



Füllstand



Druck



Durchfluss



Temperatur



Flüssigkeits-
analyse



Registrierung



Systeme
Komponenten



Services



Solutions

DIN EN IEC 61508/IEC 61511

Funktionale Sicherheit in der Prozess-Instrumentierung
zur Risikoreduzierung

Safety Integrity Level

Sicherheitsgerichtete Instrumentierung durch SIL

Klassifizierte und bewertete Geräte in der Prozessindustrie liefern einen wichtigen Beitrag zur Sicherheit der Menschen, der Umwelt und der Anlagen.

In den meisten Ländern werden die Sicherheitsanforderungen für Mensch, Anlagen und Umwelt nach dem bestmöglichen Stand der Technik gesetzlich gefordert. Der Maßstab ist die IEC 61508* („Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme“).

*liegt auch als DIN EN 61508 vor



Was ist SIL (Safety Integrity Level)?

Die Aufgabe von Sicherheitsfunktionen (safety functions) ist, das Risiko von Prozessen zu minimieren, von denen Gefahren für Mensch, Umwelt und Sachwerte ausgehen. SIL (safety integrity level) bedeutet das Maß der Risikoreduzierung auf ein vertretbares Niveau.

Die IEC 61508 beschreibt sowohl die Art der Risikobewertung (Risikograph) als auch die Maßnahmen zur Auslegung entsprechender Sicherheitsfunktionen von Sensoren, Logikverarbeitung bis hin zum Aktor bezüglich „Fehlervermeidung“ (systematische Fehler) und „Fehlerbeherrschung“ (zufällige Fehler).

Dieser anwendungsunabhängige Basisstandard (generic standard) beschreibt die Anforderungen an Komponenten und Systeme für Sicherheitsfunktionen und hilft bei der Entwicklung sektorspezifischer Normen (z. B. Entwurf IEC 61511-1 „Funktionale Sicherheit: Sicherheitstechnische Systeme für den Bereich der Prozessindustrie“). Unter anderem legt die IEC 61511-1 Auswahlkriterien für Komponenten der Sicherheitsfunktionen wie z. B. die Betriebsbewahrung von Sensoren und Aktoren fest.

Für welche Anforderungen wird die IEC 61508 herangezogen?

Die IEC 61508 gilt für alle Anwendungen, in denen elektrische, elektronische oder programmierbare elektronische sicherheitsgerichtete Systeme zur Ausführung von Sicherheitsfunktionen eingesetzt werden. Sie bezieht sich auf Anwendungen, bei denen ein Fehlverhalten von Systemen einen massiven Einfluss auf die Sicherheit von Personen, der Umwelt und der Anlagen hat.



Welche Vorteile bringt die Normierung?

- International harmonisierte Vorgehensweise bei der Beurteilung von Schutzeinrichtungen.
- Bewertung von PLT-Geräten im Hinblick auf systematische Fehler und statistisch belegbare Angaben von zufälligen Fehlern.
- Definiertes „Life-Cycle Management“ d.h. Dokumentation aller funktionsrelevanten Entwicklungsschritte.
- Komplette Bewertung der gesamten Schutzeinrichtung (Sensor/Transmitter, Steuerung, Aktor).
- Die erforderliche Sicherheit kann durch bewertete Messtechnik erreicht werden; ohne aufwändige Änderung der Verfahrenstechnik.



IEC 61508 / IEC 61511

Sicherheitsbeurteilungen und Anforderungen

Was unterscheidet die IEC 61508 von den bisherigen Normen?

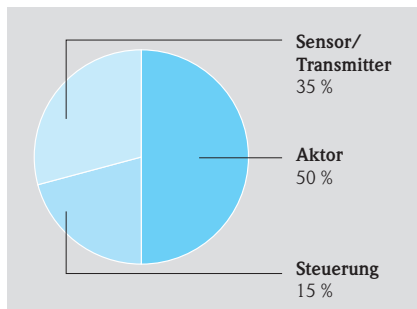
Zum ersten Mal fordert eine Norm einen quantitativen Nachweis für das verbleibende Risiko, auf der Basis einer Berechnung der gefährlichen Versagenswahrscheinlichkeiten. Diese Berechnung erfolgt für den kompletten Loop/Sicherheitssystem, von der Messstelle (Sensor), über die Steuerung (z. B. SPS) bis zum Aktor (Ventil).

Die für alle Einzelkomponenten berechneten Versagenswahrscheinlichkeiten werden addiert (PFD) und über die sicherheitstechnische Auswahlwahlung (voting), wie z. B. 1oo1 (one out of one) oder 2oo3, berücksichtigt. Bei dieser Sicherheitsnorm werden nicht nur die einzelnen Geräte, sondern auch deren Entwicklung und Fertigung berücksichtigt (safety life cycle).

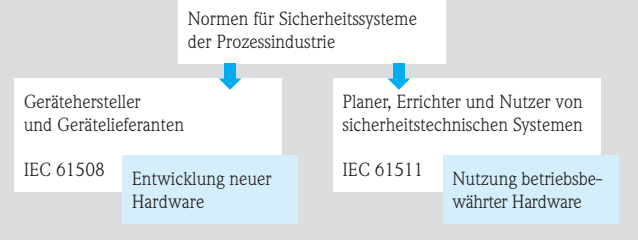
	SIL	PFD _{av}
	4 ¹⁾	$\geq 10^{-5} \dots < 10^{-4}$
	3	$\geq 10^{-4} \dots < 10^{-3}$
	2	$\geq 10^{-3} \dots < 10^{-2}$
	1	$\geq 10^{-2} \dots < 10^{-1}$

Zulässige mittlere Versagenswahrscheinlichkeiten des gesamten Sicherheitssystems in Abhängigkeit vom SIL für Systeme, die auf Anforderungen reagieren müssen (Low demand mode).

Die Bereiche des PFD_{av} teilen sich im Allgemeinen für das gesamte Sicherheitssystem wie folgt auf:



Beziehung zwischen IEC 61508 und IEC 61511



Zur Minimierung des Risikos schreiben sowohl IEC 61508 als auch IEC 61511 im Wesentlichen folgende Schritte vor:

- Risikodefinition und -bewertung nach detaillierten Versagenswahrscheinlichkeiten vom Sensor über die Steuerung bis zum Aktor über die gesamte Lebensdauer der Komponenten.
- Festlegung und Umsetzung der Maßnahmen zur Restrisikominimierung.
- Einsatz geeigneter Geräte (bewertet oder zertifiziert).
- Wiederkehrende Prüfung der korrekten Einhaltung der Sicherheitsfunktionen.

Risikograph nach IEC 61508/61511

		W3	W2	W1
C1	P1	SIL 1	–	–
	P2	SIL 1	SIL 1	–
C2	F1	SIL 2	SIL 1	SIL 1
	F2	SIL 3	SIL 2	SIL 1
C3	F1	SIL 3	SIL 3	SIL 2
	F2	SIL 4 ¹⁾	SIL 3	SIL 3
C4	–	SIL 4 ¹⁾	SIL 3	

Schadenausmaß

- C1** leichte Verletzung einer Person oder kleinere schädliche Umwelteinflüsse
- C2** schwere, irreversible Verletzung einer oder mehrerer Personen oder Tod einer Person oder vorübergehende größere schädliche Umwelteinflüsse
- C3** Tod mehrerer Personen oder lang andauernde größere schädliche Umwelteinflüsse, z. B. nach Störfallverordnung.
- C4** katastrophale Auswirkung, sehr viele Tote.

Aufenthaltsdauer

- F1** selten bis öfter
- F2** häufig bis dauernd

Gefahrenabwehr

- P1** möglich unter bestimmten Bedingungen
- P2** kaum möglich

Eintrittswahrscheinlichkeit

- W1** sehr gering
- W2** gering
- W3** relativ hoch

¹⁾ SIL 4 kann nicht ausschließlich mit PLT-Komponenten erreicht werden

SFF, HFT, SIL

Zusammenhang zwischen wichtigen Sicherheitsparametern

Die **Safe Failure Fraction (SFF)** beschreibt den prozentualen Anteil von Ausfällen ohne Potenzial, das sicherheitsbezogene System in einen gefährlichen oder unzulässigen Funktionszustand zu versetzen.

Die **Hardwarefehlertoleranz (HFT)** ist die Fähigkeit eines Systems, eine Sicherheitsfunktion bei Bestehen von Fehlern weiter korrekt auszuführen. Eine HFT von N bedeutet, dass N+1 Fehler zu einem Verlust der Sicherheitsfunktion führen können.

Zusätzlich zur Einhaltung von Maximalwerten für die gefährliche Versagenswahrscheinlichkeit (PFD) ist der erreichbare **Safety Integrity Level (SIL)** einer Sicherheitsfunktion nach IEC 61508 von der Kombination der Kenngrößen SFF und HFT abhängig.



Was ist der Unterschied zwischen „einfachen“ und „komplexen“ Geräten?

Bei „einfachen“ (Typ A) Geräten ist das Ausfallverhalten der Bauteile vollständig beschreibbar. Solche Bauteile sind z. B. Metallschichtwiderstände, Transistoren, Relais etc.

Bei „komplexen“ (Typ B) Geräten ist das Ausfallverhalten der Bauteile nicht vollständig bekannt. Solche Bauteile sind z. B. Mikroprozessoren, ASICs.

Die Ausfallraten dieser Bauteile können aus den einschlägigen Tabellenwerken entnommen werden.

Typ A: „Einfache“ Geräte (alle Fehler bekannt und beschreibbar)			
SFF Safe Failure Fraction	Hardware	HFT Fault	Tolerance
	0	1	2
< 60 %	SIL 1	SIL 2	SIL 3
60 - < 90 %	SIL 2	SIL 3	SIL 4
90 - < 99 %	SIL 3	SIL 4	SIL 4
≥ 99 %	SIL 3	SIL 4	SIL 4

Typ B: „Komplexe“ Geräte (nicht alle Fehler bekannt und beschreibbar)			
SFF Safe Failure Fraction	Hardware	HFT Fault	Tolerance
	0	1	2
< 60 %	not allowed	SIL 1	SIL 2
60 - < 90 %	SIL 1	SIL 2	SIL 3
90 - < 99 %	SIL 2	SIL 3	SIL 4
≥ 99 %	SIL 3	SIL 4	SIL 4

Für betriebsbewährte Geräte darf nach IEC 61511 unter bestimmten Bedingungen die HFT um 1 reduziert werden (nur für SIL ≤ 3).

Ihr zusätzlicher Nutzen bei Endress+Hauser

- Alle wichtigen sicherheitsrelevanten Parameter aus einer Hand im Standard bis SIL 2: Druck – Temperatur – Füllstand – Durchfluss – System-Komponenten.
- Einheitliche, kompakte „Safety Manuals“ für Transparenz und Sicherheit bei der Planung, Inbetriebnahme und Funktionsprüfung von Schutzeinrichtungen.
- Sicherheitstechnische Beurteilung von Software-Updates im Standard nach IEC 61508.



Endress+Hauser entwickelt für alle wichtigen Arbeitsgebiete der Prozessmesstechnik, Geräte nach IEC 61508.

Eine Auflistung der SIL-bewährten Feldgeräte und Dokumentationen (z. B. Safetymanual) wird unter www.de.endress.com/SIL laufend aktualisiert.

Deutschland

Endress+Hauser
Messtechnik
GmbH+Co. KG
Colmarer Straße 6
79576 Weil am Rhein

Fax 0 800 EHFAXEN
Fax 0 800 343 29 36
www.de.endress.com

Vertrieb

- Beratung
- Information
- Auftrag
- Bestellung

Tel. 0 800 EHVTRIEB
Tel. 0 800 348 37 87
info@de.endress.com

Service

- Help-Desk
- Feldservice
- Ersatzteile/Reparatur
- Kalibrierung

Tel. 0 800 EHSERVICE
Tel. 0 800 347 37 84
service@de.endress.com

Technische Büros

- Hamburg
- Hannover
- Ratingen
- Frankfurt
- Stuttgart
- München
- Berlin

Österreich

Endress+Hauser
Ges.m.b.H.
Lehnergasse 4
1230 Wien
Tel. +43 1 880 56 0
Fax +43 1 880 56 335
info@at.endress.com
www.at.endress.com

Schweiz

Endress+Hauser
Metso AG
Sternenhofstraße 21
4153 Reinach
Tel. +41 61 715 75 75
Fax +41 61 711 16 50
info@ch.endress.com
www.ch.endress.com