

DIN EN ISO 13849-1:2016-06 (D)

Sicherheit von Maschinen - Sicherheitsbezogene Teile von Steuerungen - Teil 1: Allgemeine Gestaltungsleitsätze (ISO 13849-1:2015); Deutsche Fassung EN ISO 13849-1:2015

Inhalt	Seite
Europäisches Vorwort.....	5
Anhang ZA (informativ) Zusammenhang zwischen dieser Europäischen Norm und den grundlegenden Anforderungen der EG-Richtlinie 2006/42/EG.....	6
Vorwort.....	7
Einleitung.....	8
1 Anwendungsbereich.....	11
2 Normative Verweisungen.....	11
3 Begriffe, Formelzeichen und Abkürzungen.....	12
3.1 Begriffe.....	12
3.2 Formelzeichen und Abkürzungen.....	19
4 Gestaltungsaspekte.....	20
4.1 Sicherheitsziele in der Gestaltung.....	20
4.2 Strategie der Risikominderung.....	22
4.2.1 Allgemeines.....	22
4.2.2 Beitrag der Risikominderung durch das Steuerungssystem.....	22
4.3 Bestimmung des erforderlichen Performance Levels (PL _r).....	26
4.4 Entwicklung des SRP/CS.....	26
4.5 Bewertung des erreichten Performance Levels PL und die Beziehung zum SIL.....	27
4.5.1 Performance Level PL.....	27
4.5.2 Mittlere Zeit bis zum gefahrbringenden Ausfall jedes Kanals (MTTF _D).....	29
4.5.3 Diagnosedeckungsgrad (DC).....	30
4.5.4 Vereinfachtes Verfahren zur Abschätzung der quantifizierbaren Aspekte des PL.....	31
4.5.5 Beschreibung des Ausgabeteils der SRP/CS nach Kategorien.....	33
4.6 Software-Sicherheitsanforderungen.....	34
4.6.1 Allgemeines.....	34
4.6.2 Sicherheitsbezogene Embedded-Software (SRESW).....	35
4.6.3 Sicherheitsbezogene Anwendungssoftware (SRASW).....	36
4.6.4 Softwarebasierende Parametrisierung.....	39
4.7 Verifikation, dass der erreichte PL den PL _r erfüllt.....	41
4.8 Ergonomische Aspekte der Gestaltung.....	41
5 Sicherheitsfunktionen.....	41
5.1 Spezifikation der Sicherheitsfunktionen.....	41
5.2 Nähere Angaben über die Sicherheitsfunktionen.....	44
5.2.1 Sicherheitsbezogene Stoppfunktion.....	44
5.2.2 Manuelle Rückstellungsfunktion.....	44
5.2.3 Start-/Wiederaufnahmefunktion.....	45
5.2.4 Lokale Steuerungsfunktion.....	45
5.2.5 Mutingfunktion.....	45
5.2.6 Ansprechzeit.....	46
5.2.7 Sicherheitsbezogene Parameter.....	46
5.2.8 Schwankungen, Verlust und Wiederkehr der Energiequellen.....	46

6	Die Kategorien und deren Beziehung zur $MTTF_D$ jedes Kanals, DC_{avg} und CCF	46
6.1	Allgemeines	46
6.2	Spezifikation der Kategorien	47
6.2.1	Allgemeines	47
6.2.2	Vorgesehene Architekturen	47
6.2.3	Kategorie B	48
6.2.4	Kategorie 1	48
6.2.5	Kategorie 2	50
6.2.6	Kategorie 3	51
6.2.7	Kategorie 4	52
6.3	Kombination von SRP/CS, um einen Gesamt-PL zu erreichen	55
7	Berücksichtigung von Fehlern, Fehlerausschluss	57
7.1	Allgemeines	57
7.2	Fehlerbetrachtung	57
7.3	Fehlerausschluss	57
8	Validierung	57
9	Instandhaltung	58
10	Technische Dokumentation	58
11	Benutzerinformation	59
Anhang A (informativ) Bestimmung des erforderlichen Performance Levels (PL_r)		60
A.1	Auswahl des PL_r	60
A.2	Anleitung für die Auswahl der Parameter S, F und P zur Einschätzung des Risikos	60
A.2.1	Schwere der Verletzung S1 und S2	60
A.2.2	Häufigkeit und/oder Dauer der Gefährdungsexposition F1 und F2	61
A.2.3	Möglichkeit zur Vermeidung der Gefährdungseignisse P1 und P2 und Eintrittswahrscheinlichkeit	61
A.3	Überlagerte Gefährdungen	63
Anhang B (informativ) Blockmethode und sicherheitsbezogenes Blockdiagramm		65
B.1	Blockmethode	65
B.2	Sicherheitsbezogenes Blockdiagramm	65
Anhang C (informativ) Berechnung oder Abschätzung von $MTTF_D$-Werten für einzelne Bauteile		67
C.1	Allgemeines	67
C.2	Verfahren guter ingenieurmäßiger Praxis	67
C.3	Hydraulische Bauteile	67
C.4	$MTTF_D$ von pneumatischen, mechanischen und elektromechanischen Bauteilen	70
C.4.1	Allgemeines	70
C.4.2	Berechnung der $MTTF_D$ für Bauteile aus B_{10D}	70
C.4.3	Beispiel	72
C.5	$MTTF_D$ -Daten elektrischer Bauteile	72
C.5.1	Allgemeines	72
C.5.2	Halbleiter	73
C.5.3	Passive Bauteile	73
Anhang D (informativ) Vereinfachtes Verfahren zur Abschätzung der $MTTF_D$ für jeden Kanal		76
D.1	Parts-Count-Verfahren	76
D.2	Die $MTTF_D$ für unterschiedliche Kanäle, Symmetrisierung der $MTTF_D$ für jeden Kanal	77
Anhang E (informativ) Abschätzungen des Diagnosedeckungsgrades (DC) für Funktionen und Module		78
E.1	Beispiele für den Diagnosedeckungsgrad (DC)	78
E.2	Abschätzung des durchschnittlichen DC (DC_{avg})	80
Anhang F (informativ) Abschätzungen der Ausfälle aufgrund gemeinsamer Ursache (CCF)		82
F.1	Anforderungen an CCF	82
F.2	Abschätzung der Auswirkung des CCF	82

Anhang G (informativ) Systematischer Ausfall	84
G.1 Allgemeines	84
G.2 Maßnahmen zur Beherrschung systematischer Ausfälle.....	84
G.3 Maßnahmen zur Vermeidung systematischer Ausfälle	85
G.4 Maßnahmen zur Vermeidung systematischer Ausfälle während der Integration des SRP/CS.....	86
Anhang H (informativ) Beispiel der Kombination von verschiedenen sicherheitsbezogenen Teilen einer Steuerung	87
Anhang I (informativ) Beispiele.....	90
I.1 Allgemeines	90
I.2 Sicherheitsfunktion und erforderlicher Performance Level (PL_r).....	90
I.3 Beispiel A, einkanaliges System.....	91
I.3.1 Identifikation der sicherheitsbezogenen Teile	91
I.3.2 Quantifizierung von MTTF_D, DC_{avg}, Maßnahmen gegen den Ausfall infolge gemeinsamer Ursache (CCF), Kategorie, PL	92
I.4 Beispiel B, redundantes System	93
I.4.1 Identifikation der sicherheitsbezogenen Teile	93
I.4.2 Quantifizierung der MTTF_D für jeden Kanal, DC_{avg}, Maßnahmen gegen den Ausfall infolge gemeinsamer Ursache (CCF), Kategorie und PL.....	95
Anhang J (informativ) Software.....	99
J.1 Beschreibung des Beispiels.....	99
J.2 Anwendung des V-Modells des Software-Sicherheitslebenszyklus	99
J.3 Verifikation der Softwarespezifikation.....	100
J.4 Beispiel von Programmierregeln.....	101
Anhang K (informativ) Numerische Darstellung von Bild 5	103
Literaturhinweise	107