



Armaturen

Leitfaden

Funktionale Sicherheit Safety Integrity Level - SIL -

Armaturen und Armaturenantriebe

November 2008

Entscheidungshilfen
schaffen
Klarheit

Verband Deutscher Maschinen-
und Anlagenbau e.V.

**Fachverband
Armaturen**
Vorsitzender:
Prof.-Dr.-Ing. Heinfried Hoffmann
Geschäftsführer:
Wolfgang Burchard

Lyoner Straße 18
D-60528 Frankfurt am Main
Telefon +49 69 66 03-12 41
Telefax +49 69 66 03-16 34
E-Mail armaturen@vdma.org
Internet www.vdma.org

VDMA
Wir, die Investitionsgüterindustrie

Inhalt

1.	Einführung	3
2.	Anwendungsbereich	4
3.	Funktionale Sicherheit	5
4.	Mögliche Maßnahmen zur Umsetzung von SIL (Ermittlung von Kennzahlen)	6
4.1	Sicherheitssysteme	6
4.2	Kennzahlenermittlung	7
4.3	Ermittlungsmöglichkeiten der λ-Werte	10
5.	Möglichkeiten der Veränderung der SIL-Klasse des Sicherheitssystems durch den Betreiber (DIN EN 61511-ff)	12

Anhang

Regelwerke

Begriffe

1. Einführung

Verfahrenstechnische Anlagen in der chemischen, pharmazeutischen und petrochemischen Industrie müssen „sicher“ betrieben werden, da sie ein hohes Gefährdungspotenzial für Mensch und Umwelt besitzen bzw. große Sachschäden verursachen können. Das gilt selbstverständlich auch für andere Bereiche der Industrie (z. B. Kraftwerke).

Bei der Entwicklung entsprechender Schutzkonzepte leistet Prozeßleittechnik mit so genannten PLT-Schutzeinrichtungen einen wichtigen Beitrag zur Anlagensicherheit. Dabei beachtet sie u. a. die Anforderungen der internationalen Standards DIN EN 61508 und DIN EN 61511.

Während sich die DIN EN 61508 „Funktionale Sicherheit - Sicherheitsbezogene elektrische, elektronische und programmierbare elektronische Systeme“ in erster Linie an die Hersteller von Komponenten für Schutzeinrichtungen wendet, wird mit der DIN EN 61511 „Funktionale Sicherheit - Sicherheitstechnische Systeme in der Prozeßindustrie“ vor allem der Betreiber und Planer von Schutzeinrichtungen adressiert. Die DIN EN 61511 gibt Empfehlungen und Vorgaben zur Beurteilung des Schadensrisikos von Anlagen und unterstützt bei der Auswahl geeigneter, sicherheitstechnischer Komponenten. Diese Norm definiert vier Sicherheitsstufen, die sogenannten Safety Integrity Level 1 – 4. Je höher das Risiko, das von der Anlage ausgeht, umso zuverlässiger müssen die Maßnahmen zur Risikoreduzierung durchgeführt werden und desto höher sind die Anforderungen an die eingesetzten elektrischen, elektronischen und programmierbaren elektronischen Komponenten.

Anlagenbetreiber versuchen nun seit einiger Zeit, die Methode auch auf mechanische Produkte zu übertragen und haben damit eine Diskussion in Betreiber-, Hersteller- und Zertifizierungskreisen über den tatsächlichen Anwendungsbereich und die Relevanz der genannten Normen für Armaturen und Armaturentriebe in Gang gesetzt.

Der folgende Leitfaden beschreibt die aus Sicht der Armaturenindustrie maßgeblichen Anwendungs- und Umsetzungskriterien, die für Armaturen und Armaturentriebe gegebenenfalls zu berücksichtigen sind und soll damit einen Beitrag zur Vermeidung unnötiger Diskussionen in den beteiligten Kreisen leisten.

An der Erarbeitung dieses Leitfadens waren Mitgliedsfirmen des VDMA beteiligt.

2. Anwendungsbereich

Die Norm DIN EN 61508 beschreibt den Stand der Technik in Bezug auf funktionale Sicherheit für elektrische, elektronische und programmierbare elektronische Systeme (E/E/PE), die für Sicherheitsfunktionen in sicherheitskritischen Anwendungen zum Einsatz kommen.

Armaturen, die nicht in sicherheitsgerichtete Systeme eingebunden werden können (z. B. **handbetriebene Armaturen** ohne Rückmeldung/Endschalter) stehen damit per se außerhalb des Anwendungsbereichs der Norm.

Dasselbe gilt für **selbsttätige Sicherheitsventile**, da diese nie Bestandteil der „normalen Betriebsprozesse“ sind, deren funktionale Sicherheit nach SIL überprüft werden sollen.

Schließlich ist auch für **Stellgeräte und deren Einzelkomponenten** als mechanischen Bauteilen (z. B. Armaturen, Armaturentriebe, Stellungsregler) eine Klassifizierung gemäß SIL nach DIN EN 61508-ff nicht unmittelbar möglich.

Jedoch können Kennzahlen (z. B. Ausfallraten, Hardware-Fehler-Toleranzen) definiert werden, die zu einer Bestimmung des SIL des kompletten sicherheitsrelevanten Systems verwendet werden können.

Aber hierbei gilt: Die DIN EN 61508 ist nicht unter einer für Armaturen relevanten EU-Richtlinie harmonisiert, d. h. eine automatische Vermutungswirkung zur Erfüllung der Schutzziele einer Richtlinie geht von ihr nicht aus. Ihre Einhaltung ist daher **freiwillig** und somit unverbindlich im Sinne der EU-Richtlinien.

Es bleibt also jedem Armaturenhersteller im Dialog mit seinem Kunden überlassen, ob und inwieweit sinnvoller Weise Kennzahlen definiert werden, die im Rahmen einer SIL Klassifizierung als Grundlage zur Bewertung der Komponente „Armatur“ Berücksichtigung finden sollen.

Anmerkung: Je nach Bauart, Funktion, Einsatzgebiet und Einsatzbedingungen eines nach SIL betrachteten Bauteils sind neben den in diesem Leitfaden erwähnten Normen andere Regelwerke (wie z. B. Druckgeräteverordnung, ATEX, EMV) zusätzlich zu berücksichtigen.

3. Funktionale Sicherheit

Funktionale Sicherheit ist der Teil der Gesamtsicherheit, der von der korrekten Funktion eines sicherheitsbezogenen E/E/PE-Systems, sicherheitsbezogenen Systemen anderer Technologie und externer Einrichtungen zur Risikominderung abhängt. Sie ist gegeben, wenn jede spezifizierte Sicherheitsfunktion ausgeführt wird und der für jede Sicherheitsfunktion geforderte Erfüllungsgrad erreicht wird. Die Hauptforderung der DIN EN 61508 besteht darin, den quantitativen Nachweis für das bleibende Restrisiko hinsichtlich der funktionalen Sicherheit zu erbringen. Zur Reduzierung dieses Risikos beschreibt die Norm die beiden wesentlichen Schritte:

- Definition und Bewertung des Risikos auf Basis von detaillierten Versagenswahrscheinlichkeiten für den gesamten Lebenszyklus der Anwendung.
- Periodische Überprüfung der korrekten Einhaltung von Vorgaben. Der betrachtete Lebenszyklus ist in 16 Teilaspekte untergliedert (Bild 2, DIN EN 61508-1, Nov. 2002).

In der genannten Norm DIN EN 61508-1 finden sich in Kapitel 8.2 Anforderungen an die Beurteilung der funktionalen Sicherheit. Ein Teilaspekt dieser Anforderungen sind sogenannte Unabhängigkeitsgrade von Personen, Abteilungen und Organisationen. Das Zusammenspiel von Unabhängigkeitsgraden und Sicherheits-Integritätslevels im Rahmen der 16 Teilaspekte des Sicherheitslebenszyklus ist dort in den Tabellen 4 und 5 beschrieben.

Integre Produkte und Ausfallwahrscheinlichkeit

Die Risikoreduzierung in Anlagen mit hohem Gefahrenpotenzial (z. B. in der Prozesstechnik) erfordert eine moderne Sicherheitstechnik. Dabei ist ein durchgängiges Sicherheitskonzept vom Sensor über die Steuerung bis zum Aktor erforderlich.

Das Risikopotenzial einer (Teil)Anlage kann beispielsweise gemäß DIN EN 61511 ermittelt werden. Je nach ermitteltem Risiko ist eine Risikominimierung durchzuführen. Erfolgt die Risikominimierung mithilfe elektrischer Komponenten, so müssen diese die Anforderungen der DIN EN 61508 erfüllen. Beide Normen teilen die verfahrenstechnische Anlage in vier Sicherheitsebenen (SIL) ein, die für die Risikoreduzierung notwendig sind. Ein Sicherheits-Integritätslevel (SIL) ist eine von vier diskreten Stufen, wobei jede Stufe einem Bereich für die Ausfallwahrscheinlichkeit einer Sicherheitsfunktion entspricht. SIL 4 stellt die höchste Stufe dar, SIL 1 die niedrigste. Dabei ist zu beachten, dass ein Sicherheits-Integritätslevel eine Eigenschaft eines Systems oder Teilsystems darstellt und nicht einer Komponente. In den **Tabellen 1 und 2** sind nachfolgend beispielhaft

Ausfallgrenzwerte und die nach DIN EN 61508 zugeordneten Sicherheits-Integritätslevel aufgeführt.

Sicherheits-Integritätslevel	Betriebsart mit niedriger Anforderungsrate (mittlere Ausfallwahrscheinlichkeit der entworfenen Funktion bei Anforderung; nach Tab. 2 DIN EN 61508-1)
4	$\geq 10^{-5}$ bis $< 10^{-4}$
3	$\geq 10^{-4}$ bis $< 10^{-3}$
2	$\geq 10^{-3}$ bis $< 10^{-2}$
1	$\geq 10^{-2}$ bis $< 10^{-1}$

Tab. 1 (Quelle: DIN EN 61508-1, Nov. 2002)

Sicherheits-Integritätslevel	Betriebsart mit hoher Anforderungsrate oder kontinuierlicher Anforderung (Wahrscheinlichkeit eines gefahrbringenden Ausfalls pro Stunde; nach Tab. 3 DIN EN 61508-1)
4	$> 10^{-9}$ bis $< 10^{-8}$
3	$> 10^{-8}$ bis $< 10^{-7}$
2	$> 10^{-7}$ bis $< 10^{-6}$
1	$> 10^{-6}$ bis $< 10^{-5}$

Tab. 2 (Quelle: DIN EN 61508-1, Nov. 2002)

Hinweis: In den Anwendungsbereichen von Armaturen sind i. d. R. Betriebsarten mit niedriger Anforderungsrate von Bedeutung.

4. Mögliche Maßnahmen zur Umsetzung von SIL (Ermittlung von Kennzahlen)

4.1 Sicherheitssysteme

Die Relevanz von SIL ist nicht von der Frage der Physik eines Bauteils abhängig, sondern stellt sich im Falle der konkreten Sicherheitsanforderung eines Betreibers bzw. Kunden. Mechanische Bauteile (z. B. Armaturen) können Bestandteile eines elektrischen / elektronischen / programmierbaren elektronischen Sicherheitssystems sein und unterliegen der gleichen Sicherheitsbetrachtung wie das System selbst.

Ein solches Sicherheitssystem besteht beispielsweise aus einer Verkettung von Teilsystemen, d. h. hauptsächlich aus dem Sensor, der Logik (SPS und Leitsystem), dem Aktor (Armatur, Antrieb und Zusatzgeräte wie Stellungsregler oder Magnetventil) und weiteren mechanischen/nichtelektrischen Bauelementen.

4.2 Kennzahlenermittlung

Anhand von Kennzahlen ist es für den Betreiber möglich, die SIL-Klasse eines Systems in Abhängigkeit des betrachteten Sicherheitskreises zu bestimmen. In einer Bescheinigung des Armaturenherstellers ist daher lediglich die Angabe der Kennzahlen, nicht der SIL-Klasse selbst möglich.

Die Angaben für die Kennzahlen sind stets im Zusammenhang mit der jeweils betrachteten produktspezifischen Anwendung und den entsprechenden Betriebsbedingungen zu sehen.

Bei Neukonstruktionen von Komponenten oder Anlagen ist es sinnvoll, die Relevanz der Sicherheitsthematik SIL im Vorfeld zu prüfen und ggf. frühzeitig benannte Stellen oder andere externe Expertise einzubeziehen.

Mögliche Vorgehensweise zur Beurteilung der Sicherheitsfunktion nach SIL

- Definition der Sicherheitsfunktion des Stellgliedes und des Einsatzbereiches
- Zerlegung in sicherheitsrelevante Funktionsblöcke
- Risikoanalyse z. B. mittels FME(D)A
- Felddaten als Grundlage für die Zuverlässigkeitsbetrachtung („proven in use“)
- Versuchsdurchführungen / Produktvalidierung
- Produktbeobachtung
- Qualitätsgesicherte Fertigung
- Ermittlung von Kennzahlen (wird nachfolgend näher erläutert)
- Einbindung und Pflege der Sicherheitsbetrachtung in das Qualitätsmanagementsystem
- Erweiterung der Betriebsanleitung durch sicherheitsrelevante Hinweise
- Ausstellung einer Herstellerbescheinigung

Die in diesem Leitfaden bereits angesprochenen und auf Stellgeräte anwendbaren Kennzahlen und deren Ermittlungsmöglichkeiten sind in der nachfolgenden **Tabelle 3** beschrieben.

Kennzahl	Definition	Einheit	Wert
HFT	Hardware-Fehler-Toleranz: Fähigkeit einer Funktionseinheit, eine geforderte Funktion bei Bestehen von Fehlern oder Abweichungen weiter auszuführen (siehe auch DIN EN 61511-1, Kap.11.4, Mai 2005). HFT wird vom Anwender festgelegt (Industriearmaturen 04/2005)		
SFF	Anteil ungefährlicher Ausfälle (safe failure fraction)	%	
PFD _{avg} Gesamtsystem	Mittlere Wahrscheinlichkeit Gefahr bringender Ausfälle einer Sicherheitsfunktion im Anforderungsfall (average probability of failure to perform its design function on demand)		
PFD _{avg} Teilsystem Aktor: Armatur	Mittlere Wahrscheinlichkeit Gefahr bringender Ausfälle einer Sicherheitsfunktion im Anforderungsfall		Für den Aktor kann ca. 50% des SIL-Kontingentes veranschlagt werden
PFD _{avg} Teilsystem Aktor: Magnetventil/Stellungsregler	Mittlere Wahrscheinlichkeit Gefahr bringender Ausfälle einer Sicherheitsfunktion im Anforderungsfall		Für den Aktor kann ca. 15% des SIL-Kontingentes veranschlagt werden
PFD _{avg} Teilsystem Aktor: Stellventil	Mittlere Wahrscheinlichkeit Gefahr bringender Ausfälle einer Sicherheitsfunktion im Anforderungsfall		Für den Aktor kann ca. 15% des SIL-Kontingentes veranschlagt werden

Kennzahl	Definition	Einheit	Wert
PFD_{avg} Teilsystem Aktor: Stellan- trieb	Mittlere Wahrscheinlichkeit Gefahr bringender Ausfälle einer Sicherheitsfunktion im Anforderungsfall		Für den Aktor kann ca. 15% des SIL-Kontingentes veranschlagt werden
$MTTF_d$	Angenommene mittlere Zeit bis zum Gefahr bringenden Ausfall (mean time to failure dangerous)	[Zeit- einheit]	
λ_{SD}	Rate für sichere, erkannte Ausfälle	FIT (failure in time)	
λ_{SU}	Rate für sichere, nicht erkannte Ausfälle	FIT	
λ_{DD}	Rate für gefährliche, erkannte Ausfälle	FIT	
λ_{DU}	Rate für gefährliche, nicht erkannte Ausfälle	FIT	
DC	Diagnostic coverage (Diagnosedeckungsgrad): Verhältnis der Ausfallrate der durch Diagnosetests erkannten Fehler zur Gesamtausfallrate der Komponente oder des Teilsystems. Der Diagnosedeckungsgrad beinhaltet keine bei Wiederholungsprüfungen (proof tests) festgestellten Fehler (weitere Hinweise auch zu λ siehe DIN EN 61511-1, Kap. 3.2.15, Ausgabe Mai 2005)	%	
CCF	Ausfälle infolge gemeinsamer Ursache (common caused failure). Ausfälle verschiedener Einheiten aufgrund eines einzelnen Ereignisses, wobei diese Ausfälle keine gegenseitigen Auswirkungen haben (Entwurf DIN EN ISO 13489-1, 2004, Kap. 3.1.6)		

Kennzahl	Definition	Einheit	Wert
Performance Level PL	Fähigkeit von sicherheitsbezogenen Teilen, eine Sicherheitsfunktion unter vorhersehbaren Bedingungen auszuführen (die in Betracht gezogen werden sollten), um die erwartete Risikominderung zu erfüllen (Entwurf DIN EN ISO 13489-1, 2004, Kap. 3.1.23)		

Tab. 3 Kennzahlen

Die Schlüsselkennzahlen PL, $MTTF_d$, DC und CCF weisen folgende Eigenschaften auf:

- Ergebnis einer Berechnung
- Geeignet, die Sicherheit in mechanischen Systemen zu bestimmen
- Integrieren auch elektrische Systeme

Nach der nachfolgend beschriebenen Ermittlung der λ -Werte können die folgenden weiteren Werte gemäß DIN EN 61508-ff berechnet werden:

SFF, DC, PFD_{avg}

4.3 Ermittlungsmöglichkeiten der λ -Werte

Neben den nachfolgend kurz beschriebenen Ansätzen gibt es sicherlich weitere Möglichkeiten der Ermittlung der λ -Werte. Die Auswahl hängt von vielen Parametern ab und muss von jedem Hersteller individuell erfolgen. Dabei empfiehlt sich, das Hinzuziehen des Kunden zu prüfen.

Ansatz 1

Der Hersteller verwendet vorhandene Datenbestände und Erfahrungen im Markt aktiver Institutionen (exida, oreda etc.).

Ansatz 2

Für die Ermittlung der Kennzahlen kann die Methodik nach DIN EN ISO 13849 herangezogen werden.

Ansatz 3

Genereller Eignungsnachweis für eine Sicherheitsanforderungsklasse (SIL):

- Bauteilprüfung nach einer relevanten Gerätenorm
- Festlegung der Fehlerarten über den gesamten Lebenszyklus in Anlehnung an DIN V 19251
- Abstufung von Maßnahmen zur Fehlervermeidung und Beherrschung in Anlehnung an DIN V 19251
- Durchführung einer FME(D)A
- Bereitstellung aller Daten für das Konfigurationsmanagement (gemäß DIN EN 61511)
- Sicherstellung der produktionsbegleitenden Qualitätssicherungsmaßnahmen
- Gegenüberstellung von Anforderungsklassen in Anlehnung an DIN V 19250 mit SIL unter Verwendung der DIN EN 61511-3 Anhang E

Ansatz 4

Prüfschritte für die Eignungsuntersuchung von Stellgeräten nach DIN EN 61508-ff

- Bauteilprüfung nach einer relevanten Gerätenorm (z. B. DIN EN 161)
- Durchführung einer Baugruppen-FME(D)A
- Praktische Dauerprüfung an repräsentativen Stellgeräten zum Nachweis eines PFD-Wertes
- Statistische Untersuchung der Betriebsbewährung in verschiedenen verfahrenstechnischen Anlagen
- Herstellung der Produkte auf einem entsprechend hohen nachgewiesenem Qualitätsstandard

Mit den Prüfungen in Verbindung mit den statistischen Daten kann man ausreichend zuverlässige Aussagen zur Ausfallwahrscheinlichkeit treffen.

- Festlegung der Kennzahlen (Tabelle 3) für die SIL-Klassifizierung (Anpassung der Kennzahlen sofern statistische Daten vorliegen)

5. **Möglichkeiten der Veränderung der SIL-Klasse des Sicherheitssystems durch den Betreiber (DIN EN 61511-ff)**

Der Betreiber verfügt über die beiden folgenden Möglichkeiten, die SIL-Klasse seines Sicherheitssystems zu verändern:

- Veränderung der Proof-test-Intervalle
- Veränderung der Systemarchitektur, z. B. durch Redundanz (z. B. zwei in Reihe geschaltete Armaturen).

Anhang

Regelwerke

DIN EN ISO 13849	Sicherheit von Maschinen - Sicherheitsbezogene Teile von Steuerungen
Teil 1:	Allgemeine Gestaltungsleitsätze (2007-07)
Teil 2:	Validierung (2003-12)
DIN EN 61508	Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme
Teil 0:	Funktionale Sicherheit und die DIN EN 61508 (2005-10)
Teil 1:	Allgemeine Anforderungen (2002-11)
Teil 2:	Anforderungen an sicherheitsbezogene elektrische/elektronische/programmierbare elektronische Systeme (2002-12)
Teil 3:	Anforderungen an Software (2002-12)
Teil 4:	Begriffe und Abkürzungen (2002-11)
Teil 5:	Beispiele zur Ermittlung der Stufe der Sicherheitsintegrität (2002-12)
Teil 6:	Anwendungsrichtlinie für DIN EN 61508-2 und DIN EN 61508-3 (2003-06)
Teil 7:	Anwendungshinweis über Verfahren und Maßnahmen (2003-06)
DIN EN 61511	Funktionale Sicherheit - Sicherheitstechnische Systeme für die Prozessindustrie
Teil 1:	Allgemeines, Begriffe, Anforderungen an Systeme, Software und Hardware (2005-05)
Teil 2:	Anleitungen zur Anwendung des Teils 1 (2005-05)
Teil 3:	Anleitung für die Bestimmung der erforderlichen Sicherheits-Integritätslevel (2005-05)

DIN EN 62061	Berichtigung 1 - Sicherheit von Maschinen - Funktionale Sicherheit sicherheitsbezogener elektrischer, elektronischer und programmierbarer elektronischer Steuerungssysteme (2006-06)
VDI 2180	Sicherung von Anlagen der Verfahrenstechnik mit Mitteln der Prozessleittechnik (PLT) (2007-04)
NE 031	Anlagensicherung mit Mitteln der Prozessleittechnik (NAMUR-Empfehlung 2006-07)
NE 93	Nachweis der sicherheitstechnischen Zuverlässigkeit von PLT-Schutzeinrichtungen (NAMUR-Empfehlung 2003-02)

Begriffe

EUC	=	Equipment under control (DIN EN 61508-4) [in DIN EN 61511 Prozess genannt]
Failure	=	(Versagen): Beendigung der Fähigkeit einer Funktionseinheit, eine geforderte Funktion auszuführen (DIN EN 61508-4)
Proof test	=	Wiederkehrende Prüfung zur Aufdeckung von Ausfällen in einem sicherheitsbezogenen System, so dass nötigenfalls das System in einen „Wie-Neu“-Zustand gebracht oder so nah wie unter praktischen Gesichtspunkten möglich an diesen Zustand herangebracht werden kann (DIN EN 61508-4)
Aktor	=	Baueinheit bestehend aus Stellantrieb, Stellarmatur und Zubehör (Magnetventil/Stellungsregler, Adapter, etc.)

Ansprechpartner

Hartmut Tembrink
Fachverband Armaturen im VDMA
Lyoner Straße 18
60528 Frankfurt am Main
Telefon 0 69/66 03-12 46
Telefax 0 69/66 03-22 46
E-Mail hartmut.tembrink@vdma.org