

Automation, Software and Information Technology

Type approval of Trident Version 1.0

Report-No.: 968/EZ 101.00/00

Date: 2000-02-17

Type approval of Trident Version 1.0

Report-No.: 968/EZ 101.00/00

Date: 2000-02-17

Pages: 19

Test object: Trident Version 1.0

Customer/Manufacturer: TRICONEX Corporation Ltd.
Advanced Technology
15091 Bake Parkway
USA-Irvine, California 92618
United States of America

Order-No./Date: K61430 dated 1999-02-23

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-Order-No./Date: 968/963018 dated 1999-02-01

Inspectors: Dipl.-Ing. Johannes Buschmann
Dipl.-Ing. Johannes Janssen
Dipl.-Ing. Jürgen Klassen
Dipl.-Phys. Ekkehard Pofahl
Dr. Hendrik Schäbe

Test location: see test institute

Test duration: December 1998 - February 2000

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.

Table of contents		Page
1.	Scope	5
2.	Codes and standards	5
3.	Object of inspection	6
3.1	Description of the Trident triple modular redundant controller	6
3.2	List of modules	6
3.3	Triconex documentation	7
3.4	Supplemental documentation	7
4.	Performed inspection and results	7
4.1	General approach	7
4.2	Theoretic inspection	8
4.2.1	Hardware	8
4.2.1.1	Failure Mode and Effect Analysis (FMEA)	8
4.2.1.2	Diagnostic	8
4.2.1.3	Fault insertion	8
4.2.2	Software	8
4.3	Practical inspection	9
4.3.1	Hardware	9
4.3.1.1	Application program during the inspection	13
4.3.1.2	Environmental inspection	13
4.3.1.3	EMC inspection	13
4.3.1.4	Fault insertion	13
4.3.1.5	Summary of hardware testing	13

Table of contents		Page
4.3.2	Software	14
4.3.2.1	Programming standards	14
4.3.2.2	Diagnostic routines	14
4.3.2.3	Software elements of Trident	14
4.3.2.3.1	Trident operating system	14
4.3.2.3.2	I/O modules	14
4.3.2.3.3	TriStation 1131	15
4.3.2.3.3.1	Cause and effect programming language CEMPLE	15
4.3.2.3.3.2	Installation Verification Utility	15
4.3.2.3.3.3	Download, Upload and Verify	15
4.3.2.3.3.4	TriStation 1131 validation suite	16
4.4	Integration testing	16
4.5	Calculation of probability of failure on demand	16
4.6	TRIDENT module that is not relevant to safety	17
4.7	Compliance to IEC 61508	17
4.8	Compliance to DIN 0801/A1	17
4.9	Test protocols, used investigation and measuring tools	18
4.10	Safety manual	18
5.	Summary of the results	19

Appendix A: (Part 1) Trident Documentation Index
(Part 2) TriStation 1131 Documentation Index

Appendix B: Safety considerations guide - Trident Version 1

1. **Scope**

Subject of the inspection is the programmable logic controller (PLC) Trident Version 1.0. The Trident Version 1.0 consists of the Trident hardware, the PLC operating system and the software TriStation 1131, Version 3.0. The Trident is built as a Triple Modular Redundant (TMR) Controller.

The Trident is to be installed in safety relevant areas according up to requirement class 6 [1], and in applications up to SIL 3 according to IEC 61508 [3]. It will be used in burner management systems, which are described in the German DIN VDE 0116 [4] and in the American NFPA 8501 [5] and NFPA 8502 [6].

During the type approval it has to be shown, that the Trident Version 1.0 fulfills the requirements for safety equipment in accordance with requirement up to class 6 to standard DIN V VDE 19250 [1], resp. DIN V VDE 0801 [2] and up to SIL 3 applications according to IEC 61508 [3].

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] IEC 61508, parts 1 - 7, 2000
Part 1-7: Functional safety of electrical/electronic/programmable electronic safety-related systems
- [4] DIN VDE 0116/10.89
Elektrische Ausrüstung von Feuerungsanlagen
Electrical Equipment Of Furnaces
- [5] NFPA 8501 Standard for Single Burner Boiler Operation/1997 Edition
- [6] NFPA 8502 Standard for the Prevention of Furnace Explosions/Implosions in Multiple Burner Boilers/1999 Edition

- [7] IEC 1131-part 2/1992 , EN 61131-2/August 1994
Programmierbare Steuerungen
Teil 2: Betriebsmittelforderungen und Prüfungen
Programmable Controllers
Part 2: Equipment requirements and tests
- [8] IEC 1131-part 3/1992 , EN 61131-3/August 1994
Programmierbare Steuerungen
Teil 3: Programmiersprachen
Programmable Controllers
Part 3: Programming Languages
- [9] DIN IEC 68
Grundlegende Umweltprüfverfahren
Basic environmental testing procedures
- [10] IEC 801
Elektromagnetische Verträglichkeit von Meß-, Steuer- und Regel-
einrichtungen in der industriellen Prozeßtechnik
Electromagnetic compatibility for industrial-process measurement and
control equipment
- [11] Europäische EMV Richtlinie 89/336/EWG
European EMC-directive 89/336/EWG

3. **Object of inspection**

3.1 **Description of the Trident triple modular redundant controller**

The Trident controller is a triplicated system. It is designed to continue operation after faults. The degradation behavior is transparent to the user and can be configured to meet the needs of specific installations.

The details of the Trident controller are described in the product description.

3.2 **List of modules**

Trident Version 1.0 consists of the following modules:

- 2281 I/O Bus Extender Module
- 3101 MP I Module
- 2101 MP Baseplate
- 3301 Digital Input Module
- 2301 Digital Input Baseplate
- 3401 Digital Output Module
- 2401 Digital Output Baseplate
- 3351 Analog Input Module
- 2351 Analog Input Baseplate
- 3451 Relay Output Module (Non-safety)
- 2451 Relay Output Baseplate (Non-safety)

3.3 Triconex documentation

All documents, which were used during the course of the inspection, are available in electronic form. Changes, new versions and updates were provided by means of a new issued CD ROM. Appendix A lists the content of the CD, which was issued at the moment of certification. All relevant engineering documents are listed there.

The format of this list is an Excel table, with hyperlinks to the actual documents. Because of the size of the table for the programming language TriStation (it is also reprinted) an extra table was prepared and referenced in the main table.

3.4 Supplemental documentation

The following documents were also used during the inspection:

- EMC Test report P9913 359 E01
- FM reliability analysis „Calculation of the Probability of Failure-On-Demand (PFD) for the Triconex Trident System”, February 2000, by D. Baer and B. Choquette
- Inspection Results of the Technical Report FMRC J.I. 0003003839 „Calculation of the Probability of Failure-On-Demand (PFD) for the Triconex Trident System, February 2000”, by D. Baer and B. Choquette dated 2000-03-27
- Triconex Safety Manual (reprinted as appendix B to this report)

4. Performed inspection and results

4.1 General approach

The type approval of the Trident controller was performed during the development, starting with the specification, and continued during prototyping and final testing.

The standards, which were used as a base of the testing, are listed in chapter 2.

As key generic standards the DIN V 19250 [1], DIN V VDE 0801 [2] and the IEC 61508 [3] were used.

4.2 Theoretic inspection

4.2.1 Hardware

All hardware components were checked to be consistent with the manufacturers documentation (schematics, part-lists, description).

The assembled and unassembled boards were inspected with respect to the required clearance and creepage distance according to the relevant standard IEC 1131-2 [7] with positive result.

The system power is +24 VDC. The PLCs are powered by redundant power sources. If the system shall be supplied from 115/240 V AC lines the used power supplies must be in accordance to the requirements for electrical safety according to EN 50178.

The functional and electrical requirements of chapter 3 of IEC 1131-2 [7] for inputs and outputs are met.

4.2.1.1 Failure Mode and Effect Analysis (FMEA)

All modules were subject to an FMEA. The FMEA reports were inspected with positive result.

4.2.1.2 Diagnostic

It was verified, that for all physical parts diagnostic routines are specified in the software documents.

4.2.1.3 Fault insertion

The automated system to insert faults in the system was inspected with positive result. By this system the correct implementation of the diagnostic measures could be shown.

4.2.2 Software

The theoretical software inspection concentrated on the measures, which are demanded in part 3 of IEC 61508 [3]. The following items were subject to a very detailed analysis:

- the software specification of the implemented operating system
- programming guidelines specific to the used languages
- general QA measures
- conformance to the standards
- used development tools

The investigation was done with positive result.

4.3 Practical inspection

4.3.1 Hardware

The base of the performed hardware inspection was taken from EN 61131-2 [7].

The performed inspections are summarized in the following table.

Environmental tests of Triconex Laguna system according to EN 61131-2/10.98 (IEC 1132-2)

test no.	title	standard	requirements/severity	operation mode	performance criteria
1	cold	EN 61131-2/8.3.4.2 IEC 60068-2-1, test Ab	- 25°C, 16 h	none	PFVP before and after influence
2	dry heat	EN 61131-2/8.3.4.2 IEC 60068-2-2, test Bb	+ 70°C, 16 h	none	PFVP before and after influence
3	change of temperature	EN 61131-2/8.3.4.3 IEC 60068-2-14, test Na	low temp.: -25°C high temp.: 70°C 2 cycles, Δt: 1°C/min.	none	PFVP before and after influence
4	change of temperature	EN 61131-2/8.3.4.3 IEC 60068-2-14, test Nb	low temp.: 5°C high temp.: 55°C/60°C 5 cycles, Δt: 1°C/min.	in operation	PFVP during influence
5	damp heat, cyclic	EN 61131-2/8.3.4.4 IEC 60068-2-30, test Db	high temp.: 55°C cycles: 2 variant: 2	none	PFVP before and after influence dielectric withstand test (no. 6.) after influence
6	dielectric withstand verification tests (this test shall be performed within 3 hours of the completion of test no. 5)	EN 61131-2/8.3.6.1	Voltage applied (working voltage ≤50 V): isolated circuit/isolated circuit: 500 V DC isolated circuit/accessible metal parts: 500 V DC isolated circuit/SELV circuits: 720 V DC duration: 1 min.	none	no unintentional flashover or breakdown of the insulation
7	shock	EN 61131-2/8.3.5.2 IEC 60068-2-27, test Ea	half sine, 15 g, 11 ms, 2 shocks in each axis	in operation	PFVP during influence
8	vibration	EN 61131-2/8.3.5.1 IEC 60068-2-6, test Fc	range 1: 10 - 57 Hz @ 0,075 mm Ampl. range 2: 57 - 150 Hz @ 1 g speed: 1 oct./min. cycles: 10 in each axis	in operation	PFVP during influence
9	ESD	EN 61131-2/8.3.9.2 IEC 801-2 DIN EN 61000-4-2	level: 8/4 air/contact no. of disch. 10 time betw. dis. >1 s	in operation	B PFVP during influence
10	immunity to radiated, radio frequency, electromagnetic fields, amplitude modulated	EN 61131-2/8.3.9.3 IEC 801-3 DIN EN 61000-4-3	range: 26 - 1000 MHz level: 3 (10 V/m) sweep speed: 1.5 x 10 ⁻³ decade/s	in operation	A PFVP during influence

PFVP= Proper Functioning Verification Procedure

Environmental tests of Triconex Laguna system according to EN 61131-2/10.98 (IEC 1132-2)

test no.	title	standard	requirements/severity	operation mode	performance criteria	
11	immunity to radiated, radio frequency, electromagnetic fields, pulse modulated	EN 61131-2/8.3.9.4 IEC 801-3 DIN EN 61000-4-3	frequency: 900Mhz duty cycle: 50% modulation: 100%/ 200 Hz level: 10 V/m	in operation	A PFVP during influence	
12	radiated and conducted emission	EN 61131-2/8.3.8.1;8.3.8.2 CISPR 11, CISPR 16	radiated freq. range: 30-1000 MHz distance: 10 m limits: 40-47db (class A)	conducted (DC) 0.15-30 MHz - 73-79db	in operation	
13	burst test	EN 61131-2/8.3.9.5 IEC 801-4 DIN EN 61000-4-3	severity level: Analog and DC I/O lines, shielded a. unshielded: DC main power lines: duration:	1 kV (coupling clamp) 2 kV (direct injection) 1 min. minimum	in operation	B PFVP during influence
14	surge test	EN 61131-2/8.3.9.6 IEC 801-5 DIN EN 61000-4-5	severity level: Analog and DC I/O lines, unshielded: shielded: DC power lines: No. of discharges: rep. Rate:	0.5 kV CM/DM (42 Ω) 1 kV, CM (2 Ω) 1 kV CM (12 Ω) 0.5 kV DM (2 Ω) 5 in each polarity 1/min	in operation	B PFVP during influence
15	damped oscillatory wave immunity test	EN 61131-2/8.3.9.9 DIN EN 61000-4-12 IEC 255-4	frequency repetition rate: duration: unshielded: shielded: severity level:	1 MHz 400/s 2 s min. (200 Ω)CM and DM (12 Ω) CM 2.5 kV series	in operation	B PFVP during influence

PFVP= Proper Functioning Verification Procedure

Environmental tests of Triconex Laguna system according to EN 61131-2/10.98 (IEC 1132-2)

test no.	title	standard	requirements/severity	operation mode	performance criteria
16	voltage variation immunity test	EN 61131-2/8.3.9.11 figures 14 and 15	gradual shutdown: DC: 0.85 x Ue fast variation: DC: 1.2x Ue duration: 30 min	in operation	A PFVP during influence
17	momentary interruption immunity test	EN 61131-2/8.3.9.12	supply interruption: DC: duration: 1 ms number(DC): 20	in operation	A normal operation shall be maintained
18	voltage ripple and frequency range immunity test	EN 61131-2/8.3.10.1.1 figure 14 and 15	gradual shutdown: DC: 0.85 x Ue fast variation: DC: 1.2x Ue ripple: 0.05 x Ue duration: 30 min	in operation	A PFVP during influence
19	gradual shut-down/ start-up test	EN 61131-2/8.3.10.3.2 figure 14	3 trials according to figure 13	in operation	no erratic or unintended conditions
20	supply voltage variation tests	EN 61131-2/8.3.10.3.3 figures 15 and 17	3 trials for each according to figure 15 or 17 respectively	in operation	no erratic or unintended conditions

PFVP= Proper Functioning Verification Procedure

4.3.1.1 Application program during the inspection

An application program was developed to verify the correct behavior of the Trident during the course of the practical hardware inspection. Main design rules for this application program were:

- Digital outputs were toggled and supervised by digital inputs.
- Analog voltages were applied to the analog input module. These voltages were changed on a regular basis and supervised.
- Found errors were counted.
- Stable "0" and stable "1" outputs were provided.

In addition to this special application program the internal operating system was available for enquiry's for the system behavior.

4.3.1.2 Environmental inspection

The environmental tests as detailed in the table were done with positive results.

4.3.1.3 EMC inspection

The EMC tests are documented in a separate report [Report-No.: P9913 359 E01 dated 1999-12-21] including photo documentation.

4.3.1.4 Fault insertion

Within the Triconex QA system extensive automated fault-insertion procedures are available for all modules to verify the correct design of the diagnostic measures to detect and mitigate hardware faults.

Using the schematics and specification documents as a basis, TÜV prepared an independent list of faults to be implemented into the Trident. The reaction to these implemented faults show the correct operation of the TRIDENT.

The list of the manufacturer and of TÜV were compared. Faults, which were not already in the Triconex QA procedure, were applied to the Trident. The diagnostics detected the implemented faults.

4.3.1.5 Summary of hardware testing

The Trident was subjected to the above detailed hardware tests with positive results. Because the IEC 61131-2 is listed in the European directive (European EMC-directive 89/336/EWG) as a product specific standard, the CE mark may be used for the Trident.

4.3.2 Software

Besides the tests, which were done during the integration testing, the software review concentrates on:

- inspection of the results of the static analysis
- code review of selected diagnostic code
- discussion of protocols, which were compiled during code reviews

The reviews were done with positive result.

4.3.2.1 Programming standards

For all used programming languages, programming standards have been prepared. The produced source code was subjected to a static analysis tool. By this tool the compliance between specification and the produced source code was shown.

4.3.2.2 Diagnostic routines

Within all specification documents the diagnostic measures are well described, from the specification to the implemented code.

4.3.2.3 Software elements of Trident

4.3.2.3.1 Trident operating system

The Trident is built as a redundant triplicated system. On each CPU module identical software is installed. The operating system consists of two distinct programs residing in the two microprocessors of the CPU module.

The source-code and the static analysis results of the source-code of both operating systems were spot-checked with positive results.

4.3.2.3.2 I/O modules

On the I/O modules, field programmable gate arrays are used instead of microcontrollers. The FPGA programming for I/O modules and the measures to ensure the correct programming were inspected with positive results.

Selected parts of the programming were verified by means of simulation with positive results.

4.3.2.3.3 TriStation 1131

TriStation is the a Windows-NT 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 functionality to develop programs by means of cause and effect diagrams (CEMPLE) was checked beginning from the concept phase.

The implementation of TriStation includes an install utility, which assures correct installation within a predefined Windows-NT workstation environment. Checks are performed to ensure, the Windows-NT version, which is installed on the programming PC, matches the requirements for TriStation 1131.

4.3.2.3.3.1 Cause and effect programming language CEMPLE

To simplify development of cause and effect matrices an optional tool is included in TriStation 1131. The output of CEMPLE is subject to the same compilation and download measures as conventional developed code. Therefore it can also be used for safety relevant purposes.

4.3.2.3.3.2 Installation Verification Utility

The conventional PCs are not designed for the level of data integrity, which is needed for safety relevant applications. For this reason, special verification tools are implemented to be able to verify the correct installation of TriStation 1131 on a PC. This tool should be used periodically during development of application programs.

4.3.2.3.3.3 Download, Upload and Verify

The system TriStation/Trident is equipped with a very sophisticated upload/download facility, which meets the requirements for safety related communication. It can be shown at any time, that previously downloaded programs have not changed in the meantime.

4.3.2.3.3.4 TriStation 1131 validation suite

The TriStation 1131 validation suite is divided in two major parts, the compiler and the library tests. It is performed by automated tools. The results can be inspected by means of textual protocol files.

The inspection of TS1131 included the assessment of manufacturers testing. The results of this testing were provided by means of protocol files of the automated test environment.

The testing of TriStation was performed by the Q/A department of Triconex and was not repeated in Cologne. The results of that testing were reviewed during the inspection of TriStation 1131.

Spot-checks of the cause and effect programming were performed in Cologne.

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

4.4 Integration testing

The integration testing was performed to verify, that all elements of the whole Trident system perform in a safe way, when they are combined. The main elements of the Trident system are:

- PLC-Hardware
- PLC-Software
- Operator-station Software (TriStation)

The tests were done by changing the hardware and software setup of the system. It was verified, that the system performed according to the specification.

The tests were done with positive result.

4.5 Calculation of probability of failure on demand

The methodology to calculate the probability of failure on demand was taken of IEC 61508 and of ISA 84. The result shows, that the required figure of failure for SIL 3 is met. The detailed information can be found in the Safety Manual (Appendix B) and Technical Report "Calculation of the Probability of Failure-On-Demand (PFD) for the Triconex Trident System", February 2000.

4.6 TRIDENT module that is not relevant to safety

The Trident includes a relay module. This relay module is not equipped with the diagnostic toolkit of the other modules. Therefore it should not be used for safety critical outputs.

This is appropriate since the other tested modules as listed in section 2 can detect external errors which affect their operation and still perform their function safely. In the application program it has to be ensured, that the relay modules are not used in safety relevant parts of the software.

The module was theoretically checked to not interfere with the safety relevant core of the Trident controller.

All practical tests included the module. The module operated correctly. It was used to provide stimuli for the other modules. These stimuli were constantly supervised.

Therefore, the relays module can be included in safety critical system configurations to provide non safety critical actions.

4.7 Compliance to IEC 61508

Part 1 of the IEC 61508 demands certain documentation requirements for the development of safety critical devices. As basis documents the SRS (Safety Requirements Specification) and the V&V Plan (Validation and Verification Plan) were prepared.

Table 1 in part 2 and table 1 in part 3 also show additional information requirements.

To prove that the documentation requirements per IEC 61508 are met, the original text and the pictures from the standard were taken as basis of the compliance proof document. Via hyperlinks the fulfillment of the requirements is shown.

For the specific requirements of part 2 (system architecture, safe failure fraction and diagnostic) and part 3 (software) documents with answers to the requirements of these parts are compiled.

The measures listed in the tables of IEC 61508 were taken as base of the development. The finally selected set of measures are implemented in such a way that the system meets the requirements of SIL 3.

4.8 Compliance to DIN 0801/A1

The compliance to DIN 0801/A1 was checked using checklists. The measures for diagnostic and mitigation of failures, which were chosen for compliance with IEC 61508, also fulfill the requirements of the standard DIN 0801. The measures against systematic faults are also sufficient to meet the requirements of DIN 0801/A1.

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 Safety manual

The Trident is a multipurpose device. If used in safety critical applications the Trident Safety Consideration Guide, which is reprinted as Appendix B to this report, should be followed.

This guide is one result of the type approval and gives the user a guidance on how to install and maintain the Trident in safety relevant applications.

5. Summary of the results

The Version 1.0 of the Trident was subjected to testing as a microprocessor-based system with safety features.

The testing was essentially divided into the following points:

- safety concept
- hardware analysis
- hardware test
- software analysis
- software test
- software and integration (software/hardware) test
- review of PFD calculations
- user interface

The tests were performed according to the test plan and as described under the individual sections. All tests were passed. The detailed results are archived in the files of the test lab.

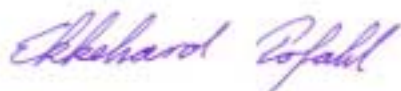
The tests document that the Trident Version 1.0 is suitable for applications up to requirement class 6 according to standard DIN V 19250 and in applications up to SIL 3 according to standard IEC 61508.

The applied measures ensure that the overall safety is in accordance with DIN V VDE 0801/A 1 and IEC 61508.

The Trident fulfills the requirements according to DIN VDE 0116 [4] and NFPA 8501 [5] and NFPA 8502 [6] and may be used for the electrical equipment of furnaces or equivalent applications.

Cologne, 2000-02-17
ASI/KST 968 pl-js-nie

The inspectors



Dipl.-Phys. Ekkehard Pofahl



Dipl.-Ing. Johannes Janssen