INVENSYS TRICONEX V10 AUDIT REPORT

1. BACKGROUND / REGULATORY AUDIT BASIS

By letters dated September 9, 2009, November 13, 2009, and July 11, 2010 (Agencywide Documents Access and Management System (ADAMS) Accession Nos. ML092870628, ML093370293, and ML102040054), Invensys submitted Topical Report (TR) 7286-545-1, Revision 2, "Triconex Topical Report" describing the platform upgrade (V10.5.1) to the U.S. Nuclear Regulatory Commission (NRC) staff for review**.**

2. AUDIT SUMMARY

The NRC staff conducted an audit of the Triconex V10 development at Invensys' Irvine, California facility on December 15-17, 2010. Following introductions, the NRC staff reviewed the objectives in the audit plan and outlined specific information the staff needed to support the objectives. Invensys presented draft request for additional information (RAI) responses related to audit objectives. The draft RAI responses were used as a starting point to support discussion elements outlined in the audit plan. Following the discussion elements, the audit team separated to address individual audit items.

The NRC staff conducted an exit meeting to summarize their findings, stating that all audit objectives were met. The NRC staff did not identify any areas of non-compliance, but highlighted two areas of concern; requirements traceability and software validation tools.

The audit team included NRC Instrumentation and Controls Branch (EICB) technical reviewers Stephen Wyman and Richard Stattel and Licensing Processes Branch project manager, Jonathan Rowley. Invensys personnel supporting the review are listed below:

Brain Haynes, Project Manager, Delivery

Jeff Larson, Director, Nuclear Quality Assurance

Gary Hufton, Director, Control Hardware Development

Andy Nguyen, Manager, Hardware Development

Kurt Otto, Hardware Engineer

Roman Shaffer, Project Engineer

Kevin Vu, Independent Verification and Validation Project Manager

Michael Kieu, Director, Safety and Critical Control Development

Naresh Desai, Project Management & Architecture

Aad Faber, Manager, Product Assurance

Gary McDonald, Consultant

Frank Kloer, Qualification Engineer

David Golden, Global Director of Quality

Trisha Stauffer, Administrative Assistant

ENCLOSURE

3. INTERNAL PROCEDURES

Verify that the modified internal procedures that govern development and qualification of nuclear products have undergone only administrative change.

As part of the submittal for the Triconex TR, Invensys submitted a document (ADAMS Accession No. ML11100642) that details the differences between the Triconex V9.5.3 system and the Triconex V10.2.1 system. The document includes a list of procedures that have changed and a brief characterization of how each procedure changed. During the audit, a representative group of engineering and quality procedures were compared side-by-side and line-by-line to determine the nature of the changes. Those changes were, in turn, compared with Invensys' assessment of the changes. The document also contained a list of new procedures that have been used after the V9.5.3 system was created. Several of the new procedures were audited.

Audit Findings of Changed Procedures

Three Quality Assurance Management (QAM) procedures, three Quality Procedure Manual (QPM) procedures, and four Engineering Department Manual (EDM) procedures were selected for audit from the list of changed procedures.

QAM
QAM 4.0, "Design Control"
QAM 8.0, "Product, Parts, and Material Identification and Traceability"
QAM 18.0, "Training"

QPM
QPM 2.1, "Quality Plan Development"
QPM 6.2, "Dedication of Commercial Grade Items"
QPM 13.2, "Product Discrepancies"

EDM
EDM 12.00, "Product Development Process"
EDM 12.30, "Design Reviews"
EDM 24.00, "Software Configuration and Change Control"
EDM 90.00, "Product Verification"

The NRC staff reviewed every revision of the listed procedures from 2001 (V9.5.3 time frame) through 2009 (V10.2.1 time frame) to identify the changes from revision to revision. In each table in the differences document, Invensys provided a summary and characterization of the changes. The NRC staff's characterization of the changes were found to be consistent with that of Invensys. Where Invensys characterized a revision change as minor, insignificant, etc., the NRC staff concluded that the change is as such. An example of a minor change is the clarification of details for configuration management, document control and design specifications in EDM 24.00, Revision 1.4, "Software Configuration and Change Control." Where Invensys characterized a revision change as major, substantive, etc., the NRC staff concluded that the change is as such. One example of a substantive change is the added commitment to Institute of Electrical and Electronics Engineers (IEEE)-1012 in engineering manual EDM 12.00, Revision 2.0, "Product Development Process." The NRC staff finds a large majority of the changes where editorial in nature.

Audit Findings of New Procedures

The NRC staff reviewed eleven new procedures added since 2001 (V9.5.3 timeframe).

EDM 11.03, "Process and Product Quality Assurance"
EDM 13.20, "Corrective Action Management"
EDM 21.30, "Change Impact Analysis"
EDM 30.20, "Hardware Design Specifications"
EDM 30.30, "Hardware Test Specifications"
EDM 74.00, "Nuclear Qualification of Triconex Products"
EDM 75.00, "Nuclear Qualified Equipment List (NQDL)"
EDM 76.00, "Dedication of Products for Nuclear Service"
EDM 90.10, "Product Validation"
EDM 90.30, "Control of Tools and Test Software"

The NRC staff reviewed the new procedures to determine the impact on the existing process. The NRC staff found that new procedures augment and improve the previously approved design process. In most cases, the new procedures result from expansion of the process. For example, EDM 90.30 implements the use of DOORS. DOORS is a requirements management tool. This change addresses the requirements traceability "weakness" statement noted in the V9 safety evaluation (SE) (ADAMS Accession No. ML013470433, page 48). EDM 90.00, "Product Verification," incorporates the V9 SE comments regarding third party verification activities (ADAMS Accession No. ML013470433, page 49).

4. PROGRAMMABLE LOGIC

Verify that the design process used for programmable logic is acceptable for safety-related systems in nuclear power plants.

Results Achieved:

The NRC staff identified issues with the programmable logic design process meeting the software development lifecycle process per Interim Staff Guidance (ISG)-4 through the RAI process. Invensys has stated that the development of all programmable devices was complete prior to the release of ISG-4. To assess the acceptability of the existing programmable logic designs, the NRC staff reviewed the existing design documentation for the Tri-Bus field programmable gate array (FPGA). This device is central to the proper operation of the system, represents the most complex programmable logic change for V10, and is a significant change to the system implementation. Invensys provided a binder of design related documents including the specification. A complete listing of the provided documentation was included in the related RAI response (ADAMS Accession No. ML110140444).

The documentation included requirements definition for the FPGA development as part of a system specification. Most of the specific requirements show no direct traceability and can only be verified through a full, active review of the test bench files. However, many of the low level requirements are directly verified by proper operation of the tribus at the product level.

Invensys also used online tools to search the "Agile" database, identifying a suite of files from the firmware development that were sufficient to reproduce the design or to support investigation of the design through the test bench files. Invensys stated during the audit that a number of files had previously been found to be missing from the active archive. The missing files were documented through an internal "action request report" (ARR 861). Invensys stated that it was able to resurrect the missing files from historic archives and is correcting the problem under the previously mentioned action request. Invensys committed to provide a listing of the restored files with the related RAI response. Invensys also committed to updating the design process and presented draft procedure EDM 40.60 in support of that claim.

5. PRODUCT CHANGES

Verify that the implementation of changes to system software is acceptable for safety-related systems in nuclear power plants.

Results Achieved:

Regarding Inspection Requirement 3.3, “Product Changes,” the audit team was able to verify that Invensys followed approved process by conducting thread audits in key development areas. The audit team pulled threads from three areas of change that included the application processor executive, addition of the “TCM” communications module, and top level requirements from Electric Power Research Institute (EPRI)-TR 107330.

The application processor system executive, entitled “ETSX,” is the main software that determines how the platform runs. The NRC staff preselected four threads that highlight critical elements of system performance from the ETSX system architecture specification including safe state, memory, and coordinating end of scan. Coordinating end of scan was selected because it was a distinct change from the V9 platform software. The audit team gained perspective on the change during the thread review. Invensys explained that the improvement reduces opportunities for the three independent legs to get out of synch. Out of synch conditions do not pose a safety-related threat as the system is designed to detect the condition, flag (alarm) as a fault, and remove the leg from service.

The audit confirmed the verification and validation (V&V) activities related to four specific requirements from the ETSX system architecture specification. Each thread demonstrated poor traceability and required multiple personnel to provide sufficient “tribal knowledge” to pull the documents from the archive. One “V&V Summary” report was missing from the database. However, Invensys was able to verify through a scanned copy of the original signed-off test procedure. Invensys also produced a trackable corrective action document that pre-dated the audit noting the database omission. Despite the traceability issues, the audit confirms that the Invensys followed process for the ETSX development.

The audit team reviewed several threads stemming from the addition of the communications module (TCM). Invensys process documentation dictated that all configuration changes stem from either a marketing request or an engineering change request. It was necessary to backtrack by several configurations on the commercial side to identify the original documented marketing request. The audit team worked from the earlier configuration item to pull threads related to the TCM, confirming a number of requirements through the V&V process. The audit team noted that the more recent TCM development demonstrated better traceability. The TCM documentation was entered into the DOORS requirements management system following the development. Efforts to improve traceability were noted, but not encompassing of all threads. The audit team concluded this effort by reviewing changes to top level configurations moving forward to the current nuclear qualified release to confirm that major changes were not made to the TCM during the configuration. The audit confirmed that Invensys followed process for integrating and testing the new communications module.

Overall, the audit team reviewed key elements of the development process related to areas of change in the updated platform. The audit team noted significant weaknesses in traceability, an area of weakness highlighted in the V9 SE, as well as evidence of Invensys' efforts to improve that weakness. The audit team did not identify any areas of noncompliance in the implementation of changes to the Triconex platform.

6. SAFETY-RELATED TO NON-SAFETY-RELATED

Verify that safety-related to non-safety-related connection through remote chassis RXM modules is acceptable for safety-related systems in nuclear power plants.

Results Achieved:

Regarding inspection requirement 3.4, "Safety to Non-Safety Communications," the audit team was able to obtain additional information to support the SE of the safety-related to non-safety-related connection through the remote chassis RXM modules. Invensys provided a revised version of the technical paper entitled, "Clarification of Safety-Related Primary RXM to Non-Safety-Related Remote RXM Chassis," for the NRC during the audit and a detailed review was conducted. From the information in this document, the NRC was able to identify the following three layers of communication isolation protection.

1. Communications Isolation at the RXM Module
2. Message Discrimination performed at the IOCCOM Module
3. Data discrimination which occurs as a result of Triple-Modular-Redundant architecture of the Triconex system.

The revised technical paper included a detailed description of the communications isolation functionality performed at the 4200 RXM modules. This includes a description of the intelligence on the RXM module which is provided by two on-board microprocessors (CPU's) in a master-slave configuration. The RXM module acts as a gate keeper for all communications between the safety-related processor and the non-safety-related remote RXM chassis. The communications path is normally blocked by a programmable array logic (PAL) device within the RXM module that is controlled by an electrical transmit enable signal from the master and slave CPU's. As long as no valid command signal is received from the safety-related processor, the PAL within the RXM disallows all communications from the non-safety-related portion of the system. Therefore, an initiating event on the non-safety-related portion of the system such as an invalid data request, or a data storm would be blocked at the safety-related RXM and would not adversely impact the communications on the safety-related portion of the system.

Within the technical paper, Invensys identified the safety-related IOCCOM module (layer 2) as the communications isolation barrier for the system. The NRC staff had expressed concerns about this barrier because of the fact that the IOCCOM module is not located within the direct communications path between the safety-related processor and the non-safety-related remote RXM chassis. In addition, Invensys has consistently labeled the demarcation point between safety-related and non-safety-related equipment at the connection between the primary and remote RXM modules which is not consistent with the concept that the IOCCOM module is providing communications isolation for the system.

These concerns and apparent inconsistency were discussed with the engineers at Invensys and they acknowledged that the paper should have characterized the RXM module data communications isolation capabilities as the primary means of communications isolation for the system. The other two layers of isolation are also discussed and should be credited in the SE, however, it was agreed that identifying the safety-related 4200 RXM module as the primary means of data communications isolation will provide a level of consistency such that all safety-related to non-safety-related isolation barriers (electrical independence, electrostatic, and electro magnetic interference (EMI) isolation, and data isolation) occur at the same architectural point within the system. Invensys also stated that the technical paper will be revised to reflect this characterization and resubmitted to the NRC.

The technical paper also included a failure modes and effects table (Table 3) which postulates credible failures of the non-safety-related remote RXM chassis. The failure modes that are identified in this table are primarily hardware related. Though it is recognized that many software or data communications related failures do manifest themselves as faults that have similar symptoms to the hardware failure modes identified, the NRC staff believes that certain additional failure modes should be included in the analysis. The audit team did not consider this table to be comprehensive and has asked Invensys to address the failure modes relating to communications that are listed in IGS-4, Position 12. These failure modes are;

- 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.
- Messages may be repeated at an incorrect point in time.
- Messages may be sent in the incorrect sequence.
- Messages may be lost, which includes both failures to receive an uncorrupted message or to acknowledge receipt of a message.
- Messages may be delayed beyond their permitted arrival time window for several reasons, including errors in the transmission medium, congested transmission lines, interference, or by delay in sending buffered messages.
- Messages may be inserted into the communication medium from unexpected or unknown sources.
- Messages may be sent to the wrong destination, which could treat the message as a valid message.
- Messages may be longer than the receiving buffer, resulting in buffer overflow and memory corruption.
- Messages may contain data that is outside the expected range.
- Messages may appear valid, but data may be placed in incorrect locations within the message.
- Messages may occur at a high rate that degrades or causes the system to fail (i.e., broadcast storm).
- Message headers or addresses may be corrupted.

Invensys agreed to address these failure modes in the updated version of the technical paper.

7. DETERMINISM

Verify that changes implemented since the previously approved version have not impacted the deterministic behavior of the system.

Results Achieved:

Regarding inspection requirement 3.5, “Determinism,” the NRC staff was able to gain new information to support the SE of deterministic behavior of the Triconex platform. Invensys provided a detailed description of the Main Processor architecture, scan protocol, and interrupt handling and described how deterministic behavior is assured. Part of the discussion focused on end of scan coordination which is a change to the V10 platform. End of scan coordination allows cleaner handling of scan overruns, improving deterministic behavior and reducing maximum scan time. The NRC staff did not identify any areas where changes to the V10 system have negatively impacted the previously accepted deterministic behavior. Invensys committed to provide the information as a response to a related RAI question.

8. QUALITY ASSURANCE

The NRC staff performed a review of the quality assurance (QA) manuals Q1 (non-nuclear) and Q2 (nuclear Appendix B program), and conducted an interview with the director of Nuclear Quality Assurance. During this interview, the level of independence from the design team that the QA and independent V&V (IV&V) personnel have was discussed. Also discussed was the challenges of maintaining this independence and maintaining the level of system expertise necessary to perform IV&V and QA tasks. Invensys does not maintain a separate software QA team, but instead, relies on the expertise of the IV&V team for matters involving software development.

The relationship between the IV&V team and the QA organization was discussed. Invensys maintains independence between these groups, and their processes identify separate activities for each organization.

The use of metrics as a means to facilitate quality process improvements was discussed. Invensys explained how the metrics of fault rates and test failure rates were incorporated into the processes for application development. Invensys also stated that the phase V&V summary reports for individual projects are the means used for reporting these metrics and that the Invensys corrective action programs are invoked to facilitate process improvements. No QA program deficiencies were identified during this audit.

9. CONCLUSION

The audit team successfully identified new information to support the Triconex V10 SE and did not identify any areas of noncompliance. The audit team confirmed that docketed descriptions of procedure changes were accurate, programmable logic development products met minimum requirements, software changes followed the accepted process, and safety-related to non-safety-related connections through the RXM provide protection for the safety-related function. Two areas of concern were identified during the exit meeting and are itemized below:

1. Requirements Traceability - Though the NRC staff noted significant improvements that have been made to the requirements traceability activities associated with the Triconex product development efforts, many of the traced requirements related to the product changes being reviewed under this TR update evaluation were not easily traceable to all of the necessary implementation documents. During the audit, the Invensys personnel had to be called upon in order to verify that requirements had been properly implemented in the Triconex design. There should not be this much reliance on design

engineering experts to assure that requirements are properly implemented. The use of a requirements traceability tool has only been partially implemented and only for recent design changes.

2. Software Validation Tools – Through discussions with the IV&V lead engineer, the NRC staff learned of the reliance on a software emulation tool to complete software Validation Testing activities. The software emulator tool that is used by Invensys for this purpose is not qualified as a safety-related application nor has it been developed under the same software development processes that are used for safety-related Triconex software. Therefore, all software that has been tested in this emulator environment must be fully re-tested at the integration stage of development in order to be compliant with IEEE 7-4.3.2. This matter was discussed at length and Invensys stated that the processes for software development include complete testing of the system software downstream of the V&V tests which rely on the use of this emulation tool. These down-stream tests will be performed for all safety-related system software.