

08.10.2010

**Automation, Software und Informationstechnologie**

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

**Bericht-Nr.: 968/EZ 128.21/10**

**Datum: 08.10.2010**

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

<b>Bericht-Nr.:</b>	968/EZ 128.21/10
<b>Datum des Berichtes:</b>	08.10.2010
<b>Seitenzahl ohne Anlagen:</b>	10
<b>Prüfgegenstand:</b>	HIMatrix MAXI-CPU V7.24 HIMatrix AM2000-CPU V7.24
<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 and Information Technology Am Grauen Stein 51105 Köln Germany
<b>Angebots-Nr. des Prüfinstitutes/Datum:</b>	Vorschlag zum Rahmenvertrag HIMA/TÜV von 10.2002
<b>Auftrags-Nr. des Prüfinstitutes/Datum:</b>	10450446 vom 01.07.2010
<b>Bearbeiter:</b>	Dipl.-Ing. (FH) Oliver Busa
<b>Prüfort:</b>	siehe Prüfinstitut
<b>Zeitraum der Prüfung:</b>	Oktober 2010

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.	Prüfgegenstand	5
3.1	Identifizierung des Prüfgegenstandes	5
3.2	Dokumentation des Herstellers	5
3.3	Dokumentation des Prüfinstituts	6
4.	Durchgeführte Prüfungen und Prüfergebnisse	7
4.1	Allgemeines	7
4.2	Functional Safety Management	8
4.3	Inspektion der Dokumentation	8
4.4	Fehlervermeidende Maßnahmen	8
4.5	Fehlerbeherrschende Maßnahmen	8
4.6	Inspektion der Softwareänderungen	9
4.6.1	Prüfung der sicherheitsgerichteten Betriebssysteme	9
5.	Zusammenfassung	10

## 1 Aufgabenstellung

Im Rahmen dieser Änderungsprüfung soll festgestellt werden, ob das programmierbare elektronische Steuerungssystem HIMatrix der Firma HIMA Paul Hildebrandt GmbH + Co. KG weiterhin die Anforderungen 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 erfüllt.

## 2 Prüfgrundlagen

### 2.1 Normen

#### Funktionale Sicherheit

- [1] IEC 61508:1998-2000, parts 1 - 7  
Functional safety of electrical/electronic/programmable electronic safety related systems

#### Applikationsspezifische Standards

- [2] EN ISO 13849-1:2008  
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 Prüfgegenstand**

### **3.1 Identifizierung des Prüfgegenstandes**

Das Softwarepaket AM2000/MAXI - CPU v7.24 ist eine modifizierte Version des bereits geprüften Softwarepaketes AM2000/MAXI – CPU v7.14 [R19]. Hierbei handelt es sich um das Betriebssystem des HIMatrix-Systems, einer Produktfamilie 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 geänderten Ausführungen des Betriebssystems für das Produkt HIMatrix mit seinen Systemkomponenten ist in der Tabelle 1: Softwaremodule des HIMatrix Systems aufgeführt.

Tabelle 1: Softwaremodule des HIMatrix Systems

Lfd. Nr.	Modul	Beschreibung	Version	CRC
S1	MAXICPU-HA-L2-BS	Sicherheitsgerichtetes Betriebssystem für HIMatrix F35, F30, F31, F20	7.24	0xe87fd14e
S2	AMCPU-HA-L2-BS	Sicherheitsgerichtetes Betriebssystem für HIMatrix F60	7.24	0xd9ca6e22

### **3.2 Dokumentation des Herstellers**

Die folgende Tabelle enthält die übergeordneten Dokumente die während dieser Prüfung betrachtet wurden sowie den Dokumentationsplan des Herstellers. Detaillierte Software-Spezifikationen sowie Verweise auf die Testspezifikationen sind im Dokumentationsplan aufgeführt.

Lfd. Nr.	Beschreibung	Rev.	Datum
D1	SysSafeStd Dokumentationsplan Dateiname: P9__PL01_DocPlan_SysSafeStd.sxw	1.71	2010-09-28
D2	Safetyplan für HIMax, HIMatrix und SILworX Dateiname: P0001H02.doc	1.0	2007-05-04

Lfd. Nr.	Beschreibung	Rev.	Datum
D3	Auswirkungsanalyse HIMAX-CPU-SB-IO-BS und RIONC-BS, ES-P.0606 Dateiname: p0606c00_HIMax-CPU_V1.22_V2.xx.doc	1.7	2010-10-07
D4	HIMatrix Sicherheitshandbuch HI 800 022 JDA Dateiname: HI 800 022 JDA_Sicherheitshandbuch.pdf	JDA (0644)	-

### 3.3 Dokumentation des Prüfinstituts

Tabelle 2: Vorangegangene Prüfberichte

Nr.	Beschreibung
R1	Report of the 6 <sup>th</sup> 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/FSM 100.07/10 vom 2010-08-10
R2	Report of the 5 <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 101.07/09 vom 2009-12-23
R3	Prüfbericht zur Bauartprüfung Sicherheitsgerichtete Automatisierungsgeräte HIMatrix F30; HIMatrix F3 DIO 20/8 01; HIMatrix F60; HIMatrix F35 Bericht-Nr. 968/EZ 128.00/02 vom 2002-05-24, TÜV Rheinland Group
R4	Prüfbericht zur Softwareprüfung AM2000/MAXI/RIO_CPU Version 3.12 für HIMatrix F30; HIMatrix F3 DIO 20/8 01; HIMatrix F60; HIMatrix F35 Bericht-Nr. 968/EZ 128.01/02 vom 2002-05-24, TÜV Rheinland Group
R5	Prüfbericht zur Bauartprüfung Sicherheitsgerichtete Automatisierungsgeräte HIMatrix F60; HIMatrix F35; HIMatrix F31; HIMatrix F30; HIMatrix F3 DIO 20/8 01 Bericht-Nr. 968/EZ 128.02/03 vom 2003-03-25, TÜV Rheinland Group
R6	Prüfbericht zur Softwareprüfung AM2000/MAXI/RIO/RIO-NC – CPU v4.28 für die sicherheitsgerichteten Automatisierungsgeräte HIMatrix F60, HIMatrix F35, HIMatrix F31, HIMatrix F30 HIMatrix F3 DIO 20/8 01, HIMatrix RIO-NC Bericht-Nr. 968/EZ 128.03/03 vom 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	Prüfbericht zur Softwareprüfung MAXI – CPU v4.32 für die sicherheitsgerichteten Automatisierungsgeräte HIMatrix F35, HIMatrix F31, HIMatrix F30 Bericht-Nr. 968/EZ 128.05/03 vom 2003-11-28, TÜV Rheinland Group
R9	Prüfbericht zur Softwareprüfung AM2000/MAXI/RIO/RIO-NC – CPU v4.50 RIOMONO – CPU v5.18 für die sicherheitsgerichteten Automatisierungsgeräte der HIMatrix, RIO, RIO-NC, RIOMONO – Serie Bericht-Nr. 968/EZ 128.06/04 vom 2004-08-11, TÜV Rheinland Group
R10	Prüfbericht über die Softwareprüfung AM2000/MAXI/RIO/RIO-NC – CPU v6.12 für die sicherheitsgerichteten Automatisierungssysteme der HIMatrix, RIO, RIO-NC – Serie Bericht-Nr. 968/EZ 128.07/05 vom 2005-09-03, TÜV Rheinland Group
R11	Prüfbericht zur Bauartprüfung Bericht-Nr. 968/EZ 128.08/05, vom 06.09.2005, TÜV Rheinland Group
R12	Prüfbericht zur Softwareprüfung Bericht-Nr. 968/EZ 128.09/05 vom 2005-09-06, TÜV Rheinland Group
R13	Prüfbericht über die Softwareprüfung RIO-NC – CPU v6.32 für die sicherheitsgerichteten Automatisierungssysteme der RIO-NC – Serie Bericht-Nr. 968/EZ 128.10/05, vom 22.12.2005, TÜV Rheinland Group

Nr.	Beschreibung
R14	Prüfbericht zur Softwareprüfung Bericht-Nr. 968/EZ 128.11/06, TÜV Rheinland Group
R15	Prüfbericht zur Softwareprüfung Bericht-Nr. 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 Bericht-Nr. 968/EZ 128.13/07, vom 10.05.2007, TÜV Rheinland Group
R17	Prüfbericht zur Bauartprüfung Bericht-Nr. 968/EZ 128.14/07 vom 12.07.2007, TÜV Rheinland Group
R18	Prüfbericht über die Softwareänderungsprüfung AM2000/MAXI/RIO/RIO-NC - CPU v6.46 für die sicherheitsgerichteten Automatisierungsgeräte der HIMatrix, RIO - Serie Bericht-Nr. 968/EZ 128.15/07 vom 20.06.2007, TÜV Rheinland Group
R19	Prüfbericht über die Änderungsprüfung der sicherheitsgerichteten Automati- sierungsgeräte HIMatrix F60, HIMatrix F35, HIMatrix F31, HIMatrix F30, HIMatrix F20 und HIMatrix RIO-NC Bericht-Nr. 968/EZ 128.16/09 vom 16.03.2009, TÜV Rheinland Group
R20	Prüfbericht über die Software - Änderungsprüfung AM2000/MAXI v6.100 der sicherheitsgerichteten Automatisierungsgeräte HIMatrix F60, HIMatrix F35, HIMatrix F31, HIMatrix F30, HIMatrix F20 Bericht-Nr. 968/EZ 128.17/09 vom 08.05.2009, TÜV Rheinland Group
R21	Prüfbericht über die Änderungen am Programmiersystem SILworX 2.46 Bericht-Nr. 968/EZ 128.18/09 vom 02.07.2009, TÜV Rheinland Group
R22	Prüfbericht über die Prüfung des sicherheitsgerichteten Automatisierungssystems HIMatrix Bericht-Nr. 968/EZ 128.19/09 vom 23.11.2009, TÜV Rheinland Group
R23	Prüfbericht über die Änderungsprüfung des sicherheitsgerichteten Automatisierungssystems HIMatrix Bericht-Nr.: 968/EZ 128 20/09 vom 16.12.2009, 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 Functional Safety Management

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

##### Ergebnis

Das positive Ergebnis der Auditierung wurde bei dieser Änderungsprüfung berücksichtigt.

#### 4.3 Inspektion der Dokumentation

Im Rahmen der Prüfung wurden die geänderte Dokumentation [D1] basierend auf der Auswirkungsanalyse [D3] einem Review unterzogen.

Im wesentlichen wurde dabei 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.

#### 4.4 Fehlervermeidende Maßnahmen

Für den gesamten Sicherheitslebenszyklus des Systems wurde entsprechend der IEC 61508 [1] seitens des Herstellers der bestehende Safetyplan [D2] 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 [R1] dokumentiert.

Die fehlervermeidenden Maßnahmen die im Rahmen der Modifikation angewandt wurden, wurden produktspezifisch nach den Anforderungen der IEC 61508 für SIL 3 betrachtet.

##### Ergebnis

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

#### 4.5 Fehlerbeherrschende Maßnahmen

Die nach IEC 61508-2 [1] geforderten Maßnahmen zur Beherrschung von Fehlern 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 Prüfergebnisse der vorangegangenen Prüfungen behalten weiterhin Ihre Gültigkeit.

## 4.6 Inspektion der Softwareänderungen

### 4.6.1 Prüfung der sicherheitsgerichteten Betriebssysteme

Die Firmwareänderungen am Softwareprodukt [S1, S2] wurden durch den Hersteller ausführlich in einer Auswirkungs- und Änderungsanalyse [D3] beschrieben und durch Modultests und Systemintegrationstests verifiziert.

Ausgehend von dieser Analyse wurden die geänderten Dokumente sowie die Softwarequellen einem Review unterzogen. Während dem Review wurden die fehlervermeidenden Maßnahmen der IEC 61508 [1] für SIL 3 zu Grunde gelegt.

Die folgenden Prüfschritte wurden durchgeführt:

- Prüfung der fehlervermeidenden Maßnahmen
- Untersuchung der durchgeführten Änderungen
- Review der durchgeführten Softwaremodultests
- Review der durchgeführten Systemintegrationstests

#### Ergebnis

Die theoretische Analyse der Firmwareänderungen sowie die Überprüfung der durchgeführten Tests hat ergeben, dass die in Tabelle 1: Softwaremodule des HIMatrix Systems aufgeführten Softwareversionen weiterhin geeignet sind, die Anforderungen entsprechend SIL 3 gemäß IEC 61508 [1] zu erfüllen.

## 5 Zusammenfassung

Basierend auf den Ergebnissen des Reviews der eingereichten Unterlagen kann bestätigt werden, dass das Produkt die Anforderungen der Prüfgrundlagen erfüllt:

EN ISO 13849-1: Kat. 4 / PL e  
EN 62061: SIL CL 3  
IEC 61508: SIL 3

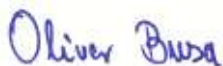
Es ist somit geeignet zum Einsatz in Anwendungen bis Kat. 4 / PL e nach EN ISO 13849-1 und SIL 3 nach EN 62061 / IEC 61508.

Einsatzbedingungen und funktionale Besonderheiten der HIMatrix Systeme sind dem Sicherheitshandbuch 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, 2010-12-08  
TIS/ASI/Kst. 968 bu-ta

Der Sachverständige



Dipl.-Ing. (FH) Oliver Busa

Bericht nach Review freigegeben:  
Datum: 2010-12-08



Dipl.-Ing. Klaus Kemp

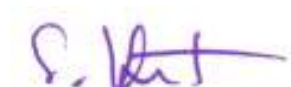
**Stellungnahme der Zertifizierungsstelle:**

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 128.19/09 weiterhin seine Gültigkeit behält.

Die zugehörige Modulliste mit den Revisionen wird entsprechend aktualisiert.

Köln, 08.10.2010  
TIS/ASI/Kst. 968 hä-ta

Der Zertifizierer



Dipl.-Ing. Stephan Hüb