in the control room and allow the operator to manipulate various plant safety equipment.

The Tricon also supports optional non-safety Maintenance Visual Display Units (MVDU), which allow maintenance technicians viewing plant variables and Tricon diagnostics during periodic functional surveillance testing. The MVDU supports maintenance technicians and engineering personnel setting/changing addressable constants, setpoints, system parameters and other programmable variables while the channel and protection loops are in bypass mode.

All Tricons support the broadcast of all critical parameters within memory, via optional non-safety communication links, to be displayed and logged at the Plant Operation Consoles and/or non-safety MVDUs.

2.0 DI&C-ISG-02 "DIVERSITY AND DEFENSE-IN-DEPTH ISSUES"

The following compares NRC ISG #2 position and Invensys compliance and comments in a point by point matrix.

NRC GUIDANCE – ISG-02	Deviation	INVENSYS COMPLIANCE & COMMENTS
ISG 02 - #1 ADEQUATE DIVERSITY	None	Diversity is one aspect of D3 relied to mitigate the consequences of extremely unlikely Common Cause Failure (CCF) in RPS/ESFAS applications. Because a CCF is not a design basis event, the alternate shutdown means need only be adequately robust consistent with 10 CFR 50.62. Depending on the specific plant RPS/ESFAS application, Tricon based system designs make extensive use of advanced technology (i.e., equipment and design practices). These designs are significantly and functionally different from current operating plant analog practice, including the use of Tricons, microprocessor based operator indicators and displays, fiber optics, multiplexing, and different isolation techniques to achieve sufficient independence and redundancy. Upon support and approval by the licensee, Invensys conducts D3 analysis of new and replacement RPS/ESFAS applications in conformance with NUREG/CR-6303 (Reference 6), IEEE Std. 279-1971(Reference 7) or IEEE Standard 603-1991 (Reference 8), Reg. Guide 1.152 Rev. 2 (Reference 9) and BTP 7-19 (Reference 3). When included in the design, the DAS, composed of diverse hardware and software, independently monitors plant process parameters and automatically initiates protective actions. Given that it independently monitors all plant process parameters, the DCS may serve as the DAS. It utilizes hardware and software technology that

		is diverse from the Tricon and therefore not considered susceptible to the same CCF. DAS designated components are configured and programmed to automatically initiate reactor shutdown and activate cooling equipment when accident conditions are sensed. The DCS also provides independent and diverse plant information displays in support of manual initiation. Another implementation may use a specifically designed DAS to actuate RPS/ESFAS equipment, provided it independently monitors plant process parameters, automatically initiates protective actions and is designed and manufactured in accordance with Generic Letter 85-06 "Quality Assurance Guidance for ATWS Equipment that is Not Safety-Related" (Reference 10).
ISG -02 - #2 MANUAL OPERATOR ACTIONS	None	Upon support and approval by the licensee, Invensys conducts a human factors engineering (HFE) analysis to confirm that operators are able to observe and maintain safe plant parameters, and take action within an acceptable time, determined by following the realistic analysis described in BTP-7-19. For actions with limited margin, such as less than 30 minutes between time available and time required for operators to perform the protective actions, a higher level of analysis will be performed. Within the RPS/ESFAS architecture, independent displays are always available to the operator in the control room. Safety-related parameters are viewed at the "Safety Parameter Display Console" or other dedicated panel. Display technology may be conventional analog indicators and status lamps, controlled by Tricon analog and discrete output modules. Displays may also be microprocessor based Safety VDUs, which are configured and programmed to "read" plant process information from each Tricon using safety-related communication media and protocols. As illustrated in Figure 1, manual operator action is supported in all Invensys-designed RPS/ESFAS architectures. The operator may 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 is independent of both systems.
ISG-02 - #3 BTP 7-19 POSITION 4 CHALLENGES AND #4 EFFECTS OF COMMON CAUSE FAILURES.	None	All replacement Invensys designed RPS/ESFAS architectures proposed for current operating reactors and all new reactors follow the guidelines of BTP 7-19. All support diverse automatic and manual initiation of safety functions at division level and at the individual component level.
ISG 02 - #5 COMMON CAUSE FAILURE (CCF) APPLICABILITY	None	All Invensys proposed RPS/ESFAS conceptual designs are composed of multiple Tricons, which have been analyzed for CCF and a loss of protection. It is recommended to all nuclear owner/operators who select the Tricon for a partial or full RPS/ESFAS application, to perform a full BTP-7-19 analysis to defend both the diversity and defense-in-depth justification for the platform configuration chosen.
ISG -02 - #6 ECHELONS OF DEFENSE	None	Invensys offers several conceptual RPS and ESFAS designs; all using the flexible Tricon in four protective channels, two RTS trains, and/or two ESFAS trains. Some architectures combine RTS and ESFAS functions into redundant trains. All configurations meet the analysis requirements of BTP-7-19, NUREG/CR-6303 and ISG-02.
ISG -02 - #7 SINGLE FAILURE	None	The Tricon design achieves the requirements stated in General Design Criteria (GDC) 21 – single-fault tolerance and on-line repair. Fault tolerance is achieved by means of its Triple-Modular Redundant (TMR) architecture, from input modules through the main processors to the output modules. It provides error-free, uninterrupted control in the presence of either hard failures of components, or transient faults from internal or

		external sources. Extensive diagnostics continually evaluate system performance and when component fault/failure is discovered, system alarms are activated, capturing the attention of operators and technicians. A more detailed description of the system is provided in the Tricon Technical Product Guide (Reference 11), and the Tricon Planning and Installation Guide (Reference 12). Since the first safety system installation in the mid 1980s, the Tricons have provided safe and reliable operation in numerous safety critical applications. With more than 9,000 units currently in service, accumulating more than 500,000,000 operating hours, no Tricon has ever failed to operate on demand, either an actual demand or simulated during surveillance testing. However, Invensys understands there remains the very rare possibility of a software 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, as stated in ISG 02, #7. 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.

3.0 DI&C-ISG-04 "HIGHLY-INTEGRATED CONTROL ROOMS – COMMUNICATIONS ISSUES"

The following compares NRC ISG-04 position and Invensys compliance and comments in a point by point matrix.

NRC GUIDANCE – ISG-04	Deviation	INVENSYS COMPLIANCE & COMMENTS
ISG-04 – #1 INTERDIVISIONAL COMMUNICATIONS		
STAFF POSITION 1 Channel Independence	None	Invensys RPS architectures are composed of four channels. Each channel monitors dedicated sensors allowing bistable logic within the Tricon to operate completely independent of other channels.
STAFF POSITION 2 Protection From Outside the Division	None	Depending on the licensee preferred architecture, bistable outputs are either communicated to other divisions, RTS and/or ESFAS via digital outputs wired to digital inputs; or via redundant Peer-to-Peer (P2P) communication networks to support voting of bistable outputs, 2-o-o-4, 2-o-o-3 or 1-o-o-2 taken twice. Failures or excessive delays in the redundant interdivisional communication results in 1-o-o-1 channel voting logic. Voting results control reactor shutdown, isolation and heat removal equipment. Depending on the specific plant architecture, each channel Tricon receives read-only communication request through three digital communication interfaces, Plant Process Computer, and/or Plant Control Network (DCS) and/or SVDUs and/or Maintenance VDU (MVDU). The position of the Tricon keyswitch (physical interlock) prevents the communication module from accepting "write" messages when placed in the RUN position. The position of the keyswitch is continuously monitored by the Tricon, which activates an annunciator window in the

		control room when not in the RUN position. Additionally, all critical data values, such as trip setpoints, are declared as constants, which may only be changed by compiling and downloading a modified program.
STAFF POSITION 3 Design Complexity	None	The typical Invensys protection system architecture design does not include digital communications between safety channel Tricons. Bistable results are communicated via hardwired DO to Digital Input (DI) connections.
STAFF POSITION 4 Communication Processor Separation	None	As described in the EQ Summary Report, all Tricon communication is conducted and supervised by one or more separate communication processors. As described, communication modules operate asynchronously, sharing information only at end of the main processor scan. When the host device requests data, the communication processor forwards the data from the main processor received at the previous end of scan. When a host device writes data, the communication processor passes the data to the main processor at next end of scan exchange.
STAFF POSITION 5 Cycle Time	None	Since all data is exchanged at each end of scan, there is no additional scan time required to satisfy a host device read or write communication function. Since it requires additional validation at both ends, P2P communications place a burden on the main processor and therefore extend the scan time. The Tricon is limited however to a maximum number of P2P "reads" and P2P "writes" within a given scan, which limits the main processor burden. Should P2P communications be included in an application program, thorough program operational testing will be conducted to determine the longest scan time duration. The Tricon continuously monitors system health and performance,

		activating an alarm should scan time exceed the predicted performance.
STAFF POSITION 6 Function Processor Communication Protocol	None	The main processor is isolated from data communications. One or more communication processors handle all communication protocol requirements, i.e. handshaking, start, stop bits, etc.
STAFF POSITION 7 Message Format	None	All host communications are limited to Tricon approved protocols. Each protocol is well defined and ordered, e.g. number of start and stop bits, timing, data frame format, number of data fields and check sum or Cyclic Redundancy Check (CRC) field. Should an error occur, the communication processor rejects the message. Message length may vary however, a host device may request different number of data points within each request. P2P messages exchanged with other Tricons have additional validation checks. P2P messages must be predefined and fixed within the program as to which Tricon is requesting the information, which Tricon is sending data, the type of data, the number of fields, and a more extensive CRC field. Each main processor responds and replies only when all data is correct.
STAFF POSITION 8 Division Data Exchange	None	As discussed above, data communications with non-safety systems are supervised by the Tricon communication processor. The non-safety system may request any data points and the communication processor will reply if the request is valid and error free. Data “writes” from the non-safety system to the Tricon are only accepted if; the data is valid and error free; the main chassis keyswitch is in correct position; and the specific memory tag name attribute is configured as ‘writeable’. Communications between safety divisions is via proprietary P2P networks. P2P messages are limited in length and number so as not to

		overburden either transmitting or receiving Tricon. Predetermined matching message blocks must be programmed in both the sending and receiving Tricons. Each message contains sending and receiving identification, fixed number of data fields, fixed data type, and extending error check coding. See Appendix 1 on Invensys guidance on non-safety to safety system communications.
STAFF POSITION 9 Message Memory Separation	None	Tricon received data is stored in fixed aliased memory locations, which are utilized by the main processor when computing application logic. Input data is segregated from output data within memory. All communication messages, via host or P2P, are conducted by, and stored in separate communication processors. Data is exchanged with the main processors at the end of each application program scan.
STAFF POSITION 10 Program Change Restriction	None	The Tricon design supports on-line changes to the application program, but only within rigid restrictions. To modify the program, the programmer must have access to the current program version loaded on the programming terminal, TS1131. To access the program, the programmer must enter the correct password. Once the program is modified and compiled, the TS1131 terminal must be physically connected to the Tricon and the keyswitch rotated to the "PROGRAM" position. Using the programming terminal, the programmer opens communications with the Tricon and downloads the program. Once downloaded the Tricon automatically changes the program version number. An alarm is activated when the version number changes and the version number is visible on several control room VDUs, if so equipped. Several administrative and programming techniques prevent

		unauthorized on-line program alterations. The programmer must obtain cabinet and chassis keys to physically gain access to the Tricon. Licensees may wish to set control room annunciator windows when the cabinet door and/or chassis key position is rotated out of the normal position. The programmer must gain access to the current program and password before the program may be altered, compiled and downloaded. It is anticipated that administrative procedures will restrict on-line program changes by "halting" the program, or taking the channel off-line before physically connecting the programming terminal to the safety channel and rotating the Main Chassis Keyswitch to the "Program" position. Some licensees may wish to enforce this requirement by programming the Tricon to initiate program halt when the keyswitch is rotated to the "Program" position.
STAFF POSITION 11 Safety Function Processor Independence	None	Tricon P2P messages support data exchange only. There are no "flow of control" message functions in the P2P protocol.
STAFF POSITION 12 Communication Fault	None	The design and operation of the Tricon prevents any communication fault altering the application program or its performance. All data "writes" must be in proper format, have the proper address and be within a given alias range. All P2P communications are further enhanced to mitigate communication faults, including, but not limited to, the following: Fault : 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. Mitigation : Mitigated

			through application-generated 32-bit CRC; requests for resend of the message; without unacceptable delay, and dealing with some maximum number of errors.
		Fault : Mitigation	Messages may be repeated at an incorrect point in time, due to errors, faults, or interference. Mitigated through tracking message identification numbers and deleting such unintended repeats, and use of multiple transmissions to increase the probability that message corruption would be detected.
		Fault : Mitigation	Messages may arrive out of order, in that message store and forward may send later messages before successfully transmitting older messages. Mitigated through software design.
		Fault : Mitigation	Messages may be lost, which includes both failures to receive an uncorrupted message or to acknowledge receipt of a message. Mitigated through unique message identification, ability to request missing data.
		Fault : Mitigation	Messages may be delayed beyond their permitted arrival time window, such as errors in the transmission medium. Mitigated through repetition and use of the lost message mechanisms.
		Fault : Mitigation	Messages may be inserted into the communication medium from unexpected or unknown sources. Mitigated through providing and checking of source and destination identifiers in all messages, discarding messages that are not intended for the receiver.
		Fault : Mitigation	Messages may be sent to the wrong destination, which could treat the message as a valid message. Mitigated through unique message identification, ability to

		request missing data.
		Fault : Mitigation — Messages may be longer than the receiving buffer, resulting in buffer overflow and memory corruption. Mitigated through application-generated 32-bit CRC; requests for resend of the message.
		Fault : Mitigation — Messages may contain data that is outside the expected range. Mitigated through application checks of data before use.
		Fault : Mitigation — Messages may appear valid, but data may be placed in incorrect locations within the message. Mitigated by fixing message format, with all data sent in each message, and sent on a periodic interval.
		Fault : Mitigation — Messages may occur at a high rate that degrades or causes the system to fail. Tricon application program configuration places an upper limit on send and receive messages in one scan.
		Fault : Mitigation — Message headers or addresses may be corrupted. Mitigated through application-generated 32-bit CRC; requests for resend of the message.
STAFF POSITION 13 Communication Fault Mitigation	None	Tricon P2P communication protocol supports applications where channel Tricons pass process trip values and status to the RTS and ESFAS Tricons for voting and safety equipment actuation. Both the transmitting and receiving Tricon validate all messages, employing message sequence numbers, connection authentication, and data integrity assurance algorithms to compensate for potential message corruption, unintended repetition, incorrect sequences, loss of message, unacceptable delay, unexpected message, and addressing errors. (See reply to Staff Position 12) Each channel Tricon is programmed to periodically send time stamped

		test messages to RTS Tricons, which return a feedback message. Should the transmitted or feedback message be lost, corrupted, miss-addressed, or significantly delayed, an alarm is activated. Additionally, the RTS Tricons are programmed to set/clear associated voter inputs upon loss of communications from channel Tricons. All communication functionality is extensively tested in accordance with Invensys SMP and SQAP..
STAFF POSITION 14 Point-to-Point Communications	None	The Tricon supports point-to-point and routed network communication protocol and media, copper and fiber optics. Both support redundant communication links.
STAFF POSITION 15 Data Communication Frequency	None	In those protective system designs that utilize P2P communications to pass channel process trip values and status to the RTS and ESFAS Tricons for voting and safety equipment actuation, each channel Tricon is programmed to pass all values each scan, whether the values have changed or not.
STAFF POSITION 16 Network Communication Functionality	None	In those protective system designs that utilize P2P communications, there are validation bits and timing within the message, so the receiving Tricon is “aware” that the messages are current and not static. If the messages are detected to be static, lost, or significantly delayed, the receiving Tricon activates an alarm, and assumes the “fail-safe” status of the transmitting Tricon.
STAFF POSITION 17 Communication Media Robustness	None	In those protective system designs that utilize P2P communications, only copper and fiber optic cables precisely designed for the anticipated conditions specified in EPRI TR-107330 (Reference 13) and Reg. Guide 1.180 Rev. 1 (Reference 14) are utilized in protective system

		applications.
STAFF POSITION 18 Communication Hazards Analysis	None	In those protective system designs that utilize P2P communications, only data communications required for accomplishing the safety requirements are included in the protective system architecture and functionality.
STAFF POSITION 19 Data Communication Link Capacity	None	In those protective system designs that utilize P2P communications, the data rate capacity of the communication processors and cabling far exceed the main processor ability to initiate and receive data. Tricons validate all data exchange between safety divisions for correctness and timeliness, setting of alarms, and assuming fail-safe state upon failure.
STAFF POSITION 20 Worst Case Response Time	None	In those protective system designs that utilize P2P communications in interdivision and across safety divisions, safety system response time is continuously evaluated against calculated response time.
ISG-04 – #2 COMMAND PRIORITIZATION	None	As illustrated in Figure 1, all Invensys-designed reactor protection systems include a DAS, as well as manual actuation in the architectural design and operational functionality, based on the results of the plant specific BTP-7-19 plant specific analysis. The architecture includes the placement of a safety-related PLM connected between all actuation logic and final safety element (circuit breaker, motor, valve, etc.)
STAFF POSITION 1 Priority Module Requirements	None	Invensys installs safety qualified physical devices in accordance with all requirements of 10CFR50 Appendix A and B. Technology may be qualified discrete devices (i.e. relays, switches, solid state) or qualified

		FPGA based devices.
STAFF POSITION 2 Diverse Actuation Independence	None	The PLM is completely independent of Tricons, DAS logic and manual initiation. No failure within the Tricon, DAS, or manual equipment will prevent the PLM from correctly arbitrating the protective action.
STAFF POSITION 3 Command Priority	None	The PLM design allocates priority to the Tricon, DAS and to the operator controlled manual devices, based on the results of the plant-specific BTP-7-19 analysis. Generally, the PLM allows any one of the three inputs to initiate protective action. For example, a RTS Tricon, or the DAS or manual input has unhindered ability to trip the Reactor Trip Breakers or initiate ESFAS equipment. Resetting the protective action may only be accomplished manually or in some situations by the DCS, but only if the cause of the Tricon initiation has cleared. Other PLM applications enforce a hierarchy of safety initiators, with manual having highest priority and the DAS the lowest.
STAFF POSITION 4 Multiple Component Control	None	Invensys-designed PLMs control only one safety-related component.
STAFF POSITION 5 Priority Module Communication Isolation	None	Invensys-designed PLMs do not support digital communications.
STAFF POSITION 6 Developmental Software Quality	None	Invensys programming terminals used in the configuration and programming of the PLM comply with the guidance of Reg. Guide 1.152, Rev. 2.

		The Invensys PLM is 100% tested to verify correct operation. Every possible combination of inputs and every possible sequence of device states in all anticipated environmental extremes are included in validation testing to eliminate CCF concern. The programming terminal is not involved in the testing.
STAFF POSITION 7 Priority Module Software	None	Logic within the PLM is contained in FPGA. Logic cannot be altered while the FPGA is installed in the module. Logic within the FPGA is considered to be software, therefore it is developed, maintained, and controlled in accordance with 10CFR50 Appendix B.
STAFF POSITION 8 Proof-of-Design Testing	None	Every possible combination of inputs and every possible sequence of states in all anticipated environmental extremes, are included in PLM validation testing to eliminate CCF concern.
STAFF POSITION 9 Priority Module Automatic Testing	None	Hardware and/or software supporting automatic testing is not included in the PLM design. Periodic surveillance testing is supported.
STAFF POSITION 10 Completion of Protective Action	None	Protective action inputs to the PLM have the capability to initiate safety actuation, but not to halt the actuation. Once initiated, the protective action will continue to completion, unless reset by manual operation external of the PLM circuitry.
ISG-04 – 3 MULTIDIVISIONAL CONTROL AND DISPLAY STATIONS	None	A fully integrated Invensys nuclear plant non-safety DCS and safety system supports multiple operator workstations. The specific plant requirements determine the number, type and locations. Invensys safety system architectures fully comply with current NRC regulations, based

		on the NRC SER (Reference 4). The DCS is used to support the operator task of monitoring, recording and logging process variables and manipulating process equipment within the plant. The DCS provides significant automation features, which allow the operator focus on abnormal situations, rather than normal operations. Typically all safety-related parameters within the Tricons are read by the DCS and are monitored and logged by the DCS.
ISG#4 – 3 STAFF POSITION		
STAFF POSITION 3.1.1 **<u>Non-safety stations receiving information from one or more safety divisions:</u>**	None	Typically all process data within each Tricon safety division is read by the non-safety DCS and/or plant computer, and/or maintenance VDUs, which complies with interdivisional communications guidelines. With the Main Chassis keyswitch in the RUN position, non-safety devices are granted "read only" access to Tricon data. The communication processor rejects all "write" messages from non-safety devices. Non-safety communications are segregated by communication processors and media. No electrical fault, software error in the non-safety VDU, or printer will effect the operation of the Main Processors.
STAFF POSITION 3.1.2 **<u>Safety-related stations receiving information from other divisions (safety or nonsafety):</u>**	None	All P2P, safety-related and non-safety VDU communications comply with interdivisional communications guidelines. It is anticipated that licensees may need to view and maintain data variables within Tricon based reactor protection systems. Appendix 1, "Non-Safety to Safety Communication Recommendation," provides Invensys guidance on the use of non-safety MVDU and DCS digital communication with Tricons.
STAFF POSITION 3.1.3	None	The PLM supports actuation of safety-related plant equipment via safety channel Tricons, non-safety workstations (DAS, DCS or dedicated

Non-safety stations controlling the operation of safety-related equipment:		VDU) and manual control devices. The Invensys protective system architecture precludes the non-safety workstation from preventing the Tricons initiating safety equipment actuation. No error or malfunction within the non-safety equipment will interrupt Tricon initiated protective action. The PLM design accepts safety initiation from any of the three inputs – Tricon, DCS and manual. The Tricon does not have the capacity to self reset the protective action. The operator must participate in the reset action and then only if the Tricon logic is restored.
STAFF POSITION 3.1.4 **Safety-related stations controlling the operation of equipment in other safety-related divisions:**	None	The PLM supports actuation of safety-related plant equipment via safety channel Tricons, safety workstations and manual control devices. The Invensys protective system architecture precludes the safety workstation from preventing the Tricons initiating safety equipment actuation. No error or malfunction within the safety workstation will interrupt Tricon initiated protective action. The PLM design accepts safety initiation from any of the three inputs – Tricon, DAS and manual. The safety-related workstation does not have the capacity to suppress any safety function. Once initiated by the Tricon, the safety actuation may not be reset until completion of the function and operation restored to a safe operating envelope. The Tricon does not have the capacity to self reset the protective action. The operator must participate in the reset action and then only if the Tricon logic is restored.

STAFF POSITION 3.1.5 **<u>Malfunctions and Spurious Actuations:</u>**	None	Malfunctions of the DCS, workstations, protective system processors, are evaluated against the assumptions of the plant safety analysis. Failure of the safety and non-safety control and display stations has no effect on the control processors. Failure of a single control processor in the DCS has no effect on control or safety-related functions. A CCF of software in the DCS or Tricons may cause a loss of protection in that system, or a spurious activation of some or all safety equipment. Operator initiated commands to the DCS and safety-related consoles, is a two step process to minimize spurious actuations. The operator selects the component to be manipulated, sets the command state, and confirms the desired action. DCS control and Tricon processors block erroneous communication commands from the non-safety and safety workstations. Safety-related control and display workstations are qualified to operate in adverse environments as specified in EPRI TR-107330. Safety-related workstations are qualified to operate in adverse electrical environments as specified in EPRI TR-107330. The Invensys DCS supports the “operator workstation disable” function. Failure of one or more operator workstations, safety or non-safety, has no affect on Tricon operation.
STAFF POSITION 3.2 **Human Factors Considerations**	None	Depending on the control and safety system architecture implemented, safety VDUs may or may not be required. Non-safety VDUs may be acceptable, provided Invensys-recommended restrictions are enforced.

		Upon support and approval by the licensee, Invensys shall commission a HFE analysis to establish the number and type of VDUs in the control room. The analysis will be in accordance with accepted human factors principles such as those in Rev.2 of NUREG 0711. HFE findings will be resolved in an appropriate manner. Safety-related Tricons typically have safety-related controls and indications and/or displays. Depending upon licensee needs, controls and displays may be individual analog indicators, switches, lamps and annunciators, or VDUs displaying the same in graphical format. Regardless of licensee requirements, safety-related devices with safety-related software will be dedicated to specific safety divisons. The Tricon supports the use of non-safety displays of safety-applications. Non-safety VDUs are optional, however. They are never considered essential for safe plant operations. Additional safety-related VDUs, switches, indicators are provided to support operator initiated safety action. Typically, all required safety parameters are monitored via safety-related VDUs and/or indicators. Operator initiated safety actions may be via panel switches and/or the safety-related VDUs. Non-safety VDUs may also be used to monitor, record and log safety-related variables. The typical Invensys architecture does not support the use of non-safety VDUs to initiate safety actions. Upon support and approval by the licensee, Invensys shall commission a HFE analysis of the specific application.
STAFF POSITION 3.3	None	The number, type, location and screen formats are included in the D3

Diversity and Defense-in-Depth (D3) Considerations		analysis to minimize the potential operator error.

4.0 REFERENCES

1) United States Nuclear Regulatory Commission (USNRC) Digital Instrumentation and Controls Task Working Group #2, "Diversity and Defense-in-Depth Issues Interim Staff Guidance," Rev. 2.

2) United States Nuclear Regulatory Commission (USNRC) Digital Instrumentation and Controls Task Working Group #4, Rev. 0 "Highly-Integrated Control Rooms—Communications Issues (HICRc)"

3) NUREG-0800 BTP-19 "GUIDANCE FOR EVALUATION OF DIVERSITY AND DEFENSE-IN-DEPTH IN DIGITAL COMPUTER-BASED INSTRUMENTATION AND CONTROL SYSTEMS

4) EPRI TR-1003114, Letter from Stuart A. Richards (NRC) to Troy Martel (Triconex Corporation), "Review of Triconex Corporation Topical Reports 7286-545, "Qualification Summary Report" and 7286-546, "Amendment 1 to Qualification Summary Report,"Revision 1" (December, 2001).

5) TRICON V10 EQUIPMENT QUALIFICATION SUMMARY REPORT, Rev. 2 (October 2008)

6) NUREG/CR-6303, "Method for Performing Diversity and Defense-in-Depth Analyses of Reactor Protection Systems."IEEE Std. 279-1971

7) IEEE Std. 603-1991 "IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations"

8) REGULATORY GUIDE 1.152, Rev. 2 "CRITERIA FOR USE OF COMPUTERS IN SAFETY SYSTEMS OF NUCLEAR POWER PLANTS"

9) QUALITY ASSURANCE GUIDANCE FOR ATWS EQUIPMENT THAT IS NOT SAFETY-RELATED (Generic Letter 85-06)

10) Technical Product Guide for Tricon v10 Systems, September 2008

11) Planning and Installation Guide for Tricon v9–v10 Systems, February 2009

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

13) Reg. Guide 1.180 Rev. 1, GUIDELINES FOR EVALUATING ELECTROMAGNETIC AND RADIO-FREQUENCY INTERFERENCE IN SAFETY-RELATED INSTRUMENTATION AND CONTROL SYSTEMS

APPENDIX 1

Non-Safety to Safety Communication Recommendation

1.0 INTRODUCTION

It is anticipated that Nuclear Power Plant (NPP) licensees may need to view and maintain data variables within Tricon based Reactor Protection Systems (RPS) and Engineered Safety Features Actuation Systems (ESFAS) applications. NRC Interim Staff Guidance (ISG) #4 – Staff Position 1 accepts bidirectional communications between safety divisions and between safety and non-safety equipment provided certain restrictions are enforced. The restrictions ensure no adverse impact on RPS and ESFAS functionality. This document provides Invensys guidance on the use of non-safety Maintenance Visual Display Units (MVDU) and Digital Control System (DCS) digital communication with Tricons in reactor protection system applications.

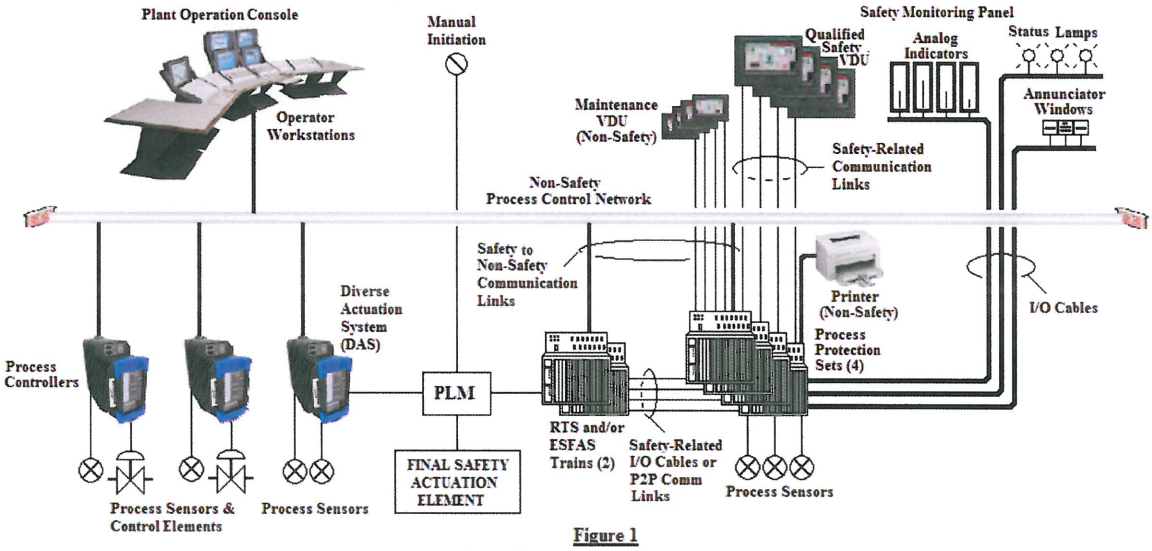

Figure 1
RPS - ESFAS Composite Architecture

2.0 RPS/ESFAS APPLICATION OVERVIEW

As shown in Figure 1, traditional Invensys safety system architectures are composed of four Process Protection Sets (PPS), channels or divisions. Each is self sufficient and its functionality is not dependent upon any information originating or resource residing outside its own safety division. Each channel monitors dedicated sensors allowing bistable logic within the Tricon to operate completely independent of other channels. Depending on the specific plant architecture, channel bistable output status is communicated to two Reactor Trip System (RTS) and ESFAS trains via Digital Outputs (DO) wired to Digital Inputs (DI); or via Peer-to-Peer (P2P) communication links. Some plant architectures combine RTS and ESFAS functionality into two Tricon trains. Other licensees prefer to distribute RTS functionality into the four channels.

3.0 TRICON COMMUNICATION FEATURES

Tricons support safe and reliable data communication links, connecting non-safety VDUs and Tricons, provided the user incorporates recommended physical interlocks and configuration guidelines. Each Tricon receives "read" communication requests through digital communication interfaces, which are separate from the Main Processors (MP). All host communications are limited to Tricon approved protocols. Each protocol is well defined and ordered, e.g. number of start and stop bits, timing, data frame format, number of data fields and check sum or CRC field. The Tricon Communication Processor (TCM) handles all protocol, start/stop bits, handshaking, etc. tasks. The MP is not burdened nor interrupted. Communication errors and malfunctions do not interfere with the execution of the safety function. Exchange of data between the communication processors and MPs occur once each MP scan cycle. Each channel may also receive "write" messages from division dedicated safety and non-safety VDUs.

Data communications with non-safety systems are supervised by the TCM. The non-safety system may request any data point and the TCM will reply if the request is valid and error free. Data writes from the non-safety system to the Tricon will only be accepted if valid, error free, keyswitches are in correct position and the memory tag name attribute is configured as 'writeable'.

The position of the Tricon Main Chassis keyswitch (physical interlock) prevents the communication module from accepting "write" messages. The position of the keyswitch is continuously monitored by the Tricon, which may enable an alarm when out of position. Additionally, all critical data values, e.g. trip setpoints, are declared as constants, which may only be changed by compiling and downloading a modified program. Invensys recommends that the Tricon Main Chassis keyswitch remain in the RUN position at all times, excepting the need to change program coding.

4.0 NON-SAFETY VDU COMMUNICATION TO TRICON EXAMPLE

As shown in Figure 1, Maintenance VDUs (MVDU) and TriStation 1131 (TS1131) may be safely utilized within the reactor protection system architecture. Although classified as non-safety devices, TS1131 and the MVDU may be used by maintenance and engineering personnel to view and change algorithmic constants utilized in RPS/ESFAS applications. It is anticipated that MVDUs will be mounted near the Tricon, out of view of the control room operator. TS1131 is an application on a laptop computer. Both the MVDU and TS1131 are connected point-to-point to the TCM and not networked.

For those licensees wishing to modify a limited set of variables via a non-safety or safety-related VDU, the Tricon supports a limited access function to enable the VDU to write to those internal tags with the "write" attribute set, even when the Main Chassis key remains in the RUN position. It is anticipated that the licensee will specify that the MVDU display all "read-only" and "writable" tags on one or more screens.

Should a technician wish to change the tag name data, it is anticipated that under administrative procedures, they will be required to inform and gain permission from the control room operator

prior to entering the change. Plant administrative controls require the control room operator issue a unique key which fits a panel board or console keyswitch.

The keyswitch is wired to a Tricon digital input (DI). The Tricon continually monitors the status of the DI and upon detecting that point "ON", it illuminates a status lamp and/or an annunciator window in the control room, informing the operator that a change is in progress and that the channel is in bypass mode. Upon the switch being placed in the "Open Access" position, the Tricon activates the pre-programmed "GATENB" and "GATDIS" functions to open a data window of limited range and duration.

The technician, utilizing the MVDU touch screen or keyboard, enters the pre-approved data and strikes the "Enter" button, whereupon the MVDU writes the data to the Tricon, immediately reading it back and displaying the data as "staged". Once the technician concurs that the "staged" data is the same as the approved data entry sheet, they press the touch screen or keyboard to confirm entry. The Tricon program will then move the 'staged" data to the tag name variable, which is used in program logic.

Upon returning the panel/console keyswitch to "Access Closed" position, disabling the gated access function, the Tricon initiates print commands to a dedicated printer which prints all programmed variables. The technician then confers with the control room operator to show that all approved changes were accomplished, and that the data access window is closed.

Should the operator fail to return the switch to "Access Closed" position within a pre-set time, the Tricon automatically closes the data access window and prints all programmed pre-formatted variables. The annunciator window and status lamps will not extinguish until the keyswitch is returned to normal, however.

5.0 SECURITY SUMMARY

Changing a limited set of variables within a protection system application may be safely accomplished through a combination of administrative controls, technician training and observation, physical interlocks and controls, and Tricon security features.

(1) Administrative control includes the development of authorized data change list and the approval by the control room operator to make the change.

(2) Depending on licensee policy, control room operator approval may include issuing a cabinet and/or panel switch key.

(3) Upon insertion of the key and rotation to "Open Access", an alarm and/or status lamp is illuminated in the control room, alerting the operator of a pending change.

(4) Configuration of the Tricon limits access to a small set of variables, which may be changed.

(5) Entering change data is a two-step process. The technician is trained to select the target variable, enter the change, observe the pending change on screen, and then confirm the change.

(6) Upon rotating the key to the normal "Close Access" position, the Tricon sends a list of all "writable" variables to the printer. The printer communication protocol is different from the non-safety VDU communications. Should the technician fail to enter the data in the allotted time, or fail to return the key to the "Close Access" position, the Tricon will automatically close access and print the list.

(7) The technician reports to the control room operator when the task is complete, showing that all changes were accomplished in accordance with the authorized work order.