

Automation, Software and Information Technology

**Test report about the modification approval of
the safety-related automation system HIMax
of HIMA Paul Hildebrandt GmbH + Co KG**

**Report No.: 968/EZ 274.06/09
Date: 2009-10-30**

This report is the English translation of
the original German report

**Test report about the modification approval of
the safety-related automation system HIMax
of HIMA Paul Hildebrandt GmbH + Co KG**

Report No.:	968/EZ 274.06/09
Date:	2009-10-30
Number of pages (excluding appendices):	12
Test object:	HIMax System
Customer/Manufacturer:	HIMA Paul Hildebrandt GmbH + Co KG Industrial Automation Albert-Bassermann-Straße 28 68782 Brühl, Germany
Order No./Date:	Framework agreement between HIMA and TÜV dated 2004-09-02
Test Institute:	TÜV Rheinland Industrie Service GmbH Automation, Software and Information Technology Am Grauen Stein 51105 Köln
TÜV Offer No./Date:	Proposal for the framework agreement between HIMA and TÜV dated 2002-10
TÜV Order No./Date:	10230605 dated 2009-07-01
Inspectors:	Dipl.-Ing. (FH) Oliver Busa Dipl.-Ing. Klaus Kemp
Test location:	See Test Institute
Testing duration:	June 2009 - October 2009

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 content		Page
1	Scope	4
2	Standards forming the basis for the requirements	4
2.1	Standards	4
3	Identification of the test object	5
3.1	Manufacturer's documentation	6
3.2	TÜV documentation	8
4	Tests and test results	8
4.1	General	8
4.2	Description of the safety concept	9
4.3	Functional safety management	9
4.4	Review documentation	9
4.5	Measures for avoiding faults	10
4.6	Fault controlling measures	10
4.7	Inspection of the hardware changes	10
4.7.1	FMEA and fault injection	10
4.7.2	Tests of the electrical safety and immunity against environmental conditions	11
4.7.3	Evaluation of the safety-related parameters in accordance with IEC 61508 / EN 62021 and EN ISO 13849-1	11
4.8	Inspection of the software change	11
4.8.1	Test of the safety-related operating systems	11
4.8.2	SILworX programming system	12
4.9	Review of the requirements detailed in the application specific standards	12
5	Summary	12

1 Scope

The purpose of this approval is to determine if the newly developed I/O modules for the HIMax programmable electronic control system of HIMA Paul Hildebrandt GmbH + Co. KG can be used for risk reduction in applications up to SIL 3 in accordance with IEC 61508, IEC 61511 and EN 62061 and Cat. 4, PL e in accordance with EN ISO 13849-1.

Further, the approval shall investigate whether the changes performed to the system have an effect on the test and certification already completed [R7]. It shall also examine whether the system also meets requirements of the revised test standards specified in Section 2.

2 Standards forming the basis for the requirements

2.1 Standards

Functional safety

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

Application specific standards

- [2] EN ISO 13849-1:2008 + AC:2009
Safety of machinery - Safety-related parts of control systems
Part 1: General principles for design
- [3] EN 62061:2005
Safety of machinery - Functional safety of safety-related electrical/electronic/programmable electronic control systems
- [4] IEC 61511:2004, parts 1 - 3
Functional safety - Safety instrumented systems for the process industry sector
- [5] EN 50156-1:2004
Electrical Equipment for Furnaces
Part 1: Requirements for Application Design and Installation
- [6] NFPA 85:2007
Boiler and Combustion Systems Hazards Code
- [7] NFPA 86:2007
Standard for Ovens and Furnaces
- [8] NFPA 72:2007
National Fire Alarm Code
- [9] EN 298:2003
Automatic gas burner control systems for gas burners and gas burning appliances with or without fans
- [10] EN 12067-2:2004
Gas/air ratio controls for gas burners and for gas burning appliances
Part 2: Electronic types
- [11] EN 230:2005
Monobloc Oil Burners
Safety, control and regulation devices and safety times
- [12] EN 54-2:1997/A1:2007
Fire detection and fire alarm systems
Part 2: Control and indicating equipment

Electrical safety and immunity against environmental conditions

- [13] EN 61131-2:2007
Programmable Controllers
Part 2: Equipment requirements and tests

Electromagnetic compatibility

- [14] EN 61000-6-2:2005
Electromagnetic Compatibility (EMC)
- Generic Standards
- Immunity for Industrial Environments
- [15] EN 61000-6-4:2007
Electromagnetic Compatibility (EMC)
- Generic emission standard
- Residential, commercial, and light industry
- [16] EN 50130-4:1998 + A1:1998 + A2:2003 + Corr. 2003
Alarm systems
Part 4: Electromagnetic compatibility

3 Identification of the test object

During this test, eight new modules with an architecture based on the I/O modules already approved in [R4] were implemented for the HIMax system. Six modules were derived from the existing I/O modules by extending the channels. The two remaining modules are new developments. Tables 1 and 2 provide an overview of the corresponding I/O modules.

Table 1: Overview of the extended modules of the HIMax system

Product code	Description	Version
X-DI 16 01	Digital input module, 16 channels, 120 VAC	00
X-DI 32 03	Digital input module, 32 channels, 48 VDC	10
X-DI 64 01	Digital input module, 64 channels, 24 VDC	10
X-DO 12 02	Digital output module, 12 channels, 24 VDC, 2 A short-circuit monitoring (LS)	10
X-DO 24 02	Digital output module, 24 channels, 48 VDC, 0.5 A line monitoring (LS/LB)	10
X-DO 32 01	Digital output module, 32 channels, 24 VDC, 0.5 A short-circuit monitoring (LS)	10

Table 2: Overview of the new modules of the HIMax system

Product code	Description	Version
X-AO 16 01	Analog output module (16 channels, 4...20 mA)	10
X-CI 24 01	Counter module (24 channels, 0...20 kHz)	10

In addition to the firmware extension for the new output module and the counter module, changes were also performed to the HIMax system firmware modules approved in [R7]. The changes apply to the following HIMax system firmware modules.

Table 3: HIMax system firmware

Product code	Description	Version	CRC
HIMaxCPU_HA1_BS	Operating System for the HIMax Processor Module	3.6	0x11092abc
HIMaxIO_HA1_BS	Operating System for the HIMax I/O Module	3.4	0x402c3a13
HIMaxIO_HA3_BS	Operating System for the HIMax I/O Module	3.4	0xd7e5a888
HIMaxSB_HA2_BS	Operating System for the HIMax System Bus Module	3.6	0xe1db7ede

The programming environment for developing safety-related application programs was also changed and released by the manufacturer in a new version.

Table 4: HIMax system programming environment

Product code	Description	Version
SILworX	Programming System	3.30.0

3.1 Manufacturer's documentation

The following table includes the manufacturer's documentation lists and governing documents. More detailed specifications and schematic diagrams are listed in the corresponding document plans.

Table 5: Manufacturer's development documents

No.	Description	Rev.	Date
D1	HIMax & HIMatrix & ELOP III Documentation plan, File name: P9__PL01_DocPlan.sxw	1.78	2009-10-21
D2	CD Document plan, Plug-in module B210 "AO" / "XAO 16 01" File name: CDP_B210_MAX - X-AO 16 01.doc	1.1	2009-10-14
D3	CD Document plan, Plug-in module B212 "DI 24V 64 channels" / "XDI 64 01" File name: CDP_B212_MAX - XDI 64 01.doc	1.1	2009-10-14
D4	CD Document plan, Plug-in module B214 "DO 0.5A LB/LS EG" / "XDO 24 02" File name: CDP_B214_MAX - XDO 24 02.doc	1.1	2009-10-14
D5	CD Document plan, Plug-in module B218 "DO 2A EG" / "XDO 12 02" File name: CDP_B218_MAX - XDO 12 02.doc	1.1	2009-10-14
D6	CD Document plan, Plug-in module B219 "DO 24V 0.5A" / "XDO 32 01" File name: CDP_B219_MAX - XDO 32 01.doc	1.1	2009-10-14
D7	CD Document plan, Plug-in module B220 "CI 01" / "XCI 24 01" File name: CDP_B220_MAX - XCI 24 01.doc	1.1	2009-10-14

No.	Description	Rev.	Date
D8	CD Document plan, Plug-in module B221 "DI 48 VDC (24VDC) EG" / "XDI 32 03" File name: CDP_B221_MAX - XDI 32 03.doc	1.1	2009-10-14
D9	CD Document plan, Plug-in module B222 "DI 115VAC (48VAC) EG" / "XDI 16 01" File name: CDP_B222_MAX - XDI 16 01.doc	1.1	2009-10-14
D10	FMEA Module B210 File name: FM_B210_MAX.doc	1.1	2009-10-08
D11	FMEA Module B212 File name: FM_B212_MAX.doc	1.1	2009-10-13
D12	FMEA Module B214 File name: FM_B214_MAX.doc	1.1	2009-10-02
D13	FMEA Module B218 File name: FM_B218_MAX.doc	1.1	2009-10-13
D14	FMEA Module B219 File name: FM_B219_MAX.doc	1.1	2009-10-02
D15	FMEA Module B220 File name: FM_B220_MAX.doc	1.1	2009-10-13
D16	FMEA Module B221 File name: FM_B221_MAX.doc	1.1	2009-10-13
D17	FMEA Module B222 File name: FM_B222_MAX.doc	1.1	2009-10-13
D18	Safety plan for HIMax, HIMatrix and SILworX File name: P0001H20.doc	1.0	2007-05-04
D19	Effect analysis HIMAX-CPU-SB-IO-BS File name: p0606c00_HIMax-CPU_V1.22_V2.xx.doc	1.2	2009-02-04
D20	Effect analysis PADT V2-V3 File name: C904_0001_PADT_V2_V3.pdf	1.1	2009-10-15
D21	Immunity Report AMS-09-03 EMV_PROTOKOLL_C_HIMax_V3.pdf	C	2009-10-09
D22	QSE type approval HX01.06 Standard tests in accordance with IEC 61131-2:2007 File name: TQ_HX01.06.pdf	01	2009-10-15
D23	QSE type approval HX01.07 Test of the temperature warning threshold File name: TQ_HX01.07.pdf	A	2009-10-14
D24	QSE type approval HX01.10 Test at increased supply voltage File name: TQ_HX01.10.pdf	00	2009-10-23
D25	Calculation of the "average probability of failure on demand" and "failure per hour" for the HIMax system in accordance with IEC 61508	1.3	2009-09-28
D26	Calculation of $MTTF_d$ and DC for the HIMax system in accordance with ISO 13849-1	1.3	2009-10-12

Table 6: Safety manual and user manual for the HIMax system

No.	Description	Rev.
D27	HIMax Safety Manual HI 801 003 D File name: HI_801_003_D_Safety Manual HIMax_Rev.3.0.pdf	3.0 (0944)
D28	Release of the operating system for HIMax family File name: HI_801_042_D_HIMax_Releasenotes.pdf	4.0
D29	SILworX Release Notes File name: HI_801_108_D_SILworX_Releasenotes_6_0.pdf	6.0

3.2 TÜV documentation

Table 7: Previous test reports

No.	Description
R1	Report of the Re-Certification Audit of the Functional Safety Management System for HIMA Paul Hildebrandt GmbH + Co KG in Brühl, Germany based on IEC 61508 requirements Report No.: 968/FSM 100.05/08 dated 2008-08-15
R2	Report of the 4 th Surveillance Audit of the Functional Safety Management System for HIMA Paul Hildebrandt GmbH + Co KG Project Management and Engineering located in Brühl, Germany based on IEC 61508 and IEC 61511 requirements Report No.: 968/FSM 101.06/08 dated 2008-12-29
R3	Type Approval Test Report of the HIMax System 968/EZ 274.00/07 dated 2007-09-28, TÜV Rheinland Group
R4	Type Approval Test Report of the HIMax System 968/EZ 274.01/08 dated 2008-01-24, TÜV Rheinland Group
R5	Report about the modification approval of the HIMax System 968/EZ 274.02/08 dated 2008-08-11, TÜV Rheinland Group
R6	Test report on the supplementary testing of the HIMax System 968/EZ 274.03/08 dated 2008-11-21, TÜV Rheinland Group
R7	Test report about the modification approval of the safety-related automation system HIMax 968/EZ 274.04/09 dated 2009-01-16, TÜV Rheinland Group
R8	Test report on the changes performed on the programming system SILworX 2.46 968/EZ 274.05/09 dated 2009-07-02, TÜV Rheinland Group

4 Tests and test results

4.1 General

The measuring and test equipment, which has been used by the TÜV Rheinland Group in the tests described in the following, is subject to regular inspection and calibration. Only devices with valid calibration have been used. The devices used in the various tests are recorded in the inspector's documentation.

All considerations concerning uncertainty of the measurements, so far applicable, are stated in the inspector's documentation, too.

In cases where tests have been executed in an external test lab or in the test lab of the manufacturer and where the results of these tests have been used within the here documented approval, this has occurred after a positive assessment of the external test lab and the achieved test results in detail according to the Quality Management procedure QMA 3.310.05.

4.2 Description of the safety concept

The safety concept of the HIMax system verified in [R4] remains unchanged and is not affected by the changes.

Results

The test results from [R4] remain valid.

4.3 Functional safety management

The requirements of IEC 61508 [1] and IEC 61511 [4] for implementing, installing and maintaining a programmable electronic system were tested by the Test Institute during an audit of the manufacturer's functional safety management system [R1, R2].

Results

The positive results of the audit were taken into account during this test.

4.4 Review documentation

IEC 61508 [1] requires sufficient information for each completed phase within the overall safety life cycle of the hardware and software comprising the safety-related programmable system.

The manufacturer's documentation is structured hierarchically in accordance with the requirements and consists primarily of the following governing central documents:

- Safety requirement specifications
- Verification and validation planning
- Architecture documents, design documents, test specifications
- Verification and test results

The structure and organization of the documents is described in the operating procedure for storing documents and the documentation plans [D1] through [D9].

The following aspects were considered individually during the inspection of the documents:

- Version management of the documents
- Unambiguous assignment, comprehensibility
- Completeness of specification and documentation
- Consistency in itself and with other documents

Results

The examination of the manufacturer's documentation was concluded with a positive result.

4.5 Measures for avoiding faults

The manufacturer developed a Safety Plan [D18] for the system's overall safety life cycle in accordance with IEC 61508 [1]. This Safety Plan is obligatory with respect to the Functional Safety Management and specifies the measures for avoiding faults in accordance with IEC 61508-2 and IEC 61508-3 [1].

Based on the manufacturer's existing certified QM system, a separate Functional Safety Management audit was performed to verify and demonstrate the use and effectiveness of the measures for avoiding faults. The results of this audit are documented in a separate report [R1].

Results

The overall and the product-specific measures used for avoiding faults are sufficient and fulfill the test requirements of the test standards.

4.6 Fault controlling measures

The measures for controlling faults and failures during operation detailed in IEC 61508-2 [1] were selected in accordance with the required Safe Failure Fraction (SFF). The fault controlling measures were not affected by the changes performed.

Results

The test results from [R7] remain valid.

4.7 Inspection of the hardware changes

The changes performed to the modules (see Table 1: Overview of the Extended Modules of the HIMax System) were described by the manufacturer in a change and effect analysis [listed in D3 through D6, D8, D9]. The two new modules (see Table 2: Overview of the New Modules of the HIMax System) were developed in accordance with the measures for avoiding and controlling faults specified at system level.

The submitted documents were subjected to a review and discussed with the manufacturer.

Results

The theoretical test of the hardware extensions has demonstrated that the HIMax system with the modules specified in Table 1: Overview of the Extended Modules of the HIMax System and in Table 2: Overview of the New Modules of the HIMax System continues to meet the requirements for SIL 3 in accordance with IEC 61508 [1].

4.7.1 FMEA and fault injection

For all new modules, an FMEA [D10] through [D17] was performed by the manufacturer in accordance with the manufacturer's specification and was verified through internal reviews.

The fault injection was performed on the new modules taking the results from the FMEAs into account and were documented accordingly.

Results

The FMEA documents and the corresponding test documentation on the fault injection was verified on random samples. The reviews of FMEAs and fault injection were completed with a positive result.

4.7.2 Tests of the electrical safety and immunity against environmental conditions

The environmental test, the tests for electromagnetic compatibility and electrical safety in accordance with EN 61131-2 [13] and EN 54-2 [12] were performed accordingly and are documented in the protocols [D21] through [D24]. The tests were performed in the manufacturer's testing laboratory approved by the Test Institute.

The required tests were completed with a positive result. The test results were verified and are present at the Test Institute [D21] through [D24].

All system components are designed as enclosed units with an IP2x protection rating. The power supply for the components must meet the requirements for SELV.

Results

The test was accomplished positively with the approval of the test results.

4.7.3 Evaluation of the safety-related parameters in accordance with IEC 61508 / EN 62021 and EN ISO 13849-1

The calculations of the safety-related parameters for the modified and new modules were performed by the manufacturer [D25, D26] and subjected to a review by the Test Institute.

Results

The review demonstrated that the safety-related parameters for the individual modules and for typical system configurations (such as digital loop, analog loop, counter loop as mono and redundant system) meet the requirements for SIL 3/ SIL CL 3 in accordance with IEC 61508 and EN 62061 and for Cat. 4, PL e in accordance with EN ISO 13849-1. The offline proof test interval is 10 years.

The specifications for the safety-related parameters PFD/PFH and SSF are provided by the manufacturer upon request. Refer to the current version of the manufacturer's Safety Manual [D27] for information on additional boundary conditions.

4.8 Inspection of the software change

4.8.1 Test of the safety-related operating systems

The firmware changes performed to the modules specified in Table 3: HIMax System Firmware are described by the manufacturer in a change and effect analysis [D19].

The changes were discussed with the manufacturer and, based on the change and effect analysis [D19], they were subjected to a review.

The inspection was based on the measures for avoiding fault for SIL 3 specified in IEC 61508-3 [1].

The following test steps were performed:

- Review of the manufacturer's documents
- Verification of the measures for avoiding faults
- Examination of the changes performed
- Review of the software module tests performed
- Review of the system integration tests performed

Results

The theoretical analysis of the firmware changes and the verification of the performed tests has demonstrated that the software versions specified in Table 3: HIMax System Firmware continue to be suitable for meeting the requirements for SIL 3 as specified in IEC 61508 [1].

4.8.2 SILworX programming system

The manufacturer described the change performed to the SILworX programming system in a change and effect analysis [D20]. All changes are traced and documented by the manufacturer using a fault management system.

The manufacturer used regression testing to verify the performed changes.

The completeness and accuracy of the test protocols was verified.

Results

The review of the protocols was concluded with a positive result. The SILworX programming tool can continue to be used to develop safety-related applications.

4.9 Review of the requirements detailed in the application specific standards

The results as from [R7] continue to be valid with respect to the application-specific standards. New system requirements did not arise from the new edition [2] since changes were only made to the informative annex of the standard.

Results

The system under examination continues to meet the requirements for Cat. 4/PL e in accordance with EN ISO 13849-1 [2].

The system continues to be suitable for use in applications as detailed in the application-specific standards provided in Chapter 2.1.

The requirements and boundary conditions specified in the Safety Manual [D27] and in the application-specific standards to be used must be taken into account when engineering, implementing and starting up the systems.

5 Summary

The product fulfills the requirements of the test standards (Cat. 4 /PL e in accordance with EN ISO 13849-1, SIL CL 3 in accordance with EN 62061 / IEC 61508 / IEC 61511) and can be used in applications up to Cat. 4 / PL e in accordance with EN ISO 13849-1 and SIL 3 in accordance with EN 62061 / IEC 61508.

All remarks and instructions specified in the corresponding installation and operating instructions must be observed.

The SILworX programming tool must be used to program safety-related applications and configure the HIMax system.

Operating conditions and special functional characteristics of the HIMax system are described in the manufacturer's Safety Manual [D27].

The currently valid hardware and software versions should be retrieved from the currently valid module and firmware control version release list. The list is released together by the manufacturer and the test house.

Cologne, 2009-10-30
 TIS/ASI/Kst. 968 bu-ke-nie

Report released after review:
 Date: 2009-10-30

The inspectors



Dipl.-Ing. (FH) Oliver Busa



Dipl.-Ing. Klaus Kemp



Dipl.-Ing Gernot Klaes