

31.08.2010

Automation, Software und Informationstechnologie

**Prüfbericht über die Änderungsprüfung des
sicherheitsgerichteten Automatisierungssystems
HIMax des Herstellers
HIMA Paul Hildebrandt GmbH + Co KG**

**Bericht-Nr.: 968/EZ 274.10/10
Datum: 31.08.2010**

**Prüfbericht über die Änderungsprüfung des
sicherheitsgerichteten Automatisierungssystems
HIMax des Herstellers
HIMA Paul Hildebrandt GmbH + Co KG**

Bericht-Nr.:	968/EZ 274.10/10
Datum des Berichtes:	31.08.2010
Seitenzahl ohne Anlagen:	11
Prüfgegenstand:	HIMax System
Auftraggeber/Hersteller:	HIMA Paul Hildebrandt GmbH + Co KG Industrie-Automatisierung Albert-Bassermann-Straße 28 68782 Brühl
Auftrags-Nr. des Auftraggebers/Datum:	Rahmenvertrag HIMA/TÜV vom 02.09.2004
Prüfinstitut:	TÜV Rheinland Industrie Service GmbH Automation, Software und Informationstechnologie Am Grauen Stein 51105 Köln
Angebots-Nr. des Prüfinstitutes/Datum:	Vorschlag zum Rahmenvertrag HIMA/TÜV von 10.2002
Auftrags-Nr. des Prüfinstitutes/Datum:	10450446 vom 01.07.2010
Bearbeiter:	Dipl.-Ing. (FH) Oliver Busa
Prüfort:	siehe Prüfinstitut
Zeitraum der Prüfung:	August 2010

Die Prüfergebnisse beziehen sich ausschließlich auf die Prüfgegenstände.

Dieser Bericht darf ohne schriftliche Genehmigung des Prüfinstitutes nicht **auszugsweise** vervielfältigt werden.

Inhaltsverzeichnis		Seite
1	Aufgabenstellung	4
2	Prüfgrundlagen	4
2.1	Normen	4
3	Identifizierung des Prüfgegenstandes	5
3.1	Dokumentation des Herstellers	5
3.2	Dokumentation des Prüfinstituts	6
4	Durchgeführte Prüfungen und Prüfergebnisse	7
4.1	Allgemeines	7
4.2	Betrachtung der Sicherheitskonzeptes	7
4.3	Functional Safety Management	8
4.4	Inspektion der Dokumentation	8
4.5	Fehlervermeidende Maßnahmen	8
4.6	Fehlerbeherrschende Maßnahmen	9
4.7	Inspektion der Hardwareergänzungen	9
4.7.1	FMEA und Fehlerversuche	9
4.7.2	Prüfungen zur elektrischen Sicherheit und Beständigkeit gegenüber Umgebungsbedingungen	9
4.7.3	Bewertung der sicherheitstechnischen Kenngrößen nach IEC 61508 / EN 62061 und EN ISO 13849-1	10
4.8	Überprüfung der Anforderungen aus den applikationsspezifischen Standards	10
5	Zusammenfassung	10

1 Aufgabenstellung

Im Rahmen dieser Prüfung soll untersucht werden, ob die Modifikationen an den bestehenden digital Ausgabebaugruppen X-DO 24 01, X-DO 24 02 und X-DO 32 01 des programmierbaren elektronischen Steuerungssystems HIMax der Firma HIMA Paul Hildebrandt GmbH + Co. KG einen Einfluss auf die Prüfergebnisse für die Risikoreduzierung in Applikationen bis SIL 3 nach IEC 61508, IEC 61511 und EN 62061 sowie Kat. 4, PL e nach EN ISO 13849-1 haben.

2 Prüfgrundlagen

2.1 Normen

Funktionale Sicherheit

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

Applikationsspezifische Standards

- [2] EN ISO 13849-1:2008 + AC:2009
Sicherheit von Maschinen - Sicherheitsbezogene Teile von Steuerungen
Teil 1: Allgemeine Gestaltungsleitsätze
- [3] EN 62061:2005
Sicherheit von Maschinen - Funktionale Sicherheit sicherheitsbezogener elektronischer und programmierbarer elektronischer Steuerungssysteme
- [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
Brandmeldeanlagen
Teil 2: Brandmeldezentralen

Elektrische Sicherheit und Beständigkeit gegenüber Umgebungsbedingungen

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

Elektromagnetische Verträglichkeit

- [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 Identifizierung des Prüfgegenstandes

Im Rahmen dieser Prüfung wurden die Änderungen an den Baugruppen X-DO 12 02, X-DO 24 01, X-DO 24 02 und X-DO 32 01 untersucht, deren Vorgänger bereits in vorangegangenen Prüfungen betrachtet und zertifiziert wurden (siehe Tabelle 4: Vorangegangene Prüfberichte). Die geänderten Baugruppen und deren neuer Versionsstand ist in der folgenden aufgeführt.

Tabelle 1: Baugruppenübersicht der geänderten Baugruppen des HIMax Systems

Produktbezeichnung	Beschreibung	Version
X-DO 12 02	HIMax Digital-Ausgabe-Baugruppe 12 Kanäle 2A	11
X-DO 24 01	HIMax Digital-Ausgabe-Baugruppe 24 Kanäle mit Leitungsdiagnose (LB/LS)	12, 13
X-DO 24 02	HIMax Digital-Ausgabe-Baugruppe 24 Kanäle mit Leitungsdiagnose (LB/LS) 48Vdc	11
X-DO 32 01	HIMax Digital-Ausgabe-Baugruppe 32 Kanäle	11

3.1 Dokumentation des Herstellers

Die folgende Tabelle enthält die während der Prüfung betrachteten Dokumente des Herstellers.

Tabelle 2: Entwicklungsdokumente des Herstellers

Nr.	Beschreibung	Rev.	Datum
D1	Dokumentenplan Steck-Baugruppe B203 "DO 24V 0,5A LB/LS" / "X-DO 24 01"	1.1	-
D2	Dokumentenplan Steck-Baugruppe B214 "DO 0,5A LB/LS EG" / "X-DO 24 02"	1.2	-
D3	Dokumentenplan Steck-Baugruppe B218 "DO 2A EG" / "X-DO 12 02"	1.2	-
D4	Dokumentenplan Steck-Baugruppe B219 "DO 24V 0,5A" / "X-DO 32 01"	1.2	-
D5	Änderungs- und Auswirkungsanalyse Modul DO01 Dateiname: AN_DO01_MAX.pdf	1.1	2010-05-12

Nr.	Beschreibung	Rev.	Datum
D6	Änderungs- und Auswirkungsanalyse Modul DO01 Dateiname: AN_DO02_MAX.pdf	1.1	2010-04-30
D7	Änderungs- und Auswirkungsanalyse (Steck-) Baugruppe B203 „DO 24V 0,5A LB/LS“ Dateiname: AN_B203_MAX.pdf	1.3	2010-05-12
D8	Änderungs- und Auswirkungsanalyse (Steck-) Baugruppe B214 „DO 0,5A LB/LS EG“ Dateiname: AN_B214_MAX.pdf	1.1	2010-05-12
D9	Änderungs- und Auswirkungsanalyse (Steck-) Baugruppe B218 „DO 2A EG“ Dateiname: AN_B218_MAX.pdf	1.0	2010-05-11
D10	Änderungs- und Auswirkungsanalyse (Steck-) Baugruppe B219 „DO 24V 0,5A“ Dateiname: AN_B219_MAX.pdf	1.1	2010-05-12
D11	Fehlerversuche (Steck-) Baugruppe B203 „DO 24V 0,5A LB/LS“ Dateiname: FV_B203_MAX.pdf	1.2	2010-04-30
D12	Fehlerversuche (Steck-) Baugruppe B214 „DO 0,5A LB/LS EG“ Dateiname: FV_B214_MAX.pdf	1.2	2010-05-12
D13	Fehlerversuche (Steck-) Baugruppe B218 „DO 2A EG“ Dateiname: FV_B218_MAX.pdf	1.2	2010-05-12
D14	Fehlerversuche (Steck-) Baugruppe B219 „DO 24V 0,5A“ Dateiname: FV_B219_MAX.pdf	1.2	2010-05-11
D15	EMV Protokoll AMS_09_05 Dateiname: EMV_PROTOKOLL_C_HIMax_XDO2401.pdf	C	2009-12-16
D16	Safetyplan für HIMax, HIMatrix, SILworX Dateiname: P0001H02.doc	1.0	2007-05-04

Tabelle 3: Sicherheits- und Benutzerhandbücher des HIMax Systems

Nr.	Beschreibung	Rev.
D17	HIMax Sicherheitshandbuch HI 801 002 D Dateiname: HI_801_002_D_Safety Manual HIMax_Rev.3.0.pdf	3.0 (0944)

3.2 Dokumentation des Prüfinstituts

Tabelle 4: Vorangegangene Prüfberichte

Nr.	Beschreibung
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 vom 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 vom 2008-12-29

Nr.	Beschreibung
R3	Bericht über die Typprüfung HIMax-System Bericht-Nr.: 968/EZ 274.00/07 vom 2007-09-28, TÜV Rheinland Group
R4	Bericht über die Typprüfung HIMax-System Bericht-Nr.: 968/EZ 274.01/08 vom 2008-01-24, TÜV Rheinland Group
R5	Bericht über die Änderungsprüfung HIMax-System Bericht-Nr.: 968/EZ 274.02/08 vom 2008-08-11, TÜV Rheinland Group
R6	Bericht über die Ergänzungsprüfung HIMax-System Bericht-Nr.: 968/EZ 274.03/08 vom 2008-11-21, TÜV Rheinland Group
R7	Prüfbericht über die Änderungsprüfung des sicherheitsgerichteten Automatisierungssystems HIMax Bericht-Nr.: 968/EZ 274.04/09 vom 2009-01-16, TÜV Rheinland Group
R8	Prüfbericht über die Änderungen am Programmiersystem SILworX 2.46 Bericht-Nr.: 968/EZ 274.05/09 vom 2009-07-02, TÜV Rheinland Group
R9	Prüfbericht über die Änderungsprüfung des sicherheitsgerichteten Automatisierungssystems HIMax Bericht-Nr.: 968/EZ 274.06/09 vom 2009-10-30, TÜV Rheinland Group
R10	Prüfbericht über die Software-Änderungsprüfung des sicherheitsgerichteten Automatisierungssystems HIMax Bericht-Nr.: 968/EZ 274.07/09 vom 2009-11-13, TÜV Rheinland Group
R11	Prüfbericht über die Änderungen am Programmiersystem SILworX 3.38 des Herstellers HIMA Paul Hildebrandt GmbH + Co KG Bericht-Nr.: 968/EZ 274.08/09 vom 2009-12-11, TÜV Rheinland Group
R12	Prüfbericht über die Änderungsprüfung des sicherheitsgerichteten Automatisierungssystems HIMax Bericht-Nr.: 968/EZ 274.09/10 vom 2010-05-20, TÜV Rheinland Group

4 Durchgeführte Prüfungen und Prüfergebnisse

4.1 Allgemeines

Die Mess- und Prüfmittel, die in den nachfolgend beschriebenen Prüfungen bei der TÜV Rheinland Group verwendet wurden, unterliegen der regelmäßigen Kontrolle und Kalibrierung. Es wurden nur gültig kalibrierte Geräte benutzt.

Welche Geräte in den verschiedenen Prüfungen eingesetzt wurden, ist in den Unterlagen der Sachverständigen festgehalten.

Bei allen Messungen, die Überlegungen hinsichtlich der Toleranz der Messwerte erforderten, sind diese ebenfalls den Unterlagen der Sachverständigen zu entnehmen.

Wurden Prüfungen in einer externen Prüfstelle oder vom Hersteller durchgeführt und wurden die Ergebnisse aus diesen Prüfungen im Rahmen der hier dokumentierten Prüfung verwendet, dann geschah dies nach einer positiven Bewertung des externen Prüflabors sowie der erzielten Prüfergebnisse im einzelnen entsprechend der Qualitätssicherungsanweisung QMA 3.310.05.

4.2 Betrachtung der Sicherheitskonzeptes

Das in [R4] geprüfte Sicherheitskonzept des HIMax Systems ist unverändert und wird durch die Änderungen nicht beeinflusst.

Ergebnis

Die Prüfergebnisse aus [R4] sind weiterhin gültig.

4.3 Functional Safety Management

Die Anforderungen der IEC 61508 [1] und IEC 61511 [4] zur Realisierung, Installation und Wartung eines programmierbaren elektronischen Systems wurden im Rahmen einer Auditierung des Functional Safety Management Systems des Herstellers durch das Prüfinstitut durchgeführt [R1, R2].

Ergebnis

Das positive Ergebnis der Auditierung wurde bei dieser Prüfung berücksichtigt.

4.4 Inspektion der Dokumentation

Die IEC 61508 [1] fordert hinreichende Informationen für jede abgeschlossene Phase des gesamten Sicherheitslebenszyklus der Hard- und Software des sicherheitsgerichteten programmierbaren Systems.

Die Dokumentation des Herstellers ist entsprechend den Anforderungen hierarchisch aufgebaut und umfasst im Wesentlichen die folgenden übergeordneten Zentraldokumente:

- Sicherheits-Anforderungsspezifikationen
- Verifikations- und Validationsplanung
- Architekturdokumente, Designdokumente, Testspezifikationen
- Verifikations- und Testergebnisse

Die Struktur und der Aufbau der Dokumentation geht aus den Arbeitsanweisungen zur Dokumentationsablage und den Dokumentationsplänen hervor [D1-D4].

Im Einzelnen wurde bei der Überprüfung der Unterlagen aus Abschnitt 3.1 auf folgende Punkte geachtet:

- Versionsverwaltung der Unterlagen
- Eindeutige Zuordenbarkeit, Verständlichkeit
- Vollständigkeit der Spezifikation und Dokumentation
- Konsistenz in sich und gegenüber anderen Unterlagen

Ergebnis

Die Überprüfung der Herstellerdokumente wurde mit einem positiven Ergebnis abgeschlossen.

4.5 Fehlervermeidende Maßnahmen

Für den gesamten Sicherheitslebenszyklus des Systems wurde entsprechend der IEC 61508 [1] seitens des Herstellers eine Safetyplan [D16] erstellt, der hinsichtlich des Functional Safety Managements bindend ist und die fehlervermeidenden Maßnahmen nach IEC 61508-2 und -3 [1] festlegt.

Zum Nachweis der Anwendung und Wirksamkeit der fehlervermeidenden Maßnahmen wurde basierend auf dem vorhandenen zertifizierten QM-System des Herstellers ein gesondertes Functional Safety Management-Audit vorgenommen. Das Ergebnis dieses Audits ist in einem gesonderten Bericht [R1] dokumentiert.

Ergebnis

Die angewandten produktspezifischen und übergeordneten fehlervermeidenden Maßnahmen sind ausreichend und erfüllen die Anforderungen der Prüfgrundlage.

4.6 Fehlerbeherrschende Maßnahmen

Die nach IEC 61508-2 [1] geforderten Maßnahmen zur Beherrschung von Fehler und Ausfällen während des Betriebes sind entsprechend der geforderten Safe Failure Fraction (SFF) ausgewählt worden.

Ergebnis

Die fehlerbeherrschenden Maßnahmen werden durch die durchgeführten Änderungen nicht beeinflusst.

Die vorangegangenen Prüfergebnisse behalten weiterhin Ihre Gültigkeit.

4.7 Inspektion der Hardwareergänzungen

Die Änderungen an den Baugruppen (siehe Tabelle 1: Baugruppenübersicht der geänderten Baugruppen des HIMax Systems) wurden durch den Hersteller in einer Änderungs- und Auswirkungsanalyse beschrieben [D5-D10].

Die eingereichten Unterlagen wurden einem Review unterzogen und mit dem Hersteller besprochen.

Ergebnis

Die theoretische Prüfung der Hardwaremodifikation hat ergeben, dass das HIMax System mit den in der Tabelle 1: Baugruppenübersicht der geänderten Baugruppen des HIMax Systems, aufgeführten Baugruppen weiterhin die Anforderungen entsprechend SIL 3 gemäß IEC 61508 [1] erfüllt.

4.7.1 FMEA und Fehlerversuche

Die Fehlerversuche an den geänderten Baugruppen wurden unter Berücksichtigung der Auswirkungsanalyse teilweise wiederholt und in [D11-D14] dokumentiert.

Die Änderungen sind geringfügig und haben keinen Einfluss auf die durchgeführten FMEAs.

Ergebnis

Die Testdokumentation der Fehlerversuche wurden stichprobenartig überprüft und mit einem positiven Ergebnis abgeschlossen.

4.7.2 Prüfungen zur elektrischen Sicherheit und Beständigkeit gegenüber Umgebungsbedingungen

Die Umweltprüfungen und Prüfungen zur elektromagnetischen Verträglichkeit nach EN 61131-2 [13] wurden basierend auf den Änderungen [D5-D10] teilweise wiederholt und sind im Protokoll [D16] dokumentiert. Die Prüfungen wurden in einem durch das Prüfinstitut anerkannten Prüflabor des Herstellers durchgeführt.

Alle Systemkomponenten sind als geschlossene Betriebsmittel mit der Schutzart IP2x ausgeführt. Die Versorgung der Komponenten muss mit einer Stromversorgung erfolgen, welche die Anforderungen für SELV erfüllt.

Ergebnis

Die als notwendig angesehenen Tests wurden wiederholt und mit positiven Ergebnis abgeschlossen. Die Prüfergebnisse wurden überprüft und liegen dem Prüfinstitut vor. Die Prüfung wurden durch die Anerkennung der Prüfergebnisse positiv abgeschlossen.

4.7.3 **Bewertung der sicherheitstechnischen Kenngrößen nach IEC 61508 / EN 62061 und EN ISO 13849-1**

Die Änderungen haben einen vernachlässigbaren Einfluss auf die Berechnungen der sicherheitstechnischen Kenngrößen.

Ergebnis

Die vorangegangenen Prüfergebnisse behalten weiterhin Ihre Gültigkeit.

Die Angaben zu den sicherheitstechnischen Kenngrößen PFD/PFH und SFF werden auf Anfrage vom Hersteller zur Verfügung gestellt. Weitere zusätzliche Randbedingungen sind dem aktuellen Sicherheitshandbuch des Herstellers [D17] zu entnehmen.

4.8 **Überprüfung der Anforderungen aus den applikationsspezifischen Standards**

Die vorangegangenen Prüfergebnisse bleiben im Bezug auf die applikationsspezifischen Standards weiterhin gültig.

Ergebnis

Das System erfüllt weiterhin die Anforderungen der EN ISO 13849-1 [2] für Kat. 4/PL e.

Das System ist weiterhin geeignet in Anwendungen der in Abschnitt 2.1 aufgeführten applikationsspezifischen Standards eingesetzt zu werden.

Die Anforderungen und Randbedingungen des Sicherheitshandbuches [D17] sowie der anzuwendenden applikationsspezifischen Standards müssen bei der Projektierung, Umsetzung und Inbetriebnahme berücksichtigt werden.

5 **Zusammenfassung**

Das Produkt erfüllt die Anforderungen der Prüfgrundlagen (Kat. 4 / PL e nach EN ISO 13849-1, SIL CL 3 nach EN 62061 / IEC 61508 / IEC 61511) und kann in Anwendungen bis Kat. 4 / PL e nach EN ISO 13849-1 und SIL 3 nach EN 62061 / IEC 61508 eingesetzt werden.

Die Ergebnisse der vorangegangenen Prüfungen (siehe Tabelle 4: Vorangegangene Prüfberichte) behalten weiterhin ihre Gültigkeit.

Zur Programmierung von sicherheitsgerichteten Applikation und Konfiguration des HIMax Systems muss die Programmierumgebung SILworX verwendet werden.

Einsatzbedingungen und funktionale Besonderheiten des HIMax Systems sind dem Sicherheitshandbuch [D17] sowie den Installations- und Betriebsanleitungen des Herstellers zu entnehmen.

Die jeweils aktuelle Hardware- und Softwareversion ist der aktuell gültigen Liste zur Verfolgung der Versionsfreigaben der Baugruppen und der Firmware zu entnehmen. Diese Liste wird gemeinsam vom Hersteller und von der Prüfstelle freigegeben.

Köln, 31.08.2010
TIS/ASI/Kst. 968 bu-ke-ta

Bericht nach Review freigegeben:
Datum: 02.09.2010

Der Sachverständige



Dipl.-Ing. (FH) Oliver Busa



Dipl.-Ing. Stephan Häb

Stellungnahme der Zertifizierungsstelle:

Entsprechend den Ergebnissen der in diesem Bericht dokumentierten Prüfung und der nachgewiesenen Konformität zu den genannten Prüfgrundlagen bzw. zu deren Schutzziele wird bestätigt, dass das Zertifikat mit der Nr. 968/EZ 274.06/09 weiterhin seine Gültigkeit behält.

Köln, 2010-09-02
TIS/ASI/Kst. 968 hae-ta

Der Zertifizierer



Dipl.-Ing. Stephan Hüb