

Automation, Software und Informationstechnologie

Prüfbericht zur Erweiterung der Bauartprüfung

**Sicherheitsgerichtete Automatisierungsgeräte
HIMatrix F60, HIMatrix F35, HIMatrix F31, HIMatrix F30,
HIMatrix F20, HIMatrix F3 DIO 20/8 01,
HIMatrix RIO-NC des Herstellers
HIMA Paul Hildebrandt GmbH + Co KG**

Bericht-Nr.: 968/EZ 128.14/07

Datum: 12.07.2007

Prüfbericht zur Erweiterung der Bauartprüfung**Sicherheitsgerichtete Automatisierungsgeräte**

**HIMatrix F60, HIMatrix F35, HIMatrix F31, HIMatrix F30, HIMatrix F20,
HIMatrix F3 DIO 20/8 01, HIMatrix RIO-NC des Herstellers
HIMA Paul Hildebrandt GmbH + Co KG**

Bericht-Nr.:	968/EZ 128.14/07
Datum des Berichtes:	12.07.2007
Seitenzahl ohne Anlagen:	7
Prüfgegenstand:	HIMatrix F60 HIMatrix F35 HIMatrix F31 HIMatrix F30 HIMatrix F20 HIMatrix F3 DIO 20/8 01 HIMatrix RIO-NC
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:	9773950 vom 01.07.2007
Bearbeiter:	Dipl.-Ing. Klaus Kemp
Prüfort:	siehe Prüfinstitut
Zeitraum der Prüfung:	Juli 2007

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	4
3.1	Dokumentation des Herstellers	4
3.2	Dokumente der Prüfstelle	4
4	Durchgeführte Prüfungen und Prüfergebnisse	5
4.1	HIMatrix F20	5
4.2	Anforderungen der EN ISO 13849-1	5
4.3	Anforderungen der EN 62061	7
4.4	NFPA 85 und NFPA 86	7
5	Zusammenfassung	7

1 Aufgabenstellung

Im Rahmen dieser Ergänzungsprüfung soll untersucht werden, ob die sicherheitstechnischen Automatisierungsgeräte auch die Anforderungen der EN ISO 13849-1 und die der EN 62061 erfüllen. Ebenso wurden die beiden neuen Ausgaben der NFPA Standards [3] und [4] berücksichtigt.

Die sicherheitsgerichteten Automatisierungsgeräte F60, F35, F31, F30, F3 DIO20/8 sowie RIO-NC der Firma HIMA Paul Hildebrandt GmbH + Co. KG sind bereits mit dem vorliegenden Prüfbericht-Nr. 968/EZ 128.08/05 vom 2005-09-06 der TÜV Industrie Service GmbH, Automation, Software und Informationstechnologie nach den Prüfgrundlagen Abs. 2 zertifiziert worden.

Das sicherheitsgerichteten Automatisierungsgerät HIMatrix F20 wurde mit dem Prüfbericht-Nr. 968/EZ 181.01/05 vom 2005-08-02 zertifiziert.

2 Prüfgrundlagen

2.1 Normen

- [1] EN ISO 13849:2006-Teil1
Sicherheit von Maschinen - Sicherheitsbezogene Teile von Steuerungen
Teil 1: Allgemeine Gestaltungsleitsätze
- [2] DIN EN 62061:2005
Sicherheit von Maschinen - Funktionale Sicherheit sicherheitsbezogener, elektronischer und programmierbarer elektronischer Steuerungssysteme
- [3] NFPA 85:2007
Boiler and Combustion Systems Hazards Code
- [4] NFPA 86:2007
Standard for Ovens and Furnaces

3 Identifizierung des Prüfgegenstandes

Für diese Ergänzungsprüfung wurden keine Testmuster benötigt, da keine praktischen Prüfungen erforderlich waren.

3.1 Dokumentation des Herstellers

Dokumente des Herstellers			
Lfd. Nr.	Beschreibung	Rev.	Datum
D1	Berechnung des MTTFd und des DC _{avg} für das HIMatrix System nach ISO 13849	1.1	2007-05-20

3.2 Dokumente der Prüfstelle

Dokumente der Prüfstelle	
Lfd. Nr.	Beschreibung
P1	Prüfbericht zur Bauartprüfung Bericht-Nr. 968/EZ 128.08/05 vom 2005-09-06, TÜV Rheinland Group
P2	Prüfbericht zur Bauartprüfung Bericht-Nr. 968/EZ 181.01/05 vom 2005-08-02, TÜV Rheinland Group
P3	Review Protocol, Datum 2007-06-14 NFPA 85 - Boiler and Combustion Systems Hazards Code - 2007 Edition

Dokumente der Prüfstelle	
Lfd. Nr.	Beschreibung
P4	Review Protocol, Datum 2007-05-21 NFPA 86 - Standard for Ovens and Furnaces - 2007 Edition

4 Durchgeführte Prüfungen und Prüfergebnisse

4.1 HIMatrix F20

Da nunmehr die zugrundegelegten Prüfgrundlagen der HIMatrix F20 und die der restlichen Systemen aus der HIMatrix Familie identisch sind wurde das HIMatrix F20 System in den Prüfrahmen der HIMatrix Systemfamilie aufgenommen. Die Aussagen aus dem Prüfbericht /P2/ für die F20 behalten weiterhin ihre Gültigkeit.

4.2 Anforderungen der EN ISO 13849-1

Für eine Abschätzung des Performance Levels (PL) müssen die folgenden Parameter bewertet werden:

- Mean Time to dangerous failure (MTTFd)
- Diagnostic coverage (DC)
- Common cause failure (CCF)
- Struktur
- Verhalten unter Fehlerbedingungen
- Sicherheitsbezogene Software
- Systematische Ausfälle
- Ausführen der Sicherheitsfunktion unter vorhersehbaren Umgebungsbedingungen

Sicherheitstechnische Kenngrößen (PFH, DC, CCF)

Entsprechend der Tabelle 3 aus der EN ISO 13849 ist für ein PL = e ein PFH von mindestens 10^{-7} 1/h gefordert. Diese Anforderung ist mit der Anforderungen der IEC 61508 SIL 3 identisch und somit erfüllt.

Für die Abschätzung der Ausfälle aufgrund gemeinsamer Ursache (CCF) wird ein β -Faktor von kleiner oder gleich 2 % in der EN ISO 13849 angenommen. Für die betrachteten Steuerungssysteme wurden im Rahmen der Qualifizierung nach IEC 61508 die Beta-Faktoren von $\beta = 2 \%$ und $\beta_D = 1 \%$ ermittelt, so dass eine Abschätzung nach der Tabelle F.1 möglich ist.

Struktur

Jede der sicherheitsgerichteten Automatisierungsgeräte aus der HIMatrix Serie, welche in der Tabelle aufgeführt sind, erfüllen die Anforderungen der IEC 61508 bis SIL 3 sowie die Kategorie 4 der EN 954-1. Somit erfüllen diese Automatisierungsgeräte auch die Architektur Anforderung aus Kapitel 6.2.7 aus [1].

Verhalten unter Fehlerbedingungen

Voraussetzung für einen PL = e bezüglich dem Verhalten im Fehlerfall ist, dass ein einzelner Fehler nicht zum Verlust der Sicherheitsfunktion führt. Wenn diese Erkennung nicht möglich ist, darf eine Anhäufung von unerkannten Fehlern nicht zum Verlust der Sicherheitsfunktion führen. Da die betrachteten Systeme die Kategorie 4 der EN 954 erfüllen, erfüllen sie auch die Voraussetzungen bezüglich dem Fehlverhalten für den PL = e.

Sicherheitsbezogene Software

Für den Entwurf- und den Entwicklungsprozess von sicherheitsbezogene Embedded-Software (SRESW) und einem PL = e müssen nach der ISO EN 13849 die Maßnahmen zur Fehlervermeidung entsprechend der IEC 61508-3, SIL 3 angewendet werden. Dies ist für die Embedded-Software dieser Geräte erfüllt.

Systematische Ausfälle

Die Maßnahmen bezüglich der Vermeidung und der Beherrschung von systematischen Ausfällen, die die ISO EN 13849 fordert, wurden bereits bei der Prüfung nach IEC 61508 betrachtet und erfüllen auch die Anforderungen nach ISO EN 13849.

Abschätzung der MTTF_d Werte

Entsprechend dem Anhang K, Tabelle K.1, aus der EN ISO 13849 ist ein PL = e für komplexe, programmierbare Elektronik prinzipiell erreichbar. Entsprechend einer durchschnittliche Wahrscheinlichkeit eines gefährlichen Ausfalls je Stunde (PFH) und einen PL = e muss nach Tabelle K.1 die mittlere Zeit bis zum gefahrbringenden Ausfall jedes Kanals (MTTF_d) größer als 30 Jahre betragen. Für die untersuchten Systeme wurden die entsprechenden Daten in /D1/ aufbereitet. Dabei wurden die einzelnen Systeme jeweils mit ihren entsprechenden Eingängen und Ausgängen betrachtet. Bei dem Modularen System F60 wurde eine typische Konfiguration zugrundegelegt. Alle Systeme liegen über der geforderten MTTF_d und erfüllen somit auch diese Anforderung der EN ISO 13849 für PL = e.

Produkt	Modell	Beschreibung
Modulare PES	F60	PSE mit 6 Slots für I/O-Module
Kompaktes PES	F20	8 digitale Eingänge 8 digitale Ausgänge konfigurierbare Feldbusschnittstellen
Kompaktes PES	F35 01 F35 02	24 digitale Eingänge 8 analoge Eingänge 2 Zähler 8 digitale Ausgänge
Kompaktes PES	F31 01 F31 02	20 digitale Eingänge 8 digitale Ausgänge 2x / 4x Ethernet
Kompaktes PES	F30 01 F30 02	20 digitale Eingänge 8 digitale Ausgänge
Remote I/O	F3 DIO20/8 01	20 digitale Eingänge 8 digitale Ausgänge
Remote I/O-NC	F1 DI 16 01	16 digitale Eingänge 4 digitale Ausgänge
Remote I/O-NC	F2 DO 16 01	16 digitale Ausgänge
Remote I/O-NC	F2 DO 16 02	16 Relais-Ausgänge
Remote I/O-NC	F2 DO 4 01	4 digitale Ausgänge
Remote I/O-NC	F2 DO 8 02	8 Relais-Eingänge
Remote I/O-NC	F3 AIO 8/4 01	8 analog Eingänge 4 analog Ausgänge
Remote I/O-NC	F3 DIO 20/8 02	20 digitale Eingänge 8 digitale Ausgänge
Remote I/O-NC	F3 DIO 16/8 01	16 digitale Eingänge 8 digitale Ausgänge
Remote I/O-NC	F3 DIO 8/8 01	8 digitale Eingänge 8 digitale Ausgänge

Tabelle 1: Modellübersicht der HIMatrix System-Familie

4.3 Anforderungen der EN 62061

Da die HIMatrix Systeme die IEC 61508 SIL 3 erfüllen, können sie ebenso im Wirkungsbereich der EN 62061 eingesetzt werden.

Hierbei muss der Anwender auch die anderen Anforderungen aus den relevanten Standards bezüglich des Betriebs beachten.

4.4 NFPA 85 und NFPA 86

Die Überprüfung der relevanten Anforderungen aus den neuen Ausgaben [3] und [4] hat ergeben, dass die HIMatrix Systeme im Wirkungsbereich der NFPA 85 und NFPA 86 weiterhin eingesetzt werden können. Die Review-Protokolle [P3] und [P4] sind bei der Prüfstelle hinterlegt.

5 Zusammenfassung

Die Prüfung hat ergeben, dass die sicherheitsgerichteten Automatisierungsgeräte der HIMatrix Systemfamilie aus Tabelle 1 grundsätzlich die Anforderungen der EN ISO 13849, PL = e sowie die der EN 62061 erfüllen.

Darüber hinaus erfüllen die HIMatrix Systeme die Anforderungen der neuen NFPA 85 und NFPA 86.

Die Ergebnisse der Typprüfungen, wie sie in den Prüfberichten-Nr. 968/EZ 128.08/05 und Nr. 968/EZ 181.01/05 dargelegt wurden, bleiben weiter gültig.

Alle erforderlichen Bedingungen, die der Anwender für den sicherheitsgerichteten Einsatz der Produkte beachten muss, sind in den jeweiligen Sicherheitshandbüchern enthalten.

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.

Entsprechend dem Prüfergebnis wird eine neues Zertifikat Nr. 968/EZ 128.14/07 ausgegeben.

Köln, 12.07.2007
TIS/ASI/Kst. 968 ke-nie

Der Sachverständige



Dipl.-Ing. Klaus Kemp