

2007-05-14

**Automation, Software and Information Technology**

**Test report about the approval  
of the safety related automation devices  
TRICON Version 10.3  
of Triconex Invensys Systems Inc.**

**Report-No.: 968/EZ 105.09/07**

**Date: 2007-05-14**

**Test report about the approval  
of the safety related automation devices  
TRICON Version 10.3  
of Triconex Invensys Systems Inc.**

**Report-No.:** 968/EZ 105.09/07

**Date:** 2007-05-14

**Pages:** 11

**Test object:** TRICON Version 10.3

**Customer/Manufacturer:** Triconex Invensys Systems Inc.  
Invensys Systems, Inc.  
15345 Barranca Parkway  
Irvine, California 92618  
United States of America

**Order-No./Date:** 117094 dated 2007-03-27

**Test Institute:** TÜV Rheinland Industrie Service GmbH  
Automation, Software and Information Technology (ASI)  
Am Grauen Stein  
51105 Köln  
Germany

**Department:** Automation, Software and Information Technology (ASI)

**TÜV-Offer-No./Date:** 968/46/07 dated 2007-02-14

**TÜV-Order-No./Date:** 9716803 dated 2007-03-28

**Inspector:** Dipl.-Ing. (FH) Oliver Busa

**Test location:** see Test Institute

**Test duration:** March 2007 - May 2007

The test results are exclusively related to the test samples.

This report must not be copied **in an abridged version** without the written permission of the Test Institute.

<b>Contents</b>	<b>Page</b>
1. Scope	4
2. Standards and previous test reports	4
3. Object of inspection	5
3.1 Documentation	6
4. Tests and test results	7
4.1 General	7
4.2 Management of Functional Safety	8
4.3 Review of the documentation	8
4.4 Inspection of the safety architecture	8
4.5 Inspection of the measures for failure avoidance	8
4.6 Inspection of the measures to detect and control failures	9
4.7 Inspection of the hardware	9
4.8 Inspection of the software	9
4.9 FMEA and fault insertion	9
4.10 Reaction time	9
4.11 PFD and PFH calculation	9
4.12 Electrical Safety	9
4.13 Environmental and EMC test	10
4.14 Inspection of the TriStation and EnDM changes	10
4.15 Review of the Safety Guidelines	10
5. Summary	10

Annex A: TRICON Version 10.3 Approved Components List

## 1. Scope

This report is related to the type approval of the TRICON Communication Modules (TCM) and the corresponding firmware changes of the TRICON Main Processor firmware (MP).

Besides the necessary modifications of the TriStation 1131 Application Development Workstation and the Enhanced Diagnostic Monitor shall be part of review.

This type approval should demonstrate that the automation devices are suitable for risk reduction in accordance to IEC 61508 [1], SIL 3.

## 2. Standards and previous test reports

### **Functional Safety**

- [1] IEC 61508:2000, parts 1 - 7  
Functional safety of electrical/electronic/programmable electronic safety related systems

### **Electrical safety and resistance against environmental conditions**

- [2] EN 50178:1997  
Electronic equipment for the use in power installations
- [3] IEC 61131-2:2003  
Programmable Controllers  
Part 2: Equipment requirements and tests

### **Electromagnetic Compatibility**

- [4] EN 61000-6-4:2001  
Electromagnetic Compatibility (EMC)  
- Generic emission standard  
- Residential, commercial, and light industry
- [5] EN 61000-6-2:2005  
Electromagnetic Compatibility (EMC)  
- Generic Standards  
- Immunity for Industrial Environments

### **Application specific standards**

- [6] ISA S84.01  
Application of safety instrumented systems for the process industry
- [7] EN 54-2:1997  
Fire detection and fire alarm systems  
Part 2: Control and indicating equipment
- [8] EN 50156-1:2004  
Electrical Equipment for Furnaces  
Part1: Requirements for application Design and Installation
- [9] IEC 61511-1:2003  
Functional safety  
Safety instrumented systems for the process industry sector

[10] NFPA 72:2002  
National Fire Alarm Code

[11] NFPA 85:2001  
Boiler and Combustion Systems Hazards Code

#### **Previous test reports**

[P1] Report-No.: 968/EZ 105.03/01, dated 2001-09-13, TÜV Rheinland

[P2] Report-No.: 968/EZ 105.04/05, dated 2005-08-15, TÜV Rheinland

[P3] Report-No.: 968/EZ 105.05/06, dated 2006-10-31, TÜV Rheinland

[P4] Report-No.: 968/EZ 105.06/06, dated 2006-10-31, TÜV Rheinland

[P5] Report-No.: 968/EL 326.00/05, dated 2005-02-28, TÜV Rheinland

[P6] Report-No.: 968/EL 405.01/06, dated 2006-10-31, TÜV Rheinland

### **3. Object of inspection**

Object of this approval is the TRICON Version 10.3 as described within the Engineering Project Plan [D3]. The focus of this system version is targeted to new models of the Tricon Communication Modules (TCM), which implements in the new version the support of an Embedded OPC Server.

The TCM modules allows non-safety related communication using several industry standard communication protocols. The modules act as a black channel for safety related communication between Tricon PLCs or safety related modules.

The new modules are identified as:

- TCM 4351B (Tricon Communication Module, Copper, without OPC),  
- Build 108, Version number 6241
- TCM 4352B (Tricon Communication Module, Fiber, without OPC)  
- Build 108, Version number 6241
- TCM 4353 (Tricon Communication Module, Copper, with OPC),  
- Build 108, Version number 6241
- TCM 4354 (Tricon Communication Module, Fiber, with OPC),  
- Build 108, Version number 6241

All the above listed models are based on the already certified [P2] TCM models 4351, 4351A, 4352, 4352A.

In addition the ETSX firmware of the Main Processor module (MP) needs to be modified to support the new TCM modules.

The following module firmware was modified within TRICON Version 10.3:

- Main Processor (MP), EMP 3008 firmware (ETSX)  
- Build 108, Version number 6236

The Main Processor firmware related to Version 10.3 is based on the version number 6198, build 90 certified with TRICON Version 10.2 [P3].

Further the changes to the Tricon programming tool "TriStation" and the Enhanced Diagnostic Monitor were reviewed during this approval.

In detail the following versions were part of review:

- TriStation 1131, V4.2 (Application Development Workstation)
  - Build 449
- Enhanced Diagnostic Monitor (EnDM) V2.0
  - Build 131

### 3.1 Documentation

The table below shows the basis documentation which were used during the approval. Further documentation including verification and validation results are referenced within the documentation list [D1] on the manufacturer CD-ROM "TRICON v10.3, dated 2007-05-12".

All project related documents are available in electronic form and are archived by the Test Institute.

D1	Tricon IEC 61508-3 Figure 4 for TRICON V10.3.xls Filelist on CD-ROM dated 2007-05-12
D2	Triconex Engineering Procedure, EDM Rev. 014, dated December 22, 2005
D3	Tricon V10.3 Engineering Project Plan, 9100109-001 v1.3, dated March 9, 2007
D4	Tricon V10.3 Project Verification Plan, 9600186-001 v1.0, dated November 9, 2006
D5	MP 3008 Verification Plan - Tricon V10.3, 9600186-002 v1.0, dated August 25, 2006
D6	TCM 2.0 Verification Plan, 9600186-003 v1.0, dated November 11, 2006
D7	Tricon V10.3 System Validation Plan, 9600190-001 v1.0, dated November 9, 2006
D8	Validation Test Procedure - Tricon ETSX and Communications, 9600077-001 v2.0, dated January 23, 2007
D9	Validation Test Procedure - Tricon Communication Module, 9600159-001 v1.1, dated January 11, 2006
D10	Validation Test Procedure - TCM OPC Server, 9600193-001 v1.1, dated March 13, 2007
D11	Tricon System Requirement Specification, 9100038-002 v2.1, dated March 12, 2007
D12	Tricon System Architecture Specification, 9100038-100 v1.1, dated March 12, 2007
D13	OPC Interface Requirements Specification, 6200154-011 v1.0, dated October 12, 2006
D14	OPC Interface Design Specification, 6200154-012 v1.0, dated December 8, 2006

D15	TCM System Requirements Specification, 6200152-001 v3.1, dated March 7, 2007
D16	TCM System Architecture Specification, 6200152-002 v3.1, dated March 12, 2007
D17	TCOM Software Requirements Specification, 6200152-003 v3.0, dated December 1, 2006
D18	TCOM Software Design Specification, 6200152-004 v3.0, dated December 8, 2006
D19	TCM OPC Software Requirements Specification, 6200152-005 v1.0, dated December 1, 2006
D20	TCM OPC Software Design Specification, 6200152-006 v1.0, dated December 8, 2006
D21	TCM Software Test Plan, 6500155-000 v4.0, dated December 1, 2006
D22	TCM Software Test Description, 6500155-001 v3.2, dated March 24, 2007
D23	TCM OPC Software Test Plan, 6500155-002 v1.0, dated December 1, 2006
D24	TCM OPC Software Test Description, 6500155-003 v1.0, dated December 8, 2006
D25	V10.3 ETSX Change Impact Analysis, 9100125-002 v1.0, dated February 1, 2007
D26	V10.3 TCM Change Impact Analysis, 9100130-001 v2.0, dated January 31, 2007
D27	V10.3 TCM Source Code Analysis, 6500174-001 v1.0, dated March 28, 2007
D28	FMEA Tricon TCM, 7800281-001 v1.0, dated April 23, 2007
D29	Technical Product Guide for Tricon Systems, 9791007-014, March 2007
D30	Planning and Installation Guide for Tricon v9-v10 Systems, 9700077-002, March 2007
D31	Communication Guide for Tricon v9-v10 Systems, 9700088-001, March 2007
D32	Safety Consideration Guide for Tricon v9-v10 Systems, 9700097-001, March 2007

Table 1: Manufacturer Documentation

#### 4. **Tests and test results**

##### 4.1 **General**

The measuring and test equipment, which has been used by the TÜV Rheinland Group in the tests described in the following, is subject to regular inspection and calibration. Only devices with valid calibration have been used. The devices used in the various tests are recorded in the inspector's documentation.

All considerations concerning tolerance of the measurements, so far applicable, are stated in the inspector's documentation, too.

In cases where tests have been executed in an external test lab or in the test lab of the manufacturer and where the results of these tests have been used within the here documented approval, this has occurred after a positive assessment of the external test lab and the achieved test results in detail according to the Quality Management procedure QMA 3.310.05.

#### **4.2 Management of Functional Safety**

The Management of Functional Safety in accordance to IEC 61508 have been reviewed on product level. The modifications and extensions to the product were done considering the requirements of IEC 61508, following the safety lifecycle and including the appropriate documentation with respect to specification, verification and validation.

The manufacturer specified detailed verification and validation plans [D4-D10]. They specify all activities at each phase of the development cycle to check the outputs of a given phase to ensure correctness and consistency with respect to the inputs to that phase. The plans are based on the verification process described in [D2].

The development lifecycle of the manufacturer follows a well defined and hierarchical process and was inspected for compliance with IEC 61508 considering the requirements for the Management of Functional Safety.

The Management of Functional Safety complies with SIL 3 of IEC 61508 [1].

#### **4.3 Review of the documentation**

The manufacturer documents as listed in chapter 3.1 have been reviewed partly together with the manufacturer and were assessed concerning the completeness, consistency and conformity in accordance to the IEC 61508.

In detail the following points were considered during the inspection of the documentation:

- accuracy and consistency
- clear relationship between the documents
- comprehensibility
- completeness of the specification and documentation
- accessibility and maintainability

Contradiction in the documentation have been discussed with the manufacturer and were corrected in the documents.

The inspection of the documentation have been finished with a positive result.

#### **4.4 Inspection of the safety architecture**

The TCM modules are based on an own microcontroller architecture and do not have direct access to the main processor module (MP) [D16]. All information transmissions are checked by the main processor and will be discarded if the messages are malformed. Data mismatches are voted between the three legs of the system. Therefore it can be considered as a "black channel" communication. The safety core provides isolation from the TCM module using a keyswitch where ETSX do not allow any system change in the RUN position. As a consequence the TCM modules reacts interference free to the safety core.

Note:

On application level the user is responsible for correct use of non-safety related data in a safety related application.

#### **4.5 Inspection of the measures for failure avoidance**

The measures to avoid failures have been inspected during a Functional Safety Assessment (FSA) within the manufacturer facilities in Irvine (CA), USA (March, 5<sup>th</sup> to 9<sup>th</sup> 2007). The application and effectiveness of the measures to avoid failures during the safety lifecycle have been assessed.

It was demonstrated that the manufacturer complies with SIL 3 according to the safety lifecycle requirements of IEC 61508.

#### **4.6 Inspection of the measures to detect and control failures**

There have been no changes to the already specified measures to detect and control failures.

The results of the previous approvals are still valid [P1 - P4].

#### **4.7 Inspection of the hardware**

No major hardware changes were introduced between the previous certified TCM versions [P2]. There have been only the change of a flash memory module due to the fact that the previous module becomes obsolete.

As a consequence the previous type approval reports are still valid [P1-P4].

#### **4.8 Inspection of the software**

Based on the change and impact analysis [D25, D26] the modification related to firmware of the TCM modules and the firmware related to the MP module were reviewed and discussed with the manufacturer.

The major changes to the TCM are related to the introduction of an embedded OPC server functionality and additional modifications [D26]. The changes to the ETSX firmware of the MP module are related to fix and to support the new TCM modules [D25].

Within the TRICON Version 10.3 the older TCM modules 4351, 4351A, 4352 and 4352A are not supported any longer.

The manufacturer has prepared a verification and validation plans [D4 - D10] and defined test specifications [D21-D24] to verify and validate the correct implementation of the firmware modifications.

The verification, validation and test plans were reviewed under consideration of sufficient test coverage related to the modification and implementation. The final test reports [D1] was reviewed for completeness and accuracy.

The review of the firmware implementation and modifications was finished with a positive result.

#### **4.9 FMEA and fault insertion**

The original FMEAs and corresponding fault injection tests were adapted to the modification [D28].

The review of the FMEAs and the fault insertion tests were closed with positive results.

#### **4.10 Reaction time**

System reaction time of the Tricon PLC is not affected by TCM communication.

#### **4.11 PFD and PFH calculation**

The TCM communication module does not affect the PFD or PFH of the Tricon PLC system, because it is considered as a black channel communication.

#### **4.12 Electrical Safety**

The electrical safety is tested in accordance with EN 61131-2 [2,3]. The performed tests are documented in [P5, P6].

All products are supplied with SELV (Safe Extra Low Voltage) in accordance with [6] and laid out for SELV with respect to isolation.

The results in [P5, P6] are still valid due to the fact the no hardware architectural changes were done.

#### **4.13 Environmental and EMC test**

The tests were performed in accordance with the following standards:

- EN 61131-2
- EN 61000-6-2
- EN 61000-6-4
- EN 50156-1
- EN 54-2

The tests have been performed by accredited test laboratories and have been recognized by the Test Institute. During the tests, the safety-related system properties have been monitored.

The environmental simulation tests have been documented in test report [P5].

The results in [P5] are still valid due to the fact the no hardware changes were done.

#### **4.14 Requirements resulting from application standards**

The application specific requirements resulting from [6] to [11] are still fulfilled. Conditions concerning the application of the programmable electronic system are documented in the safety considerations guide [D32].

#### **4.15 Inspection of the TriStation and EnDM changes**

The TriStation programming environment TS1131 and the Enhanced Diagnostic Monitor EnDM were updated to integrate the new TCM modules and to implement pending modifications.

The modifications are described within a change and impact analysis. Appropriate verification and validations steps have been planned and performed. All documentation are compiled and listed in [D1].

The new NGIO modules can be used in conjunction with TriStation 1131 V4.2, Build 448 respectively EnDM V2.0, build 131.

#### 4.16 Review of the Safety Guidelines

The changes to the safety guidelines and user documentation were reviewed with respect to comprehensibility and user assistance.

The safety guidelines and user documentation describes all conditions which shall be maintained for safety related use of the products.

The reviews were finished with a positive result.

#### 5. Summary

The approval of the TRICON Version 10.3 has shown that the results of the previous type approval Report-No.: 968/EZ 105.03/01 [P1] and Report-No.: 968/EZ 105.04/05 [P2] are still valid and the TRICON Version 10.3 can be used in applications up to SIL 3 as defined in IEC 61508 [1].

The actual Safety and User Guides released by Triconex must be observed [D29-D32].

Application firmware must be created using TriStation 4.2 and higher to support the new TCM modules and must consider the guidelines specified within the Safety and User Guides [D29-D31].

The actual valid hardware and software versions shall be retrieved from the currently valid module and firmware release list. This list is released together by the manufacturer and the Test Institute and can be obtained at <http://www.tuv-fs.com> or on request from the manufacturer.

Cologne, 2007-05-14  
TIS/ASI/Kst. 968 bu-nie

The inspector



Dipl.-Ing. (FH) Oliver Busa