

# DIN EN ISO 13849-1:2008-12 (D)

## Sicherheit von Maschinen - Sicherheitsbezogene Teile von Steuerungen - Teil 1: Allgemeine Gestaltungsleitsätze (ISO 13849-1:2006); Deutsche Fassung EN ISO 13849-1:2008

---

Inhalt	Seite
Vorwort .....	4
Einleitung .....	5
1 Anwendungsbereich .....	7
2 Normative Verweisungen .....	7
3 Begriffe, Formelzeichen und Abkürzungen .....	8
3.1 Begriffe .....	8
3.2 Formelzeichen und Abkürzungen .....	14
4 Gestaltungsaspekte .....	15
4.1 Sicherheitsziele in der Gestaltung .....	15
4.2 Strategie der Risikominderung .....	17
4.2.1 Allgemeines .....	17
4.2.2 Beitrag der Risikominderung durch das Steuerungssystem .....	17
4.3 Bestimmung des erforderlichen Performance Levels (PL <sub>r</sub> ) .....	21
4.4 Entwicklung des SRP/CS .....	21
4.5 Bewertung des erreichten Performance Levels PL und die Beziehung zum SIL .....	22
4.5.1 Performance Level PL .....	22
4.5.2 Mittlere Zeit bis zum gefahrbringenden Ausfall jedes Kanals (MTTF <sub>d</sub> ) .....	24
4.5.3 Diagnosedeckungsgrad (DC) .....	25
4.5.4 Vereinfachtes Verfahren zur Abschätzung eines PL .....	25
4.6 Software-Sicherheitsanforderungen .....	28
4.6.1 Allgemeines .....	28
4.6.2 Sicherheitsbezogene Embedded-Software (SRESW) .....	29
4.6.3 Sicherheitsbezogene Anwendungssoftware (SRASW) .....	30
4.6.4 Softwarebasierende Parametrisierung .....	32
4.7 Verifikation, dass der erreichte PL den PL <sub>r</sub> erfüllt .....	33
4.8 Ergonomische Aspekte der Gestaltung .....	34
5 Sicherheitsfunktionen .....	34
5.1 Spezifikation der Sicherheitsfunktionen .....	34
5.2 Nähere Angaben über die Sicherheitsfunktionen .....	37
5.2.1 Sicherheitsbezogene Stoppfunktion .....	37
5.2.2 Manuelle Rückstellungsfunktion .....	37
5.2.3 Start-/Wiederaufnahmefunktion .....	38
5.2.4 Lokale Steuerungsfunktion .....	38
5.2.5 Mutingfunktion .....	38
5.2.6 Ansprechzeit .....	38
5.2.7 Sicherheitsbezogene Parameter .....	39
5.2.8 Schwankungen, Verlust und Wiederkehr der Energiequellen .....	39
6 Die Kategorien und deren Beziehung zur MTTF <sub>d</sub> jedes Kanals, DC <sub>avg</sub> und CCF .....	39
6.1 Allgemeines .....	39
6.2 Spezifikation der Kategorien .....	40
6.2.1 Allgemeines .....	40
6.2.2 Vorgesehene Architekturen .....	40
6.2.3 Kategorie B .....	41
6.2.4 Kategorie 1 .....	41
6.2.5 Kategorie 2 .....	43
6.2.6 Kategorie 3 .....	44

6.2.7	Kategorie 4 .....	45
6.3	Kombination von SRP/CS, um einen Gesamt-PL zu erreichen.....	48
7	Berücksichtigung von Fehlern, Fehlerausschluss .....	50
7.1	Allgemeines .....	50
7.2	Fehlerbetrachtung .....	50
7.3	Fehlerausschluss.....	50
8	Validierung .....	50
9	Instandhaltung .....	51
10	Technische Dokumentation .....	51
11	Benutzerinformation.....	52
Anhang A	(informativ) Bestimmung des erforderlichen Performance Levels (PL <sub>r</sub> ).....	53
Anhang B	(informativ) Blockmethode und sicherheitsbezogenes Blockdiagramm .....	56
Anhang C	(informativ) Berechnung oder Abschätzung von MTTF <sub>d</sub> -Werten für einzelne Bauteile .....	58
Anhang D	(informativ) Vereinfachtes Verfahren zur Bestimmung der MTTF <sub>d</sub> für jeden Kanal .....	66
Anhang E	(informativ) Abschätzungen des Diagnosedeckungsgrades (DC) für Funktionen und Module .....	68
Anhang F	(informativ) Abschätzungen der Ausfälle aufgrund gemeinsamer Ursache (CCF) .....	72
Anhang G	(informativ) Systematischer Ausfall.....	74
Anhang H	(informativ) Beispiel der Kombination von verschiedenen sicherheitsbezogenen Teilen einer Steuerung.....	77
Anhang I	(informativ) Beispiele.....	80
Anhang J	(informativ) Software .....	87
Anhang K	(informativ) Numerische Darstellung von Bild 5 .....	90
Anhang ZA	(informativ) Zusammenhang zwischen dieser Europäischen Norm und den grundlegenden Anforderungen der EG-Richtlinie 98/37/EG geändert durch Richtlinie 98/79/EG .....	92
Anhang ZB	(informativ) Zusammenhang zwischen dieser Europäischen Norm und den grundlegenden Anforderungen der EG-Richtlinie 2006/42/EG .....	93
Literaturhinweise	.....	94