

Automation, Software and Information Technology

**Test report on the changes of the
safety-related automation system
HIMA H41q: H41q-MS, H41q-HS, H41q-HRS
HIMA H51q: H51q-MS, H51q-HS, H51q-HRS
manufactured by HIMA Paul Hildebrandt GmbH + Co KG**

**Report No.: 968/EZ 129.16/10
Date: 2010-11-09**

This report is the English translation of the
original German report

Test report on the changes of the safety-related automation system
HIMA H41q: H41q-MS, H41q-HS, H41q-HRS
HIMA H51q: H51q-MS, H51q-HS, H51q-HRS
manufactured by HIMA Paul Hildebrandt GmbH + Co KG

| | |
|--|---|
| Report No.: | 968/EZ 129.16/10 |
| Date: | 2010-11-09 |
| Number of pages (excluding appendices): | 11 |
| Test objects: | HIMA H41q: H41q-MS, H41q-HS, H41q-HRS HIMA H51q: H51q-MS, H51q-HS, H51q-HRS Operating system BS41q/51q - v7.0-8 (07.14) |
| 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: | Framework agreement between HIMA and TÜV dated 2002-10 |
| TÜV Order No./Date: | 10450446 dated 2010-07-07 |
| Inspectors: | Dipl.-Ing. (FH) Oliver Busa Dipl.-Ing. Klaus Kemp |
| Test location: | See Test Institute |
| Testing period: | May 2010 - November 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 | 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 | Tests of the electrical safety and immunity against environmental conditions | 8 |
| 4.7 | Requirements of EN ISO 13849-1 | 9 |
| 4.8 | Review of the requirements of the application specific standards | 11 |
| 5 | Summary | 11 |

1 **Scope**

The purpose of this review is to determine if the safety-related automation system of the H41q/H51q family continue to meet the requirements of the standards specified in Chapter 2.1 after the structural software changes.

Additionally, the safety-related automation system ability to fulfill the EN ISO 13849-1 requirements for Cat. 4/PL e must be verified. The revised editions of EN 61131-2 [13], EN 54-2 [12] and NFPA 72 [8] must be taken into account to ensure that the previous test results do not conflict with potential new requirements.

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
Safety of machinery - Safety-related parts of control systems
Part 1: General principles for design
- [3] IEC 61511:2004, parts 1-3
Functional safety - Safety instrumented systems for the process industry sector
- [4] EN 50156-1:2004
Electrical Equipment for Furnaces
Part 1: Requirements for Application Design and Installation
- [5] NFPA 85:2007
Boiler and Combustion Systems Hazards Code
- [6] NFPA 86:2007
Standard for Ovens and Furnaces
- [7] NFPA 72:2010
National Fire Alarm Code
- [8] EN 298:2003
Automatic gas burner control systems for gas burners and gas burning appliances with or without fans
- [9] EN 12067-2:2004
Gas/air ratio controls for gas burners and for gas burning appliances
Part 2, Electronic types
- [10] EN 230:2005
Monobloc Oil Burners
Safety, control and regulation devices and safety times
- [11] EN 54-2:1997 + AC:1999 + A1:2006
Fire detection and fire alarm systems
Part 2: Control and indicating equipment

Electrical safety and resistance against environmental conditions

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

Electromagnetic Compatibility

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

3 Identification of the test object

The object of this approval are the changes performed to the operating system of the safety-related H41q/H51q automation system. The v7.0-8 (07.14) version to be verified is a modification of the already approved v7.0-8 (06.04) version [R12], which also includes the change performed to v7.0-8 (06.05) version approved in [R15].

The system hardware remains unchanged compared to the previous tests.

Table 1: Released software version

| Seq. no. | Product | System | Version | CRC |
|----------|-----------|-----------|--------------|--------|
| S1 | BS41q/51q | H41q/H51q | 7.0-8(07.14) | 0x729F |

3.1 Manufacturer's documentation

The product documentation including the software sources of the operating system and the test documentation were provided by the manufacturer and archived by the Test Institute.

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

Table 2: Manufacturer's development documents

| No. | Description | Rev. | Date |
|-----|---|------|------------|
| D1 | Product documentation H51q(e), h51q__over.doc | 1.3 | 2010-09-09 |
| D2 | Documentation plan H41q/H51q, p0610pl00.doc | 1.2 | 2010-09-28 |
| D3 | Project manual BS41q/51q V7.0-8 (07.14), p0610h00.doc | 1.0 | 2010-09-21 |
| D4 | Requirement specification BS41q/51q V7.0-8 (07.14) p0610lp00.doc | 0.2 | 2010-09-08 |

| No. | Description | Rev. | Date |
|-----|--|------|------------|
| D5 | Change and effect analysis operating system BS41q/51q V7.0-8 (07.14), p0610c00.doc | 1.8 | 2010-09-09 |
| D6 | Product documentation revised documents, p0610d2.doc | 1.2 | 2010-09-28 |
| D7 | Testing coverage change and effect analysis of BS41q/51q V7.0-8 (07.14), p0610d3.doc | 1.1 | 2010-09-17 |
| D8 | Average probability of failures on demand and of failures per hour for the H41q/H51q system in accordance with IEC 61508 | 1.9 | 2005-03-22 |
| D9 | Calculation of MTTFd and DCavg for the H41q/H51q system in accordance with EN ISO 13849 | 1.3 | 2010-10-29 |
| D10 | Technical report No. 71377503 | - | 2010-10-28 |
| D11 | EMC Test table for HIQuad, TUEV_HIQUAD_EMCC_Overview_Rev0_1.xls | 0.1 | 2010-11-08 |

Table 3: Safety manual and user manual for the H41q/H51q system

| No. | Description | Rev. |
|-----|---|------|
| D12 | H41q/H51q safety-related controller H41q/H51q safety manual, HI 800 013 D | 1.0 |
| D13 | H41q/H51q safety-related controller H41q / H51q operating system manual OS41q/51q V7.0-8 (07.14), HI 800 104D | 1.0 |

3.2 TÜV documentation

Table 4: Previous test reports

| No. | Description |
|-----|--|
| R1 | Test report No.: 968/EZ 129.00/02 dated 2002-05-24 |
| R2 | Test report No.: 968/EZ 129.01/03 dated 2003-09-10 |
| R3 | Test report No.: 968/EZ 129.02/04 dated 2005-03-08 |
| R4 | Test report No.: 968/EZ 129.03/05 dated 2005-05-02 |
| R5 | Test report No.: 968/EZ 129.04/05 dated 2005-05-23 |
| R6 | Test report No.: 968/EZ 129.05/05 dated 2005-07-08 |
| R7 | Test report No.: 968/EZ 129.06/05 dated 2005-08-02 |
| R8 | Test report No.: 968/EZ 129.07/06 dated 2006-02-13 |
| R9 | Test report No.: 968/EZ 129.08/06 dated 2006-02-27 |
| R10 | Test report No.: 968/EZ 129.09/06 dated 2006-03-08 |
| R11 | Test report No.: 968/EZ 129.10/06 dated 2006-05-03 |
| R12 | Test report No.: 968/EZ 129.11/06 dated 2006-11-10 |
| R13 | Test report No.: 968/EZ 129.12/07 dated 2007-07-11 |
| R14 | Test report No.: 968/EZ 129.13/07 dated 2007-07-09 |

| No. | Description |
|-----|---|
| R15 | Test report No.: 968/EZ 129.14/07 dated 2007-09-04 |
| R16 | Test report No.: 968/EZ 129.15/08 dated 2008-10-31 |
| R17 | Test report No.: 968/FSM 100.07/10 dated 2010-08-10 |
| R18 | Test report No.: 968/FSM 101.07/09 dated 2009-12-23 |

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 [3] for implementing, installing and maintaining a programmable electronic system were tested by the test institute during the audit of the manufacturer's functional safety management system [R17, R18].

Results

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

4.3 **Inspection of the 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 - D3].

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.

4.4 Measures for avoiding faults

As far as applicable, the manufacturer took the IEC 61508 [1] requirements for SIL 3 into account to perform the changes to operating system and to document them to a satisfactory extent.

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 [R17].

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 previous approval results remain valid.

4.6 Tests of the electrical safety and immunity against environmental conditions

Based on the modified requirements from the revised editions of EN 61131-2 [13] few environmental tests were repeated and are documented in [D10].

The modified EMC requirements were reviewed by the manufacturer and compared to the tests already performed [D11]. The additional tests were repeated by the manufacturer and completed with a positive result.

The repeated tests were performed in an accredited testing laboratory or in a manufacturer's testing laboratory approved by the Test Institute.

The electrical safety requirements did not change. All system components are designed as enclosed units with an IP20 protection rating. The power supply for the components must meet the requirements for SELV/PELV.

Results

The environmental tests and the tests for electromagnetic compatibility were repeated and completed with a positive result. The test results were verified and admitted.

4.7 Requirements of EN ISO 13849-1

The following parameters must be evaluated to be able to estimate the performance level (PL):

- Mean Time to dangerous failure (MTTFd)
- Diagnostic coverage (DC)
- Common cause failure (CCF)
- Structure
- Behavior under fault conditions
- Safety-related software
- Systematic failures
- Safety function performed under predictable environmental conditions

Safety-related parameters (PFH, DC, CCF)

In accordance with Table 3 provided in EN ISO 13849, a PFH of at least 10^{-7} 1/h is required for a PL = e. This requirement is identical to the SIL 3 requirements in IEC 61508 [1] and therefore met.

To estimate the common cause failures (CCF), EN ISO 13849 assumes a β factor less than or equal to 2 %. During qualification in accordance with IEC 61508, the beta factors $\beta = 2$ % and $\beta_D = 1$ % were determined for the control systems under consideration such that an estimate according to Table F.1 can be made.

Structure

Each of the safety-related automation systems composing the H41q/H51q series and listed in Table 5, meet the requirements up to SIL 3 in accordance with IEC 61508 and Category 4 in accordance with EN 954-1. Therefore, these automation systems also meet the architecture requirements specified in Chapter 6.2.7 in [1].

Behavior under fault conditions

The requirement for PL = e with respect to the system behavior in the event of faults is that a single fault does not cause the loss of the safety function. If this detection is not possible, an accumulation of undetected faults must not cause the loss of the safety function. As the systems under consideration meet the requirements for Category 4 in accordance with EN 954, they also comply with the requirement for PL = e with respect to the behavior in the event of faults.

Safety-related software

For the design and development process of safety-related embedded software (SRESW), the measures for avoiding faults required for SIL 3 in accordance with IEC 61508-3 must be used to achieve PL = e in accordance with EN ISO 13849. The embedded software of these devices meets this requirement.

Systematic failures

The measures for avoiding and controlling systematic faults required in EN ISO 13849 were already considered during the approval in accordance with IEC 61508 and also meet the requirements in accordance with EN ISO 13849.

Estimation of the MTTF_d value

In accordance with Annex K, Table K.1 in EN ISO 13849-1, PL = e can be achieved in principle for complex, programmable electronics. According to an average probability of a dangerous failure per hour (PFH) and a PL = e in accordance with Table K.1, the mean time to the dangerous failure (MTTF_d) of each channel must be greater than 30 years. The corresponding data for the systems under consideration were treated in [D9]. The individual systems were considered with their respective inputs and outputs. The inspection of the H41q/H51q modular system was based on a typical configuration. All systems lie above the required MTTF_d and therefore also meet this requirement of EN ISO 13849 for PL e.

Table 5: Overview of the modules of the H41q/H51q System Family

| Product designation | Description of the safety-related module |
|----------------------------|--|
| F3236 | 16-channel input module |
| F3237 | 8-channel input module for proximity switches and mechanical contacts with line monitoring |
| F3238 | 8-channel input module, (Ex)i, for proximity switches and mechanical contacts with line monitoring |
| F3240 | 16-channel input module 120 VAC/DC |
| F3248 | 16-channel input module 48 VAC/DC |
| F3330 | 8-channel output module 12 W |
| F3331 | 8-channel output module with line monitoring 12 W |
| F3333 | 4-channel output module 48 W |
| F3334 | 4-channel output module with line monitoring 48 W |
| F3335 | 4-channel output module (Ex)i |
| F3348 | 8-channel output module 48 V, 24 W |
| F3349 | 8-channel output module with line monitoring 24/48 V, 24 W |
| F5220 | 2-channel counter module |
| F6213 | 4-channel analog input module |
| F6214 | 4-channel analog input module |
| F6217 | 8-channel analog input module |
| F6220 | 8-channel thermocouple input module (Ex)i |
| F6221 | 8 channel analog input module (Ex)i |
| F6705 | 2-channel analog output module |
| F7553 | Connection module EABUS2 |
| F8621A | Co-processor module |
| F8625 | Ethernet communication module |

| Product designation | Description of the safety-related module |
|---------------------|---|
| F8626 | PROFIBUS communication module |
| F8627 | Ethernet communication module 10/100BaseT |
| F8628 | PROFIBUS communication module |
| F8650X | Central module for H51q-MS, HS, HRS |
| F8652X | Central module for H51q-MS, HS, HRS |

Results

The test demonstrated that the modules listed in Table 5: Overview of the Moduels of the H41q/H51q System Family meet the EN ISO 13849 requirements for Cat. 4 / PL e.

4.8 Review of the requirements of the application specific standards

The verification of the relevant requirements from the new editions [7] and [11] demonstrates that the H41q/H51q system can continue to be used within the scope of EN 54-2 and NFPA 72.

Results

The system meets the requirements from the applications-specific standards [2] through [11] and 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 [D12] and in the application-specific standards to be used must be taken into account when engineering, implementing and commissioning the system.

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

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.

All remarks and instructions specified in the corresponding installation and operating instructions [D12] must be observed.

The ELOP II programming tool must be used to program safety-related applications and configure the H41q/H51q system.

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, 2010-11-09
 TIS/ASI/Kst. 968 bu-ke-nie

Report released after review:
 Date: 2010-11-09

The expert



Dipl.-Ing. (FH) Oliver Busa



Dipl.-Ing. Heinz Gall