

# 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**

---

<b>Inhalt</b>	<b>Seite</b>
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 <sub>D</sub> ohne MTTFD .....	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 <sub>D</sub> -Werte .....	63
6.2.3	Unbekannte PFH <sub>D</sub> -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

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