

16.03.2009

**Automation, Software und Informationstechnologie**

**Prüfbericht über die Änderungsprüfung der  
sicherheitsgerichteten Automatisierungsgeräte  
HIMatrix F60, HIMatrix F35, HIMatrix F31, HIMatrix F30,  
HIMatrix F20 und HIMatrix RIO-NC  
des Herstellers  
HIMA Paul Hildebrandt GmbH + Co KG**

**Bericht-Nr.: 968/EZ 128.16/09  
Datum: 16.03.2009**

**Prüfbericht über die Änderungsprüfung der  
sicherheitsgerichteten Automatisierungsgeräte  
HIMatrix F60, HIMatrix F35, HIMatrix F31, HIMatrix F30,  
HIMatrix F20 und HIMatrix RIO-NC  
des Herstellers  
HIMA Paul Hildebrandt GmbH + Co KG**

<b>Bericht-Nr.:</b>	968/EZ 128.16/09
<b>Datum des Berichtes:</b>	16.03.2009
<b>Seitenzahl ohne Anlagen:</b>	10
<b>Prüfgegenstand:</b>	HIMatrix F60 HIMatrix F35 HIMatrix F31 HIMatrix F30 HIMatrix F20 HIMatrix RIO-NC
<b>Auftraggeber/Hersteller:</b>	HIMA Paul Hildebrandt GmbH + Co KG Industrie-Automatisierung Albert-Bassermann-Straße 28 68782 Brühl
<b>Auftrags-Nr. des Auftraggebers/Datum:</b>	Rahmenvertrag HIMA/TÜV vom 02.09.2004
<b>Prüfinstitut:</b>	TÜV Rheinland Industrie Service GmbH Automation, Software und Informationstechnologie Am Grauen Stein 51105 Köln
<b>Angebots-Nr. des Prüfinstitutes/Datum:</b>	Vorschlag zum Rahmenvertrag HIMA/TÜV von 10.2002
<b>Auftrags-Nr. des Prüfinstitutes/Datum:</b>	10015410 vom 01.07.2008
<b>Bearbeiter:</b>	Dipl.-Ing.(FH) Oliver Busa Dipl.-Ing. Klaus Kemp
<b>Prüfort:</b>	siehe Prüfinstitut
<b>Zeitraum der Prüfung:</b>	September 2008 - März 2009

Die Prüfergebnisse beziehen sich ausschließlich auf die Prüfgegenstände.

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

<b>Inhaltsverzeichnis</b>		<b>Seite</b>
1	Aufgabenstellung	4
2	Prüfgrundlagen	4
2.1	Normen	4
3	Identifizierung des Prüfgegenstandes	5
3.1	Dokumentation des Herstellers	6
3.2	Dokumentation des Prüfinstituts	7
4	Durchgeführte Prüfungen und Prüfergebnisse	7
4.1	Allgemeines	7
4.2	Inspektion der Dokumente	7
4.3	Functional Safety Management	8
4.4	Betrachtung der Sicherheitskonzeptes	8
4.5	Fehlervermeidende Maßnahmen	8
4.6	Prüfungen zur elektrischen Sicherheit und Beständigkeit gegenüber Umgebungsbedingungen	8
4.7	Bewertung der sicherheitstechnischen Kenngrößen nach IEC 61508	9
4.8	Inspektion der Softwareänderungen	9
4.9	Überprüfung der Anforderungen aus den applikationsspezifischen Standards	9
5	Zusammenfassung	10

16.03.2009

## **1 Aufgabenstellung**

Im Rahmen dieser Änderungsprüfung soll untersucht werden, ob die sicherheitstechnischen Automatisierungsgeräte der HIMatrix Systemfamilie nach der Umstrukturierung der Software die Anforderungen der in Kapitel 2.1 aufgeführten Standards weiterhin erfüllen. Darüber hinaus soll geklärt werden, ob auch die erhöhten Störfestigkeitsgrade, die sich aus der EN 62061 ergeben, von den sicherheitsgerichteten Automatisierungsgeräten erfüllt werden und ob die neuen Ausgabestände der EN 230 [11] und der NFPA 72 [8] nicht im Widerspruch zu den Ergebnissen aus den vorrangegangenen Prüfungen stehen.

Die sicherheitsgerichteten Automatisierungsgeräte F60, F35, F31, F30, F20 sowie RIO-NC der Firma HIMA Paul Hildebrandt GmbH + Co. KG sind bereits mit dem vorliegenden Prüfbericht-Nr. 968/EZ 128.14/07 vom 2007-07-12 der TÜV Industrie Service GmbH, Automation, Software und Informationstechnologie nach den Prüfgrundlagen Abs. 2 zertifiziert worden mit Ausnahme der beiden neuen Ausgabestände der EN 230 [11] und der NFPA 72 [8].

## **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 13849-1:2006  
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

16.03.2009

- [11] EN 230:2005  
 Monobloc Oil Burners  
 Safety, control and regulation devices and safety times
- [12] EN54-2:1997 / A1:2007  
 Brandmeldeanlagen  
 Teil 2, Brandmeldezentralen

#### Elektrische Sicherheit und Beständigkeit gegenüber Umgebungsbedingungen

- [13] EN 61131-2:2003  
 Programmable Controllers  
 Part 2, Equipment requirements and tests

#### Elektromagnetische Verträglichkeit

- [14] EN 61000-6-2:2001  
 Electromagnetic Compatibility (EMC)  
 - Generic Standards  
 - Immunity for Industrial Environments
- [15] EN 61000-6-4:2001  
 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**

Das Softwarepaket AM2000/MAXI/RIO-NC - CPU v7.14 ist eine modifizierte Version des bereits geprüften Softwarepaketes AM2000/MAXI/RIO-NC - CPU v6.46 [R2]. Hierbei handelt es sich um das Betriebssystem einer Familie von sicherheitsgerichteten Automatisierungsgeräten des Herstellers HIMA Paul Hildebrandt GmbH + Co. KG. Das Softwarepaket dient als Basis für die unterschiedlichen Firmwareausführungen innerhalb der HIMatrix-Produktfamilie. Die verschiedenen Ausprägungen des Betriebssystems sowie die dazugehörigen Produktnamen sind in Tabelle 1 aufgeführt.

Tabelle 1: Freigegebene Softwareversionen

Softwareversionen				
Lfd. Nr.	Produkt	System	Version	CRC
[S1]	AMCPU-HA-BS	HIMatrix F60	V7.14	0x063E50F4
[S2]	MAXICPU-HA-BS	HIMatrix F35, F31, F30, F20	V7.14	0xF17A7732
[S3]	RIONCCPU-HA-BS	HIMatrix F1 DI 16 01 HIMatrix F2 DO 16 01 HIMatrix F2 DO 16 02 HIMatrix F2 DO 4 01 HIMatrix F2 DO 8 01 HIMatrix F3 AIO 8/4 01 HIMatrix F3 DIO 20/8 02 HIMatrix F3 DIO 16/8 01 HIMatrix F3 DIO 8/8 01	V7.14	0x49B535E0

16.03.2009

### 3.1 Dokumentation des Herstellers

Die folgende Tabelle enthält die Dokumentationslisten sowie übergeordneten Dokumente des Herstellers. Detaillierte Spezifikationen und Schaltpläne sind in den entsprechenden Dokumentationsplänen aufgelistet.

Tabelle 2: Entwicklungsdokumente des Herstellers

Nr.	Beschreibung	Rev.	Datum
D1	HIMax & HIMatrix & ELOP III Dokumentationsplan Dateiname: P9__PL01_DocPlan.sxw	1.71	2009-01-13
D2	SysSafestd Dokumentenplan Dateiname: P9__PL01_DocPlan_SysSafeStd.sxw	1.71	2009-01-28
D3	Safetyplan für HIMax, HIMatrix und SILworX Dateiname: P0001H02.doc	1.0	2007-05-04
D4	Immunity Report F1DI1601_EMV_PROTOKOLL_B_FS.pdf	B	2008-11-06
D5	Immunity Report F2D01601_EMV_PROTOKOLL_B_FS.pdf	B	2008-12-05
D6	Immunity Report F2D0401_EMV_PROTOKOLL_B_FS.pdf	B	2008-12-05
D7	Immunity Report F2DO801_EMV_PROTOKOLL_B_FS.pdf	B	2008-10-20
D8	Immunity Report F30_EMV_PROTOKOLL_B_FS.pdf	B	2008-10-14
D9	Immunity Report F31_EMV_PROTOKOLL_B_FS.pdf	B	2008-09-01
D10	Immunity Report F3DIO16801_EMV_PROTOKOLL_B_FS.pdf	B	2008-09-19
D11	Immunity Report F3DIO20802_EMV_PROTOKOLL_B_FS.pdf	B	2008-09-03
D12	Immunity Report F3DIO8801_EMV_PROTOKOLL_B_FS.pdf	B	2008-08-25
D13	Immunity Report F60_Teil1_EMV_PROTOKOLL_B_FS.pdf	B	2009-02-16
D14	Immunity Report F60_Teil2_EMV_PROTOKOLL_B_FS.pdf	B	2009-03-02
D15	Immunity Report F20_EMV_PROTOKOLL_B_FS.pdf	B	2008-12-11
D16	Immunity Report F35_EMV_PROTOKOLL_B_FS.pdf	B	2009-03-05
D17	Immunity Report F2DO1602_EMV_PROTOKOLL_B_FS.pdf	B	2009-03-06
D18	Immunity Report F3AIO8401_EMV_PROTOKOLL_B_FS.pdf	B	2009-03-10
D19	QSE-Typprüfung ES-P.0606	1.20	2008-12-12

16.03.2009

Tabelle 3: Sicherheits- und Benutzerhandbuch des HIMax Systems

Nr.	Beschreibung	Rev.
D20	HIMax Sicherheitshandbuch HI 800 022 JDA Dateiname: HI 800 022 JDA_Sicherheitshandbuch.pdf	JDA (0644)

### 3.2 Dokumentation des Prüfinstituts

Tabelle 4: Dokumentation des Prüfinstituts

Nr.	Beschreibung
R1	Prüfbericht zur Bauartprüfung Bericht-Nr. 968/EZ 128.14/07 vom 12.07.2007, TÜV Rheinland Group
R2	Prüfbericht zur Softwareänderung Bericht-Nr. 968/EZ 128.15/07 vom 20.06.2007, TÜV Rheinland Group
R3	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
R4	Report of the 4 <sup>th</sup> 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
R5	Review Protocol, Datum 2009-01-16 NFPA 72 - National Fire Alarm code 2007 -Edition - 2007 Edition

## 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 Inspektion der Dokumente

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

- Anforderungsspezifikationen
- Verifikations- und Validationsplanung
- Architekturdokumente
- Designdokumente
- Testspezifikationen
- Testprotokolle

16.03.2009

Die Struktur und der Aufbau der Dokumentation geht aus den Arbeitsanweisungen zur Dokumentationsablage und dem Dokumentationsplan hervor (siehe [D1]).

Im Einzelnen wurde bei der Überprüfung der Unterlagen 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.

### **4.3 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 [R3,R4].

#### Ergebnis

Das positive Ergebnis der Auditierung wurde bei dieser Änderungsprüfung berücksichtigt.

### **4.4 Betrachtung der Sicherheitskonzeptes**

Das in [R1] geprüfte Sicherheitskonzept des HIMatrix Systems ist unverändert und durch die Umstrukturierung der Software nicht beeinflusst.

#### Ergebnis

Die Prüfaussagen bezüglich des Sicherheitskonzeptes aus [R1] sind weiterhin gültig.

### **4.5 Fehlervermeidende Maßnahmen**

Für den gesamten Sicherheitslebenszyklus des Systems wurde entsprechend der IEC 61508 [1] seitens des Herstellers der bestehende Safetyplan verwendet, 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 [3] dokumentiert.

#### Ergebnis

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

### **4.6 Prüfungen zur elektrischen Sicherheit und Beständigkeit gegenüber Umgebungsbedingungen**

Die EMV-Prüfungen mit den erhöhten Störfestigkeitsgrade, die sich aus der EN 62061 [3] ergeben, wurden für alle Baugruppen durchgeführt [D4 - D18]. Die in der EN 54-2 [12] neu definierten Prüfungen zur EMV [16] wurden ebenfalls berücksichtigt und sind in [D4 - D18] dokumentiert.

16.03.2009

Die in der neuen Ausgabe der EN 230 [11] eingeflossenen Anforderungen für den Schutz gegen Umwelteinflüsse entsprechen denen der EN 298 [9]. Deshalb war eine erneute Prüfung nicht notwendig.

Die Prüfungen wurden in einem durch das Prüfinstitut anerkannten Prüflabor des Herstellers durchgeführt.

Die dokumentierten Ergebnisse zu den EMV-Prüfungen wurden im Rahmen eines Reviews überprüft.

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 zusätzlichen Prüfungen haben gezeigt, dass die Baugruppen auch die erhöhten Anforderungen der EN 62061 [3] sowie aus EN 54-2 [12] erfüllt werden.

#### **4.7 Bewertung der sicherheitstechnischen Kenngrößen nach IEC 61508**

Die Berechnungen der sicherheitstechnischen Kenngrößen wurden durch den Hersteller durchgeführt und bereits in [R1] grundsätzlich bewertet.

Ergebnis

Die Angaben zu den sicherheitstechnischen Kenngrößen PFD/PFH und SFF sowie zusätzliche Randbedingungen sind dem aktuellen Sicherheitshandbuch des Herstellers [D20] zu entnehmen und sind weiterhin gültig.

#### **4.8 Inspektion der Softwareänderungen**

Ausgehend von den Dokumentationsplänen [D1 - D3] wurden die entsprechenden Softwarearchitektur- und Designunterlagen einem Review unterzogen. Die Reviews fanden teilweise in Zusammenarbeit mit dem Hersteller statt.

Während der Durchführung der Prüfung wurden die fehlervermeidenden Maßnahmen der IEC 61508 [1] für SIL 3 zu Grunde gelegt.

Die Software wurde schwerpunktmäßig durch folgende Prüfschritte untersucht:

- Analyse der Änderungen
- Review der durchgeführten Modultests
- Review der durchgeführten QSE Tests

Ergebnis

Die Analyse der Softwareänderungen sowie die Überprüfung der durchgeführten Tests hat ergeben, dass die Software weiterhin geeignet ist die Anforderungen entsprechend SIL 3 gemäß IEC 61508 [1] zu erfüllen.

#### **4.9 Überprüfung der Anforderungen aus den applikationsspezifischen Standards**

Die sich aus den applikationsspezifischen Standards [2] bis [12] ergebenden produktspezifischen Anforderungen wurden bereits im Rahmen der Prüfungen [R1, R2] betrachtet.

Durch die neuen Ausgabestände der Standards [8], [11], [12] ergaben sich keine neuen Anforderungen an das System.

16.03.2009

### Ergebnis

Die Ergebnisse aus [R1, R2] bleiben im Bezug auf die applikationsspezifischen Standards weiterhin gültig.

Die Anforderungen und Randbedingungen aus dem Benutzerhandbuch [D20] sowie der anzuwendenden applikationsspezifischen Standards müssen bei der Projektierung, Umsetzung und Inbetriebnahme berücksichtigt werden.

## **5 Zusammenfassung**

Die Änderungsprüfung hat ergeben, dass die sicherheitsgerichteten Automatisierungsgeräte der HIMatrix Systemfamilie aus Tabelle 1 weiterhin die Anforderungen der IEC 61508 [1], IEC 61511 [4], EN 62061 [3] bis SIL 3, sowie Kat.4, PL e der EN ISO 13849-1 [2] erfüllen.

Bezüglich der Anwendung der Systeme im Bereich der EN 54-2 und NFPA 72 ist anzumerken, dass nur die Geräte F35 und F60 über die Möglichkeit verfügen, Eingangs- und Ausgangskreise bezüglich Leitungsbruch/Leitungsschluss zu überwachen. Diese Geräte sind daher für Applikationen im Anwendungsbereich der EN 54-2 und NFPA 72 einsetzbar.

Einsatzbedingungen und funktionale Besonderheiten der einzelnen sicherheitsgerichteten Automatisierungsgeräte sind den aktuell gültigen Versionen der Sicherheitshandbücher des Herstellers zu entnehmen.

Die freigegebenen Hardware- und Softwareversionen sind der aktuell gültigen „Liste zur Verfolgung der Versionsfreigaben der Baugruppen und der Firmware“ zu entnehmen. Diese Liste wird gemeinsam vom Hersteller und dem Prüfinstitut freigegeben.

Köln, 16.03.2009  
TIS/ASI/Kst. 968 bu-ke-nie

Die Sachverständigen



Dipl.-Ing. (FH) Oliver Busa



Dipl.-Ing. Klaus Kemp

Bericht nach Review freigegeben:  
Datum: 16.03.2009



Dipl.-Ing. Heinz Gall