TRICONEX

September 25, 2001

Document Control Desk
United States Nuclear Regulatory Commission
Washington, DC 20555

Subject: Nuclear 1E Qualification of the TRICON TMR Programmable Logic Controller
             (PLC) – Additional Information – TÜV Report for TRICON Version 9.5.3

References: 1. Letter, T. Martel (Triconex) to NRC, March 20, 2001, subject; Nuclear 1E
             Qualification of the TRICON TMR Programmable Logic Controller (PLC) –
             Inclusion of Recent Upgrades in NRC Qualification Review.

             2. Project Number 709

Gentlemen:

As part of the NRC review of the TRICON qualification documents, various product certification
reports by an independent certifying agency, TÜV Rheinland, were reviewed by the Staff. In
earlier correspondence (Reference 1, et. al.), Triconex requested that TRICON Version 9.5.3 be
considered as the 1E qualified TRICON system. Since the TÜV report for this version was not
available when the Staff visited our Irvine CA facility earlier this year, we agreed to forward a
copy of the TÜV Report and Certification for TRICON V9.5.3, when available.

Accordingly, we are enclosing for your information and review, TÜV Report No. 968/EZ
105.02/01 for TRICON V9.5.3, and also a copy of the TÜV Certificate for this product version. If
you have any questions or wish further information, please contact me at (281) 360-6401 or Mr.
Michael Phillips at (949) 885-0711.

Sincerely,

J. Troy Martel, P. E.
Triconex Nuclear Qualification Project Director

DO62

Enclosures
cc: L. Raynard Wharton, NRC
      P. Loeser, NRC

invensys

An Invensys Company

TÜV Rheinland / Berlin-Brandenburg

TÜV

TÜV Anlagentechnik GmbH
Automation, Software und Informationstechnologie

ZERTIFIKAT
CERTIFICATE

Nr./No. 968/EZ 105.02/01

Prüfgegenstand Product tested	TRICON (Triple Modular Redundant (TMR) Controller) Version 9.5.3; TriStation 1131 Version 3.1.2 (Including CEMPLE 3.1.2); TriStation MSW 3.1.2		Hersteller Manufacturer	TRICONEX Corporation Invensys Process Automation (IPA) 15345 Barranca Parkway USA-Irvine. California 92618 United States of America
Typbezeichnung Type designation	3006/3006N, 3007 (EMPII), 3504E/3504EN, 3505E/3505EN (Dig.In), 3604E/3604EN, 3607E/3607EN (EDO), 3623T/3623TN (SDO KV), 3700, 3700A/3700AN (AI), 3704E/3704EN (HDAI), 3805E/3805EN (EAO), 4200-3, 4201-3 (RXM), 4409 (SMM), 3515 (PT), Power Supplies, Chassis, TRICON Interface Library*.	3501T/3501TN (EDI KV), 3564 (FSDI), 3614E, 3615E, (ESDO) 3624/3624N (SDO), 3701/3701N, 3701A (AI), 3706A/3706AN (NITC), 4119 (EICM), 4210/4210N, 4211/4211N (SRXM), 4609/4609N (ACM), 3636T/3636TN (ERO), Termination Products: Triconex Library*.		3502E/3502EN, 3503E/3503EN (EDI), 3603T/3603TN (EDO KV), 3617E (ESDO), 3664 (FSDO), 3703E/3703EN (EIAI), 3708E/3708EN (EITC), 4119A/4119AN (EICM), 4329/4329N (NCM), 3674 (DDO FS, CARS), 3601T/3601TN. IEC 1131-3 Standard Library*
	*for TriStation 1131 Version 3.1.2			
Verwendungszweck Intended application	Safety relevant applications according to requirement class 6 (DIN V 19250) and DIN VDE 0116.			
Prüfgrundlagen Codes and standards forming the basis of testing	DIN V VDE 0801/01.90; DIN V VDE 0801/A1 10/94; DIN VDE 0116/10.89; IEC 61131-2/1992; DIN VDE 0110/01.89; DIN V 19250/05.94; IEC 801 Part 1 - 5; DIN EN 54, part 2/1997-12 Components of automatic fire detection systems.			
Prüfungsergebnis Test results	Suitable for safety related applications according to requirement classes 1 - 6 (DIN 19250) according to the test report no. 968/EZ 105.02/01.			
Besondere Bedingungen Specific requirements	The shutdown function and the user software must be tested individually for each application. For the use of the TRICON controller the safety manual "Safety Consideration Guide", Version 9 Tricon Systems, in the Triconex user documentation has to be considered.			

Der Prüfbericht Nr. 968/EZ 105.02/01 vom 2001-09-17 ist Bestandteil dieses Zertifikates.
Der Inhaber eines für den Prüfgegenstand gültigen Genehmigungs-Ausweises ist berechtigt, die mit dem Prüfgegenstand übereinstimmenden Erzeugnisse mit dem abgebildeten Prüfzeichen zu versehen.

The test report No. 968/EZ 105.02/01 dated 2001-09-17 is an integral part of this certificate.
The holder of a valid licence certificate for the product tested is authorized to affix the test mark shown opposite to products which are identical with the product tested.

TÜV Anlagentechnik GmbH
Geschäftsfeld ASI
Automation, Software und Informationstechnologie
Am Grauen Stein, 51105 Köln
Postfach 91 09 51, 51101 Köln

2001-09-17

Datum/Date

Firmenstempel/Company seal

M. Schmidt

Unterschrift/Signature

Automation, Software and Information Technology

Type approval of TRICON version 9.5.3

Report-No.: 968/EZ 105.02/01
Date: 2001-09-17

Type approval of TRICON version 9.5.3

Report-No.:	968/EZ 105.02/01
Date:	2001-09-17
Pages:	24
Test object:	TRICON version 9.5.3
Customer/Manufacturer:	Triconex Corporation Invensys Process Automation (IPA) 15345 Barranca Parkway USA-Irvine, California 92618 United States of America
Order date:	2001-02-05
Order no.:	K61431
Test Institute:	TÜV Anlagentechnik GmbH Automation, Software and Information Technology Postfach 91 09 51 D-51101 Köln Am Grauen Stein D-51105 Köln
Department:	Automation, Software and Information Technology
TÜV-Offer-No./Date:	Email dated 2001-01-29
TÜV-Order-No./Date:	968/963017 dated February 2001
Inspectors:	Dipl.-Phys. Ekkehard Pofahl Dipl.-Ing. Johannes Buschmann Dipl.-Ing. Johannes Janssen Dipl.-Ing. Jürgen Klassen
Test location:	see Test Institute
Test duration:	February 2001 - September 2001

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

Contents

1. **Scope**

Subject of the type approval is the programmable logic controller (PLC) TRICON version 9.5.3. The TRICON version 9.5.3 consists of the TRICON hardware, the TSX operating system and the software TriStation 1131 and TriStation MSW. The TRICON is built as a Triple Modular Redundant (TMR) Controller.

In version 9.5.3 the module replacement for the obsolete microprocessor, which is used for some I/O boards, was introduced.

New N model numbers have been introduced for Tricon modules intended for nuclear application. The modules themselves do not differ from the original module, but now all nuclear module numbers can be referenced by attaching the letter "N" to the former type designation.

The TRICON is to be installed in safety relevant areas up to and including requirement class 6 according to standard DIN V 19250 [1] and according to standard DIN VDE 0116 [3].

The TRICON, equipped with fail-operational modules, will also be installed in safety related systems, where the low (0) state is typically not the safe state, as for example in Fire & Gas Applications.

During the type approval it must be shown, that the TRICON version 9.5.3 fulfils the requirements for safety equipment in accordance with requirement class 6 to standard DIN V VDE 19250 [1], resp. DIN V VDE 0801 [2].

All steps of the type approval are defined and documented by a test plan according to the Quality Assurance Guidelines QME 27 of the Business Sector Automation, Software and Information Technology of TÜV Anlagentechnik GmbH.

2. **Codes and standards**

[1]   DIN V 19250/05.94
      Grundlegende Sicherheitsbetrachtungen für MSR-Schutzeinrichtungen

      Fundamental Safety Aspects To Be Considered For Measurement And
      Control Protective Equipment

[2]   DIN V VDE 0801/01.90
      Grundsätze für Rechner in Systemen mit Sicherheitsaufgaben
      Änderung A1: Oktober 1994

      Principles For Computers In Safety Related Systems
      Amendment A1: October 1994

[3] DIN VDE 0116/10.89
     Elektrische Ausrüstung von Feuerungsanlagen

     Electrical Equipment Of Furnaces

[4] IEC 1131-part 2/1998 (Draft), EN 61131-2/May 1995
     Programmierbare Steuerungen
     Teil 2: Betriebsmittelforderungen und Prüfungen

     Programmable Controllers
     Part 2: Equipment requirements and test

[5] DIN EN 50178/04.1998
     Ausrüstung von Starkstromanlagen mit elektronischen Betriebsmitteln

     Electrical equipment for use in power installations

[6] DIN IEC 68
     Grundlegende Umweltprüfverfahren

     Basic environmental testing procedures

[7] EN 50081-2:1993
     Elektromagnetische Verträglichkeit (EMV): Fachgrundnorm Störaussendung;
     Teil 2: Industriebereiche

     EMC Requirements,
     Generic emission standard, industrial environment

[8] EN 61000-6-2:1999

     Elektromagnetische Verträglichkeit (EMV) - Teil 6-2: Fachgrundnormen -
     Störfestigkeit im Industriebereich

     EMC requirements
     Generic immunity standard, industrial environment

[9] DIN EN 54, Teil 2, Januar 1990 (Entwurf/Draft)
     Bestandteile automatischer Brandmeldungen, Brandmelderzentralen

     Components of automatic fire detection systems; control and indicating
     equipment

[10] Europäische EMV Richtlinie 89/336/EWG
     European EMC-directive 89/336/EWG

3.   Object of inspection

3.1   Description of the TRICON triple modular redundant controller

The TRICON is a fault tolerant controller based on Triple-Modular Redundant (TMR) architecture. The basic TRICON architecture is fully triplicated throughout, from the input modules through the Main Processors to the output modules.

Every I/O Module houses the circuitry for three independent legs. Each leg on the input modules reads the process data and passes that information to its respective Main Processor. The three Main Processors can communicate with each other using a proprietary high-speed bus system called the TRIBUS.

Once per scan the three Main Processors synchronize and communicate with their two neighbours via the TRIBUS. The TRIBUS votes digital input data, compares output data, and sends copies of analog input data to each Main Processor.

The TRIBUS also sets flags to indicate discrepancies and disagreements found during the TRIBUS comparison and voting operations. The Main Processors use these flags to diagnose problems on the input modules and the Main Processors.

The Main Processors execute the control calculations and compute outputs which are sent to the output modules. In addition to voting the input data, the TRICON votes the output data. This is done on the output modules as close to the field as possible, to correct any errors that could occur between the Main Processor and the final output driven to the field.

TRICON Architecture
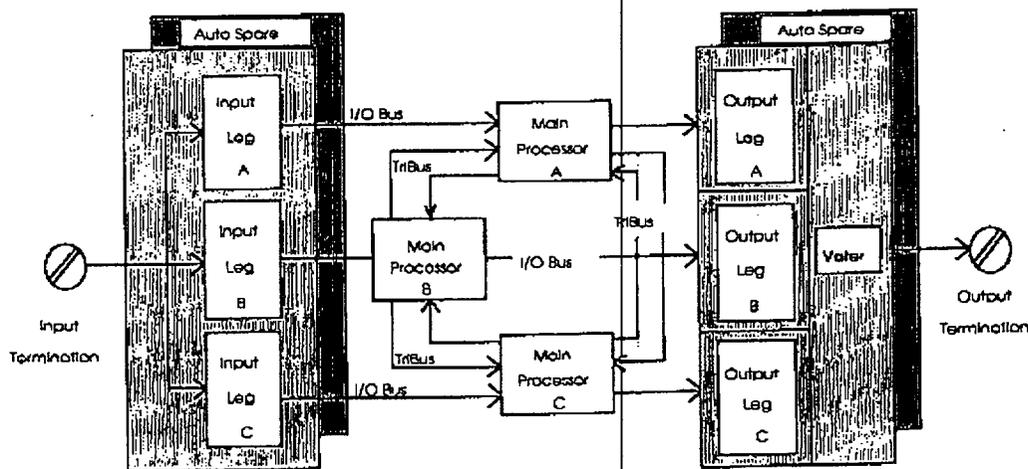
By these measures, especially by complete comparison of all results between the three legs, it is guaranteed, that each active fault is found and voted out after at least two cycle times.

The digital input modules contain three completely independent microprocessors with associated input circuitry which provide three independent readings of the digital inputs connected to the module.

The digital input module checks for "stuck ON" or unsafe conditions on each digital input on each I/O leg. The "stuck ON" test routine periodically zeroes the inputs to the optical isolation equipment on each input and checks for proper zero input reading through the optical isolation circuitry. The High Density Digital Input Module 3504E checks also for "stuck-OFF" conditions.

The digital output modules contain three independent microprocessors which receive commanded outputs from the three Main Processors and send each digital output to a fault tolerant "quad" output voter circuit. The output voter circuit consists of two independent switching paths with two switches in each path. This voter circuit ensures the correct output even in the presence of a single fault in the voter. The three microprocessors on the digital output module continuously run diagnostics on the output voter circuit to check for shorted or open switches.

The analog input modules are also fully triplicated and each leg contains multiple voltage references which allow the analog inputs to be calibrated automatically.

The TRICON provides two physical I/O slots for each functional I/O slot in the system. If a fault is detected on an I/O module, the module can be replaced without effecting the system operation by inserting a spare module in the second slot provided next to the faulty module.

When the newly inserted module takes over operation, the inactive faulty module can be removed for repair. The TRICON system also provides automatic hot repair of a faulty module if a spare module is provided in the second I/O slot of the functional I/O slot.

Each chassis houses two power supply modules. They are arranged in a dual-redundant configuration so that each power supply is individually capable of supporting the power requirements of all the modules in that chassis. Each leg on every I/O module derives power from both power supplies using independent power regulators. Thus in the event of a power supply failure all legs of all I/O modules continue to operate as they can derive power from the other power supply.

3.2 Application dependent system states

From all possible applications where the triplicated Triconex PLCs may be used there are two typical classes:

- Emergency Shutdown Systems (ESD systems)
- Continuous Run Systems (CR systems), e. g. Fire & Gas Applications.

For an ESD system, depending on the application class, it may not be allowed to continue operation with only one channel, if the other two channels have failed. This is true for applications equal to or higher than class 5. It is safer to shut down the process to the safe state than to continue operation with only one channel in operation.

This is not true for CR systems (e. g. Fire & Gas Systems). Typically there is no safe state in these systems. Therefore a typical fire detection system may continue operation with only one channel after losing the two other channels. The safety is not increased by shutting the system down. However, after degradation from two channels to one channel there must be a higher alarm level to the operator about the system state.

The triplicated TRICON architecture consists of three channels. Each channel consists of one input leg, one main processor and one output leg. The TRICON controller is designed to continue operation after failures. These failures may occur in an input leg, in a main processor, or in an output. All failures are transparent to the application program; the programmed logic will be executed regardless of detected failures.

A set of system variables is implemented within the TRICON to determine the state of the system. These variables allow an exact fault localization. Besides these fault specific variables, there are variables built into the TRICON system to determine, how many "sane" channels, from input through main processor to output, are working in the system. The calculation for these variables takes into account the loss of an I/O channel, a main processor, or any combination of these. These variables indicate if the system is operating, from the input to the output, with three channels, two channels or one channel. They allow an easy configuration of the application- (user-) program for either ESD or Fire & Gas Applications.

The user program has to be developed to consider the different states of operation of the TRICON. The TRICON user documentation gives guidelines how to use these variables for the different applications in either ESD or Fire & Gas applications.

Extensive self tests are executed internally to allow exact failure localization.

3.3 Modules for version 9.5.3

The following modules are part of version 9.5.3.

Model-No.	Name of module
	TriStation 1131 version 3.1.2 (including CEMPLE)
	TriStation MSW 3.1.2
	IEC 1131-3 Standard Library version 3.1.2
	TRICON Interface Library version 3.1.2
	Triconex Library version 3.1.2
3006/3006N	Enhanced Main Processor, 2 Mbyte SRAM (EMP II)
3007	Enhanced Main Processor, 1 Mbyte SRAM (EMP II)

Model-No.	Name of module
3501T/3501TN	Enh. Digital Input 115 V AC/DC HighKV
3502E/3502EN	Enh. Digital Input 48 V AC/DC (EDI)
3503E/3503EN	Enh. Digital Input 24 V AC/DC (EDI)
3504E/3504EN	High Density Digital Input, 24/48 VDC (HDI)
3505E/3505EN	Enh. Digital Input 24 VDC, low Threshold (Dig.In)
3515	Pulse Totalizer Module (PT)
3564	FSDI, Fail Safe Digital Input 24 V (FSDI)
3601T/3601TN	Enh. Digital Output 115 V AC non commoned HighKV (EDO)
3603T/3603TN	Enh. Digital Output 120 V DC HighKV (TSDO)
3604E/3604EN	Enh. Digital Output 24 V DC (EDO)
3607E/3607EN	Enh. Digital Output 48 V DC (EDO)
3614E	Enh. Superv. Digital Output 24 VDC (ESDO)
3615E	Enh. Superv. Digital Output 24 VDC, Low Power (ESDO)
3617E	Enh. Superv. Digital Output 48 VDC (ESDO)
3623T/3623TN	Enh. Digital Output 120 V DC Supervised HighKV (TSDO)
3624/3624N	Supervised Digital Output 24 V (TSDO)
3636T/3636TN	Relay Output Dry contact HighKV (ERO)
3664	Fail Safe Digital Output 24 V (FSDO)
3674	Fail Safe Digital Output 24 V (DDOFS, CARS)
3700, 3700A/3700AN	Analog Input (0-5 VDC) (AI)
3701/3701N, 3701A	Analog Input (0-10 VDC) (AI)
3703E/3703EN	Isolated Analog Input Module 0-5/0-10 V DC (EIAI)
3704E/3704EN	Analog Input (0-5/0-10 VDC) (HDAI)
3706A/3706AN	Non Isolated Thermocouple Input (NITC)
3708E/3708EN	Isolated Thermocouple Input Module (EITC)
3805E/3805EN	Enhanced Analog Output Module (4-20 mA) (EAO)
4119, 4119A/4119AN	Enhanced Intell. Comm. Module (EICM)
4200-3	Primary RXM Module (RXM)
4201-3	Remote RXM Module (RXM)
4210/4210N	Primary Single Mode Fiber Optic RXM (SRXM)
4211/4211N	Remote Single Mode Fiber Optic RXM (SRXM)
4329/4329N	Network Communication Module (NCM)
4409	Safety Manager Module (SMM) for Honeywell's Universal Control Network (UCN)
4609/4609N	Advanced Communication Module (ACM)
8110	High Density Main Chassis
8111	High Density Expansion Chassis
8112	High Density Remote Expansion Chassis
8310	120 VAC/VDC High Density Power Module
8311	24 VDC High Density Power Module
8312	230 VAC High Density Power Module
	Power Supplies
	Chassis
	Termination Products

3.4 Documentation

All the documentation related to revision 9.5.3 is available as printout and in electronic form.

The specific revision levels are documented in the following release definitions:

6200003-120 SRD 9-5-3 Release (for overall system), release 1.2, September 2001, 8 pages

6200097-006 SRD TS1131 (for TS 1131), 12. September 2001, 18 pages

4. Performed inspection and results

4.1 General remarks

The inspection of the Tricon was done in a incremental way. This incremental approval consisted of

- checking new boards, as they became available

- checking of new hardware and firmware revisions

- spot-checking of Triconex internal quality measures to ensure constant products

- checking of product updates

In the following chapters the procedure is described.

4.2 Hardware inspection of the TRICON modules

4.2.1 Theoretical hardware inspection

4.2.1.1 Hardware documents

For all modules the following documents were checked

- functional description, data sheets

- hardware design specification

- input, output and bus specifications

- schematics

- detail PCB

- layouts

- material/part list

- test specification

- test procedures

- PAL equations

- fault insertion procedure

- assembly, module

- approved vendors and manufacturers list (parts, PCBs)

- quality assurance procedure for this documentation

The documents are complete and correct. All documents are consistent with one another and with the modules. The data-sheets contain all relevant information needed for installation to any application.

4.2.1.2 Design analysis

Base for the design analysis are the concept papers together with the actual schematic. The design is checked to be fit for purpose.

Hardware sections that are equivalent among different modules were checked once thoroughly. The corresponding sections of the derived module were accepted without major further inspections.

Used ASIC circuitry's were inspected for compatibility with the surrounded areas.

The functions of the modules according to the manufacturers specification were checked within the functional and environmental tests according to IEC 1131-2 [4].

No design problems were found during this process.

4.2.1.3 Failure consideration and failure mode and effect analysis (FMEA)

The safety of the TRICON controller systems depends on the redundant (triplex) structure and on the high effective diagnostic system implemented to the TRICON operating system.

Based on the structure and diagnostics the TRICON controller system has the ability to control any single fault and to detect dormant faults.

The fault behaviour of the TRICON system and of the modules was checked by the method of an FMEA (Failure Mode Effect Analysis).

For each fault assumed it was checked by analysing the behaviour of the system or of the relevant portion of the diagnostic system if the fault would be controlled or detected respectively. The results of this theoretical inspection were compared with fault insertion lists of the manufacturer, which are based on an extensive fault insertion procedure carried out on a TRICON system.

Faults for which the FMEA method did not lead to an clear result and which were not considered by the fault insertion procedure of the manufacturer were listed and presented to the manufacturer for further steps of the fault insertion procedure.

It has been proved that all assumed and inserted faults are controlled by the triplex structure or by the fault diagnostics respectively.

4.2.2 Practical hardware Inspections and tests

4.2.2.1 Inspection of unassembled and assembled modules

For all modules the following was inspected:

1. Visual checks of the assembled board

   - identification of the modules

   - consistency between modules and modul documentation

   - quality of manufacturing

     - clearness
     - correctness of soldering
     - positioning of the components

2. Visual checks of the unassembled boards (PCBs)

   - inspection of the clearance and creepage distances according to the requirements of EN 61131-2 with respect to the working voltage, overvoltage category II and pollution degree 2

   - quality of manufacturing

The clearance and creepage distances of the modules fulfil the requirements of the standard EN 61131-2.

The manufacturing of the modules is correct and without any visual faults.

4.2.2.2 Environmental and EMC tests

The following environmental tests according IEC 1131-2 [4] were carried out in the laboratory of TUV Rheinland Anlagentechnik GmbH, Cologne.

The performed tests are listed in the following table:

Title	Used standard	Used severity	PLC operation
Cold, test Ab	IEC 60068-2-1	-25°C, 96 h	no
Dry heat, test Bb (Bc)	IEC 60068-2-2	+70°C, 96 h	no
Shock, test Ea	IEC 60068-2-27	halfsine, 15 g, 11 ms. 3 shocks in each axis	yes
Change of temperature, test Nb	IEC 60068-2-14	low temperature: 5°C high temperature: 55°C 5 cycles, 1 degree/minute	yes
Damp heat, cyclic test Db	IEC 60068-2-30	high temp.: 55°C, non-condensing variant 2, cycles: 2 cycle 1 cycle 2	no yes
Vibration, test Fc	IEC 60068-2-6	range 1: 10 - 31 Hz @ 1 mm pp, range 2: 31 - 500 @ 1 g speed: 1 oct./min. cycles: 10 in each axis	yes
Electrostatic discharge	IEC 801-2	level 3: 8 kV (air) 4 kV (contact) > 10 positive and > 10 negative discharges for each test point R = 330 Ohm C = 150 pF	yes
Burst	EN 50 082-2 IEC 801-4	levels: + signal lines: (capacitive coupling) analog and digital I/O-lines (fig 5): class 3 (1 kV) + 2 kV + power lines: (direct coupling) AC or DC: class 3 (2 kV) duration: > 30 sec.	yes
Surge Shape of pulses: 1,2 μs/50 μs free running 8 μs/20 μs shorted	IEC 801-5	power lines 110 V: **level 3: (2 kV, 4 kV PE)** power lines 24 V, signal lines, analog and digital I/O-lines: **level 2: (1 kV, 2 kV PE)** pulses: AC: 4 @ 0,90,270 Degree. DC: 5 positive and 5 negative. Steps of 250 Volt until target level	yes
Conducted disturbance	EN 50 081-2 EN 55 011: KI A	0,15 - 0,5 MHz 79 dBμV (QP) 66 dBμV (Av) 0,5 - 5 MHz 73 dBμV (QP) 60 dBμV (Av) 5 - 30 MHz 73 dBμV (QP) 60 dBμV (Av)	yes

Title	Used standard	Used severity	PLC operation
Radiated disturbance	EN 50 081-2 EN 55 011 : KI A	30 - 230 MHz 40 dBμV/m 230 - 470 MHz 47 dBμV/m 470 - 1000 MHz 47 dBμV/m	yes
Conducted immunity	EN 50 082-2 ENV 50 141	0,15 - 80 MHz > 240 steps per dec. 10 V (rms) Modulation AM 80 %, 1 kHz	yes
Immunity radiated fields	EN 50 082-2	80 - 1000 MHz > 240 steps per dec 10 V/m horizontal and vertical Spot frequency 900 +/- 5 MHz Modulation Pulse, 50 % duty rate 200 Hz repetition rate	yes
Voltage dips	EN 50 082-2 EN 61 000 - 4-11	- 30 % 10 ms - 95 % 5.000 ms +/- 10 % > 1 minute - 60 % 100 ms	yes

The tests of radiated and conducted emissions was done as a part of the compliance testing for the European CE mark. The test system used for this testing included all representative modules.

4.2.2.3 Testing according to EN 54

The standard EN 54 "Components of automatic fire detection systems; control and indicating equipment" [9] was chosen as the guideline to qualify the TRICON also for use in fire and gas applications. Characteristic for these applications is, that normally no safe state of a fire&gas signalling central is defined. Specifically the safety is not increased by removing power from a fire&gas central.

The set of tests, which is defined in this standard, was included in the earlier described suite environmental and electromagnetic compatibility tests.

The test high humidity (95 % humidity), 21 days, at 40° Celsius, without operation, was done to show, that the equipment can withstand high environmental stress.

4.2.2.4 Functional tests according to IEC 1131-2

The behaviour of the approved modules was tested according to the data specified in the manufacturers documentation with respect to the requirements of the standard IEC 1131-2.

For discrete input modules:

- test and verification of input characteristics
- test of the thresholds for 0/1- and 1/0-transition
- reversal input polarity test

- inspection of sufficient isolation between leg inputs (input impedance)
- di-electrical withstand test/Hi Pot test with respect to the working voltage of the module
- check for the right status indications
- check of the right switching over to hot stand by modules in cases of faults

For discrete output modules:

- test and verification of the output characteristics
- test of the specified values for current ranges and voltage drops
- test of the behaviour under overloaded situations
- dI-electrical withstand test/Hi Pot test with respect to the working voltage or specification respectively
- check for the right status indications
- check of the right switching over to hot stand by modules in cases of faults

For analog input modules:

- test and verification of input characteristics
    - range
    - resolution/accuracy
    - overrange protection
- inspection of sufficient leg isolation
- check for the right status indications
- check of the right switching over to hot stand by modules in cases of faults

For the counter modules the right counting function of the module was tested by connecting the inputs of the module to two pulse outputs of a pulse converter module. The pulse converter module converted the incoming pulse of an stabilized pulse generator to a low pulse with a minimum pulse width (300 μs) and a high pulse with a minimum pulse width. In addition the high level or the low level respectively were varied by variable resistors.

All 32 counter of the module were connected alternatively to the pulse converter. Different alarm level values were set for all 32 counter. Every time if a counter reached the alarm level the point number and the level were printed out together with a time stamp. The right counting was checked by comparison of the stamped time distance between 2 following print outs of the same counter with the expected time.

4.3 Software Inspection of the TRICON

The correct operation of the TRICON depends on correct software, which is used in several areas of the TRICON.

The software of the TRICON can be divided in the development software (ladder-editor MSW and TriStation 1131) and the software/firmware on the TRICON hardware.

4.3.1 Theoretical software inspection

During the theoretical software inspection all specifications for the software and for the internal communication protocols were investigated to prove the correctness of the documents and to find deviations between specification and other documentation.

The inspections were carried out on the basis of the following documents:

- Triconex Software Coding and Practices Guideline
- TriStation 1131 software requirements specification
- Specification and Test documents for each module
- CFLOW evaluations, partly contained in the description documents
- ProMet evaluations for assembly programs
- Source code in machine readable form

4.3.1.1 Documentation

The code specific documentation (besides the general documentation on software development) is divided into the main areas of operating system TSX for TRICON, firmware for the I/O modules and the software TriStation 1131, which provides the user interface.

Object of closer investigation was the TSX operating system and the I/O module firmware documentation. Here it was checked, that every software module is sufficiently described in a specification document and that the source code is implemented according to the specification. Also the documents describing the test verification procedures for the I/O modules and the Main Processor modules were investigated.

The documentation is sufficient and complete.

4.3.1.2 Operating system TSX

The operating system resident in the TRICON is called TSX. The TSX operating system is responsible for the basic functions as for example keeping track of the internal clock and all fundamental functions. It is located on the main processor boards on the TRICON.

By analysis it was investigated, that TSX ensures the comparison of all results between the Main Processors every cycle. By this measure every failure which leads to a different result in one of the channels is detected in the 2 and 3 Main Processor operation mode.

4.3.1.3 Module firmware

The firmware of the modules is partly developed in the language "C", partly in assembly language. The specification documents for each module were investigated to check, that the firmware is able to provide the function and to have a high diagnostic coverage to detect broken parts and other problems in the hardware.

Static analysis tools were used to investigate the final coded software.

The firmware of all modules was investigated with positive result.

4.3.2 Practical software Inspection

During the practical software inspection it was shown that the implemented programs are in conformance to the specifications. This was done as described in the following procedures.

4.3.2.1 TriStation 1131

TriStation is the PC based software to develop, compile and test application programs. It was developed to conform to the PLC standard IEC 1131- part 3, programming languages.

It forms the user interface to the system during the development of the application program. All programs, which were used for the hardware and software tests, were developed using TriStation during the inspection. By this procedure the TriStation software was checked thoroughly together with the functionality of the provided programming languages (ladder diagram, function block diagram, structured text).

The inspection of TS1131 began in the early project state and included the assessment of the installed quality assurance methods for TS1131.

4.3.2.2 System security

TriStation 1131 provides a security system that defines users and their privileges with regard to editing, library changes, TRICON state changes and other operations.

It is possible to define 10 levels with a different set of privileges. Every user has to be introduced into the system by name and privilege. The access to TriStation 1131 is checked by a password.

A project log is kept, so that every change to the application can be traced down to the originator.

The security information is stored together with the other program data.

The security system is sufficient to protect application programs from unintended or unauthorized changes.

4.3.2.3 TriStation 1131 validation suite

A validation suite was developed to prove the correct operation of TriStation 1131. This development was done by the manufacturer (Triconex). A mirror installation was brought up at TÜV in Cologne to be able to repeat the testing.

The validation suite is divided in two major parts, the compiler and the library test. It is performed by automated tools. The results can be inspected by means of textual protocol files.

The validation suite worked and did not show faults or failures within the TriStation 1131 or the TRICON.

No safety critical errors or anomalies of TriStation 1131 software were found.

4.3.3 Feature tables

The IEC 1131 does not require, that a language has all elements, which are defined in the standard. It is mandatory however to have all elements listed in a so called feature table. This feature table summarizes, which element of the 1131 language is implemented.

These feature table can be found in the document TriStation, Software requirements specification, doc. no. 6200033-001, Revision 1.3, 1997-01-19.

4.3.4 IEC 1131 compliant languages

From 5 languages described in the standard IEC 1131-3 there are three languages chosen for TriStation 1131. A special feature of TriStation 1131 is, that modules from different languages can be compiled together to form an application program. From the possible languages the following are implemented:

- Ladder diagram
- Function block diagram
- Structured text

4.3.5 Intermediate code

The application program, which is written in one of the IEC 1131 languages, will be transformed in Intermediate code, which is readable ASCII format. This intermediate code is Pascal-like and is used by the compiler to produce the binary, which is loaded into the TRICON.

The production of the intermediate code is transparent for the user. The intermediate code files were checked during the software inspection.

This is a very powerful feature in tracing back application programs, should it be necessary. Specifically the transformation from graphical programming to traditional line-by-line code can be investigated.

Each project is defined by one project file. The project file is built as a container file and includes all project dependent information.

No anomalies were found.

4.3.6 Tricon library functions

The TRICON library elements can be used with any of the editors in TriStation 1131 to develop functions, function blocks, and programs for downloading to the TRICON controller.

The TRICON Library consists of the categories:

- Fire
- Ladder
- Logic
- Math
- Print
- Process
- System
- Time
- Utility

The Library to connect to the system services of TSX is mainly an interface. The basic functions of TRICON controller were not changed in order to process 1131 compliant programs. Some functions have been ported from assembly/C-language within the TSX-system to the library.

All elements are checked out by means of TS1131 validation suite.

No errors were found.

4.3.7 Black box tests

The TSX Functional Verification Procedure describes the checks of the TRICON. The procedure was repeated for some specific situations:

- Hard errors on I/O module
- Transients on I/O bus
- Download changes
- Key switch operation
- Rack maintenance variables.

The rest of the documented tests were inspected in a walk through procedure.

Additional tests, which were made independent of the documented procedure, included diverse manipulations on the PLC:

- withdrawal of I/O modules
- disconnection of power supplies
- shorting of the output signals
- shorting on the serial lines.

The Black box testing included different programs, which were developed for the environmental and EMC tests.

The result was as expected.

4.4 Integration testing/application program during the inspection

Several application programs were developed to show the correct behaviour of the modules. The programs were active during all functional and environmental tests. By these programs the correct and proper implementation of hardware dimensioning and software algorithms was checked by means of comparison between channels and checks against expected results. In addition the internal behaviour was logged constantly with an event logger.

4.5 Diagnostic measures

On all boards functional parts are subject to very sophisticated self tests. The components supervised include watchdog circuitry, ROM, RAM, dual-ported RAM, voltage regulators, bus driver circuits, optocoplers, voltage references and multiplexers.

In the following paragraphs board specific diagnostics are listed.

4.5.1 CPU

All used microprocessors perform extensive self tests. In addition all functional parts, specifically the TriBus, are subject to several diagnostic tests.

4.5.2 Input boards

On all input boards the diagnostics are designed in a way, to stimulate the actual inputs as far to the field as possible to verify the correct signals passing to the control program.

4.5.2.1 Digital input

For the digital input board special tests were implemented to detect the ability to see the "0" level. Several other tests check for cross talk effects on a bit level.

4.5.2.2 Analog input

On the analog input board several reference voltages are used to verify the correct operation of the analog to digital converters and the multiplexers.

4.5.2.3 Pulse totalizer module

Due to the redundant structure (triplex) the modules are fault tolerant and highly available. The online diagnostics implemented on the module is similar to the diagnostic implemented on the enhanced DI module with the exception that the inputs are not auto-tested. The dynamic behaviour of input pulses discovers faults on the inputs or counter circuits immediately by verifying the input data of a leg against the data of the other legs. The complete set of diagnostic functions is sufficient to fulfil the range of diagnostic coverage (safe failure fraction) of > 90 %

4.5.3 Output boards

On the output boards measures are implemented to verify the possibility to switch or change the output, when it is demanded.

4.5.3.1 Digital output

Digital outputs are subject to a pulse test. During the pulse test the final switch is checked for the ability to switch. On the supervised digital output modul diagnostic measures are implemented, which do not need to switch the outputs to verify correct operation.

4.5.3.2 Analog output

On the analog output board three separate output drivers are implemented. Each of it can drive the output on its own. The control of the output points is changed between the legs on a regular basis. The output values are read back and compared against the commanded values.

4.6 Fault insertion procedures

The manufacturer Triconex provided the documentation of fault insertion procedures, which are done during the development cycle of new or changed modules.

These fault insertion procedures were object to investigation. Spot-checking of some of the fault insertion procedures was done.

In addition the fault insertion lists provided by Triconex the inspectors prepared additional lists with fault to be implemented.

The finally released modules could detect all implemented faults as required. The faults are diagnosed by the operating system and are available to the user program to initiate the appropriate actions.

4.7 Measures according to DIN V VDE 0801

The measures which are necessary for requirement class 6 according to DIN V VDE 0801 Appendix A1 are fulfilled. These measures include provisions to detect and control single and multiple faults and failures in hardware and software.

The measures have, compared to earlier versions of the Tricon, not changed for version 9.5.3.

4.8 TRICON modules that are not relevant to safety

Triconex modules not tested by TÜV can be used for inputs and outputs that are not relevant to safety. This is allowed since the TÜV tested modules as listed in the previous sections of this report can detect external errors which affect their operation and still perform their function safely. In the application program it has to be ensured, that these modules are not used in safety relevant parts of the software (in safety relevant networks).

4.9 Test protocols, used investigation and measuring tools

The used investigation and measuring tools are documented together with the protocols of the respective investigation. This is also true for all material stored on electronic media and printouts of source code and listings. Also the minutes of meetings and exchanged email correspondence are stored.

This material will be stored for a period of ten years within the rooms of the test location, together with all other documentation supplied for the investigation.

4.10 User documentation

The user documentation for all modules was checked. It addresses sufficiently the specific properties of the modules.

5.   **Summary of the results**

The version 9.5.3 of the TRICON was subjected to testing as a microprocessor-based systems with safety features.

The testing was essentially divided into the following points:

- safety concept
- theoretical hardware inspection
-- practical hardware inspection
- software analysis
- software test
- software and integration (software/hardware) test
- user interface

The tests were performed according to the test plan and as described under the individual sections. All tests were passed.

The TRICON is a multipurpose device. If used in safety critical applications, the Guidelines specified in the "Safety Consideration Guide", Version 9 Tricon systems, must be adhered to. These guidelines are reviewed and approved by TÜV.

The tests document that the TRICON version 9.5.3 is suitable for applications in requirement class 6 according to standard DIN V 19250.
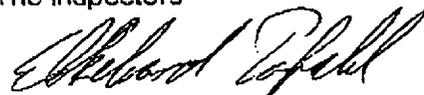
The applied measures ensure that the overall safety is in accordance with DIN V VDE 0801 Appendix 1.

The TRICON also fulfills the requirements according to DIN VDE 0116 and may be used for the electrical equipment of furnaces or equivalent applications.
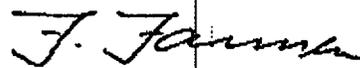
The TRICON may be used as a part of Fire & Gas applications according to DIN EN 54. The site specific codes and standards for the whole application have to be followed.

Cologne, 2001-09-17
ASI/Kst. 968-pl-js-nie

The inspectors

Dipl.-Phys. Ekkehard Pofahl   Dipl.-Ing. Johannes Janssen