

E DIN EN ISO 13849-1:2020-08 (D/E)

Erscheinungsdatum: 2020-07-17

**Sicherheit von Maschinen - Sicherheitsbezogene Teile von Steuerungen - Teil 1:
Allgemeine Gestaltungsleitsätze (ISO/DIS 13849-1:2020); Deutsche und Englische
Fassung prEN ISO 13849-1:2020**

**Safety of machinery - Safety-related parts of control systems - Part 1: General
principles for design (ISO/DIS 13849-1:2020); German and English version prEN ISO
13849-1:2020**

| Inhalt | Seite |
|---|--------------|
| Europäisches Vorwort..... | 6 |
| Vorwort..... | 7 |
| Einleitung..... | 8 |
| 1 Anwendungsbereich..... | 12 |
| 2 Normative Verweisungen..... | 12 |
| 3 Begriffe..... | 13 |
| 3.1 Begriffe..... | 13 |
| 3.2 Symbole und Abkürzungen..... | 22 |
| 4 Überblick..... | 24 |
| 4.1 Anforderungen an die Risikobeurteilung und Risikominderung..... | 24 |
| 4.2 Beitrag der Sicherheitsfunktion zur Risikominderung..... | 26 |
| 4.3 Risikominderung mithilfe eines SRP/CS..... | 27 |
| 4.4 Verfahren..... | 29 |
| 4.5 Erforderliche Informationen..... | 30 |
| 4.6 Ausführung von Sicherheitsfunktionen mithilfe von Teilsystemen..... | 30 |
| 5 Spezifikation der Sicherheitsfunktionen..... | 31 |
| 5.1 Allgemeines..... | 31 |
| 5.2 Spezifikation der Sicherheitsanforderungen (SRS, en: safety requirements specification)..... | 31 |
| 5.2.1 Allgemeine Anforderungen..... | 31 |
| 5.2.2 Zerlegung eines SRP/CS in Teilsysteme..... | 34 |
| 5.2.3 Anforderungen an spezifische Sicherheitsfunktionen..... | 36 |
| 5.3 Bestimmung des erforderlichen Performance Levels (PL _r) für jede Sicherheitsfunktion..... | 41 |
| 5.4 Überprüfung der Spezifikation der Sicherheitsanforderungen..... | 41 |
| 6 Gestaltungsaspekte..... | 41 |
| 6.1 Bewertung des erreichten Performance Levels PL..... | 41 |
| 6.1.1 Allgemeine Übersicht der Performance Level PL..... | 41 |
| 6.1.2 Zusammenhang zwischen PL und SIL..... | 43 |
| 6.1.3 Architektur - Kategorien und deren Beziehung zur MTTF _D jedes Kanals, zum DC _{avg} und zum CCF..... | 44 |
| 6.1.4 Mittlere Zeit bis zum gefahrbringenden Ausfall (MTTF _D)..... | 52 |
| 6.1.5 Diagnosedeckungsgrad (DC)..... | 53 |
| 6.1.6 Ausfälle infolge gemeinsamer Ursache (CCF)..... | 54 |
| 6.1.7 Systematische Ausfälle..... | 54 |
| 6.1.8 Vereinfachtes Verfahren zur Abschätzung des PL..... | 54 |
| 6.1.9 Alternatives Verfahren für die Bestimmung von PL und PFH _D ohne MTTF _D | 56 |
| 6.1.10 Fehlerbetrachtung und Fehlerausschluss..... | 58 |
| 6.1.11 Bewährtes Bauteil..... | 59 |

| | | |
|-----------------------|--|----|
| 6.2 | Kombination von Teilsystemen zum Erreichen eines Gesamt-PL für die Sicherheitsfunktion | 60 |
| 6.2.1 | Allgemeines | 60 |
| 6.2.2 | Bekannte PFH _D -Werte | 60 |
| 6.2.3 | Unbekannte PFH _D -Werte | 61 |
| 7 | Software-Sicherheitsanforderungen | 61 |
| 7.1 | Allgemeines | 61 |
| 7.2 | Sicherheitsbezogene Embedded-Software (SRESW) | 62 |
| 7.3 | Sicherheitsbezogene Anwendungssoftware (SRASW) | 64 |
| 7.4 | Programmiersprache mit eingeschränktem Sprachumfang (LVL) | 67 |
| 7.4.1 | Allgemeines | 67 |
| 7.4.2 | Programmiersprache mit nicht eingeschränktem Sprachumfang (FVL) | 67 |
| 7.4.3 | Entscheidung zwischen LVL oder FVL | 68 |
| 7.5 | Softwarebasierte Parametrisierung | 69 |
| 7.5.1 | Allgemeines | 69 |
| 7.5.2 | Einflüsse auf sicherheitsbezogene Parameter | 70 |
| 7.5.3 | Anforderungen an die softwarebasierte manuelle Parametrisierung | 70 |
| 7.5.4 | Verifizierung des Parametrisierungswerkzeugs | 72 |
| 7.5.5 | Ausführung der softwarebasierten manuellen Parametrisierung | 72 |
| 8 | Verifizierung, ob der erreichte PL dem PL _r entspricht | 72 |
| 9 | Ergonomische Aspekte der Gestaltung | 73 |
| 10 | Validierung | 73 |
| 10.1 | Grundsätze der Validierung | 73 |
| 10.1.1 | Allgemeines | 73 |
| 10.1.2 | Validierungsplan | 75 |
| 10.1.3 | Allgemeine Fehlerlisten | 76 |
| 10.1.4 | Spezielle Fehlerlisten | 76 |
| 10.1.5 | Angaben zur Validierung | 76 |
| 10.2 | Validierung durch Analyse | 78 |
| 10.2.1 | Allgemeines | 78 |
| 10.2.2 | Analysetechniken | 78 |
| 10.3 | Validierung durch Prüfung | 79 |
| 10.3.1 | Allgemeines | 79 |
| 10.3.2 | Messgenauigkeit | 79 |
| 10.3.3 | Zusätzliche Prüfanforderungen | 80 |
| 10.3.4 | Anzahl der Prüflinge | 80 |
| 10.3.5 | Prüfverfahren | 80 |
| 10.4 | Validierung der Spezifikation der Sicherheitsanforderungen (SRS) | 81 |
| 10.5 | Validierung der Sicherheitsfunktion | 81 |
| 10.6 | Validierung der Sicherheitsintegrität des SRP/CS | 82 |
| 10.6.1 | Validierung von Teilsystem(en) | 82 |
| 10.6.2 | Validierung der Maßnahmen zur Vermeidung systematischer Ausfälle | 84 |
| 10.6.3 | Validierung der sicherheitsbezogenen Software | 85 |
| 10.6.4 | Validierung der Kombination von Teilsystemen | 86 |
| 10.6.5 | Überprüfung/Verifizierung der Sicherheitsintegrität | 86 |
| 11 | Instandhaltung | 86 |
| 12 | Technische Dokumentation | 87 |
| 13 | Benutzerinformation | 87 |
| 13.1 | Allgemeines | 87 |
| 13.2 | Informationen für den SRP/CS-Integrator | 87 |
| 13.3 | Informationen für den Benutzer | 88 |
| Anhang A (informativ) | Bestimmung des erforderlichen Performance Levels (PL _r) | 90 |
| A.1 | Auswahl des PL _r | 90 |
| A.2 | Anleitung für die Auswahl der Parameter S, F und P zur Einschätzung des Risikos | 91 |

| | | |
|--|--|------------|
| A.2.1 | Schwere der Verletzung S1 und S2 | 91 |
| A.2.2 | Häufigkeit und/oder Dauer der Gefährdungsexposition F1 und F2 | 91 |
| A.2.3 | Möglichkeit zur Vermeidung des Schadens | 92 |
| A.3 | Überlagerte Gefährdungen..... | 94 |
| Anhang B (informativ) Blockmethode und sicherheitsbezogenes Blockdiagramm | | 95 |
| B.1 | Blockmethode..... | 95 |
| B.2 | Sicherheitsbezogenes Blockdiagramm | 95 |
| Anhang C (informativ) Berechnung oder Abschätzung von MTTFD-Werten für einzelne Bauteile..... | | 97 |
| C.1 | Allgemeines..... | 97 |
| C.2 | Verfahren guter ingenieurmäßiger Praxis | 97 |
| C.3 | Hydraulische Bauteile..... | 97 |
| C.4 | MTTF _D von pneumatischen, mechanischen und elektromechanischen Bauteilen | 99 |
| C.4.1 | Allgemeines..... | 99 |
| C.4.2 | Berechnung der MTTFD für Bauteile aus B _{10D} | 100 |
| C.4.3 | Erläuterung der Gleichungen | 101 |
| C.4.4 | Beispiel | 101 |
| C.5 | MTTF _D -Daten für elektrische Bauteile | 102 |
| C.5.1 | Allgemeines..... | 102 |
| C.5.2 | Halbleiter | 102 |
| C.5.3 | Passive Bauteile | 103 |
| Anhang D (informativ) Vereinfachtes Verfahren zur Abschätzung der MTTFD für jeden Kanal..... | | 105 |
| D.1 | Parts-Count-Verfahren | 105 |
| D.2 | MTTF _D für unterschiedliche Kanäle, Symmetrisierung der MTTFD für jeden Kanal | 106 |
| Anhang E (informativ) Abschätzungen des Diagnosedeckungsgrades (DC) für Funktionen und Module | | 108 |
| E.1 | Beispiele für den Diagnosedeckungsgrad (DC) | 108 |
| E.2 | Abschätzung des durchschnittlichen DC (DC _{avg}) | 111 |
| Anhang F (informativ) Maßnahmen gegen Ausfälle infolge gemeinsamer Ursache (CCF) | | 112 |
| F.1 | Allgemeines..... | 112 |
| F.2 | Abschätzung der Auswirkung eines CCF..... | 112 |
| F.3 | Beschreibung der Maßnahmen gegen CCF nach Tabelle F.1 | 113 |
| F.4 | Maßnahmen gegen CCF und weitere einschlägige Normen..... | 115 |
| Anhang G (informativ) Systematischer Ausfall | | 116 |
| G.1 | Allgemeines..... | 116 |
| G.2 | Maßnahmen zur Beherrschung systematischer Ausfälle..... | 116 |
| G.3 | Maßnahmen zur Vermeidung systematischer Ausfälle | 117 |
| G.4 | Maßnahmen zur Vermeidung systematischer Ausfälle während der Integration des SRP/CS..... | 118 |
| Anhang H (informativ) Beispiel für eine Kombination von mehreren Teilsystemen..... | | 119 |
| Anhang I (informativ) Beispiele..... | | 122 |
| I.1 | Allgemeines..... | 122 |
| I.2 | Sicherheitsfunktion und erforderlicher Performance Level (PL _r)..... | 122 |
| I.3 | Beispiel A, einkanaliges System..... | 123 |
| I.3.1 | Identifikation der sicherheitsbezogenen Teile | 123 |
| I.3.2 | Quantifizierung von MTTFD, DC _{avg} , Maßnahmen gegen den Ausfall infolge gemeinsamer Ursache (CCF), Kategorie, PL | 124 |
| I.4 | Beispiel B, redundantes System | 125 |
| I.4.1 | Identifikation der sicherheitsbezogenen Teile | 125 |
| I.4.2 | Quantifizierung der MTTFD für jeden Kanal, DC _{avg} , Maßnahmen gegen den Ausfall infolge gemeinsamer Ursache (CCF), Kategorie und PL | 127 |
| Anhang J (informativ) Software..... | | 131 |
| J.1 | Beschreibung des Beispiels..... | 131 |
| J.2 | Anwendung des V-Modells des Software-Sicherheitslebenszyklus | 132 |

| | | |
|--------------------------------|---|------------|
| J.3 | Verifizierung der Softwarespezifikation | 132 |
| J.4 | Beispiel von Programmierregeln..... | 133 |
| Anhang K (informativ) | Numerische Darstellung von Bild 12..... | 135 |
| Anhang L (informativ) | Anforderungen an die elektromagnetische Störfestigkeit | 139 |
| Anhang M (informativ) | Zusätzliche Informationen zur Spezifikation der Sicherheitsanforderungen | 142 |
| Anhang N (informativ) | Vermeiden eines systematischen Ausfalls durch den Softwareentwurf..... | 144 |
| N.1 | Auswahl von Maßnahmen zur Fehlervermeidung für den Softwareentwurf..... | 144 |
| Anhang ZA (informativ) | Zusammenhang zwischen dieser Europäischen Norm und den grundlegenden Anforderungen der abzudeckenden EU-Richtlinie 2006/42/EG..... | 156 |
| Literaturhinweise | | 157 |