

E DIN EN ISO 13849-1:2021-08 (D/E)

Erscheinungsdatum: 2021-07-09

**Sicherheit von Maschinen - Sicherheitsbezogene Teile von Steuerungen - Teil 1:
Allgemeine Gestaltungsleitsätze (ISO/DIS 13849-1.2:2021); Deutsche und Englische
Fassung prEN ISO 13849-1:2021**

**Safety of machinery - Safety-related parts of control systems - Part 1: General
principles for design (ISO/DIS 13849-1.2:2021); German and English version prEN ISO
13849-1:2021**

Inhalt	Seite
Europäisches Vorwort.....	5
Anhang ZA (informativ) Zusammenhang zwischen dieser Europäischen Norm und den grundlegenden Anforderungen der abzudeckenden Richtlinie 2006/42/EG.....	6
Vorwort	8
Einleitung	10
1 Anwendungsbereich.....	13
2 Normative Verweisungen	13
3 Begriffe, Symbole und Abkürzungen.....	14
3.1 Begriffe	14
3.2 Symbole und Abkürzungen	24
4 Überblick.....	26
4.1 Prozess zur Risikobeurteilung und Risikominderung an der Maschine	26
4.2 Beitrag zur Risikominderung.....	28
4.3 Entwurfsprozess eines SRP/CS	28
4.4 Verfahren	29
4.5 Erforderliche Informationen	30
4.6 Ausführung von Sicherheitsfunktionen mithilfe von Teilsystemen	31
5 Spezifikation der Sicherheitsfunktionen.....	31
5.1 Identifizierung und allgemeine Beschreibung der Sicherheitsfunktion.....	31
5.2 Spezifikation der Sicherheitsanforderungen.....	32
5.2.1 Allgemeine Anforderungen.....	32
5.2.2 Anforderungen an spezifische Sicherheitsfunktionen.....	35
5.3 Bestimmung des erforderlichen Performance Levels für jede Sicherheitsfunktion.....	41
5.4 Überprüfung der Spezifikation der Sicherheitsanforderungen.....	41
5.5 Zerlegung eines SRP/CS in Teilsysteme	41
6 Entwurfsaspekte.....	43
6.1 Bewertung des erreichten Performance Levels	43
6.1.1 Allgemeine Übersicht der Performance Levels	43
6.1.2 Zusammenhang zwischen dem Performance Level und dem Sicherheits-Integritätslevel	45
6.1.3 Architektur — Kategorien und deren Beziehung zur MTTF _D jedes Kanals, zum durchschnittlichen Diagnosedeckungsgrad und zum Ausfall infolge gemeinsamer Ursache	46
6.1.4 Mittlere Dauer bis zum gefahrbringenden Ausfall	54
6.1.5 Diagnosedeckungsgrad	55
6.1.6 Ausfälle infolge gemeinsamer Ursache	56
6.1.7 Systematische Ausfälle	56
6.1.8 Vereinfachtes Verfahren für die Abschätzung des Performance Levels für Teilsysteme	57

6.1.9	Alternatives Verfahren für die Bestimmung des Performance Levels und der PFH _D ohne MTTF _D	59
6.1.10	Fehlerbetrachtung und Fehlerausschluss.....	61
6.1.11	Bewährtes Bauteil.....	62
6.2	Kombination von Teilsystemen zum Erreichen eines gesamten Performance Levels für die Sicherheitsfunktion	63
6.2.1	Allgemeines.....	63
6.2.2	Bekannte PFH _D -Werte	63
6.2.3	Unbekannte PFH _D -Werte	64
7	Software-Sicherheitsanforderungen	64
7.1	Allgemeines.....	64
7.2	Programmiersprache mit eingeschränktem Sprachumfang und Programmiersprache mit nicht eingeschränktem Sprachumfang.....	65
7.2.1	Programmiersprache mit eingeschränktem Sprachumfang.....	65
7.2.2	Programmiersprache mit nicht eingeschränktem Sprachumfang.....	66
7.2.3	Entscheidung zwischen Programmiersprache mit eingeschränktem Sprachumfang und Programmiersprache mit nicht eingeschränktem Sprachumfang.....	66
7.3	Sicherheitsbezogene Embedded-Software	68
7.4	Sicherheitsbezogene Anwendungssoftware.....	69
7.5	Softwarebasierte manuelle Parametrisierung.....	72
7.5.1	Allgemeines.....	72
7.5.2	Einflüsse auf sicherheitsbezogene Parameter.....	73
7.5.3	Anforderungen an die softwarebasierte manuelle Parametrisierung	74
7.5.4	Verifizierung des Parametrisierungswerkzeugs	75
7.5.5	Dokumentation der softwarebasierten manuellen Parametrisierung.....	75
8	Verifizierung, ob der erreichte Performance Level dem erforderlichen Performance Level entspricht.....	76
9	Ergonomische Entwurfsaspekte.....	76
10	Validierung.....	76
10.1	Grundsätze der Validierung.....	76
10.1.1	Allgemeines.....	76
10.1.2	Validierungsplan	78
10.1.3	Allgemeine Fehlerlisten	79
10.1.4	Spezielle Fehlerlisten.....	79
10.1.5	Angaben zur Validierung.....	79
10.2	Validierung der Spezifikation der Sicherheitsanforderungen	81
10.3	Validierung durch Analyse	81
10.3.1	Allgemeines.....	81
10.3.2	Analysetechniken.....	82
10.4	Validierung durch Prüfung	82
10.4.1	Allgemeines.....	82
10.4.2	Messgenauigkeit	83
10.4.3	Zusätzliche Prüfanforderungen.....	83
10.4.4	Anzahl der Prüflinge	83
10.4.5	Prüfverfahren	84
10.5	Validierung der Sicherheitsfunktionen	84
10.6	Validierung der Sicherheitsintegrität des SRP/CS	85
10.6.1	Validierung von Teilsystem(en)	85
10.6.2	Validierung der Maßnahmen zur Vermeidung systematischer Ausfälle	87
10.6.3	Validierung der sicherheitsbezogenen Software.....	87
10.6.4	Validierung der Kombination von Teilsystemen	88
10.6.5	Gesamtvalidierung der Sicherheitsintegrität	89
10.7	Validierung der Umgebungsanforderungen	89
10.8	Aufzeichnung der Validierung	89
10.9	Validierung der Instandhaltungsanforderungen.....	90

11	Wartungsfreundlichkeit von SRP/CS	90
12	Technische Dokumentation	91
13	Benutzerinformation	91
13.1	Allgemeines	91
13.2	Informationen für die Integration des SRP/CS	91
13.3	Informationen für den Benutzer	92
Anhang A (informativ) Leitlinien für die Bestimmung des erforderlichen Performance Levels.....		94
Anhang B (informativ) Blockmethode und sicherheitsbezogenes Blockdiagramm		99
Anhang C (informativ) Berechnung oder Abschätzung von MTTF _D -Werten für einzelne Bauteile...		101
Anhang D (informativ) Vereinfachtes Verfahren zur Abschätzung der MTTF _D für jeden Kanal.....		109
Anhang E (informativ) Abschätzungen des Diagnosedeckungsgrades für Funktionen und Teilsysteme		111
Anhang F (informativ) Maßnahmen gegen Ausfälle infolge gemeinsamer Ursache		116
Anhang G (informativ) Systematischer Ausfall		120
Anhang H (informativ) Beispiel für eine Kombination von mehreren Teilsystemen.....		124
Anhang I (informativ) Beispiele		127
Anhang J (informativ) Beispiel für die Ausführung einer SRESW		136
Anhang K (informativ) Numerische Darstellung von Bild 12		141
Anhang L (informativ) Elektromagnetische Störfestigkeit		146
Anhang M (informativ) Ergänzende Informationen zur Spezifikation der Sicherheitsanforderungen		150
Anhang N (informativ) Vermeiden eines systematischen Ausfalls durch den Softwareentwurf.....		152
Anhang O (informativ) Sicherheitsbezogene Werte von Bauteilen oder Komponenten der Steuerungen		166
Literaturhinweise		169