

DIN EN ISO 13849-1:2007-07 (D)

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

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 _r)	20
4.4 Entwicklung des SRP/CS	20
4.5 Bewertung des erreichten Performance Levels PL und die Beziehung zum SIL	21
4.5.1 Performance Level PL	21
4.5.2 Mittlere Zeit bis zum gefahrbringenden Ausfall jedes Kanals (MTTF _d)	23
4.5.3 Diagnosedeckungsgrad (DC)	24
4.5.4 Vereinfachtes Verfahren zur Abschätzung eines PL	24
4.6 Software-Sicherheitsanforderungen	27
4.6.1 Allgemeines	27
4.6.2 Sicherheitsbezogene Embedded-Software (SRESW)	28
4.6.3 Sicherheitsbezogene Anwendungssoftware (SRASW)	29
4.6.4 Softwarebasierende Parametrisierung	31
4.7 Verifikation, dass der erreichte PL den PL _r erfüllt	32
4.8 Ergonomische Aspekte der Gestaltung	33
5 Sicherheitsfunktionen	33
5.1 Spezifikation der Sicherheitsfunktionen	33
5.2 Nähere Angaben über die Sicherheitsfunktionen	36
5.2.1 Sicherheitsbezogene Stoppfunktion	36
5.2.2 Manuelle Rückstellungsfunktion	36
5.2.3 Start-/Wiederaufnahmefunktion	37
5.2.4 Lokale Steuerungsfunktion	37
5.2.5 Mutingfunktion	37
5.2.6 Ansprechzeit	38
5.2.7 Sicherheitsbezogene Parameter	38
5.2.8 Schwankungen, Verlust und Wiederkehr der Energiequellen	38
6 Die Kategorien und deren Beziehung zur MTTF _d jedes Kanals, DC _{avg} und CCF	38
6.1 Allgemeines	38
6.2 Spezifikation der Kategorien	39
6.2.1 Allgemeines	39
6.2.2 Vorgesehene Architekturen	39
6.2.3 Kategorie B	40
6.2.4 Kategorie 1	40
6.2.5 Kategorie 2	42
6.2.6 Kategorie 3	43

6.2.7	Kategorie 4	44
6.3	Kombination von SRP/CS, um einen Gesamt-PL zu erreichen	47
7	Berücksichtigung von Fehlern, Fehlerausschluss	49
7.1	Allgemeines	49
7.2	Fehlerbetrachtung	49
7.3	Fehlerausschluss	50
8	Validierung	50
9	Instandhaltung	50
10	Technische Dokumentation	50
11	Benutzerinformation	51
	Anhang A (informativ) Bestimmung des erforderlichen Performance Levels (PL_r)	53
	Anhang B (informativ) Blockmethode und sicherheitsbezogenes Blockdiagramm	56
	Anhang C (informativ) Berechnung oder Abschätzung von MTTF_d-Werten für einzelne Bauteile	58
	Anhang D (informativ) Vereinfachtes Verfahren zur Bestimmung der MTTF_d 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)	71
	Anhang G (informativ) Systematischer Ausfall	73
	Anhang H (informativ) Beispiel der Kombination von verschiedenen sicherheitsbezogenen Teilen einer Steuerung	76
	Anhang I (informativ) Beispiele	79
	Anhang J (informativ) Software	86
	Anhang K (informativ) Numerische Darstellung von Bild 5	89
	Anhang ZA (informativ) Beziehung zwischen dieser Norm und den wesentlichen Anforderungen der EG-Richtlinie 98/37/EG geändert durch Richtlinie 98/79/EG	91
	Literaturhinweise	92