

2005-09-15



TÜV Rheinland Group

Automation, Software and Information Technology

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

GuardPLC 1200

GuardPLC 1600

GuardPLC 1800

GuardPLC 2000

GuardPLC Distributed I/O

Report-No.: 968/EZ 164.03/05

Date: 2005-09-15

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

Report-No.:	968/EZ 164.03/05
Date:	2005-09-15
Number of pages: (excluding appendices)	11
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 Industrie Service 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:	July 2005 - September 2005

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.

1 Scope

Scope of this report are the safety-related automation devices

- GuardPLC 1753-IF8XOF4
- GuardPLC 1753-OW8
- GuardPLC 1753-IB8XOB8
- GuardPLC 1753-IB16XOB8

including the in paragraph 3 listed hardware and software components.

The modules above are newly developed distributed I/O modules for the GuardPLC product.

Furthermore the already type approved modules were reconsidered to ensure that the products fulfil the new releases of the standards in paragraph 2.

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, IEC 61511 and category 3/4 according to EN 954-1.

Scope of this report is to certify the products according to the standards mentioned in paragraph 2.

The former report-no.: 968/EZ 164.00/04 dated 2004-01-30 remains still valid.

2 Standards

Functional Safety

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

Electrical safety and resistance against environmental conditions

- [2] IEC 61131-2:2003
Programmable Controllers
Part 2, Equipment requirements and tests

Electromagnetic Compatibility

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

Application specific standards

- [5] DIN VDE 0116:1989
Electrical Equipment of Furnaces

- [6] EN 50156-1:2004
Electrical Equipment for Furnaces
Part1: Requirements for application Design and Installation
- [7] NFPA 85: 2001
Boiler and Combustion Systems Hazards Code
- [8] EN 954-1, Cat 3, 4:1996
Safety of machinery - Safety related parts of control systems
- Part 1: General principles for design
- [9] EN 60204-1:1997
Safety of machinery
- Electrical equipment of machines
- [10] EN 298:2003
Automatic gas burner control systems for gas burners and gas burning appliances
with or without fans
- [11] ISA S84.01
Application of safety instrumented systems for the process industry
- [12] IEC 61511, Parts 1-3:2004
Functional safety
Safety instrumented systems for the process industry sector
- [13] EN 54-2:1997
Fire detection and fire alarm systems
Part 2: Control and indicating equipment
- [14] NFPA 72:2002
National Fire Alarm Code

3 Test object

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 synchronous 1002 processor system with diagnostics.

Also the system firmware and operating system used for all devices bases on one software product which has been slightly adapted to support the different products.

The operating software of the GuardPLC Distributed I/O cannot execute application logic.

Application related logic is exclusively executed by the main PLC (GuardPLC 1200, 2000, 1600, 1800). Main PLC and Distributed I/O are communicating by a safety related proprietary protocol which uses Ethernet as physical layer.

The individual Distributed I/O systems differ concerning the respective I/O.

The most current hardware and software version can be retrieved from the manufacturers module and firmware release list [P7]. The list is issued together by the manufacturer and the Test Institute.

The following tables give a product overview of the GuardPLC-Products to be certified.

Distributed I/O	DI	DO	Counter	AI	AO	Ethernet-Switch	Bus
1753-IF8XOF4	---	---	---	8	4 non safety-related	yes	---
1753-OW8	---	8 relay	---	---	---	yes	---
1753-IB8XOB8	8	8+/2-	---	---	---	yes	---
1753-IB16XOB8	16	8+/8-	---	---	---	yes	---

Note: 1753-IB8XOB8 and 1753-IB16XOB8 outputs can switch to supply voltage or to ground potential. Both devices include additionally two pulsed outputs for line supervision purposes.

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.

Safety-related software components

The GuardPLC Distributed I/O uses the firmware version V 6.28.

The valid firmware CRC can be obtained from the actual module and firmware release list [P7].

Non safety-related software components

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

Programming tools

The tool RSLogixGuardPLUS! needs to be used to create safety related application programs.

The actual version can be obtained from the module and firmware release list [P7].

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 F2 DO 8 01 for GuardPLC 1753-OW8
H4	Documentation plan F3 AIO 8/4 01 for GuardPLC 1753-IF8XOF4
H5	Documentation plan F3 DIO 8/8 01 for GuardPLC 1753-IB8XOB8
H6	Documentation plan F3 DIO 16/8 01 for GuardPLC 1753-IB16XOB8
H7	Test Reports IEC 61131-2 for HIMatrix: F2 DO 8 01 TQ_HM08_HMX.pdf, dated 09.07.2003 F3 AIO 8/4 01 TQ_HMX10_F3AIAO8-401.1.pdf, dated 09.08.2003 F3 DIO 8/8 01 TQ_F3DIO8801.pdf, dated 19.08.2005 F3 DIO 16/8 01 TQ_F3DIO16801.pdf, 09.08.2005

H8	Test Reports EMC 5200-317, 5200-318, 5200-338, 5200-341
H9	Test Reports Environmental Test Vibration and Shock MHM-EST-7.70047719c, MHM-EST-7.70047719a, MHM-EST-7.70102439a, MHM-EST-7.70102439b
H10	Average probability of failure on demand and of failure per hour for HIMatrix F3x Systems, Rev. 1.2 for RIO-NC Valid for GuardPLC Distributed I/O

3.1.2 User documentation

B1	GuardPLC TM Controller Systems Bulletin 1753, 1754 and 1755 Safety Reference Manual, October 2005
B2	GuardPLC Controller System User Manual, October 2005

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 approval
P4	Report-No. 968/FSM 100.00/02 dated 2002-03-15, Safety management
P5	Report-No. 968/EZ 164.00/04 dated 2004-01-30
P6	Report-No. 968/EZ 164.04/05 dated 2005-09-15, Software approval
P7	Module and firmware version control release list to the certificate number 968/EZ 164.03/05

4 Result type approval

4.1 General requirements

IEC 61508 distinguishes between measures to control and measures to avoid failures and considers the complete product lifecycle, which results in the following categories of requirements:

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

The requirements of the first and second categories are addressed during the type approval of the product.

The requirements of the third category need to be fulfilled by the end-user of the system. The documentation [B1, B2], especially the safety manual [B1] provides the PLC related information for proper use of the safety related PLC, which includes planning, operation and maintenance.

4.2 Safety requirements

The products are fulfilling the SIL 1 - 3 requirements of IEC 61508 and IEC 61511 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 sub-systems that are based on Type B components must meet the following requirements concerning the Safe Failure Fraction (SFF):

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 are resulting from [5] to [14] and are covering applications in the process industry and the machinery industry.

Restrictions and conditions concerning the use of the programmable electronic systems within the specified application standards are described by the safety manual [B1].

4.4 Existing type approvals

The products under consideration are derived from the already certified products GuardPLC 1200, 1600, 1800, 2000. The certification of these products are documented by [P1 to P5].

4.5 Test results

4.5.1 Safety concept of the Distributed I/O

The safety concept of the GuardPLC Distributed I/O is unchanged compared to the already certified products [P1 to P5].

The distributed GuardPLC Distributed I/O is identical to the already type approved HIMatrix remote I/O types [H1] to [H6] except changes to enable Device Net specific communication. The following chapters are summarizing the results of the type approval.

4.5.2 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 H6]).

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.

4.5.3 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.

4.5.4 FMEA and fault injection

The original FMEAs and corresponding fault injection tests were adapted to the made changes and have been repeated as far as necessary by the manufacturer.

The FMEAs and fault injection tests have been reviewed and were positive [see H3 to H6].

4.5.5 Reaction times

4.5.5.1 Reaction times without Peer to Peer communication

The reaction time for external demands is at maximum the double cycle time.

Single failures, which lead to a dangerous system state, will be recognized within the projected safety time by internal diagnostics. The system is suitable for configurations which are requiring a process safety time of 20 ms to 30 ms (see safety manual for details).

Failures which are dangerous in combination with other failures, will be recognized within the specified multiple fault tolerance time because of additional diagnostic measures. Independent from the safety time, the multiple fault tolerance time is 24 hours.

4.5.5.2 Reaction times with Peer to Peer communication

Reaction time and timeout must be specified and set according to the procedures defined by the safety manual if safety relevant signals are transmitted by Ethernet to other GuardPLC's. The timeout must be suitable for the maximum reaction time of the application. The reaction time of locally processed signals are not influenced by Peer-to-Peer communication.

4.5.6 Calculation of the probability of failure on demand

The PFD and PFH calculations were carried out by HIMA [H10] 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.

4.5.7 Software

The software packages AM2000/MAXI/RIO/RIO-NC - CPU v6.28 was approved in [P6].

The approved software packages AM2000/MAXI/RIO/RIO-NC - CPU v6.28 are suitable to meet the SIL 3 requirements of IEC 61508.

4.5.8 Programming environment

Application programs shall be exclusively created by RSLogixGuard *Plus!* tool 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 mandatory application verification tests by validating the safety functions.

4.5.9 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 [H7]. The documentation was reviewed.

All products are supplied with SELV (Safe Extra Low Voltage) according to [2].

4.5.10 Electromagnetic compatibility and environmental simulation tests

The following standards were used to test electrical safety, environmental conditions and EMC requirements:

- EN 61000-6-2
- EN 61000-6-4
- EN 61131-2
- EN 298
- EN 54-2
- VDE 0116/EN 50156

During the tests the safety-related system properties have been monitored. The environmental simulation tests were documented by test reports [H7, H8, H9].

Note: The above-mentioned tests were carried out by an accredited test laboratories and have been accepted by the Test Institute after review of the test results.

The products covered by report-no.: 968/EZ 164.00/04 have been reviewed regarding changed requirements of the newer releases of the standards listed in paragraph 2. Necessary tests were repeated.

5 Summary

The carried out tests and analyses have shown that the system can be used for applications up to SIL 3 according to IEC 61508, IEC 61511 and category 3, 4 according to EN 954-1.

Basis for the classification is the low and high demand mode. The safe state is the de-energized state.

Application programs are required to be created with RSLogixGuard Plus! tool, the safety manual needs to be considered to build safety related applications.

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

The actual version of hard and software can be obtained from the module and firmware release list released by the manufacturer and the TÜV Rheinland Group .

Cologne, 2005-09-15
TIS/ASI/Kst. 968 vt-nie

The expert



Dipl.-Ing. Wolfgang Velten-Philipp