

30.10.2009

Automation, Software und Informationstechnologie

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

**Bericht-Nr.: 968/EZ 274.06/09
Datum: 30.10.2009**

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

Bericht-Nr.: 968/EZ 274.06/09

Datum des Berichtes: 30.10.2009

Seitenzahl ohne Anlagen: 12

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:** 10230605 vom 01.07.2009

Bearbeiter: Dipl.-Ing. (FH) Oliver Busa
Dipl.-Ing. Klaus Kemp

Prüfort: siehe Prüfinstitut

Zeitraum der Prüfung: Juni 2009 - Oktober 2009

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	6
3.2	Dokumentation des Prüfinstituts	8
4	Durchgeführte Prüfungen und Prüfergebnisse	8
4.1	Allgemeines	8
4.2	Betrachtung der Sicherheitskonzeptes	8
4.3	Functional Safety Management	9
4.4	Inspektion der Dokumentation	9
4.5	Fehlervermeidende Maßnahmen	9
4.6	Fehlerbeherrschende Maßnahmen	10
4.7	Inspektion der Hardwareergänzungen	10
4.7.1	FMEA und Fehlerversuche	10
4.7.2	Prüfungen zur elektrischen Sicherheit und Beständigkeit gegenüber Umgebungsbedingungen	10
4.7.3	Bewertung der sicherheitstechnischen Kenngrößen nach IEC 61508 / EN 62061 und EN ISO 13849-1	11
4.8	Inspektion der Softwareänderungen	11
4.8.1	Prüfung der sicherheitsgerichteten Betriebssysteme	11
4.8.2	Programmiersystem SILworX	11
4.9	Überprüfung der Anforderungen aus den applikationsspezifischen Standards	12
5	Zusammenfassung	12

1 Aufgabenstellung

Im Rahmen dieser Prüfung soll untersucht werden, ob die neu entwickelten E/A Module für das programmierbare elektronische Steuerungssystem HIMax der Firma HIMA Paul Hildebrandt GmbH + Co. KG 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 eingesetzt werden können.

Weiterhin wird betrachtet, ob die durchgeführten Änderungen am System einen Einfluss auf die bereits durchgeführte Prüfung und Zertifizierung [R7] haben. Zusätzlich gilt es zu betrachten ob das System auch die Anforderungen der geänderten Prüfgrundlagen in Abschnitt 2 erfüllt.

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] EN54-2:1997/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 acht neue Baugruppen für das HIMax System eingeführt die auf der Architektur der bereits in [R4] geprüften E/A Baugruppen basieren. Sechs der Baugruppen wurden aus bestehenden E/A Baugruppen durch Erweiterung der Kanäle abgeleitet. Die beiden restlichen Baugruppen sind Neuentwicklungen. Die Tabellen 1 und 2 geben eine Übersicht über die entsprechenden E/A Baugruppen.

Tabelle 1: Baugruppenübersicht der erweiterten Baugruppen des HIMax Systems

Produktbezeichnung	Beschreibung	Version
X-DI 16 01	Digital-Eingabe-Baugruppe 16-kanalig, 120 Vac	00
X-DI 32 03	Digital -Eingabe-Baugruppe 32-kanalig, 48 Vdc	10
X-DI 64 01	Digital-Eingabe-Baugruppe 64-kanalig, 24 Vdc	10
X-DO 12 02	Digital-Ausgabe -Baugruppe 12-kanalig, 24V dc, 2 A Leitungsschlussüberwachung (LS)	10
X-DO 24 02	Digital-Ausgabe-Baugruppe 24-kanalig, 48 Vdc, 0,5 A Leitungsüberwachung (LS/LB)	10
X-DO 32 01	Digital-Ausgabe-Baugruppe 32-kanalig, 24 Vdc, 0,5 A Leitungsschlussüberwachung (LS)	10

Tabelle 2: Baugruppenübersicht der neuen Baugruppen des HIMax Systems

Produktbezeichnung	Beschreibung	Version
X-AO 16 01	Analoges Ausgangsmodul (16-kanalig, 4-20 mA)	10
X-CI 24 01	Zählmodul (24-kanalig, 0-20 kHz)	10

Neben der Firmwareerweiterung für das neue analoge Ausgangsmodul und der Zählerbaugruppe wurden Änderungen an den in [R7] geprüften Firmwaremodulen des HIMax Systems durchgeführt. Von den Änderungen sind die folgenden Firmwaremodule des HIMax Systems betroffen.

Tabelle 3: Firmware HIMax System

Produktbezeichnung	Beschreibung	Version	CRC
HIMaxCPU_HA1_BS	Betriebssystem HIMax CPU-Baugruppe	3.6	0x11092abc
HIMaxIO_HA1_BS	Betriebssystem HIMax IO-Baugruppen	3.4	0x402c3a13
HIMaxIO_HA3_BS	Betriebssystem HIMax IO-Baugruppen	3.4	0xd7e5a888
HIMaxSB_HA2_BS	Betriebssystem HIMax System-Baugruppe	3.6	0xe1db7ede

Die Programmierumgebung zur Erstellung sicherheitsgerichteter Applikationsprogramme wurde ebenfalls geändert und in einer neuen Version durch den Hersteller freigegeben.

Tabelle 4: Programmierumgebung HIMax System

Produktbezeichnung	Beschreibung	Version
SILworX	Programmier System	3.30.0

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 5: Entwicklungsdokumente des Herstellers

Nr.	Beschreibung	Rev.	Datum
D1	HIMax & HIMatrix & ELOP III Dokumentationsplan Dateiname: P9__PL01_DocPlan.sxw	1.78	2009-10-21
D2	CD Dokumentenplan Steck-Baugruppe B210 „AO“ / „XAO 16 01“ Dateiname: CDP_B210_MAX - XAO 16 01.doc	1.1	2009-10-14
D3	CD Dokumentenplan Steck-Baugruppe B212 „DI 24V 64Kanäle“ / „XDI 64 01“ Dateiname: CDP_B212_MAX - XDI 64 01.doc	1.1	2009-10-14
D4	CD Dokumentenplan Steck-Baugruppe B214 „DO 0,5A LB/LS EG“ / „XDO 24 02“ Dateiname: CDP_B214_MAX - XDO 24 02.doc	1.1	2009-10-14
D5	CD Dokumentenplan Steck-Baugruppe B218 „DO 2A EG“ / „XDO 12 02“ Dateiname: CDP_B218_MAX - XDO 12 02.doc	1.1	2009-10-14
D6	CD Dokumentenplan Steck-Baugruppe B219 „DO 24V 0,5A“ / „XDO 32 01“ Dateiname: CDP_B219_MAX - XDO 32 01.doc	1.1	2009-10-14
D7	CD Dokumentenplan Steck-Baugruppe B220 „CI 01“ / „XCI 24 01“ Dateiname: CDP_B220_MAX - XCI 24 01.doc	1.1	2009-10-14
D8	CD Dokumentenplan Steck-Baugruppe B221 „DI 48VDC (24VDC) EG“ / „XDI 32 03“ Dateiname: CDP_B221_MAX - XDI 32 03.doc	1.1	2009-10-14

Nr.	Beschreibung	Rev.	Datum
D9	CD Dokumentenplan Steck-Baugruppe B222 „DI 115VAC (48VAC) EG“ / „XDI 16 01“ Dateiname: CDP_B222_MAX - XDI 16 01.doc	1.1	2009-10-14
D10	FMEA Baugruppe B210 Dateiname: FM_B210_MAX.doc	1.1	2009-10-08
D11	FMEA Baugruppe B212 Dateiname: FM_B212_MAX.doc	1.1	2009-10-13
D12	FMEA Baugruppe B214 Dateiname: FM_B214_MAX.doc	1.1	2009-10-02
D13	FMEA Baugruppe B218 Dateiname: FM_B218_MAX.doc	1.1	2009-10-13
D14	FMEA Baugruppe B219 Dateiname: FM_B219_MAX.doc	1.1	2009-10-02
D15	FMEA Baugruppe B220 Dateiname: FM_B220_MAX.doc	1.1	2009-10-13
D16	FMEA Baugruppe B221 Dateiname: FM_B221_MAX.doc	1.1	2009-10-13
D17	FMEA Baugruppe B222 Dateiname: FM_B222_MAX.doc	1.1	2009-10-13
D18	Safetyplan für HIMax, HIMatrix und SILworX Dateiname: P0001H02.doc	1.0	2007-05-04
D19	Auswirkungsanalyse HIMAX-CPU-SB-IO-BS Dateiname: p0606c00_HIMax-CPU_V1.22_V2.xx.doc	1.2	2009-02-04
D20	Auswirkungsanalyse PADT V2-V3 Dateiname: C904_0001_PADT_V2_V3.odt	1.1	2009-10-15
D21	Immunity Report AMS-09-03 EMV_PROTOKOLL_C_HIMax_V3.pdf	C	2009-10-09
D22	QSE-Typprüfung HX01.06 Standardtests nach IEC 61131-2:2007 Dateiname: TQ_HX01.06.pdf	01	2009-10-15
D23	QSE-Typprüfung HX01.07 Prüfung der Temperaturwarnschwellen Dateiname: TQ_HX01.07.pdf	A	2009-10-14
D24	QSE-Typprüfung HX01.10 Prüfung bei erhöhter Versorgungsspannung Dateiname: TQ_HX01.10.pdf	00	2009-10-23
D25	Berechnung von „Average probability of failure on demand“ und „of failure per hour“ für das HIMax System nach IEC 61508	1.3	2009-09-28
D26	Berechnung des MTTF _d und des DC für das HIMax System nach ISO 13849-1	1.3	2009-10-12

Tabelle 6: Sicherheits- und Benutzerhandbücher des HIMax Systems

Nr.	Beschreibung	Rev.
D27	HIMax Sicherheitshandbuch HI 801 003 D Dateiname: HI_801_003_D_Safety Manual HIMax_Rev.3.0.pdf	3.0 (0944)
D28	Freigabe des Betriebssystems für die HIMax-Gerätefamilie Dateiname: HI_801_042_D_HIMax_Releasenotes.pdf	4.0
D29	SILworX Freigabenotizen Dateiname: HI_801_108_D_SILworX_Releasenotes_6_0.pdf	6.0

3.2 Dokumentation des Prüfinstituts

Tabelle 7: 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
R3	Bericht über die Typprüfung HIMax-System 968/EZ 274.00/07 vom 2007-09-28, TÜV Rheinland Group
R4	Bericht über die Typprüfung HIMax-System 968/EZ 274.01/08 vom 2008-01-24, TÜV Rheinland Group
R5	Bericht über die Änderungsprüfung HIMax-System 968/EZ 274.02/08 vom 2008-08-11, TÜV Rheinland Group
R6	Bericht über die Ergänzungsprüfung HIMax-System 968/EZ 274.03/08 vom 2008-11-21, TÜV Rheinland Group
R7	Prüfbericht über die Änderungsprüfung des sicherheitsgerichteten Automatisierungssystems HIMax 968/EZ 274.04/09 vom 2009-01-16, TÜV Rheinland Group
R8	Prüfbericht über die Änderungen am Programmiersystem SILworX 2.46 968/EZ 274.05/09 vom 2009-07-02, 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] bis [D9].

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.

4.5 Fehlervermeidende Maßnahmen

Für den gesamten Sicherheitslebenszyklus des Systems wurde entsprechend der IEC 61508 [1] seitens des Herstellers eine Safetyplan [D18] 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. Die fehlerbeherrschenden Maßnahmen werden durch die durchgeführten Änderungen nicht beeinflusst.

Ergebnis

Die Prüfergebnisse aus [R7] behalten weiterhin Ihre Gültigkeit.

4.7 Inspektion der Hardwareergänzungen

Die Änderungen an den Baugruppen (siehe Tabelle 1: Baugruppenübersicht der erweiterten Baugruppen des HIMax Systems) wurden durch den Hersteller in einer Änderungs- und Auswirkungsanalyse beschrieben [gelistet in den Dokumentenplänen D3 - D6, D8, D9]. Die beiden neuen Baugruppen (siehe Tabelle 2: Baugruppenübersicht der neuen Baugruppen des HIMax Systems) wurden entsprechend den fehlervermeidenden und den fehlerbeherrschenden Maßnahmen, die systemweit festgelegt sind, entwickelt.

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

Ergebnis

Die theoretische Prüfung der Hardwareergänzungen hat ergeben, dass das HIMax System mit den in der Tabelle 1: Baugruppenübersicht der erweiterten Baugruppen des HIMax Systems und in der Tabelle 2: Baugruppenübersicht der neuen Baugruppen des HIMax Systems aufgeführten Baugruppen die Anforderungen entsprechend SIL 3 gemäß IEC 61508 [1] erfüllen.

4.7.1 FMEA und Fehlerversuche

Für alle neuen Baugruppen wurde eine FMEA [D10] bis [D17] durch den Hersteller entsprechend den allgemeinen Herstellervorgaben erstellt und durch interne Reviews überprüft.

Die Fehlerversuche an den neuen Baugruppen wurden unter Berücksichtigung der Ergebnissen aus den FMEA's durchgeführt und wurden entsprechend dokumentiert.

Ergebnis

Die Unterlagen zu den FMEA's und die entsprechende Testdokumentation der Fehlerversuche wurden stichprobenartig überprüft. Die Reviews der FMEA's und der Fehlerversuche wurde mit einem positiven Ergebnis abgeschlossen..

4.7.2 Prüfungen zur elektrischen Sicherheit und Beständigkeit gegenüber Umgebungsbedingungen

Die Umweltprüfungen und Prüfungen zur elektromagnetischen Verträglichkeit sowie die Untersuchungen der elektrischen Sicherheit nach EN 61131-2 [13] und EN 54-2 [12] wurden entsprechend durchgeführt und sind in Protokollen [D21] bis [D24] dokumentiert. Die Prüfungen wurden in einem durch das Prüfinstitut anerkannten Prüflabor des Herstellers sowie in einem externen, akkreditierten Prüflabor durchgeführt.

Die notwendigen Tests wurden mit einem positiven Ergebnis abgeschlossen. Die Prüfergebnisse wurden überprüft und liegen dem Prüfinstitut vor [D21] bis [D24].

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 Prüfungen 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 Berechnungen der sicherheitstechnischen Kenngrößen der modifizierten und der neuen Baugruppen wurde durch den Hersteller durchgeführt [D25, D26] und durch das Prüfinstitut einem Review unterzogen.

Ergebnis

Das Review zeigt, dass die sicherheitstechnischen Kenngrößen der einzelnen Baugruppen sowie typischer Konfigurationen des Systems (digital loop, mixed loop, analog loop, counter loop als Monosystem und redundantes System) die Anforderungen entsprechend SIL 3/SIL CL 3 gemäß IEC 61508 und EN 62061 sowie Kategorie 4, PL e nach EN ISO 13849-1 erfüllen. Das Offline-Proof Test Intervall beträgt 10 Jahre.

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 [D27] zu entnehmen.

4.8 Inspektion der Softwareänderungen

4.8.1 Prüfung der sicherheitsgerichteten Betriebssysteme

Die Firmwareänderungen an den, in Tabelle 3: Firmware HIMax System aufgeführten, Modulen wurden durch den Hersteller in eine Änderungs- und Auswirkungsanalyse [D19] beschrieben.

Die Änderungen wurden mit dem Hersteller besprochen und auf Basis der Änderungs- und Auswirkungsanalyse [D19] einem Review unterzogen.

Während der Prüfung wurden die Maßnahmen zur Fehlervermeidung der IEC 61508-3 [1] für SIL 3 zu Grunde gelegt.

Die folgenden Prüfschritte wurden durchgeführt:

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

Ergebnis

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

4.8.2 Programmiersystem SILworX

Die Änderung am Programmiersystem SILworX wurden durch den Hersteller in einer Auswirkungs- und Änderungsanalyse [D20] beschrieben. Alle Änderungen werden durch den Hersteller mit Hilfe eines Fehlerverwaltungs-Systems gesteuert und dokumentiert.

Die durchgeführten Änderungen wurden durch den Hersteller mittels Regressionstest überprüft.

Die Protokolle der Tests wurden auf Vollständigkeit und Fehlerfreiheit überprüft.

Ergebnis

Das Review der Protokolle wurde mit einem positiven Ergebnis abgeschlossen. Die Programmierumgebung SILworX kann weiterhin für die Erstellung von sicherheitsgerichteten Anwendungen verwendet werden.

4.9 Überprüfung der Anforderungen aus den applikationsspezifischen Standards

Die Ergebnisse aus [R7] bleiben im Bezug auf die applikationsspezifischen Standards weiterhin gültig. Durch den neuen Ausgabestand von [2] ergaben sich keine neuen Anforderungen an das System, da nur Anpassungen im informativen Anhang des Standards vorgenommen wurden.

Ergebnis

Das hier untersuchte 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 [D27] 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 Hinweise in der zugehörigen Installations- und Betriebsanleitung sind zu beachten.

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 [D27] 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, 30.10.2009
 TIS/ASI/Kst. 968 bu-ke-nie

Bericht nach Review freigegeben:
 Datum: 30.10.2009

Die Sachverständigen



Dipl.-Ing. (FH) Oliver Busa



Dipl.-Ing. Klaus Kemp



Dipl.-Ing. Gernot Klaes