TÜV NORD CERT GmbH
Langemarckstraße 20

45141 Essen

TÜV NORD
Zertifizierung

Technischer Bericht

Prüflabor
Produktsicherheit

Bericht Nr. 3513 3273 / 3516 7236 vom 17.09.2015

Auftraggeber:	**Weidmüller Interface GmbH & Co. KG** Klingenbergerstr. 16 32758 Detmold
Prüfgegenstand:	**Fehlersicheres I/O-Modul:** UR20-8DI-PN-FSPS, UR20-8DI-PN-FSOE UR20-4DI-4DO-PN-FSPS, UR20-4DI-4DO-PN-FSOE
Hardware:	UR20-8DI-PN-FS**: **HW 01.11.00** UR20-4DI-4DO-PN-FS**: **HW 01.02.00**
Software:	UR20-4DI-4DO-PN-FSPS: **Version V01.00.02**, UR20-4DI-4DO-PN-FSOE, UR20-8DI-PN-FSPS, UR20-8DI-PN-FSOE: **Version V01.00.06**
Beurteilungsgrundlagen:	**EN 61508:2010 Teile 1-7** **EN 62061:2005 + A1:2013** **EN ISO 13849-1:2008**
Auftragsnummer:	8000428721 / 8000451740
Bearbeiter:	Herr Marc Willemeit
Prüfzeitraum:	November 2014 – September 2015
Ort der Prüfung:	Essen / Detmold

Dieser Bericht umfasst 20 Seiten

Inhalt

1 Allgemeines

Die Fa. Weidmüller Interface GmbH & Co. KG (im folgenden Auftraggeber genannt) hat im Rahmen eines Entwicklungsprojektes die Fehlersicheren I/O-Module UR20-8DI-PN-FSPS, UR20-4DI-4DO-PN-FSPS, UR20-8DI-PN-FSOE und UR20-4DI-4DO-PN-FSOE entwickelt. Mit der Entwicklung der Software der Module wurde die Firma ISH Ingenieursozietät GmbH beauftragt. Die Bewertung der Funktionalen Sicherheit übernahm die TÜV NORD CERT GmbH (SRS), die folgende Prüfungen durchführte:

- Prüfung und Zertifizierung der Fehlersicheren I/O-Module gemäß EN ISO 13849 (Kat 4, PL'e')
- Prüfung und Zertifizierung der Fehlersicheren I/O-Module gemäß EN 61508 (SIL 3)
- Prüfung und Zertifizierung der Fehlersicheren I/O-Module gemäß EN 62061 (SIL_{CL} 3)

Dieser Bericht fasst die Ergebnisse der im Rahmen der durchgeführten Sicherheitsbetrachtung aller relevanten Schaltungsteile hinsichtlich ihrer Architektur, des Verhaltens im Fehlerfall, sowie die Betrachtung von systematischen Fehlern gemäß den Anforderungen an die EN 61508, EN 62061 und EN ISO 13849-1 zusammen.

Weiterhin sind die Maßnahmen entsprechend den Anforderungen an die Qualitätssicherung - und dem damit verbunden Sicherheitsmanagement zur Einhaltung der Anforderungen - im Hause des Auftraggebers untersucht und bewertet worden.

Der positive Abschluss der Prüfungen wird durch eine EG-Baumusterprüfbescheinigung nach RL 2006/42/EG, sowie ein „Approved Safety Function"-Zertifikat der TÜV NORD CERT GmbH SRS bestätigt.

Aus organisatorischen Gründen wurden in diesem Projekt für die Ausstellung von zwei Zertifikaten zwei interne Aufträge angelegt. Somit findet dieser Bericht Anwendung auf die folgenden internen Aufträge:

	Hauptprojekt:	Projekt-„Dummy“
Auftrag Nummer:	**8000428721**	8000451740
ZA-Nummer:	**3513 3273**	3516 7236
Zertifikat-Nummer:	**44 205 13 773701**	44 207 13 773701
Art der Zertifizierung:	**EG-Baumusterprüfbescheinigung gemäß Richtlinie 2006/42/EG**	Approved Safety Function

2 Systembeschreibung

Die Fehlersicheren I/O-Module UR20-8DI-PN-FSPS, UR20-4DI-4DO-PN-FSPS, UR20-8DI-PN-FSOE und UR20-4DI-4DO-PN-FSOE dienen dem Einlesen von sicherheitsgerichteten, Informationen (z.B. Sensormesswerte) über die sicherheitsgerichteten digitalen Eingänge (DI), der Übermittlung der Daten mittels Busanbindung an eine übergeordnete Sicherheits-SPS, sowie dem Empfang von Daten (ebenfalls über die Busverbindung) von der Sicherheits-SPS und infolge dessen das sicherheitsgerichtete Schalten der digitalen Ausgänge (DO) an nachgelagerte Systemkomponenten (sicherheitsgerichtete Ausgabe von Informationen nur für die Module vom Typ UR20-4DI-**4DO**-PN-FSPS und UR20-4DI-**4DO**-PN-FSOE).

Die Buskommunikation erfolgt mittels der zertifizierten ProfiSafe- (Siemens AG) und FailSafe Over EtherCAT- (Beckhoff Automation GmbH) Busprotokolle. Die Module vom Typ UR20-8DI-PN-FS**PS** und UR20-4DI-4DO-PN-FS**PS** kommunizieren über den ProfiSafe-Bus, die Module UR20-8DI-PN-**FSOE** und UR20-4DI-4DO-PN-**FSOE** kommunizieren über den FailSafe Over EtherCAT-Bus. Die korrekte und sichere Implementierung der (zertifizierten) Slave-Protokollstacks zur Anbindung an den ProfiSafe- bzw. den FailSafe Over EtherCAT-Bus wurde gesondert geprüft und die Ergebnisse dokumentiert ([56], [65] bis [69]). Die Übertragung der Informationen zwischen den Fehlersicheren I/O-Modulen und der übergeordneten Safety SPS erfolgt über von einem der internen Mikrocontroller (µC1) über einen ASIC (Siemens SNAP+) als Black-Channel-Datenübertragung zur Sicherheits-SPS. Der Kommunikationspfad wurde aufgrund der Verwendung zertifizierter Protokollstacks,

sowie der gesondert geprüften Busankopplung der Module ([56], [65] bis [69]), keiner ergänzenden Prüfung unterzogen.
Die Parametrierung des Systems erfolgt durch die Sicherheits-SPS und die sichere ProfiSafe- bzw. FSoE-Kommunikation. Die Parametrierkomponente (Sicherheits-SPS) selbst war nicht Gegenstand der Betrachtung.

Die sicherheitsgerichteten digitalen Eingänge können einkanalig (1oo1) oder redundant (1oo2) verschaltet zur Anwendung kommen. Die interne Datenverarbeitung und die sicherheitsgerichteten Ausgänge (nur für Module vom Typ UR20-4DI-4**DO**-PN-FSPS und UR20-4DI-4**DO**-PN-FSOE) sind ab Werk immer zweikanalig (1oo2) aufgebaut.

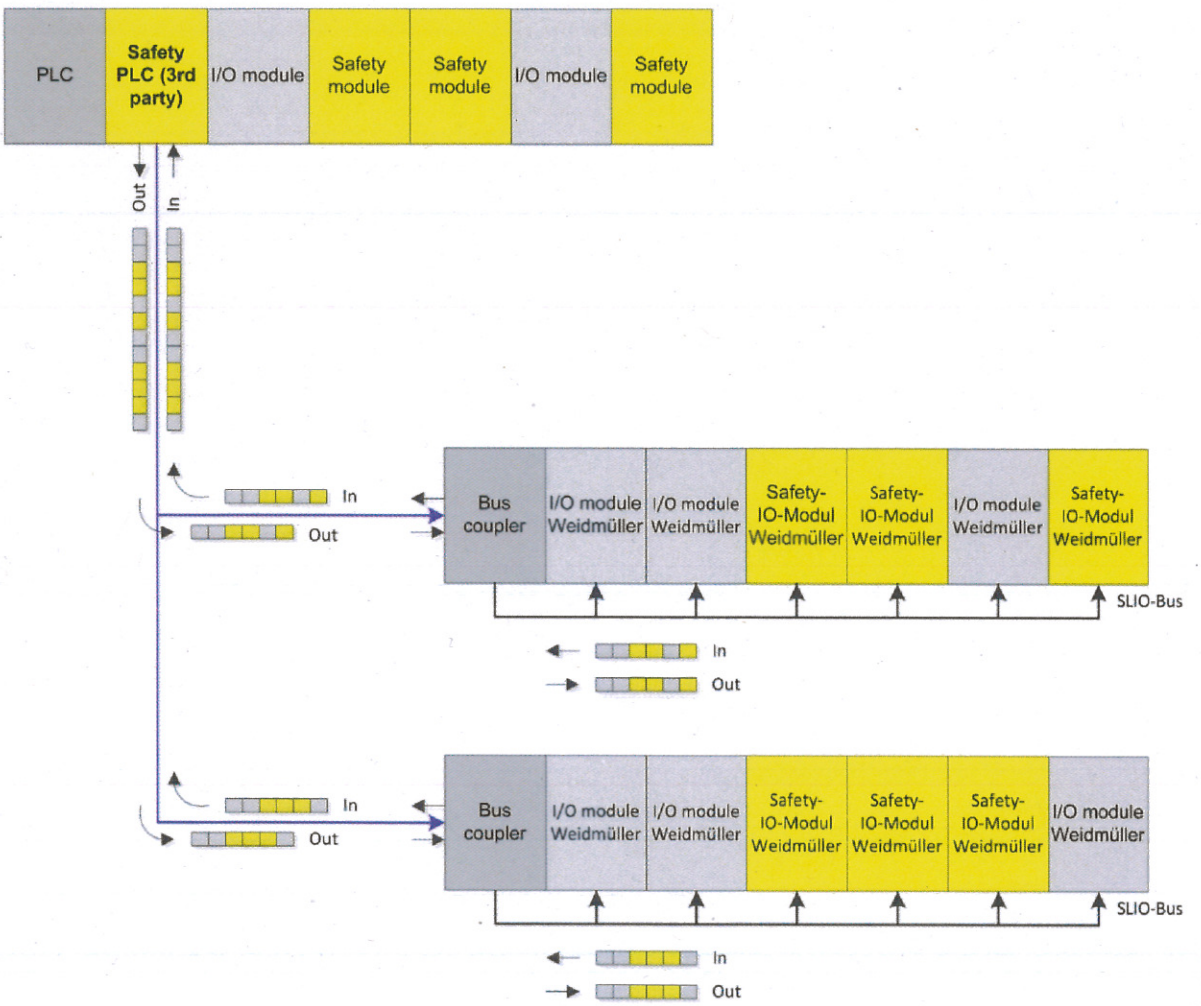

Abb. 1 Systemübersicht

Sicherheitsfunktionen:

Funktionsgruppe:	Sicherheitsfunktion:	Sicherer Zustand:	Konfiguration:
Sicherheitsgerichtete (digitale) Eingänge	Einlesen sicherheitsgerichteter (digitaler) Eingänge und senden dieser Informationen über den ProfiSafe- oder FSOE-Bus via black channel-Kommunikation an eine übergeordnete Sicherheits-SPS	Übermitteln des Eingangszustandes ‚false' an die Sicherheits-SPS. Das Signal wird übermittelt wenn der Eingang hochohmig ist, sich die Spannung am Eingang in einem ungültigen Bereich befindet oder bei Fehlererkennung	Optional ein- oder zweikanalig **Einkanalig (1oo1):** SIL 2, PL ‚d', Kategorie 2, SIL_{CL} 2 **Zweikanalig (1oo2):** SIL 3, PL ‚e', Kategorie 4, SIL_{CL} 3
Sicherheitsgerichtete (digitale) Ausgänge	Sicherheitsgerichtetes Schalten der digitalen Ausgänge aufgrund von Informationen, die von der Sicherheits-SPS über den ProfiSafe- oder FSOE-Bus an die I/O-Module gesendet wurden	Abschaltung des Ausgangs: P-Schaltend: Ausgangsspannung < 5 V, Ausgangsstrom < 2 mA N-Schaltend: Ausgangsstrom > - 2 mA bezogen auf die pos. Spannungsversorgung	**Zweikanalig (1oo2):** SIL 3, PL ‚e', Kategorie 4, SIL_{CL} 3

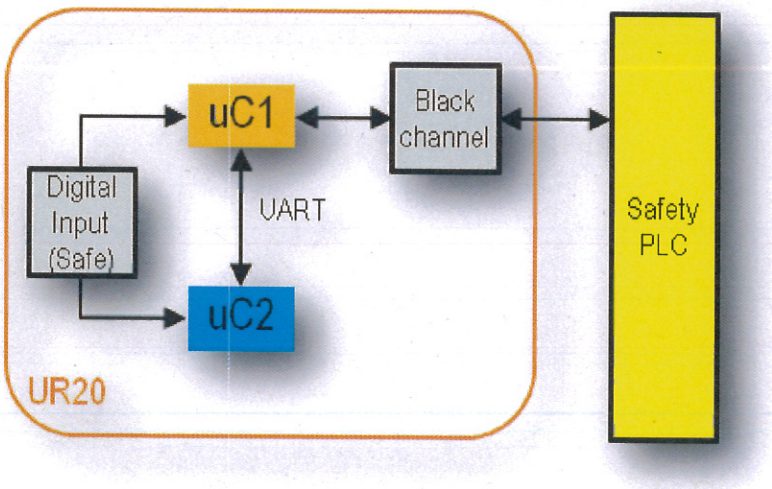

Abb.2 Verwendung der sicherheitsgerichteten (digitalen) Eingänge

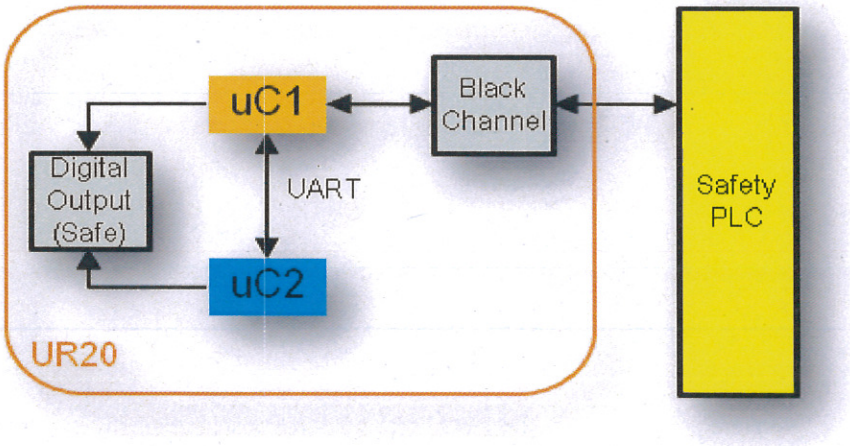

Abb.3 Verwendung der sicherheitsgerichteten (digitalen) Ausgänge

3 Eingereichte Unterlagen

Ref.	Inhalt / Titel	Datum
[1]	Antrag auf Ausstellung einer EG-Baumusterprüfbescheinigung gemäß Richtlinie 2006/42/EG sowie des Zertifikat	
[2]	Beschreibung, Weidmüller: Safety Concept, UR20-8DI-PN-SIL, UR20-4DI-4DO-PN-SIL, UR20-4AI-UIT-SIL, Rev. 00.06, 43 Seiten	25.02.2014
[3]	Beschreibung, Weidmüller, Hardware / Firmware Functional Description (HFFD) UR20-8DI-PN-SIL, UR20-4DI-4DO-PN-SIL, UR20-4AI-UIT-SIL, Rev. 01.08, 85 Seiten	08.09.2015
[4]	FSM, Weidmüller, Functional Safety Management Plan (FSMP), draft, Rev. 0.6, 36 Seiten	01.09.2015
[5]	FSM, ISH, Functional safety management plan, Rev. 00.04, 15 Seiten	06.06.2014
[6]	Beschreibung, Weidmüller, Hardware Design Description (HDD) UR20-8DI-PN-SIL, UR20-4DI-4DO-PN-SIL, UR20-4AI-UIT-SIL, Rev. 01.03, 90 Seiten	22.06.2015
[7]	Schaltplan, Weidmüller, PCBA UR20 4DI 4DO PN FS, Drawing-No.: 3 60749, 11 Seiten	17.04.2015
[8]	Stückliste, Weidmüller, PCBA UR20 4DI 4DO PN FS, Drawing-No.: 60749, Issue No. 1, 5 Seiten	07.05.2015
[9]	Bestückungsplan, Weidmüller, PCBA UR20 4DI 4DO PN FS, Top und Bottom Assembly Drawing, Drawing-No.: 3 60749, 2 Seiten	17.04.2015
[10]	Leiterplattenspezifikationen, Weidmüller, PCBA UR20 4DI 4DO PN FS PCB Specification, Drawing -No.: 4 57757, PCB Index 04, 11 Seiten	04.03.2015
[11]	Schaltplan, Weidmüller, PCBA UR20 8DI PN FS, Drawing-No.: 3 60746, 14 Seiten	17.03.2015
[12]	Stückliste, Weidmüller, PCBA UR20 8DI PN FS, Drawing-No.: 60746, Issue No. 1, 6 Seiten	24.04.2015

[13]	Bestückungsplan, Weidmüller, PCBA UR20 8DI PN FS, Top und Bottom Assembly Drawing, Drawing-No.: 3 60746, 2 Seiten	17.03.2015
[14]	Leiterplattenspezifikationen, Weidmüller, PCBA UR20 8DI PN FS PCB Specification, Drawing -No.: 4 57755, PCB Index 03, 11 Seiten	04.03.2015
[15]	Spezifikationen, ISH, Specification of software architecture, Rev. 01.08, 43 Seiten	31.08.2015
[16]	V+V-Plan, Weidmüller, Validation and Verification Plan, ID: A351, Draft, Rev. 0.3, 19 Seiten	17.02.2015
[17]	V+V-Plan, ISH, Validation and Verification Plan, Rev. 00.05, 30 Seiten	17.02.2015
[18]	HMTP, Weidmüller, Hardware Module Test Plan UR20-8DI-PN-FS, Rev. 1.1, 5 Seiten	14.08.2015
[19]	HMTR, Weidmüller, Hardware Module Test Report UR20-8DI-PN-FS, Rev. 1.0, 4 Seiten	07.05.2015
[20]	HMTP, Weidmüller, Hardware Module Test Plan UR20-4DI-4DO-PN-FS, Rev. 1.2, 6 Seiten	28.08.2015
[21]	HMTR, Weidmüller, Hardware Module Test Report UR20-4DI-4DO-PN-FS, Rev. 1.1, 4 Seiten	31.08.2015
[22]	HITP, Weidmüller, Hardware Integration Test Plan UR20-8DI-PN-FS, Rev. 1.1, 4 Seiten	14.08.2015
[23]	HITR, Weidmüller, Hardware Integration Test Report UR20-8DI-PN-FS, Rev. 1.1, 5 Seiten	31.08.2015
[24]	HITP, Weidmüller, Hardware Integration Test Plan UR20-4DI-4DO-PN-FS, Rev. 1.3, 4 Seiten	28.08.2015
[25]	HITR, Weidmüller, Hardware Integration Test Report UR20-4DI-4DO-PN-FS, Rev. 1.3, 6 Seiten	31.08.2015
[26]	FITS, Weidmüller, Failure Insertion Test Specification UR20-4DI-4DO-PN-FS, Rev. 1.2, 8 Seiten	02.06.2015
[27]	FITR, Weidmüller, Failure Insertion Test Report UR20-4DI-4DO-PN-FS, Rev. 1.1, 9 Seiten	20.04.2015
[28]	FITS, Weidmüller, Failure Insertion Test Specification UR20-8DI-PN-FS, Rev. 1.1, 6 Seiten	02.06.2015
[29]	FITR, Weidmüller, Failure Insertion Test Report UR20-8DI-PN-FS, Rev. 1.0, 9 Seiten	07.05.2015
[30]	FMEDA, Weidmüller, Failure Modes Effects and Diagnostic Analysis Digital Inputs -FS Modules, Rev. 1.3, 7 Seiten	07.09.2015
[31]	FMEDA, Weidmüller, Failure Modes Effects and Diagnostic Analysis Digital Outputs -FS Modules, Rev. 1.2, 6 Seiten	07.09.2015
[32]	Analyse, Weidmüller, Derating Analysis, Rev. 1.1, 25 Seiten	03.09.2015
[33]	HARA, Weidmüller, Hazard and Risc Analysis acc. to EC machinery directive (2006/42/EG), Rev. 1.0, 7 Seiten	29.04.2015
[34]	Analyse, Weidmüller, Analysis of two faults safety, Rev. 1.0, 9 Seiten	03.09.2015
[35]	Spezifikationen, ISH, Safety CRC Configurator SWASafety CRC Configurator Specification of software architecture, Rev. 00.04, 21 Seiten	01.09.2015
[36]	Laboratory Report, Weidmüller, LAB20053E, UR20-8DI-PN-FSPS, Ref.-No.: LO15-00233 (GF059), 39 Seiten	21.08.2015
[37]	Laboratory Report, Weidmüller, LAB20063E, UR20-4DI-4DO-PN-FSPS, Ref.-No.: LO15-00233 (GF059), 47 Seiten	21.08.2015

[38]	Laboratory Report, Weidmüller, LAB20064E, UR20-4DI-4DO-PN-FSPS, UR20-8DI-PN-FSPS, Ref.-No.: LO015-00233 (GF059), 23 Seiten	20.08.2015
[39]	Laboratory Report, Weidmüller, LAB20065E, UR20-4DI-4DO-PN-FSOE, UR20-8DI-PN-FSOE, Ref.-No.: LO15-00222 (GF059), 34 Seiten	28.07.2015
[40]	Laboratory Report, Weidmüller, LAB20066E, UR20-4DI-4DO-PN-FSOE, Ref.-No.: LO15-00233 (GF059), 5 Seiten	21.08.2015
[41]	Laboratory Report, Weidmüller, LAB20067E, UR20-8DI-PN-FSOE, Ref.-No.: LO15-00233 (GF059), 5 Seiten	21.08.2015
[42]	Laboratory Report, Weidmüller, LAB20082E, UR20-8DI-PN-FSPS, Ref.-No.: LO15-00233 (GF059), 5 Seiten	21.08.2015
[43]	Laboratory Report, Weidmüller, LAB20102E, UR20-8DI-PN-FSPS, Ref.-No.: LO15-00233 (GF059), 9 Seiten	11.09.2015
[44]	Beschreibung, ISH, Requirement Tracking, Rev. 00.04, 7 Seiten	17.09.2014
[45]	Verzeichnis, ISH, Requirement Tracking Result: *„Requ_Tracking_Result.xls“*	01.09.2015 (Dateidatum)
[46]	Beschreibung, Weidmüller, System Configuration Management Process, Rev. 1.0, 18 Seiten	25.11.2014
[47]	Beschreibung, Weidmüller, Engineering Change Management Instruction, Rev. 2.0, 32 Seiten	05.12.2014
[48]	Beschreibung, ISH, Development Tools, Rev. 00.03, 8 Seiten	06.06.2014
[49]	Programmierrichtlinie, ISH, QM-ARBEITSANWEISUNG Fachanweisung C Codierrichtlinien mit Einschränkun-gen für sicherheitskritische Systeme, Rev. 1.9, 33 Seiten	29.10.2012
[50]	Beschreibung, ISH, Handling of documents, Rev. 00.04, 8 Seiten	17.09.2014
[51]	Spezifikation, ISH, Safety CRC Configurator SWASafety CRC Configurator Specification of software architecture, Rev. 00.04, 21 Seiten	01.09.2015
[52]	Validierung, ISH, Checklist Codereview, Rev. 008, (Projekt-CD: *WM2012-10009_checklist_codereview.xls*)	01.09.2015
[53]	Testspezifikation, ISH, Module Integration Test, Rev. 00.04, 32 Seiten	26.08.2015
[54]	Validierung, ISH, Module Integration Test Report, Rev. 00.03, 116 Seiten	25.08.2015
[55]	Spezifikation, ETG, Conformance Test Specification, Part 2: FSoE Conformance Test Record, ETG.7100.2 S (R) V1.1.0, Rev. 1.1.0, 15 Seiten	06.2013
[56]	Testprotokoll: ISH, EtherCAT Conformance Test Tool Report; FSoE Slave State Machine Test, 84 Seiten	12.08.2015
[57]	Betriebsanleitung, Remote I/O-System u-remote Original-Handbuch Module zur funktionalen Sicherheit, Dokument-Nr. 1484590000, Revision 02/September 2015	10.09.2015
[58]	Typenschilder (UR20-8DI-PN-FS**, UR20-4DI-4DO-PN-FS**), Weidmüller, 4 Seiten	17.12.2014
[59]	Verifikation, ISH, Software Verification of the "Safety CRC Configurator", Rev. 00.04, 31 Seiten	28.08.2015
[60]	Verifikation, ISH, Integration of FSoE protocol stack, Safety I/O modules UR20-8DI-PN-SIL, UR20-4DI-4DO-PN-SIL, UR20-4AI-UIT-SIL, Rev. 00.02, 10 Seiten	26.08.2015

[61]	Anforderung, ISH Integration of ProfiSafe protocol stack, Rev. 00.02, 8 Seiten	16.06.2015
[62]	Verifikation, ISH, Integration of ProfiSafe protocol stack, Safety I/O modules UR20-8DI-PN-SIL, UR20-4DI-4DO-PN-SIL, UR20-4AI-UIT-SIL, Rev. 00.03, 27 Seiten	26.08.2015
[63]	Anforderung, ISH, Integration of hardware test library (Cortex M3), Safety I/O modules UR20-8DI-PN-SIL, UR20-4DI-4DO-PN-SIL, UR20-4AI-UIT-SIL, Rev. 00.03, 14 Seiten	16.06.2015
[64]	Integrationshandbuch, ISH, HWT (hardware test library, CORA793) - integration guide, Rev. 01.14, 48 Seiten	01.08.2014
[65]	Testbericht: SIEMENS AG, ComDeC Fürth, PNO Test Report PN357-1, 7 Seiten	21.08.2015
[66]	Testbericht: SIEMENS AG, ComDeC Fürth, PI Test Report IRT089-1, 4 Seiten	21.08.2015
[67]	Testbericht: SIEMENS AG, ComDeC Fürth, PNO Test Report 618-1, 12 Seiten	26.06.2015
[68]	Testbericht: SIEMENS AG, ComDeC Fürth, PI Test Report PS089-1, 16 Seiten	21.08.2015
[69]	Testbericht: SIEMENS AG, ComDeC Fürth, PI Test Report PS090-1, 16 Seiten	21.08.2015

4 Prüfdokumentation

Ref.	Inhalt / Titel		Datum
[1]	P10F01_WM_UR20:	Projektcheckliste Prüfung Funktionale Sicherheit	17.09.2015
[2]	P10F03_WM_UR20:	Software Beurteilung nach DIN EN 61508:2010 Teil 3	17.09.2015
[3]	P10F04_WM_UR20:	Validierung der Kategorie 4 gemäß EN ISO 13849-2:2012	16.09.2015
[4]	P10F09_WM_UR20:	Prüfprogramm nach EN ISO 13849-1:2008	16.09.2015
[5]	P10F10_WM_UR20:	Functional Safety Management (FSM) gemäß EN 61508-1:2010, EN 61508-2:2010, EN 61508-3:2010	17.09.2015
[6]	P10F15_WM_UR20:	Prüfprogramm für EN 61508-1:2010	17.09.2010
[7]	P10F20_WM_UR20:	Funktions- und Fehlereinbautest: Funktions- und Fehlereinbautest, Gerät: Profibusmodul UR20	22. bis 23.04.2015

5 Prüfgrundlagen

EN ISO 13849-1:2008	Sicherheit von Maschinen – Sicherheitsbezogene Teile von Steuerungen – Teil 1: Allgemeine Gestaltungsleitsätze
EN ISO 13849-2:2012	Teil 2: Validierung
EN 61508-1:2010	Funktionale Sicherheit sicherheitsbezogener elektrischer/ elektronischer/programmierbarer elektronischer Systeme Teil 1: Allgemeine Anforderungen
EN 61508-2: 2010	Teil 2: Anforderungen an sicherheitsbezogene elektrische/ elektronische/programmierbare elektronische Systeme
EN 61508-3: 2010	Teil 3: Anforderungen an Software
EN 61508-4: 2010	Teil 4: Begriffe und Abkürzungen
EN 61508-5: 2010	Teil 5: Beispiele zur Ermittlung der Sicherheitsintegrität (safety integrity level)
EN 61508-6: 2010	Teil 6: Anwendungsrichtlinie für IEC 61508-2 und IEC 61508-3
EN 61508-7: 2010	Teil 7: Anwendungshinweise über Verfahren und Maßnahmen
EN 62061:2005 + A1:2013	Sicherheit von Maschinen - Funktionale Sicherheit sicherheitsbezogener elektrischer/ elektronischer/ programmierbarer elektronischer Steuerungssysteme
SN 29500-1 bis -14	Ausfallraten Bauelemente (unterschiedliche Ausgabestände der einzelnen Teile)

6 Durchgeführte Prüfungen und Bewertungen

Es sind die normativen Vorgaben der EN 61508 (SIL 3), EN 62061 (SIL_{CL} 3) und der EN ISO 13849 (Kat 4, PL ‚e') gegen die hier betrachtete Produktentwicklung und deren Ergebnisse geprüft und bewertet worden. Grundlage für die Zertifizierung bilden folgende Prüfsegmente:

- Funktionale Sicherheit
  - Analyse und Bewertung der sicherheitsgerichteten Dokumentation
  - Anforderungen an den Sicherheitslebenszyklus
  - Durchführung von Fehlereffektanalysen (FMEDA[1])
    - Berechnung von PFH[2] und SFF[3]
    - Berechnung von $MTTF_D$[4] und DC_{avg}[5]
  - Sicherheitshinweise in der Betriebs- und Sicherheitsdokumentation
  - Hardware-Fehlertoleranz
  - Validierung der Sicherheitskategorie

- Systematische Sicherheitsintegrität
  - Analyse des Managementsystems und der Dokumentation
    - Functional Safety Management (FSM)
    - Projektorganisation
    - Qualitätssichernde Maßnahmen
    - V-Modell Dokumentation Hard- und Software
  - Analyse und Bewertung der Software
    - Architektur
    - Design
    - Modulbildung
    - Source Code Integrität
    - Modul- und Integrationstests
    - Validierung

1 Ausfallarten- und Auswirkungsanalyse (Failure Mode, Effects and Diagnostic Analysis).

2 Betriebsart mit hoher Anforderungsrate oder Betriebsart mit kontinuierlicher Anforderung (en: high demand or continuous mode): wobei die Anforderungsrate an das sicherheitsbezogene System mehr als einmal pro Jahr beträgt.

3 Anteile ungefährlicher Ausfälle (Safe Failure Fraction).

4 Erwartungswert der mittleren Zeit bis zum gefahrbringenden Ausfall (Mean Time To Dangerous Failure).

5 Maß für die Wirksamkeit der Diagnose, die bestimmt werden kann, als Verhältnis der Ausfallrate der bemerkten gefährlichen Ausfälle zur Ausfallrate der gesamten gefährlichen Ausfälle (Gemäß EN ISO 13849-1).

- Diagnoseeigenschaften
- Einfluss von Fehlern aufgrund einer gemeinsamen Ursache (CCF)
- Modifikations- und Konfigurationsmanagement
- Umgebungsbedingte Einflüsse

Die einzelnen Teilergebnisse sind mit Hilfe von Checklisten dokumentiert und bei der Prüfstelle hinterlegt worden (Anhänge [1-7] in Abschnitt 4). Die Einhaltung der quantitativen Anforderungen gemäß EN 61508 und EN 62061 (SFF, Ausfallraten[6] λ_D und λ_S, PFH) sind vom Auftraggeber im Rahmen von FMEDAs ermittelt worden. Die FMEDAs sind im Rahmen der Prüfung einem Review unterzogen und anerkannt worden. Die zulässigen Grenzwerte gemäß EN ISO 13849-1 (CCF, $MTTF_D$, DC_{avg}) sind ebenfalls im Zuge der FMEDAs ermittelt worden.

Des Weiteren sind die, durch das nach ISO 17025 akkreditierte Labor des Auftraggebers durchgeführten, Umwelttests wie EMV-, Temperatur-, Vibrations- und Schocktests in Form eines Reviews bewertet und anerkannt worden.

6.1 Qualitätssichernde Maßnahmen im Rahmen der Produktentwicklung

Das sicherheitsgerichtete Qualitätsmanagement des Auftraggebers (FSM - Functional Safety Management) wurde im Rahmen der Prüfung des Fehlersicheren I/O-Moduls UR20 bewertet. Wo relevant, wurden solche Betrachtungen auch beim Softwareersteller ISH Ingenieursozietät GmbH durchgeführt.

Der Nachweis einer sicherheitsgerichteten Entwicklung hinsichtlich der geforderten Anforderungen für ein SIL 3-System nach EN 61508 und EN 62061 ist durch entsprechende Dokumentation der einzelnen Fachbereiche des Auftraggebers erbracht worden. Die definierten Anforderungen an die Spezifikation der Sicherheitsfunktion, sowie die Anforderungen an die notwendige Sicherheitsintegrität, sind im Dokument *Hardware/ Firmware Functional Description (HFFD)* ([3]), welche inhaltlich die Aufgaben einer Safety Requirement Specification (SRS) übernimmt, klar dargestellt und definiert. Dieses Dokument umfasst alle relevanten und für das Produkt notwendigen Angaben zum Erreichen und Aufrechterhalten der Funktionalen Sicherheit für das geforderte Sicherheits-Integritätslevel.

6 Unterteilung der Ausfallraten Lambda (λ) in gefährliche (λD=λDU+λDD) und nicht gefährliche Anteile (λS=λSD+λSU), sowie die Möglichkeit, die Fehler zu erkennen (λDD, λSD).

Insbesondere Phase neun und zehn des Lebenszyklus gemäß EN 61508 sind anwendbar auf die Produktentwicklung und wurden in referenzierten Spezifikationen und Unterdokumenten des Auftraggebers umgesetzt.

Die generellen sicherheitsrelevanten Anforderungen, wie Zielsetzung der Entwicklung, Produktgrenzen, Umgebungsbedingungen, externe Schnittstellen etc. sowie die anzuwendenden Normen und Richtlinien werden ebenfalls innerhalb der *HFFD* vollständig dokumentiert bzw. verlinkt.

Das Dokument *Functional Safety Management Plan (FSMP)* beschreibt alle qualitätssichernden Aktivitäten der im Rahmen des Entwicklungsablaufes notwendigen Managementtätigkeiten. Die relevanten Phasen des Sicherheitslebenszyklus wurden ausreichend definiert und sind im Rahmen der Entwicklung umgesetzt worden. Darüber hinaus ist die erforderliche Projektorganisation wie die Zeitplanung, Regelung von Verantwortlichkeiten und Kompetenzen aller am Projekt beteiligten Mitarbeiter eindeutig geregelt und dokumentiert.

Entsprechend dem Stand der einzelnen Entwicklungsstufen ist eine Validierung des Fehlersicheren I/O-Moduls durch den Auftraggeber durchgeführt worden.

Insgesamt erfolgte die Umsetzung der sicherheitsgerichteten Dokumentation gemäß der Anforderungen an das V-Modell für Hard- und Software.

6.2 Sicherheitsintegrität der Software

Die erstellte Software ist im Rahmen der Prüfung durch ein Review der relevanten Bereiche und der entsprechenden Dokumentation untersucht worden. Zusätzlich wurde eine Softwarebeurteilung hinsichtlich der Sicherheitsanforderungen, der Softwarearchitektur, des Desings, der Module, der verwendeten Werkzeuge, etc. gemäß Anhang A+B der EN 61508-3 durchgeführt.

In der Dokumentation des Auftraggebers ist die gewählte Softwarearchitektur inklusive der implementierten on- und offline Diagnosemaßnahmen (Start-Up und während des Betriebs) beschrieben, sowie die Darstellungen zum gesamten Softwareentwicklungsprozess

enthalten. Die Dokumentation beschreibt ausführlich die Anforderungen an die einzelnen Softwaremodule und deren Schnittstellen mit Hilfe der geforderten Verfahren und Maßnahmen für ein SIL 3 bzw. PL ‚e'.

Tätigkeiten zur Planung und Durchführung der Softwarevalidierung sind ebenfalls dokumentiert. Die durch den Auftraggeber getroffenen Maßnahmen zur Fehlervermeidung sind dokumentiert und entsprechend durch die durchgeführten Softwaretests verifiziert worden. Die im Rahmen des Softwareentwicklungsprozesses verankerten und umgesetzten Maßnahmen zur Vermeidung von systematischen Fehlern decken die Anforderung gemäß EN 61508-3, EN 62061 und EN ISO 13849-1 ab.

6.3 Sicherheitsintegrität der Hardware

Im Rahmen der Systemanalyse ist zum Nachweis der Sicherheitsintegrität bezüglich der zufälligen Hardwarefehler jeweils eine FMEDA - für das sicherheitsgerichtete Lesen von Informationen über die digitalen Eingänge sowie für das sicherheitsgerichtete Schalten der Digitalen Ausgänge - durch den Auftraggeber durchgeführt worden. Alle Fehlermöglichkeiten wurden entsprechend EN 61508-2, EN ISO 13849-2 und EN 62061 und den damit zu unterstellenden Fehlermöglichkeiten betrachtet und bewertet. Die Berechnung der Ausfallwahrscheinlichkeiten des Systems beruht auf der Betrachtung und Untersuchung der Schaltung im Hinblick auf die Ausfallwahrscheinlichkeiten der Bauteile und ihre Einordnung in sichere und gefahrbringende Fehler. Die durchgeführte FMEDA wurde einem Review unterzogen und anerkannt.

Im zweiten Schritt wurde die Diagnosefähigkeit der Schaltung untersucht, indem die Fähigkeit, aufgetretene Fehler zu entdecken, beurteilt wurde. Mittels mathematischer Modelle und Berechnungsmethoden lässt sich die Restfehlerwahrscheinlichkeit (Probability of Failure on Demand, PFD und Probability of Failure per Hour; PFH) der zufälligen Hardwarefehler bestimmen.

Anhand der durchgeführten FMEDA wurde der Anteil ungefährlicher Ausfälle SFF (Safe Failure Fraction) ermittelt und die hierfür erforderlichen Kenngrößen λ_{SD}, λ_{SU}, λ_{DD} und λ_{DU} für das System bestimmt. Für einen Sicherheits-Integritätslevel 3 ist unter Berücksichtigung der vorhandenen Systemstruktur für das zweikanalige System (1oo2D) die Ausfallrate für einen

Kanal jedes Teilsystems ermittelt worden. Als Quelle für die Bauteilausfallraten wurde die Siemens-Norm SN 29500 herangezogen.

Die Einteilung der Fehlersicheren I/O-Module erfolgte aufgrund der Verwendung komplexer Technologien als Typ B-System. Entsprechend den Rechenvorschriften ergeben sich die in Tabelle 1 dargestellten Zuverlässigkeitskennzahlen gemäß EN 61508 bzw. EN 62061 für eine System-Gesamtausfallrate bzw. Gesamt-SFF zu:

EN 61508: Digitale Eingänge (ab Werk 1oo1, konfigurierbar zu 1oo2, homogen):

Architektur	λ_{SD} [1/h]	λ_{SU} [1/h]	λ_{DD} [1/h]	λ_{DU} [1/h]	PFD	PFH [1/h]	SFF [%]
1oo1	$1{,}65 * 10^{-7}$	$2{,}65 * 10^{-7}$	$1{,}26 * 10^{-7}$	$1{,}00 * 10^{-8}$	$8{,}77 * 10^{-4}$	$1{,}0 * 10^{-8}$	98,20
1oo2	$1{,}65 * 10^{-7}$	$2{,}65 * 10^{-7}$	$1{,}26 * 10^{-7}$	$1{,}00 * 10^{-8}$	$1{,}85 * 10^{-5}$	$2{,}17 * 10^{-10}$	98,20

Tabelle 1: Gesamtausfallraten, PFD, PFH und SFF für die digitale Eingangsstufe Fehlersicheres I/O-Modul UR20

EN 61508: Digitale Ausgänge (ab Werk 1oo2, heterogen, nicht konfigurierbar):

Kanal	λ_{SD} [1/h]	λ_{SU} [1/h]	λ_{DD} [1/h]	λ_{DU} [1/h]	PFD	PFH [1/h]	SFF [%]
1	$2{,}75 * 10^{-7}$	$1{,}01 * 10^{-8}$	$2{,}46 * 10^{-7}$	$1{,}00 * 10^{-8}$	$1{,}85 * 10^{-5}$	$2{,}17 * 10^{-10}$	98,20
2	$2{,}67 * 10^{-7}$	$1{,}15 * 10^{-7}$	$1{,}43 * 10^{-7}$	$1{,}00 * 10^{-8}$			

Tabelle 2: Gesamtausfallraten, PFD, PFH und SFF für die digitale Ausgangsstufe Fehlersicheres I/O-Modul UR20

EN 62061: Digitale Eingänge (ab Werk 1oo1, konfigurierbar zu 1oo2, homogen):

Architektur	λ_{SD} [1/h]	λ_{SU} [1/h]	λ_{DD} [1/h]	λ_{DU} [1/h]	PFH [1/h]	SFF [%]
1oo1	$1{,}65 * 10^{-7}$	$2{,}65 * 10^{-7}$	$1{,}26 * 10^{-7}$	$1{,}00 * 10^{-8}$	$1{,}0 * 10^{-8}$	98,20
1oo2	$1{,}65 * 10^{-7}$	$2{,}65 * 10^{-7}$	$1{,}26 * 10^{-7}$	$1{,}00 * 10^{-8}$	$2{,}94 * 10^{-9}$	98,20

Tabelle 3: Gesamtausfallraten, PFH und SFF für die digitale Eingangsstufe Fehlersicheres I/O-Modul UR20

EN 62061: Digitale Ausgänge (ab Werk 1oo2, heterogen, nicht konfigurierbar):

Kanal	λ_{SD} [1/h]	λ_{SU} [1/h]	λ_{DD} [1/h]	λ_{DU} [1/h]	PFH [1/h]	SFF [%]
1	$2{,}75 * 10^{-7}$	$1{,}01 * 10^{-8}$	$2{,}46 * 10^{-7}$	$1{,}00 * 10^{-8}$	$5{,}56 * 10^{-9}$	98,20
2	$2{,}67 * 10^{-7}$	$1{,}15 * 10^{-7}$	$1{,}43 * 10^{-7}$	$1{,}00 * 10^{-8}$		

Tabelle 4: Gesamtausfallraten, PFH und SFF für die digitale Ausgangsstufe Fehlersicheres I/O-Modul UR20

In diesem Zusammenhang wurden bei der Durchführung der FMEDA die (ggf. konfigurierbaren) Ein- und Ausgangsstufen bewertet. Die Ergebnisse (PFD- und PFH-Werte) wurden ins Safety Manual der Baugruppe übernommen.

Eine praktische Verifikation des erwarteten Ausfallverhaltens wurde durch einen Test mit Fehlereinbau beim Auftraggeber durchgeführt. Die Ergebnisse sind im Protokoll zum Fehlereinbau dokumentiert. Die Integrität, Funktionsweise und Rückwirkungsfreiheit des Diagnosesystems auf sicherheitsrelevante Schaltungsteile wurde durch die Betrachtung im Rahmen der FMEDA und des Fehlereinbautests beim Auftraggeber festgestellt.
Im Nachgang des Fehlereinbautests wurde die Hardware der I/O-Module geringfügig modifiziert. Der Hersteller hat hierauf den Fehlereinbautest wiederholt und die Ergebnisse dokumentiert (siehe [27] und [29])

Gemäß der in der EN ISO 13849-1 genannten Anforderungen an sicherheitsbezogene Teile einer Steuerung (SRP/CS[7]) sind im Rahmen der Systemanalyse die Kriterien für einen Performance Level ‚e' (PL ‚e')[8] ebenfalls betrachtet und bewertet worden. Unter Berücksichti-

7 Teil einer Steuerung, das auf sicherheitsbezogene Eingangssignale reagiert und sicherheitsbezogene Ausgangssignale erzeugt (EN ISO 13849-1).

8 Diskreter Level, der die Fähigkeit von sicherheitsbezogenen Teilen einer Steuerung spezifiziert, eine Sicherheitsfunktion unter vorhersehbaren Bedingungen auszuführen.

gung der Maßgaben für eine Hardwarearchitektur der Kategorie 4, der Mindestanforderung der mittleren Zeit bis zum gefahrbringenden Ausfall ($MTTF_D$) und des durchschnittlichen Diagnosedeckungsgrades (DC_{avg}) ergeben sich die in Tabelle 3 dargestellten Kennwerte (zur Interpretation der Ergebnisse siehe auch Tabelle 5 und 6 der EN ISO 13849-1:2008):

EN ISO 13849-1: Digitale Eingänge (ab Werk 1oo1, konfigurierbar zu 1oo2, homogen):

Kategorie	$MTTF_D$ [Jahre]	DC_{avg} [%]	PL
Kategorie 2	100 (840) / (hoch)	90 (mittel)	‚d'
Kategorie 4	100 (840) (hoch)	99 (hoch)	‚e'

Tabelle 5: Ermittelte Kenngrößen gem. EN ISO 13849-1: Kategorie, $MTTF_d$, DC_{avg} und PL für die digitale Eingangsstufe, Fehlersicheres I/O-Modul UR20

EN ISO 13849-1: Digitale Ausgänge (ab Werk 1oo2, heterogen, nicht konfigurierbar):

Kategorie	$MTTF_D$ [Jahre]	DC_{avg} [%]	PL
Kategorie 4	100 (279) / (hoch)	99 (hoch)	‚e'

Tabelle 6: Ermittelte Kenngrößen gem. EN ISO 13849-1: Kategorie, $MTTF_d$, DC_{avg} und PL für die digitale Ausgangsstufe, Fehlersicheres I/O-Modul UR20

Die Validierung der Kategorie 4 ist gemäß EN ISO 13849-2 (Abschnitt 7.2.3, s. Anhang) durchgeführt worden. Ein Fehlverhalten bei Spannungsausfall und - wiederkehr, sowie Über- und Unterspannung ist durch entsprechende schaltungs- und softwaretechnische Maßnahmen auszuschließen und wurde im Rahmen des Fehlereinbautests verifiziert.

Die Maßnahmen zur Vermeidung eines Fehlers aufgrund gemeinsamer Ursache im redundanten System (Common Cause Failure, siehe Anhang F2, EN ISO 13849-2) sind mit 75 Punkten als ausreichend bewertet worden. Die durch den Auftraggeber durchgeführten Umwelttests wie EMV-, Temperatur-, Vibrations- und Schocktests stellen die Tauglichkeit für den bestimmungsgemäßen Einsatzort unter Berücksichtigung der spezifizierten Betriebsparameter sicher.

Die Einhaltung der Mindestanforderung an die Luft- und Kriechstrecken ist durch die Verwendung der verifizierten und geprüften „Design-Rules" des Auftraggebers sichergestellt.

7 Ergebnis und Bewertung

Die erforderlichen Grenzwerte (SFF, PFD und PFH) werden für das einkanalige (SIL 2) und das zweikanalige (SIL 3) Typ B Gesamtsystem (HFT^9 = 1) entsprechend EN 61508 und EN 62061 eingehalten.

Die erforderlichen Grenzwerte (DC_{avg}, $MTTF_D$), sowie die Anforderung an die Kategorie 4, werden für die einkanalige Modularchitektur für einen Performance Level ‚d' (PL ‚d') und für die zweikanalige Modularchitektur für einen Performance Level ‚e' (PL ‚e') ebenfalls eingehalten.

Neben der Einhaltung der erforderlichen probabilistischen Grenzwerte, wurden auch die Anforderungen an die systematische Sicherheitsintegrität hinsichtlich der strukturierten und sicherheitsgerichteten Entwicklung von Hard- und Software erfüllt.

Die Vorgaben, die an das Functional Safety Management (FSM) bezüglich der qualitätssichernden Maßnahmen im Zuge einer sicherheitsgerichteten Produktentwicklung gestellt werden, wurden umfassend dokumentiert und erfüllt.

Das von der TÜV NORD CERT GmbH geprüfte Fehlersichere I/O-Modul entspricht bei bestimmungsgemäßer Verwendung und unter Berücksichtigung der in Abschnitt 8 gegeben Hinweise den zugrunde gelegten Prüfgrundlagen (s. Abschnitt 5 dieses Berichts).

9 Hardware Fehlertoleranz: Fehlertoleranz der Hardware von N bedeutet, dass N + 1 Fehler zu einem Verlust der Sicherheitsfunktion führen können.

8 Besondere Hinweise / Auflagen

Die beschriebenen Prüfergebnisse sind unter der Berücksichtigung folgender Punkte gültig:

1. Zum Erreichen eines Performance Levels ‚e' nach EN ISO 13849-1 bzw. eines Sicherheits-Integritätslevels SIL 3 gemäß EN 61508/ EN 62061 ist es erforderlich, die sicherheitsgerichteten digitalen Eingänge in redundanter (1oo2) Architektur zu verwenden.

2. Für die vollständige Beurteilung der funktionalen Sicherheit einer Sicherheitsfunktion müssen alle Anforderungen der EN 62061 und EN ISO 13849-1 auf die gesamte Sicherheitsfunktion angewendet werden, in der das fehlersichere I/O-Modul (UR20-8DI-PN-FSPS, UR20-8DI-PN-FSOE, UR20-4DI-4DO-PN-FSPS, UR20-4DI-4DO-PN-FSOE) zur Anwendung kommt.

3. Die Gültigkeit der Prüfergebnisse ist nur für die folgenden Versionen gegeben:

   Hardware:
   UR20-8DI-PN-FS**: HW 01.11.00
   UR20-4DI-4DO-PN-FS**: HW 01.02.00

   Software:
   UR20-4DI-4DO-PN-FSPS:
   Version V01.00.02, Md5-Checksum: 8d7a97a5865bda5e5b8aa7115484e440

   UR20-4DI-4DO-PN-FSOE, UR20-8DI-PN-FSPS und UR20-8DI-PN-FSOE:
   Version:V01.00.06, Md5-Checksum: f47252d03991dc9754dd09cd7c8f08be

M.Sc. Matthias Springer
(Reviewer)

Dipl.-Ing.(FH) Marc Willemeit
(Prüfer)