

2006-10-31



TÜV Rheinland Group

Automation, Software and Information Technology

**Test report about the type approval of
safety-related automation devices
Tricon Version 10.2.1
of Triconex Invensys Systems Inc.**

**Report-No.: 968/EZ 105.06/06
Date: 2006-10-31**

**Test report about the type approval of
safety-related automation devices
Tricon Version 10.2.1
of Triconex Invensys Systems Inc.**

Report-No.:	968/EZ 105.06/06
Date:	2006-10-31
Pages:	13
Test object:	Tricon Version 10.2.1
Customer/Manufacturer:	Triconex Invensys Systems Inc. Invensys Systems, Inc. 15345 Barranca Parkway USA-Irvine, California 92618 United States of America
Order-No./Date:	113281 dated 2006-01-25
Test Institute:	TÜV Rheinland Industrie Service GmbH Automation, Software and Information Technology (ASI) Am Grauen Stein D-51105 Köln (Poll)
TÜV-Offer-No./Date:	968/218/05 dated 2005-11-08
TÜV-Order-No./Date:	9444872 dated 2006-01-18
Inspector:	Dipl.-Ing. Jürgen Schön Dipl.-Ing. (FH) Oliver Busa
Test location:	see Test Institute
Test duration:	January 2006 - October 2006

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.

Contents	Page
1. Scope	4
2. Standards and previous test reports	4
3. Object of inspection	5
3.1 Documentation	5
4. Tests and test results	7
4.1 General	7
4.2 Management of Functional Safety	7
4.3 Inspection of the measures for failure avoidance	7
4.4 Inspection of the measures to detect and control failures	7
4.5 Review of the documentation	8
4.6 Hardware and Software inspection of the Tricon Version 10.2.1	8
4.6.1 Safety Requirements	8
4.6.1.1 General safety requirements	8
4.6.1.2 Requirements resulting from application standards	9
4.6.2 Hardware inspection of the Tricon Release 10.2.1	9
4.6.2.1 Overview	9
4.6.2.2 FMEA inspection of the Tricon Version 10.2.1	11
4.6.2.3 Inspection of the reliability data and PFD calculation	11
4.6.2.4 Inspection of the electrical safety	12
4.6.2.5 Inspection of environmental and EMC Tests	12
4.6.3 Software inspection of the Tricon Version 10.2.1	12
4.6.3.1 Overview	12
4.6.3.2 Inspection of the AID 3721 firmware	12
5. Summary	13

1. **Scope**

Scope of this report are changes to the components of the already approved Tricon System.

Together with these changes a new Analog Input Module - Single Ended (AIS 3720) and a new Supervised Digital Output Module (SDO 3625) for the Tricon System Version 10.2.1 has been approved.

The type approval should demonstrate that the automation devices are suitable for risk reduction in applications up to SIL 3 according to IEC 61508 and IEC 61511.

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

Electromagnetic Compatibility

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

Application specific standards

- [6] ISA S84.01
Application of safety instrumented systems for the process industry
- [7] IEC 61511-1:2003
Functional safety
Safety instrumented systems for the process industry sector
- [8] EN 50156-1:2004
Electrical Equipment for Furnaces
Part1: Requirements for application Design and Installation
- [9] NFPA 85:2001
Boiler and Combustion Systems Hazards Code

[10] EN 54-2:1997
Fire detection and fire alarm systems
Part 2: Control and indicating equipment

[11] NFPA 72:2002
National Fire Alarm Code

Previous type approval 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

Previous environmental test reports

[P4] Report-No.: 968/EL 260.00/03, dated 2003-12-10, TÜV Rheinland

[P5] Report-No.: 968/EL 310.00/04, dated 2004-11-11, TÜV Rheinland

[P6] Report-No.: 968/EL 326.00/05, dated 2005-02-28, TÜV Rheinland

[P7] Report-No.: 968/EL 405.01/06, dated 2006-10-31, TÜV Rheinland

3 Object of inspection

Test object of this type approval are the new Analog Input Module - Single Ended (64 point), model AIS 3720 and a Supervised Digital Output Module (32 points), model SDO 3625.

3.1 Documentation

The necessary documentation and software sources needed for this approval were handed over by the manufacturer and have been archived by the Test Institute (see Tricon 10.2.1, CD-ROM, dated 2006-10-27).

The following tables include only the primary documents. Further detailed documents including Verification & Validation reports are referenced in [H1].

H1	Tricon IEC 61508-3 Figure 4.xls Document list on Tricon 10.2.1, CD-ROM, dated 2006-10-27
H2	NGIO Engineering Project Plan (9100046-001) v1.2, dated June 21, 2006
H3	NGIO System Requirements Specification (9100042-001) v4.1, dated July 20, 2006
H4	NGAI System Requirements Specification (9100117-001) v2.0, dated July 20, 2006
H5	NGDO System Requirements Specification (9100118-001) v1.3, dated August 04, 2006
H6	Tricon V10 System Safety Requirement Specification (9100113-001) v1.0, dated June 23, 2006
H7	Tricon V10 System Safety Concepts (9100112-001) v1.0, dated June 22, 2006
H8	NGIO Core System Architecture Specification (9100042-002) v2.0, dated July 31, 2006
H9	NGIO Core HW Requirements Specification (9100098-001) v1.2, dated August 2, 2006
H10	NGIO Core SW Requirements Specification (6200155-001) v2.1, dated August 10, 2006

H11	NGIO Core HW Design Specification (9100098-002) v1.0, dated August 30, 2006
H12	NGIO Core SW Architecture and Design Specification (6200156-001) v1.3, dated September 18, 2006
H13	NGAI System Architecture Specification (9100117-002) v1.0, dated August 21, 2006
H14	NGAI HW Requirement Specification (7100243-001) v1.0, dated August 30, 2006
H15	NGAI SW Requirement Specification (6200169-001) v1.0, dated September, 2006
H16	NGAI HW Design Specification (7100243-002) v1.0, dated September 8, 2006
H17	NGAI SW Design Specification (6200169-002) v1.0, dated September 26, 2006
H18	NGDO System Architecture Specification (9100118-002) v1.0, dated September 21, 2006
H19	NGDO HW Requirement Specification (7100247-001) v1.0, dated October 07, 2006
H20	NGDO SW Requirement Specification (6200170-001) v1.0, dated October, 2006
H21	NGDO HW Design Specification (7100247-002) v1.0, dated October, 2006
H22	NGDO SW Design Specification (6200170-002) v1.0, dated October 26, 2006
H23	NGIO Project Quality Plan v1.0, dated July 07, 2006
H24	Software Quality Assurance Plan Tricon NGIO (9600168-800) v1.0, dated July 18, 2006
H25	Software Verification and Validation Plan Tricon NGIO (9600168-600) v1.0
H26	NGIO Core HW Test Requirements Specification (7600242-200) v1.0, dated September 1, 2006
H27	NGIO Core SW Test Plan (6200159-001) v1.4, dated September 18, 2006
H28	NGAI Unit Test Requirement Specification (7600243-200), v1.0, dated August 15, 2006
H29	Tricon v10.2.1 Release, Software Release Definition (6200003-196) v2.1, dated October 26, 2006
H30	TRICONV10.2MarkovModel_PFD_0906.DOC, dated September 09, 2006
H31	TRICONV10.2MarkovModel_FS_0906.DOC, dated September 09, 2006
H32	TRICONV10.2_0906.xls, dated September 09, 2006
H33	TRICONV10.2_0906Spreadsheet.DOC, dated September 09, 2006
H34	TRICON Table D.xls, dated September 18, 2006
H35	Selection of XLS and YLS for Items in Table D.doc, dated September 18, 2006
H36	Failure Mode and Effect Analysis with Diagnostics Analysis (7800243-001) v1.0, dated September 07, 2006
H37	NGAID FMEA & DA.xls Spreadsheet, dated September 18, 2006
H38	NGAI Electrical Safety Evaluation.doc, dated September 14, 2006
H39	Safety Considerations Guide for Tricon v9–v10 Systems (9700097-001) dated August 2006
H40	Developer's Guide TriStation 1131, Version 4.1 (9700100-003) dated August 2006
H41	Planning and Installation Guide for Tricon v9–v10 Systems (9700077-002) dated August 2006

Table 1: Tricon v10.2.1, NGIO documents

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 inspectors documentation.

All considerations concerning tolerance of the measurements, so far applicable, are stated in the inspectors 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 QMA3.310.05.

4.2 Management of Functional Safety

The Management of functional safety has been carried out on product level. The modifications and extensions to the product have been made taking into account the requirements of IEC 61508, following the safety lifecycle and including the appropriate documentation for verification and validation.

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

4.3 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 (January, 24th-26th and September 11th-15th 2006). 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 the safety lifecycle requirements of IEC 61508.

All the measures have been applied for the Tricon Version 10.2.1 including the new AIS 3720 module and SDO 3625 modules.

4.4 Inspection of the measures to detect and control failures

The measures to detect and control failures have been inspected during a Functional Safety Assessment (FSA) within the manufacturer facilities in Irvine, CA USA (September 11th-15th 2006). During this assessment a lab inspection and witness tests of the AIS 3720, SDO 3625 modules have been performed with a positive result.

The Verification & Validation tests (V&V) for the Tricon Version 10.2.1 have been successfully completed and include:

- System Level verification tests
- Module level functional verification tests
- Automated Fault Insertion tests for the AIS 3720 and SDO 3625 modules
- Unit level hardware tests
- Unit level software tests

- System Level validation tests
- Module level functional validation tests

The V&V reports have been inspected with a positive result.

4.5 Review of the documentation

The documentation has been presented by the manufacturer with the documents listed in chapter 3.1. The documents have been reviewed together with the manufacturer and were assessed concerning the completeness, consistency and conformity in accordance with the IEC 61508. Based on the overall document plan [H1] the documents were inspected regarding comprehensibility, completeness and consistency.

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

- revision control system of the documents
- unambiguous attributes
- clear relationship between the documents
- comprehensibility
- completeness of the specification and documentation

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

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

4.6 Hardware and Software inspection of the Tricon Version 10.2.1

4.6.1 Safety Requirements

4.6.1.1 General safety requirements

The manufacturer of the Tricon System Version 10.2.1, Triconex Invensys, maintain a functional safety management system according to the general requirements of IEC 61508, in order to manage and specify all technical activities during the safety lifecycle phases which are necessary to achieve the required safety integrity level (SIL) of a safety related system.

The process, plant or other safety relevant applications under the control of the Tricon System Version 10.2.1 must have a defined safe state (de-energized or energized) according to the table 2.

	Normally energized	Normally de-energized
Safety Function	De-energize to trip	Energize to trip
Safe State	De-energized outputs	De-energize the outputs or hold last state and perform alarm

Table 2: Definition of the Safe State

The hardware safety integrity as listed in table 3 of IEC 61508, part 2, must be considered for systems with microprocessor based components (Type B). The Analog Input Module AIS 3720 and the Digital Output Module SDO 3625 must fully comply with this standard.

The safe failure fraction of the AIS 3720 and SDO 3625 modules is $\geq 90\%$.

The hardware fault tolerance of the module is 1 or 2, depending of the operating mode.

The safety life cycle requirements are described in chapter 7 and listed in table 1 of IEC 61508, part 2.

The requirements can be divided into the following categories:

1. Requirements which have to be considered for the design of a safety related system. These requirements are mostly independent of the applications.
2. Requirements to ensure sufficient assistance during all phases of the safety lifecycle of safety related applications with all aspects of:
 - specification and planning
 - operation and maintenance
 - verification/validation and modification

The requirements of the first category is addressed during this type approval.

The requirements of the second category need to be fulfilled by the end-user of the system. The documentation [H39-H41], especially the Safety Considerations Guide [H39] provides the related information for proper use of the safety related system.

4.6.1.2 Requirements resulting from application standards

The application specific requirements are resulting from [6] to [11]. They are suitable for applications in the process industry, for emergency shut down, burner management and for fire and gas. Conditions concerning the application of the programmable electronic systems are documented in the safety consideration guide [H39]. The Tricon System Version 10.2.1, including the Single-Ended Analog Input Module AIS 3720 and the Digital Output Module SDO 3625 fulfils the new releases of the listed application standards.

4.6.2 Hardware inspection of the Tricon Release 10.2.1

4.6.2.1 Overview

The following modules are new parts for the Tricon System Version 10.2.1:

- Analog Input Module - single ended (64 points), model AIS 3720; Version number 6200, Build 92
- Digital Output Module (32 points), model SDO 3625; Version number 6213, Build 92

The Single-Ended Analog Input Module AIS 3720 and the Digital Output Module SDO 3625 are part at the Triconex Invensys "Next Generation" Input / Output Modules (NGIO) development.

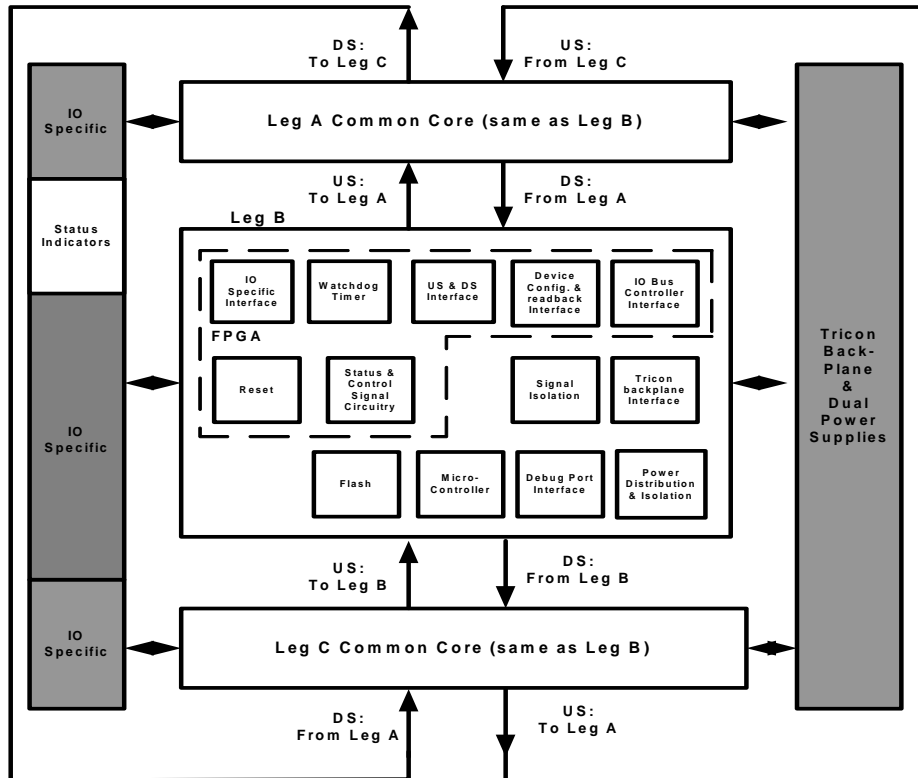
Both modules are part of the approval for release 10.2.1. All NGIO Modules have the same "core" architecture. The NGIO Modules are compatible to the existing certified Tricon I/O Modules [P1, P2].

The common core has been designed to support the Next Generation IO modules, Tricon V9.6+ systems, Tristation TS1131 V3.2+, Tricon/Trident Firmware manager, and redundant power supplies. It provides common features to all NGIO modules.

The common core is a Triple Modular Redundant (TMR) architecture which allows the Main Processors (MP) to interface to specific types of inputs and/or outputs. Detailed information about the NGIO core can be found in the NGIO Core HW Design Specification [H9].

The picture below gives a more detailed overview of the internal architecture of the NGIO Module:

Analog Input Module-Single-Ended (AIS 3720)



Picture 1: Overview of the internal architecture of the NGIO Module

The AIS 3720 provides an interface between the field devices and the Tricon System. Each analog input is triplicated and isolated to meet the design requirements for the TMR. The NGAI reads single ended voltage inputs from a Tricon ETP. The analog voltages are signal conditioned, converted to digital data, and communicated to the Main Processor via the Tricon IO bus.

The basic operation of the NGAI module is to act as a triple redundant interface between the field analog inputs and the common core. The NGAI conditions the inputs, samples and scales the data, converts the analog data to digital data and stores the results in FPGA memory, which can then be read by the common core microprocessor on a per leg basis. The single version consists of two banks of 64 differential inputs. Detailed information about the AIS 3720 can be found in the NGAI Hardware Design Specification [H16].

Digital Output Module (SDO 3625)

The NGDO Module provides 32 output channels (24 VDC TMR digital outputs) to the field. The interface between the Common Core Design and the field load circuitry is through the Tricon backplane. Commands from the Field Software to toggle switch outputs, light LEDs or perform diagnostics on the field circuitry are physically executed in the NGDO Field Hardware. The NGDO Field Hardware maintains status that enables the Field Software to verify execution of commands and verify hardware health. The Field Hardware consists of four functional subsystems:

- NGDO FPGA Subsystem
- Low Voltage Switch Interface Subsystem

- Front Panel Point & Load Fault LEDs
- High Voltage Output Switch Subsystem

Detailed information about the NGDO can be found into the NGDO Hardware Requirement Specification [H19] and and NGDO Hardware Design Specification [H21].

4.6.2.2 FMEA inspection of the Tricon Version 10.2.1

Within the framework of the hardware inspection of the AIS 3720 and SDO 3625 modules a FMEA was carried out by the manufacturer to check the failure control mechanisms and the implemented diagnostic functions. This was done by assuming representative failures and analyzing the effect of these failures. Where necessary the analysis was extended to system level if the fault detection was assured by the structure of system or by the operating software. The FMEA was completed by fault insertion for those cases where an analysis could not lead to definite results. In addition the Test Institute has performed witness tests together with the manufacturer.

Results:

The design analysis of the AIS 3720 and SDO 3625 module has shown, that the module can be used in the Tricon System Version 10.2.1. The results of the FMEA are documented in the document "Failure Mode and Effect Analysis with Diagnostics Analysis" [H36].

All assumed or inserted failures, which have been inspected within the FMEA, result in fault detection or the system reacted to the safe state (shut down).

4.6.2.3 Inspection of the reliability data and PFD calculation

The basic failure rates were computed using the Parts Count Method of the Bellcore, Issue 6 Model.

The Triconex Invensys spreadsheets [H32, H33] calculates the PFDavg and MTTFspurious with a common cause factor of Beta equal to 1 %. This Beta value was computed using the Beta determination technique described in the IEC 61508 Part 6 standard. Finally the spreadsheet assumes the MTTRot (mean time to repair) is 8 hours and TI (the proof test interval) is one year.

The spreadsheet [H33] can be used to calculate PFDavg and Safety Availability by entering the user configuration data. The speed sheet provides also the input data and results for the MTTFspurious calculations.

The PFDavg will be computed for an I/O configuration that is required for a typical safety shutdown function. A typical safety shutdown function normally requires a few digital and/or analog inputs and a few digital or analog outputs. A conservative calculation of PFDavg can typically be made by using one or two input modules and one output module.

The MTTFspurious will be calculated using all the I/O modules in the TRICON system configuration that could cause a shutdown of part or all of the process being protected by the TRICON controller.

The spreadsheet also calculates the Average Safe Failure Fraction using the configuration data that is used to calculate the MTTFspurious.

Results:

The inspection of the spreadsheet and the associated documents [H30] to [H37] have been inspected by the Test Institute with a positive result.

4.6.2.4 Inspection of the electrical safety

The inspection of the electrical safety of the AIS 3720 and SDO 3625 modules was observed under the requirements of IEC 61131-2 [2] and EN 50178 [3] (Electronic Equipment for use in power installations). The safety related modules must fulfil the requirements.

Result:

The results of the inspection are documented in [H38]. The defined over voltage category for the Tricon System is II. The pollution degree is 1 due to conformal coating. The PCB material is FR4 and therefore has a group IIIa ($175 \leq CTI \leq 400$ comparative tracking index) according to EN 50178. The protection against direct contact is not required because the PCBA is isolated from direct contact via the following mechanisms:

- When inserted in a Tricon chassis there are no exposed conductive parts. The front face exposed to the user is protected with a non-conductive anodize
- The PCBA mounting holes around the perimeter of the PCB are metal plated and connected to chassis ground via connector J3. Signals are separated from chassis ground by the minimum space between copper clad surfaces of 0.009".

The different PCB Gerber Files have been verified by the Test Institute. The practical test (e.g. dielectrical withstand test, verification of clearance and creep age) have been performed in line with the IEC 61131-2. The results are documented in the Environmental and EMC Test Report [P7]. The AIS 3720 and SDO 3625 fulfil the requirements concerning the electrical safety.

4.6.2.5 Inspection of environmental and EMC Tests

The environmental and EMC tests for the NGIO Modules have been performed by the Test Institute according to the requirements of IEC 61131-2 (Programmable Controllers, Equipment requirements and tests) [2] and EN 54-2 (Fire detection and fire alarm systems Part 2: Control and indicating equipment) [10].

The environmental and EMC tests were finished with a positive result. The results are documented [P7].

4.6.3 Software inspection of the Tricon Version 10.2.1

4.6.3.1 Overview

The Tricon System Version 10.2.1 contains the following new firmware releases:

- new firmware for the AIS 37201 analog input module - single-ended
Version number 6200, Build 92
- new firmware for the SDO 3625 digital output module - supervised
Version number 6213, Build 90

4.6.3.2 Inspection of the AID 3721 firmware

The development lifecycle for the NGIO firmware follows the software V-model of IEC 61508 and has been carried out considering the measures to avoid failures according to the IEC 61508, part 3 [1].

Based on the system requirement and architecture specifications [H3-H6, H8] a NGIO software requirement specification has been prepared [H10]. These requirements form the input for a core architecture and design specification [H12] which is common for all NGIO modules.

This core documents are the bases for further detailed architecture and design documents for each of the different IO design [H13, H15, H17, H18, H20, H22].

As part of the verification and validation (V&V) activities, a project and software quality assurance respectively a software V&V plan were defined by the manufacturer [H23 - H25]. Further detailed test plans and specifications related to E/E/PES integration test, system and unit level test as well as fault insertion test are listed and compiled in [H1].

Results:

The software architecture and design has been reviewed together with the manufacturer and evaluated regarding safety relevant aspects.

Corresponding to software design and development the V&V activities have been reviewed and witnessed considering the test coverage.

The V&V results [H1] have been reviewed for completeness and accurateness.

The review of the software development process and the theoretical review of the design and development of the AIS 3720 and SDO 3625 modules was finished with a positive result.

5. Summary

The carried out tests and analyses have shown that the new AIS 3720 and the new SDO 3625 modules can be used for applications up to SIL 3 according to IEC 61508, IEC 61511.

The Tricon Version 10.2.1 still can be used for applications up to SIL3 according to IEC 61508, IEC 61511.

The report-no.: 968/EZ 105.03/01 for Tricon Version 9.6 and report-no.: 968/EZ 105.04/05 for Tricon Version 10 remain valid.

Application programs must be created using the Tristation V4.1 and higher considering the guidelines specified in the Safety Consideration Guide [H39] and the Developer's Guide TriStation 1131 [H40].

All conditions, which the user must comply with for safely using the products, are described in detail in the corresponding manuals [H39 - H41].

The actual valid hardware and software versions should be retrieved from the currently valid module and firmware release list. The list is released together by the manufacturer and the Test Institute.

Cologne, 2006-10-31
TIS/ASI/Kst. 968 bu-sn-la

The inspectors

A handwritten signature in blue ink, appearing to read 'J. Schön'.

Dipl.-Ing. Jürgen Schön

A handwritten signature in blue ink, appearing to read 'Oliver Busa'.

Dipl.-Ing. (FH) Oliver Busa