

Automation, Software and Information Technology

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

**Report No.: 968/EZ 128.21/10
Date: 2010-10-08**

This report is the English translation of
the original German report

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

Report No.:	968/EZ 128.21/10
Date:	2010-10-08
Number of pages (excluding appendices):	9
Test objects:	HIMatrix MAXI-CPU V7.24 HIMatrix AM2000-CPU V7.24
Customer/Manufacturer:	HIMA Paul Hildebrandt GmbH + Co. KG Industrial Automation Albert-Bassermann-Straße 28 68782 Brühl Germany
HIMA 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 2010-07-07
Inspector:	Dipl.-Ing. (FH) Oliver Busa
Test location:	See Test Institute
Testing period:	October 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	Test object(s)	5
3.1	Identification of the test objects	5
3.2	Manufacturer's documentation	5
3.3	TÜV documentation	6
4	Tests performed and test results	7
4.1	General	7
4.2	Functional Safety Management	7
4.3	Inspection of the documentation	7
4.4	Measures for avoiding faults	8
4.5	Measures for controlling faults	8
4.6	Inspection of the software changes	8
4.6.1	Approval of the safety-related operating systems	8
5	Summary	9

1 **Scope**

The purpose of this review is to determine if the programmable electronic control system HIMatrix of HIMA Paul Hildebrandt GmbH + Co. KG continues to meet the requirements for risk reduction in applications up to SIL 3 in accordance with IEC 61508, IEC 61511 and EN 62061, 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: 1998-2000, parts 1-7
Functional safety of electrical/electronic/programmable electronic safety-related systems

Application specific standards

- [2] EN ISO 13849:2008
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 **Test object(s)**

3.1 Identification of the test objects

The AM2000/MAXI - CPU v7.24 software package is a modified version of the already certified AM2000/MAXI - CPU v7.14 [R19]. This is the operating system for the HIMatrix system, a product family of safety-related automation system from HIMA Paul Hildebrandt GmbH + Co. KG. All the various firmware versions within the HIMatrix product family are based on this software package. The modified operating system versions for HIMatrix with their system components are specified in Table 1: Software Modules of the HIMatrix System.

Table 1: Software modules of the HIMatrix system

Seq. no.	Module	Description	Version	CRC
S1	MAXICPU-HA-L2-BS	Safety-related operating system for the HIMatrix F35, F30, F31, F20	7.24	0xe87fd14e
S2	AMCPU-HA-L2-BS	Safety-related operating system for the HIMatrix F60	7.24	0xd9ca6e22

3.2 Manufacturer's documentation

The following table specifies the governing documents that were taken into account during this approval and the manufacturer's documentation plan. Detailed specifications and references to the documentation are defined in the documentation plan.

Seq. no.	Description	Rev.	Date
D1	SysSafeStd Documentation plan File name: P9__PL01_DocPlan_SysSafeStd.sxw	1.71	2010-09-28
D2	Safety plan for HIMax, HIMatrix and SILworX File name: P0001H02.doc	1.0	2007-05-04
D3	Effect analysis HIMAX-CPU-SB-IO-BS and RIONC-BS, ES-P.0606 File name: p0606c00_HIMax-CPU_V1.22_V2.xx.doc	1.7	2010-10-07
D4	HIMatrix Safety Manual HI 800 023 JEA File name: HI 800 023 JEA Safety Manual.pdf	JEA (0644)	

3.3 TÜV documentation

Table 2: Previous test reports

No.	Description
R1	Report of the 6 th Surveillance 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/FMS 100.07/10 dated 2010-08-10
R2	Report of the 5 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/FMS 101.07/09 dated 2009-12-23
R3	Test report of the type approval safety-related automation devices HIMatrix F30, HIMatrix F3 DIO 20/8 01, HIMatrix F60, HIMatrix F35 Report No. 968/EZ 128.00/02 dated 2002-05-24, TÜV Rheinland Group
R4	Test report to the software test AM2000/MAXI/RIO_CPU version 3.12 for HIMatrix F30, HIMatrix F3 DIO 20/8 01, HIMatrix F60, HIMatrix F35 Report No. 968/EZ 128.01/02 dated 2002-05-24, TÜV Rheinland Group
R5	Test report of the type approval safety-related automation devices HIMatrix F60, HIMatrix F35, HIMatrix F31, HIMatrix F30, HIMatrix F3 DIO 20/8 01, Report No. 968/EZ 128.00/02 dated 2002-05-24, TÜV Rheinland Group
R6	Test report to the software test AM2000/MAXI/RIO/RIO-NC - CPU v4.28 for the safety-related automation devices HIMatrix F60, HIMatrix F35, HIMatrix F31, HIMatrix F30, HIMatrix F3 DIO 20/8 01, HIMatrix RIO-NC Report No. 968/EZ 128.03/03 dated 2003-10-16, TÜV Rheinland Group
R7	Report about the type approval Report No.: 968/EZ 128.04/03 dated 2003-10-17, TÜV Rheinland Group
R8	Test report to the software test MAXI - CPU v4.32 for the safety-related automation devices HIMatrix F35, HIMatrix F31, HIMatrix F30 Report No. 968/EZ 128.05/03 dated 2003-11-28, TÜV Rheinland Group
R9	Test report to the software test AM2000/MAXI/RIO/RION-NC - CPU v4.50 RIOMONO - CPU v5.18 for the safety-related automation devices of the HIMatrix RIO, RIO-NC, RIOMONO series Report No. 968/EZ 128.06/04 dated 2004-08-11, TÜV Rheinland Group
R10	Test report to the software test AM2000/MAXI/RIO/RIO-NC - CPU v6.12 for the safety-related automation systems of the HIMatrix, RIO, RIO-NC series Report No. 968/EZ 128.07/05 dated 2005-09-03, TÜV Rheinland Group
R11	Test report of the type approval Report No. 968/EZ 128.08/05 dated 2005-09-06, TÜV Rheinland Group
R12	Test report to the software test Report No. 968/EZ 128.09/05 dated 2005-09-06, TÜV Rheinland Group
R13	Test report to the software test RIO-NC - CPU v6.32 for the safety-related automation systems of the RIO-NC series Report No. 968/EZ 128.10/05 dated 2005-12-22, TÜV Rheinland Group
R14	Test report to the software test Report No. 968/EZ 128.11/06, TÜV Rheinland Group
R15	Test report to the software test Report No. 968/EZ 128.12/06, TÜV Rheinland Group
R16	Test report about the software modification of the programming tool ELOP II Factory v8.52.0 Report No. 968/EZ 128.13/07 dated 2007-05-10, TÜV Rheinland Group

No.	Description
R17	Test report of the type approval Report No. 968/EZ 128.14/07 dated 2007-07-12, TÜV Rheinland Group
R18	Test report about the software modification AM2000/MAXI/RIO/RIO-NC - CPU v6.46 for the safety-related automation devices of the HIMatrix RIO series Report No. 968/EZ 128.15/07 dated 2007-06-20, TÜV Rheinland Group
R19	Test report on the change test of the safety-related automation devices HIMatrix F60, HIMatrix F35, HIMatrix F31, HIMatrix F30, HIMatrix F20 and HIMatrix RIO-NC Report No. 968/EZ 128.16/09 dated 2009-03-16, TÜV Rheinland Group
R20	Test report about the software modification AM2000/MAXI v6.100 of the safety-related automation devices HIMatrix F60, HIMatrix F35, HIMatrix F31, HIMatrix F30, HIMatrix F20 Report No. 968/EZ 128.17/09 dated 2009-05-08, TÜV Rheinland Group
R21	Test report on the changes performed on the programming system SILworX 2.46 Report No. 968/EZ 128.18/09 dated 2009-07-02, TÜV Rheinland Group
R22	Test report on the inspection of the safety-related automation system HIMatrix of the manufacturer Report No. 968/EZ 128.19/09 dated 2009-11-23, TÜV Rheinland Group
R23	Report to the change test of the safety-related automation system HIMatrix Report No.: 968/EZ 128 20/09 dated 2009-12-16, 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 Functional Safety Management

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

Results

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

4.3 Inspection of the documentation

During the approval, the modified documentation [D1] was subjected to a review based on the effect analysis [D3].

Primarily, the following aspects were considered 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.

4.4 Measures for avoiding faults

The manufacturer used the existing safety plan [D2] 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].

The measures for avoiding faults used during the modification were considered specific to the product and in accordance with the requirements of IEC 61508 for SIL 3.

Results

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

4.5 Measures for controlling faults

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 results from the previous approval remain valid.

4.6 Inspection of the software changes

4.6.1 Approval of the safety-related operating systems

The firmware changes performed to the software product [S1, S2] were described in details by the manufacturer in a change and effect analysis [D3] and verified with system integration and module tests.

Based on this analysis, the corresponding documents and software sources were subjected to a review. The review was based on the fault avoiding measures for SIL 3 specified in IEC 61508 [1].

The following test steps were performed:

- Review of the manufacturer's documents
- 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 1: Software Modules of the HIMatrix System continue to be suitable for meeting the requirements for SIL 3 as specified in IEC 61508 [1].

5 Summary

Based on the results of the inspection / review of the submitted documents and the test sample it can be confirmed that the product complies with the requirements of the relevant standards:

EN ISO 13849-1: Cat. 4 / PL e

EN 62061: SIL CL 3

IEC 61508: SIL 3

Hence it is suitable for the use in applications up to Cat. 4 / PL e acc. to EN ISO 13849-1 and SIL 3 acc. to EN 62061 / IEC 61508.

Operating conditions and special functional characteristics of the HIMatrix systems are described in the manufacturer's Safety Manual and shall be considered.

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, 2010-12-08
TIS/ASI/Kst. 968 bu-ta

Report released after review:
Datum: 2010-12-08

The expert



Dipl.-Ing. (FH) Oliver Busa



Dipl.-Ing. Klaus Kemp

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 128.19/09 dated 2009-11-23 remains further valid.

The associated "Revision List" is updated accordingly.

Cologne, 2010-10-08
TIS/ASI/Kst. 968 hä-ta

The certifier



Dipl.-Ing. Stephan Hüb