2. SIL – SLAM

Irrtümer rund um den SIL

13.09.2021

Fred Stay - Director Safety Consulting

Referent

Fred Stay

Senior Safety Consultant / Director Safety Consulting

f.stay@hima.com

HIMA Paul Hildebrandt GmbH

Albert-Bassermann-Str. 28
68782 Brühl, Germany

Phone: +49 6202 5770 -130
Mobile: +49 1624250759

E-mail: info@hima.com
Internet: www.hima.com

© HIMA Paul Hildebrandt GmbH 2020

“Der SIL steht im Zertifikat”

© HIMA Paul Hildebrandt GmbH 2021

“Der SIL steht im Zertifikat”

+

EC Type-Examination Certificate

Product Safety
Functional
Safety

TÜVRheinland
CERTIFIED

www.tuv.com
ID 9650000000

Reg.-Nr./No.: 01/205/0727.03/19

Prüfgegenstand **Product tested**	Safety Related Programmable Electronic System	**Zertifikats-inhaber** **Certificate holder**	HIMA Paul Hildebrandt GmbH Albert-Bassermann-Str. 28 68782 Brühl bei Mannheim Germany
Typbezeichnung **Type designation**	HIMax - System, Details see actual "Revision List of the HIMax System"		
Prüfgrundlagen **Codes and standards**	EN ISO 13849-1:2015 EN 62061:2005 + AC:2010 + A1:2013 + A2:2015 IEC 61508 Parts 1-7:2010 EN 61131-2:2007		EN 61326-3-1:2017 EN 61000-6-7:2015 DIN IEC 60533:2010-11 EN 50130-4:2011 + A1:2014
Bestimmungsgemäße Verwendung **Intended application**	Safety Related Programmable Electronic System for process control, Burner Management (BMS), emergency shut down and machinery, where the demand safe state is the de-energized state. Applications, where the demand state is the de-energized or energized state. The product is suitable for safety related applications up to SIL 3 (IEC 61508 / EN 62061), Cat. 4 and PL e (EN ISO 13849-1). The product was also reviewed in reference to the requirements of the following standards applicable during a type examination and can be used in application as such. IEC 61511-1:2016+ Corr.1:2016 + AMD1:2017 EN 50156-1:2015 EN 12067-2:2004 EN 298:2012 EN 54-2:1997 + AC:1999 +A1:2006 NFPA 72:2019 NFPA 85:2019 NFPA 86:2019		
Besondere Bedingungen **Specific requirements**	For the use of the systems the Safety Manual, the user guides and the official list of product documentation, hardware components and software modules released by HIMA and TÜV Rheinland have to be considered		

It is confirmed, that the product tested complies with the requirements for machines defined in Annex I of the EC Directive 2006/42/EC.

Gültig bis / Valid until 2024-03-26

Der Ausstellung dieses Zertifikates liegt eine Prüfung zugrunde, deren Ergebnisse im Bericht Nr. 968/FSP 1832.01/19 vom 26.03.2019 dokumentiert sind.
Dieses Zertifikat ist nur gültig für Erzeugnisse, die mit dem Prüfgegenstand übereinstimmen.
The issue of this certificate is based upon an examination, whose results are documented in Report No. 968/FSP 1832.01/19 dated 2019-03-26.
This certificate is valid only for products which are identical with the product tested.

Köln, 2019-03-26 | Notified Body for Machinery, NB 0035 | Dipl.-Ing. Eberhard Freyno

www.fs-products.com
www.tuv.com

TÜVRheinland®
Precisely Right.

=

Funktionale Sicherheit?

“Der SIL steht im Zertifikat”

Schaufensterdokument

© HIMA Paul Hildebrandt GmbH 2021

Zertifikat vs Sicherheitshandbuch (1)

4. Sicherheitshandbuch/ Safety Manual

Seite 8 von 52

4.1. Normengrundlage

- IEC61508 — Funktionale Sicherheit sicherheitsbezogener elektrischer, elektronischer und programmierbarer elektronischer Systeme
- IEC61511 — Funktionale Sicherheit – Sicherheitstechnische Systeme für die Prozessindustrie
- EN ISO 13849-1 (in Anlehnung) — Sicherheitsbezogene Teile von Steuerungen

Mit der Kennzeichnung des Gerätes mit dem CE-Zeichen bestätigt die [redacted] die Erfüllung der gesetzlichen Anforderungen der zutreffenden EG-Richtlinien.

Der Schallgeber [redacted] erfüllt die Anforderungen an die funktionale Sicherheit nach IEC 61508 bzw. IEC61511.

4.2. Besonderheit

Der beschriebene Schallgeber alleine übt keine Schutzfunktion aus (Teilsystem), sondern ist zum Einbau als Ausgabeeinheit mit Diagnose (Output) in den Loop einer Schutzfunktion (SIF) konzipiert. Das Gerät (siehe Abb. 1 und Abb. 2) stellt somit immer nur ein Teilsystem eines sicherheitstechnischen Systems (SIS) dar. Durch den Systemintegrator ist zu beachten, dass der gesamte Loop entsprechend der Anwendung den geforderten SIL-Level erreichen muss. Der Systemintegrator muss alle Maßnahmen festlegen, um im Fehlerfall in der SIS den sicheren Zustand zu erreichen oder aufrechtzuerhalten.

Das Diagnosesystem des Gerätes diagnostiziert bei Anforderung des akustischen Warnsignals dessen Nichtauslösung und Funktion und meldet dieses über ein Alarmrelais an ein übergeordnetes Leitsystem.

---

ufacturer Declaration

[redacted]

/ IEC 61511 u. IEC 62061 bis zu SIL 2

C 61511 a. IEC 62061 up to SIL 2.

Sicherheitshandbuch:
nual:

Zertifikat vs Sicherheitshandbuch (2)

CERTIFICAT

COMPLIA

with IEC EN 61508

E/EE/EP safety-related system (final element)	[redacted] actuators Rack & Pinion produced by [redacted]					
System type	Type A					
Size	[redacted] Type		[redacted] Type		[redacted] Type	
Safety Function Definition	*Complete switching on demand (open to closed & closed to open) with correct torque as for technical data sheets in low demand mode of operation*					
Max SIL	**SIL 2 with HFT = 0 (single actuator configuration)**	**SIL3 with HFT = 1 (redundant configuration)**	**SIL 2 with HFT = 0 (single actuator configuration**	**SIL3 with HFT = 1 (redundant configuration)**	**SIL 2 with HFT = 0 (single actuator configuration**	**SIL3 with HFT = 1 (redundant configuration)**
Additional requirements for the max SIL classification	*Execution of Partial Stroke Test with time interval not higher than 12 months AND Full Functional Proof Test with time interval not higher than 36 months*		*Execution of Partial Stroke Test with time interval not higher than 4 months AND Full Functional Proof Test with time interval not higher than 18 months*		*Execution of Partial Stroke Test with time interval not higher than 3 month AND Full Functional Proof Test with time interval not higher than 9 months*	
λ_{TOT}	1,472E-08		4,854E-08		7,939E-07	
λ_{SD}	9,478E-09		3,126E-08		5,113E-07	
λ_{SU}	0,000E+00		0,000E+00		0,000E+00	
λ_{DD}	0,000E+00		0,000E+00		0,000E+00	
λ_{DU}	5,238E-09		1,728E-08		2,826E-07	
$\lambda_{DU,PST}$	4,346E-09		1,434E-08		2,345E-07	
$\lambda_{DU,FPT}$	8,916E-10		2,941E-09		4,810E-08	
$PFD^{(1)}$	3,075E-05		4,025E-05		4,147E-04	
β and β_D factor	10%		10%		10%	
MTTR	8 h		8 h		8 h	
Hardware Safety Integrity	Route 2_H		Route 2_H		Route 2_H	
Systematic Safety Integrity	Route 2_S		Route 2_S		Route 2_S	

„SIL2 Ventil“ – aber nur mit Partial Stroke Test und vollständigem Test <= 9Monate

© HIMA Paul Hildebrandt GmbH 2021

“Der SIL steht im Zertifikat”

Zertifizierung selbst → JA,
sehr wichtig und richtig!

© HIMA Paul Hildebrandt GmbH 2021

“SIL-Nachweis = Rechnen”

© HIMA Paul Hildebrandt GmbH 2021

Blick durchs Schlüsselloch

Aufgabenstellung: SIL Berechnung für Schutzfunktion mit SIL2 Anforderung

SIF Beschreibung:
Überwachung des Tanklevels (LS++) und schließen des Zulaufventils

Ist doch ganz einfach!
Oder ?

© HIMA Paul Hildebrandt GmbH 2021

“SIL-Nachweis = Rechnen”

SIL2 + SIL3 + SIL2 = SIL7? ☺

© HIMA Paul Hildebrandt GmbH 2021

“SIL-Nachweis = Rechnen”

Subsystem	Sensor	Logic Solver	Final Elements
SIF Loop	SENSOR / SENSOR	LOGIC SOLVER	FINAL ELEMENT / FINAL ELEMENT
Voting	1oo2	1oo1	1oo2
PFDavg	1,60E-04	2,40E-04	9,17E-05
SIL (PFD, HFT, SFF)	3	3	3
Prove Test (Jahren)	1	10	1
MTTR (h)	8	8	8
Typical	S-00024 E+H Diversitäre 1oo2-Architektur: (Liquiphant M/S FTL 50/ FTL 51/ FTL 51C / FTL 70/ FTL71 + FEL57 + FTL 325P) - (Vegapuls Serie 60) Füllstandsmessung LEVEL MAX	LS-0001 Siemens S7F/FH incl. I/O (1oo1) und Kommunikation in SIL3 Konfiguration Safety PLC	FE-0002 NAMUR SAV mit Sicherheitsrelais 1. SAV (Kugelhahn oder Drehkegelventile) mit Antrieb u. Magnetventil 2.Sicherheitsrelais - DETAILLIERTE AUSWAHL möglicher GERÄTE siehe AKTOR-Liste -
Typical / ID	S-L-1oo2-SIL3-014	LS-0001	F-V-1oo2-SIL3-001
	PFDavg Sensor: 1,60E-04	PFDavg Logic Solver: 2,40E-04	PFDavg Final Element: 9,17E-05

SIL acc. PFD, HFT and SFF	3	SIL total:	3	PFD total:	4,92E-04	made by:	verified by
SIL acc. PFD	3					Date 29.04.2012	Date 02.05.2012
Proof test intervall (Years)	1					Name FS	Name GG
						Behälteranlage XYZ 5110064	Rev. 0
							MASTER SIF x

Funktional:
Erfüllt die SIF wirklich die Funktion, die in der Gefahren- und Risikoanalyse gefordert wurde?

PFD, HFT, systematische Eignung:
Sind ALLE geforderten SIF- und gerätespezifischen Kriterien des SIL erfüllt?

© HIMA Paul Hildebrandt GmbH 2021

SIL Verifikation – mehr als nur Berechnungen

Blick durchs Schlüsselloch

Aufgabenstellung: SIL Berechnung für Schutzfunktion mit SIL2 Anforderung

SIF Beschreibung:
Überwachung des Tanklevels (LS++) und schließen des Zulaufventils

Ist doch ganz einfach!
Oder ?

© HIMA Paul Hildebrandt GmbH 2021

Das volle Bild – ganzheitliche Verifikation

Vermischung von Schutz- und Regelfunktion

SIF:
Überwachung des Tanklevels (LS++) und schließen des Zulaufventils **wenn die Betriebseinrichtung zur Füllstands-Regelung (LC) versagt (Störung)**

Das Regelventil selbst kann die Ursache sein → in der Regel kein SIL2 erreichbar

© HIMA Paul Hildebrandt GmbH 2021

“…Irrtümer erkennen – und handeln”

© HIMA Paul Hildebrandt GmbH 2021

Vielen Dank
Haben Sie noch Fragen ?

HIMA Paul Hildebrandt GmbH

Albert-Bassermann-Str. 28
68782 Brühl, Germany

Phone: +49 6202 5770 -130
Mobile: +49 1624250759

E-mail: info@hima.com
Internet: www.hima.com

© HIMA Paul Hildebrandt GmbH 2020