

2004-01-30



TÜV Rheinland Group

Automation, Software and Information Technology

**Test report of the type approval
safety-related automation devices**

**GuardPLC 1200
GuardPLC 1600
GuardPLC 1800
GuardPLC 2000
GuardPLC Distributed I/O**

**Report-No.: 968/EZ 164.00/04
Date: 2004-01-30**

**Test report of the type approval
safety-related automation devices
GuardPLC 1200
GuardPLC 1600
GuardPLC 1800
GuardPLC 2000
GuardPLC Distributed I/O
of Rockwell Automation**

Report-No.: 968/EZ 164.00/04

Date: 2004-01-30

**Number of pages:
(excluding appendices)** 14

Object(s) subject to testing: GuardPLC 1200
GuardPLC 1600
GuardPLC 1800
GuardPLC 2000
GuardPLC Distributed I/O

Client/Manufacturer: HIMA Paul Hildebrandt GmbH + Co. KG
Albert-Bassermann-Straße 28
D-68782 Brühl

P.O. number client/Date: Application for Certification, Rockwell Automation
dated 2004-01-28

Test Institute: TÜV Anlagentechnik GmbH
Automation, Software, Information Technology (ASI)
Am Grauen Stein
D-51105 Köln

Quotation Test Institute/Date: Contract HIMA/TÜV dated 2002-10

Order number Test Institute/Date: 968/264223 dated 2002-11-14

Processor: Dipl.-Ing. Wolfgang Velten-Philipp

Place of testing: see Test Institute

Testing period: January 2004

The test results exclusively related to the test objects.

It is prohibited to duplicate this report in parts without written permission of the Test Institute.

Table of contents		Page
1	Objective	4
2	Basis of testing	4
3	Test object(s)	5
3.1	Test documentation	7
3.1.1	Documentation of manufacturer	7
3.1.2	User documentation	8
3.1.3	Documentation Test Institute	8
4	Protocol and results type approval	8
4.1	General requirements	8
4.2	Safety requirements	8
4.3	Requirements that result from application standards	9
4.4	Existing type approvals	9
4.5	Test results	9
4.5.1	Safety concept of the systems	9
4.5.2	Products GuardPLC 1200	9
4.5.3	Products GuardPLC 1600 and 1800	9
4.5.4	Product GuardPLC 2000	11
4.5.5	Product Distributed I/O	11
4.5.6	Review documentation	11
4.5.7	Measures to avoid failures	12
4.5.8	FMEA and fault injection	12
4.5.9	Reaction times	12
4.5.10	Calculation of the probability of failure on demand	13
4.5.11	Software	13
4.5.12	Programming environment	13
4.5.13	Electrical safety tests	13
4.5.14	Electromagnetic compatibility and environmental simulation tests	13
5	Summary results	14

1 **Objective**

Objects of testing are the safety-related automation devices

GuardPLC 1200
GuardPLC 1600
GuardPLC 1800
GuardPLC 2000
GuardPLC Distributed I/O

with the in paragraph 3 listed hardware and software components.

The carried out type approval shall demonstrate that the automation devices are suitable for risk reduction applications up to SIL 3 according to IEC 61508 and requirement class 5/6 according to DIN V VDE 0801 and category 3/4 according to EN 954-1.

The devices GuardPLC 1200 and GuardPLC 2000 are already certified according the above mentioned standards by TÜV Süddeutschland [H1, H2].

Scope of this report is to overtake the already carried out type approval of TÜV Süddeutschland and to approve modifications of Guard PLC 1200 and 2000.

Further the products GuardPLC 1600, 1800 and Distributed I/O are new released products for approval.

2 **Basis of testing**

Functional safety

- [1] DIN V 19250:1994
Fundamental Safety Aspects to be considered for Measurement and Control Protective Equipment
- [2] DIN V 19251:1995
Process Measurement and Control Protection Devices Requirements and measures for Safe Function
- [3] IEC 61508:2000, parts 1 - 7
Functional safety of electrical/electronic/programmable electronic safety related systems
- [4] DIN V VDE 0801:1990, Amendment A1 to VDE 0801:1994
Principles for Computers in Safety Related Systems

Electrical safety and resistance against environmental conditions

- [5] IEC 61131-2:1994
+A11:1996
+A12:2000
Programmable Controllers
Part 2, Equipment requirements and tests

Electromagnetic Compatibility

- [6] EN 61000-6-2:2000, EN 50082-2:1996
Electromagnetic Compatibility (EMC)
 - Generic Standards
 - Immunity for Industrial Environments

- [7] EN 50081-2:1993
Electromagnetic Compatibility (EMC)
 - Generic emission standard
 - Residential, commercial, and light industry

Application specific standards

- [8] DIN VDE 0116:1989
Electrical Equipment of Furnaces
- [9] prEN 50156-1:2000
Electrical Equipment for Furnaces
Part 1: Requirements for Application Design and Installation
- [10] NFPA 8501:1997
Standard for single burner boiler operation
- [11] NFPA 8502:1999
Standard for the prevention of furnace explosions/implosions in multiple burner boilers
- [12] EN 954-1, Cat 3, 4:1996
Safety of machinery - Safety related parts of control systems
 - Part 1: General principles for design
- [13] EN 60204-1:1997
Safety of machinery
 - Electrical equipment of machines
- [14] EN 298:1994
Automatic gas burner control systems for gas burners and gas burning appliances with or without fans
- [15] EN 54-2:1997
Fire detection and fire alarm systems
 - Part 2: Control and indicating equipment
- [16] NFPA 72:1999
National Fire Alarm Code
- [17] ISA S84.01
Application of safety instrumented systems for the process industries

3 Test object(s)

The products listed on the following table are compact programmable electronic systems, whose I/O configuration is not changeable.

All products are basing on a synchronic 1oo2 processor system with diagnostics.

Also the operating system for the products is based on one software product which has been slightly modified to support the different products.

The operating software of the GuardPLC Distributed I/O was modified so that no application program can be executed.

The individual systems differ concerning the respective I/O.

The most current hardware and software version should be retrieved from the manufacturers release list [P5]. The list is released together by the manufacturer and the Test Institute.

The following tables give a product overview of all GuardPLC -Products.

GuardPLC	DI	DO	Counter	AI	Ethernet-Switch	Bus
1200	20	8	2	---	---	RS232
1600	20	8	---	---	yes	Modbus Profibus
1800	24	8	2	8	yes	Modbus Profibus
Distributed I/O	DI	DO	Counter	AI	Ethernet-Switch	Bus
1753-IB16	16	4	---	---	yes	---
1753-OB16	---	16	---	---	yes	---
1753-IB20XOB8	20	8	---	---	yes	---

The specified devices are delivered as a complete unit. Changes to the system configuration are not possible.

The devices are capable to have safety related communication with each other.

The product GuardPLC 2000 is a slot-based PLC system with configurable I/O modules. The following table contains the modules available for this system. Hard- and Software of GuardPLC 2000 uses the same principles as the other products.

Module	Description
1755-A6	6 Slot GuardPLC Chassis
1755-L1	GuardPLC 2000 CPU
1755-PB720	Power Supply
1755-IB24XOB16	Safe Digital I/O Module
1755-IF8	Safe Analog In Module
1755-OF8	Safe Analog Out Module
1755-HSC	Safe Counter Module

Safety-related software components

The systems GuardPLC 1200, 1600/1800 and 2000 are using the firmware version V4.32 with different implementations for the systems. The GuardPLC Distributed I/O uses the firmware version V4.28. Therefore the CRC-Checksums differ between the different product versions.

The actual firmware CRC can be obtained from the list of current releases.

GuardPLC 1600 and 1800 are using exactly the same firmware.

The GuardPLC 2000 is slightly modified as this PLC owns no Ethernet switch.

GuardPLC 1200 is modified as this PLC owns no counter modules.

The Distributed I/O is modified as distributed I/O is not able to execute application programs.

Non safety-related software components

The end-user cannot install non safety-related software.

Programming tools

The tool RSLogixGuard*PLUS!* needs to be used to create safety related application programs.

The valid version is available from the list of current releases.

3.1 Test documentation

3.1.1 Documentation of manufacturer

H1	Report to the certificate Z2 01 03 19183 034 and Z2 01 03 43246 001, Rep 70001328, dated 2002-22-01 by TÜV Süddeutschland
H2	Technical report type approval HB61941A1, Rev. 1.0 dated 07.12.2001 by TÜV Automotive GmbH
H3	Documentation plan AM2000/RA-Maxi Rev. 1.1 (GuardPLC1200 and 2000)
H4	Documentation plan HIMA-MAXI 15 F30 Rev. 1.0 (GuardPLC 1600)
H5	Documentation plan HIMA-MAXI 16 F35 Rev 1.0 (GuardPLC 1800)
H6	Documentation plan HIMA-MAXI 06 F1 DI 16 01 Rev 1.0 (GuardPLC Distributed I/O 1753-IB16)
H7	Documentation plan HIMA-MAXI 08 F3 DO 16 01 Rev 1.0 (GuardPLC Distributed I/O 1753-OB16)
H8	Documentation plan HIMA-MAXI 11 F3 DIO 20/8 02 Rev1.0 (GuardPLC Distributed I/O 1753-IB20XOB8)
H9	Test Reports IEC 61131-2 : RA-MAXI.1 RA-AM2000.1 HIMA-MAXI 15 HIMatrix F35 HIMA-MAXI 16 HIMatrix F30 HIMatrix F1 DI 16 01 HIMatrix F2 DO 16 01 HIMatrix F3 DIO 20/8 02
H10	Test Reports EMC 5200-302e, 5200-303e, 5200-317e, 5200-319, 5200-320
H11	Test Reports Environmental Test Vibration and Shock MHM-EST-7.70061160a, MHM-EST-7.70036744c, MHM-EST-7.70002880b, MHM-EST-7.700047719a, MHM-EST-7.700047719c,
H12	Average probability of failure on demand and of failure per hour for HIMatrix F3x Systems, Rev. 1.4 Valid for GuardPLC 1600, 1800 and Distributed I/O
H13	Average probability of failure on demand and of failure per hour for HIMatrix F60 Systems, rev 1.6, valid for GuardPLC 2000
H14	Probabilistic Evaluation of failure on demand and of failure per hour of RA-Maxi System, rev 1.1, valid for GuardPLC 1200

3.1.2 User documentation

B1	GuardPLC TM Controller Systems Bulletin 1753, 1754 and 1755 Safety Reference Manual
B2	GuardPLC Controller System User Manual

3.1.3 Documentation Test Institute

P1	Report No. 968/EZ 128.03/03 dated 2003-10-16
P2	Report No. 968/EZ 128.04/03 dated 2003-10-17
P3	Report No. 968/EZ 128.05/03 dated 2003-11-28 software testing
P4	Report Nr. 968/FSM 100.00/02 dated 2002-03-15 safety management
P5	Module and firmware version control release list to the certificate number 968/EZ 164.00/04

4 Protocol and results type approval

4.1 General requirements

DIN V VDE 0801 and IEC 61508 distinguish between measures to control and measures to avoid failures. Both cases consider the complete product lifecycle, which results in the following categories of requirements:

1. Requirements that relate to the design of the safety-related product.
2. Requirements that depend are application specific and related to the specific lifecycle phases:
 - Planning, specification and design of the application
 - Operation and maintenance of the product
 - Validation/Verification/Modification of the application

The main testing of the requirements of the first category is addressed during the type approval product.

The requirements of the second category need to fulfilled by the end-user of the system

The manufacturer's documentation (safety manual, user manual) are addressed in the context of the type approval and required editions and boundary conditions will be defined.

4.2 Safety requirements

The products are fulfilling the SIL 1 - 3 requirements of IEC 61508 in high as well as low demand mode.

That means that the PFH is lower than 15 % of the limit defined in IEC 61508-1 of 10^{-8} to 10^{-7} failures per hour. In low demand mode, the PFD is lower than 15 % of the limit 10^{-4} to 10^{-3} defined by IEC 61508-1.

All system that are based on Type B components must meet he following requirements concerning the Safe Failure Fraction:

Safe failure fraction	Hardware fault tolerance		
	0	1	2
< 60 %	not allowed	SIL 1	SIL 2
60 % - ≤ 90 %	SIL 1	SIL 2	SIL 3
90 % - ≤ 99 %	SIL 2	SIL 3	SIL 4
≥ 99 %	SIL 3	SIL 4	SIL 4

The grey shaded area is the basic architecture used by GuardPLC products.

4.3 Requirements that result from application standards

The application specific requirements result from [8, 9] and cover applications in the process industry and the manufacturing and machinery industry.

Restrictions and conditions concerning the use of the programmable electronic systems within the specified application standards are described in the safety manual.

4.4 Existing type approvals

The products under consideration are derived from the already certified products GuardPLC 1200 and 2000. The certification of these products took place in 2001 by TÜV Süddeutschland. The Test Institute made the associated documentation (technical report and certification report [H1, H2]) available.

The documents have been reviewed, the results are accepted and are used to approve the products.

The type approval of the products GuardPLC 1600, 1800 [H1] and Distributed I/O [P2] took also into account the already existing certification reports.

4.5 Test results

4.5.1 Safety concept of the systems

The safety concept of the GuardPLC products is not changed compared to the already certified products [H1, H2, P2].

4.5.2 Products GuardPLC 1200

There is no modification compared to the approved product except the value of a fuse used in the 3.3VDC internal power supply has been modified to a bigger value. The related fault injection tests which are proof that the fuse fails if the 3.3VDC regulator outputs over -voltage have been repeated. The results [H5] are positive.

4.5.3 Products GuardPLC 1600 and 1800

Hardware

The system CPU structure (synchronous 1oo2D processor system with hardware bus comparison and diagnostics) was not changed compared to the existing certification [H1].

The accomplished changes concern the I/O level of the devices. The following tables are presenting an overview of the accomplished changes compared to the already certified product GuardPLC 1200.

	GuardPLC 1200	GuardPLC 1600 (M, P)	GuardPLC 1800 (M, P)
CPU -Board	1oo2D with bus comparison und diagnostics	1oo2D with bus comparison und diagnostics	1oo2D with bus comparison und diagnostics
Communication	Safety-related Communication (Ethernet, RS232)	Additional Ethernet switch	Additional Ethernet switch
Field bus	not available	M: Modbus P: Profibus	M: Modbus P: Profibus
Digital Input	20 DI	20 DI	24 DI with line Monitoring
Digital Output	8 DO	8 DO modified	8 DO modified
Counter	2 CO	No counter	2 CO
Analog Input	No Analog input	No Analog input	8 AI no changes compared to GuardPLC 2000

Next, the accomplished changes are described in detail.

Communication and field bus interfaces

An Ethernet switch was added to the communication part of the CPU.

The communication part of the CPU has its own processor, which is connect via a dual port memory with the safety-related processor system. The safety-related messages are created in the safety-related processor part according to the safety data protocol and stored in the dual port memory. The communication processor retrieves the data from there and translates the data into the required format for TCP/IP transmission.

Safe transmission does not depend on the transmission protocol or medium because the safety-related data protocol contains all required failure recognition measures.

The additional Ethernet switch has therefore, as well as the transmission path, no influence on the safety-related data content.

The functional properties of the switches have been reviewed as part of the product tests.

The implemented field bus interfaces can complete non safety-related data transmission and are interference free to the safety data protocol.

Digital Input

No changes were made in relation to the already existing certification to the digital input circuits used by GuardPLC 1200.

The GuardPLC 1800 has digital inputs that resulted from modified analog inputs. This makes it possible to realize line monitoring (short circuit, line break).

Digital Output

For all products the digital outputs (DO) were modified. The control/bus interface of the DO was completely copied. The actual output stage, which originally consisted of a within 'fault tolerance time' testable switch structure, was replaced by a structure consisting of diverse switches (Fault Tolerance 2, Type A-component).

Read back of the output states and the test of the output switches take place within the multiple fault tolerance time.

Software changes

Based on the already tested software of the GuardPLC 1200 and 2000 version 2.04 the functional changes to the software were tested and the results are summarized in [P1, P3].

The actual version of the software can be obtained from the hard- and software version control list [P5] released by the manufacturer and TÜV Rheinland (www.tuvasi.com).

4.5.4 Product GuardPLC 2000

There is no modification compared to the approved product [H1, H2, P3], except the software has been upgraded to the actual version which is identical in the functionality to GuardPLC 1200, 1600 and 1800. The difference in software is only in the hardware depended settings.

4.5.5 Product Distributed I/O

There is no modification compared to the approved product [P1], except the software has been upgraded to the actual version which is identical in the functionality to GuardPLC 1200, 1600, 1800 and 2000.

The difference in software is that the parts which are responsible for application execution have been removed.

4.5.6 Review documentation

The HIMA documentation is hierarchical and contains the following main documents:

- Safety requirements specification
- Architectural documentation
- Design documentation
- Validations and Verification proof

The overall and internal document structure result from the documentation guidance paper and the documentation plan (see [H3 to H8]).

As a result the documentation is arranged as follows:

- Safety plan
- Requirement specification
- Specification architecture
- System Requirements
- Safety Requirements
- System-FMEA, FMEAs

- Test specification
- Test protocol
- Quantitative calculations
- Review protocol (reviews by manufacturer)

This above mentioned documentation have been reviewed during the test for the following aspects:

- Completeness
- Consistency
- Comprehensibility
- Clarity

Contradictions in the documentation were discussed with the manufacturer and corrected in the documents.

The examination of the manufacturer documents was concluded with a positive result.

4.5.7 Measures to avoid failures

The manufacturer created a safety plan describing the complete test sequence. The verification and validations steps can be derived from the V&V plan of the Test Institute.

The manufacturer has carried out an impact analysis to evaluate the hardware and software changes. The Test Institute carried out a review of the changes made based on the impact analysis and the corresponding documentation.

A separate Management of Functional Safety audit was carried out on the already certified QM system of the manufacturer to proof the application and effectiveness of the measures to avoid failures. The results of this audit are documented in a separate report [P4]. In summary the audit demonstrated that HIMA complies with the lifecycle specific requirements of IEC 61508.

4.5.8 FMEA and fault injection

The original FMEAs and corresponding fault injection test were adapted to the made changes and have been reviewed.

Sample fault injection tests have been carried out together with the Test Institute.

The FMEAs and fault injection reviews have been reviewed and were positive.

4.5.9 Reaction times

4.5.9.1 Reaction times without Peer to Peer communication

The reaction time for external demands is as a maximum the double cycle time of the automation time.

Single failures, which can lead to a dangerous operational state, will be recognized within the projected safety time by the internal diagnostics. The system can be used for configurations that required a process safety time within a minimum of 20 ms to 30 ms (with analog outputs).

Loss of function, which can only be fail dangerous if in combination with other failures, will be recognized within the multiple fault tolerance time because of additional tests. Independent of the safety time the multiple fault tolerance time was determined to be 24 hours.

4.5.9.2 Reaction times with Peer to Peer communication

The reaction time and timeout-time must be determined according to the data in the safety manual when safety relevant signals are transmitted via Ethernet between several PLC's.

The timeout time must be in agreement with the maximum reaction time (maximum multiple fault tolerance time) of the application.

The reaction time of locally processed signals is not influenced because of Peer-to-Peer communication.

4.5.10 Calculation of the probability of failure on demand

The PFD system calculations were carried out by HIMA [H12] and reviewed by TÜV.

The calculations show that the required SIL 3 criteria (15 % of the acceptable SIL 3 value) is achieved within an offline proof test interval of 10 years.

4.5.11 Software

The software changes were tested on the basis of the already tested software version 2.04. The results are separately documented in [P1, P3].

The tested software package for GuardPLC 1200, 1600, 1800, 2000 version v4.32 and Distributed I/O version v4.28 is principle suitable to meet the SIL 3 requirements of IEC 61508.

4.5.12 Programming environment

Application programs must be created with the tool RSLogixGuard *Plus* and take into account the safety manual.

The programming tool gives the user the opportunity to create and change safety-related applications. The tool allows the creation of safety-related applications within a framework that supports reduction of the following application tests by reviewing the safety functions.

4.5.13 Electrical safety tests

EN 61131-2 has been used as basis for electrical safety testing. The tests carried out by the manufacturer have been documented in the test protocols [H9]. The documentation was reviewed.

All products are supplied with SELV (Safe Extra Low Voltage) according to [5] and are concerning isolation laid out for SELV.

4.5.14 Electromagnetic compatibility and environmental simulation tests

The following standards were used:

- EN 61000-6-2
- EN 61131-2
- EN 50081-2

- EN 298
- EN 54-2
- VDE 0116/prEN 50156

During the tests the safety-related system properties have been monitored.

The environmental simulation tests have been documented in test report [H9, H10, H11].

Note: The above-mentioned tests have been carried out by an accredited test laboratory and have been recognized by the Test Institute.

5 Summary results

The carried out tests and analyses have shown that the system in principle can be used for applications up to SIL 3 and AK 5/6 according to IEC 61508 respectively DIN V VDE 19250 and category 3, 4 according to EN 954-1.

Basis for the classification is the low and high demand mode with and without continuous monitoring. The safe state is the energy less state.

All safety configurations meet with appropriate parameter settings the requirements of the basic standards.

Application programs need to be created with the RSLogixGuard 1200/2000 tool and need to take into account the safety manual.

The safety manual compiles all conditions which must be maintained for safety related use of the products.

The actual version of hard and software can be obtained from the hard- and software version control list released by manufacturer and the TÜV Rheinland Group (<http://www.tuvasi.com>).

Cologne, 2004-01-30
ASI/Kst. 968 vt-nie

The expert



Dipl.-Ing. Wolfgang Velten-Philipp