

Automation, Software and Information Technology

**Test report on the changes of
the safety-related automation system
HIMax manufactured by
HIMA Paul Hildebrandt GmbH + Co KG**

**Report No.: 968/EZ 274.10/10
Date: 2010-08-31**

This report is the English translation of the
original German report

**Test report on the changes of
the safety-related automation system
HIMax manufactured by
HIMA Paul Hildebrandt GmbH + Co KG**

Report-No.:	968/EZ 274.10/10
Date:	2010-08-31
Number of pages:	11
Test object:	HIMax System
Customer/Manufacturer:	HIMA Paul Hildebrandt GmbH + Co KG Industrial Automation Albert-Bassermann-Straße 28 68782 Brühl Germany
TÜV 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 Germany
TÜV Offer No./Date:	Proposal for the framework agreement between HIMA and TÜV dated 2002-10
TÜV Order No./Date:	10450446 dated 2010-07-01
Inspectors:	Dipl.-Ing. (FH) Oliver Busa
Test location:	See Test Institute
Testing period:	August 2010

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	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	5
3.2	TÜV documentation	6
4	Tests performed and test results	7
4.1	General	7
4.2	Description of the safety concept	7
4.3	Functional Safety Management	8
4.4	Review documentation	8
4.5	Measures for avoiding faults	8
4.6	Fault controlling measures	9
4.7	Inspection of the hardware extensions	9
4.7.1	FMEA and fault injection	9
4.7.2	Tests of the electrical safety and immunity against environmental conditions	9
4.7.3	Evaluation of the safety-related parameters in accordance with IEC 61508 / EN 62061 and EN ISO 13849-1	10
4.8	Review of the requirements detailed in the application specific standards	10
5	Summary	10

1 Scope

The purpose of this test is to determine if the changes performed to the existing digital output modules X-DO 24 01, X-DO 24 02 and X-DO 32 01 of the programmable electronic control system HIMax from HIMA Paul Hildebrandt GmbH + Co KG have an influence on the certification for risk reduction in applications up to SIL 3 in accordance with IEC 61508, IEC 61511 and EN 62061, and up to Cat. 4 and PL e in accordance with EN ISO 13849-1.

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 resistance 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**

The modified modules X-DO 12 02, X-DO 24 01, X-DO 24 02 and X-DO 32 01, derived from the earlier modules already certified, were examined during this approval (see Table 4: Previous test reports). The modified modules and their versions are specified in the following table.

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

Product code	Description	Version
X-DO 12 02	HIMax digital output module 12 channels 2 A	11
X-DO 24 01	HIMax digital output module 24 channels with line diagnosis (OC/SC)	12, 13
X-DO 24 02	HIMax digital output module 24 channels with line diagnosis (OC/SC) 48 VDC	11
X-DO 32 01	HIMax digital output module 32 channels	11

3.1 **Manufacturer's documentation**

The following table includes the manufacturer's documents taken into account during the approval.

Table 2: Manufacturer's development documents

No.	Description	Rev.	Date
D1	Document plan (plug-in) module B203 "DO 24V 0.5A OC/SC" / "X-DO 24 01"	1.1	-
D2	Document plan (plug-in) module B214 "DO 0.5A OC/SC EG" / "X-DO 24 02"	1.2	-
D3	Document plan, (plug-in) module B218 "DO 2A EG" / "X-DO 12 02"	1.2	-
D4	Document plan, (plug-in) module B219 "DO 24V 0.5A" / "X-DO 32 01"	1.2	-
D5	Change and effect analysis module DO01 File name: AN_DO01_MAX.pdf	1.1	2010-05-12

No.	Description	Rev.	Date
D6	Change and effect analysis module DO01 File name: AN_DO02_MAX.pdf	1.1	2010-04-30
D7	Change and effect analysis (plug-in) module B203 "DO 24V 0.5A OC/SC" File name: AN_B203_MAX.pdf	1.3	2010-05-12
D8	Change and effect analysis (plug-in) module B214 "DO 0.5A OC/SC EG" File name: AN_B214_MAX.pdf	1.1	2010-05-12
D9	Change and effect analysis (plug-in) module B218 "DO 2A EG" File name: AN_B218_MAX.pdf	1.0	2010-05-11
D10	Change and effect analysis (plug-in) module B219 "DO 24V 0.5A" File name: AN_B219_MAX.pdf	1.1	2010-05-12
D11	Fault injection (plug-in) module B203 "DO 24V 0.5A OC/SC" File name: FV_B203_MAX.pdf	1.2	2010-04-30
D12	Fault injection (plug-in) module B214 "DO 0.5A OC/SC EG" File name: FV_B214_MAX.pdf	1.2	2010-05-12
D13	Fault injection (plug-in) module B218 "DO 2A EG" File name: FV_B218_MAX.pdf	1.2	2010-05-12
D14	Fault injection (plug-in) module B219 "DO 24V 0.5A" File name: FV_B219_MAX.pdf	1.2	2010-05-11
D15	EMC protocol AMS_09_05 File name: EMV PROTOKOLL_C_HIMax_XDO2401.pdf	C	2009-12-16
D16	Safety plan for HIMax, HIMatrix, SILworX File name: P0001H02.doc	1.0	2007-05-04

Table 3: HIMax system's Safety Manual and User Manual

No.	Description	Rev.
D17	HIMax Safety Manual HI 801 003 E File name: HI_801_002_D_Safety Manual HIMax_Rev.3.0.pdf	3.0 (0944)

3.2 TÜV documentation

Table 4: 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

No.	Description
R3	Type approval test report of the HIMax system Report No.: 968/EZ 274.00/07 dated 2007-09-28, TÜV Rheinland Group
R4	Type approval test report of the HIMax system Report No. 968/EZ 274.01/08 dated 2008-01-24, TÜV Rheinland Group
R5	Report to the change test of the HIMax system Report No. 968/EZ 274.02/08 dated 2008-08-11, TÜV Rheinland Group
R6	Test report on the supplementary testing of the HIMax system Report no. 968/EZ 274.03/08 dated 2008-11-21, TÜV Rheinland Group
R7	Report to the change test of the safety-related automation system HIMax Report No.: 968/EZ 274.04/09 dated 2009-01-16, TÜV Rheinland Group
R8	Test report on the changes performed to the programming system SILworX 2.46 Report No.: 968/EZ 274.05/09 dated 2009-07-02, TÜV Rheinland Group
R9	Report to the change test of the safety-related automation system HIMax Report No.: 968/EZ 274.06/09 dated 2009-10-30, TÜV Rheinland Group
R10	Report to the software change test of the safety-related automation system HIMax Report No.: 968/EZ 274.07/09 dated 2009-11-13, TÜV Rheinland Group
R11	Test report on the changes performed to the programming system SILworX 3.38 from HIMA Paul Hildebrandt GmbH + Co KG Report No.: 968/EZ 274.08/09 dated 2009-12-11, TÜV Rheinland Group
R12	Report to the change test of the safety-related automation system HIMax Report No.: 968/EZ 274.09/10 dated 2010-05-20, TÜV Rheinland Group

4 **Tests performed 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 reviewed 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 approval.

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-D4).

The following aspects were considered individually during the inspection of the documents specified in Section 3.1:

- 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 [D16] 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).

Results

The fault controlling measures were not affected by the changes performed.

The previous test results remain valid.

4.7 Inspection of the hardware extensions

The changes performed to the modules (see Table 1: Overview of the changed modules of the HIMax system) were described by the manufacturer in a change and effect analysis listed in [D5-D10].

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

Results

The theoretical assessment of the hardware modification has demonstrated that the HIMax system with the modules specified in Table 1: Overview of the changed 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

The fault injection was repeated on the changed modules taking the results from the effect analysis into account and was documented in [D11-D14].

The changes are minor and have no effect on the performed FMEAs.

Results

The test documentation on the fault injection was verified on random samples and was completed with a positive result.

4.7.2 Tests of the electrical safety and immunity against environmental conditions

Based on the changes [D5-D10], the environmental tests and the tests for electromagnetic compatibility in accordance with EN 61131-2 [13] were repeated to some extent and are documented in the protocol [D16]. The tests were performed in the manufacturer's testing laboratory approved by the Test Institute.

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

All tests that were considered as necessary, were repeated and completed with a positive result. The test results were verified and are present at the Test Institute. The review was successfully concluded by the acceptance of test.

4.7.3 Evaluation of the safety-related parameters in accordance with IEC 61508 / EN 62061 and EN ISO 13849-1

The changes have a negligible effect on the calculations of the safety-related parameters.

Results

The previous test results remain valid.

The information of the safety-related parameters PFD/PFH and SFF are provided by the manufacturer upon request. Refer to the current version of the manufacturer's Safety Manual [D17] for information on additional boundary conditions.

4.8 Review of the requirements detailed in the application specific standards

The previous test results continue to be valid with respect to the application-specific standards.

Results

The system continues to meet the requirements for Cat. 4 and 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 [D17] and in the application-specific standards to be used must be taken into account when engineering, implementing and commissioning the system.

5 Summary

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

The results of the previous tests (see Table 4: Previous test reports) continue to be valid.

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 [D17] and installation and operating instructions.

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 Institute.

Cologne, 2010-08-31
TIS/ASI/Kst. 968 bu-ke-ta

Report released after review:
Date: 2010-09-02

The expert



Dipl.-Ing. (FH) Oliver Busa



Dipl.-Ing. Stephan Hüb

Statement of the certification body

According to the test results documented in this report and the shown conformity to the relevant and applied standards respectively to their protection goals it is confirmed, that the certificate with the no.: 968/EZ 274.06/09 continues to be valid.

Cologne, 2010-09-02
TIS/ASI/Kst. 968 hä-ta

The Certifier



Dipl.-Ing. Stephan Hüb