

DIN EN ISO 13849-1:2023-12 (D)

Sicherheit von Maschinen - Sicherheitsbezogene Teile von Steuerungen - Teil 1: Allgemeine Gestaltungsleitsätze (ISO 13849-1:2023); Deutsche Fassung EN ISO 13849-1:2023

| Inhalt | Seite |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------|
| Europäisches Vorwort..... | 7 |
| Anhang ZA (informativ) Zusammenhang zwischen dieser Europäischen Norm und den grundlegenden Anforderungen der abzudeckenden Richtlinie 2006/42/EG..... | 8 |
| Vorwort..... | 11 |
| Einleitung..... | 13 |
| 1 Anwendungsbereich..... | 17 |
| 2 Normative Verweisungen..... | 17 |
| 3 Begriffe, Symbole und Abkürzungen..... | 18 |
| 3.1 Begriffe..... | 18 |
| 3.2 Symbole und Abkürzungen..... | 28 |
| 4 Überblick..... | 30 |
| 4.1 Prozess zur Risikobeurteilung und Risikominderung an der Maschine..... | 30 |
| 4.2 Beitrag zur Risikominderung..... | 32 |
| 4.3 Entwurfsprozess eines SRP/CS..... | 33 |
| 4.4 Verfahren..... | 34 |
| 4.5 Erforderliche Informationen..... | 35 |
| 4.6 Ausführung von Sicherheitsfunktionen mithilfe von Teilsystemen..... | 35 |
| 5 Spezifikation der Sicherheitsfunktionen..... | 36 |
| 5.1 Identifizierung und allgemeine Beschreibung der Sicherheitsfunktion..... | 36 |
| 5.2 Spezifikation der Sicherheitsanforderungen..... | 36 |
| 5.2.1 Allgemeine Anforderungen..... | 36 |
| 5.2.2 Anforderungen an spezifische Sicherheitsfunktionen..... | 39 |
| 5.2.3 Minimierung des Anreizes zum Umgehen von Sicherheitsfunktionen..... | 44 |
| 5.2.4 Fernzugriff..... | 45 |
| 5.3 Bestimmung des erforderlichen Performance Levels (PL _r) für jede Sicherheitsfunktion..... | 45 |
| 5.4 Überprüfung der Spezifikation der Sicherheitsanforderungen (SRS)..... | 45 |
| 5.5 Zerlegung eines SRP/CS in Teilsysteme..... | 45 |
| 6 Entwurfsaspekte..... | 47 |
| 6.1 Bewertung des erreichten Performance Levels..... | 47 |
| 6.1.1 Allgemeine Übersicht der Performance Level..... | 47 |
| 6.1.2 Zusammenhang zwischen dem Performance Level (PL) und dem Sicherheits- Integritätslevel (SIL)..... | 49 |
| 6.1.3 Architektur — Kategorien und deren Beziehung zur MTTFD jedes Kanals, zum durchschnittlichen Diagnosedeckungsgrad und zum Ausfall infolge gemeinsamer Ursache (CCF)..... | 50 |
| 6.1.4 Mittlere Dauer bis zum gefahrbringenden Ausfall (MTTF _D)..... | 58 |
| 6.1.5 Diagnosedeckungsgrad (DC)..... | 59 |
| 6.1.6 Ausfälle infolge gemeinsamer Ursache (CCF)..... | 60 |
| 6.1.7 Systematische Ausfälle..... | 60 |
| 6.1.8 Vereinfachtes Verfahren für die Abschätzung des Performance Levels für Teilsysteme..... | 61 |

| | | |
|--------|-----------------------------------------------------------------------------------------------------------------------------------------------------------|----|
| 6.1.9 | Alternatives Verfahren für die Bestimmung des Performance Levels und der PFH ohne MTTFD | 63 |
| 6.1.10 | Fehlerbetrachtung und Fehlerausschluss..... | 64 |
| 6.1.11 | Bewährtes Bauteil..... | 66 |
| 6.2 | Kombination von Teilsystemen zum Erreichen eines gesamten Performance Levels für die Sicherheitsfunktion..... | 66 |
| 6.2.1 | Allgemeines..... | 66 |
| 6.2.2 | Bekannte PFH-Werte | 66 |
| 6.2.3 | Unbekannte PFH-Werte | 67 |
| 6.3 | Softwarebasierte manuelle Parametrierung | 68 |
| 6.3.1 | Allgemeines..... | 68 |
| 6.3.2 | Einflüsse auf sicherheitsbezogene Parameter..... | 68 |
| 6.3.3 | Anforderungen an die softwarebasierte manuelle Parametrierung..... | 69 |
| 6.3.4 | Verifizierung des Parametrierungswerkzeugs | 70 |
| 6.3.5 | Dokumentation der softwarebasierten manuellen Parametrierung..... | 70 |
| 7 | Software-Sicherheitsanforderungen | 71 |
| 7.1 | Allgemeines..... | 71 |
| 7.2 | Programmiersprache mit eingeschränktem Sprachumfang (LVL) und Programmiersprache mit nicht eingeschränktem Sprachumfang (FVL)..... | 72 |
| 7.2.1 | Programmiersprache mit eingeschränktem Sprachumfang (LVL)..... | 72 |
| 7.2.2 | Programmiersprache mit nicht eingeschränktem Sprachumfang (FVL)..... | 73 |
| 7.2.3 | Entscheidung zwischen Programmiersprache mit eingeschränktem Sprachumfang (LVL) und Programmiersprache mit nicht eingeschränktem Sprachumfang (FVL) | 73 |
| 7.3 | Sicherheitsbezogene Embedded-Software (SRESW) | 75 |
| 7.3.1 | Entwurf der sicherheitsbezogenen Embedded-Software (SRESW) | 75 |
| 7.3.2 | Alternative Verfahren für nicht zugängliche Embedded-Software..... | 76 |
| 7.4 | Sicherheitsbezogene Anwendungssoftware (SRASW) | 77 |
| 8 | Verifizierung des erreichten Performance Levels..... | 80 |
| 9 | Ergonomische Entwurfsaspekte..... | 80 |
| 10 | Validierung..... | 80 |
| 10.1 | Grundsätze der Validierung..... | 80 |
| 10.1.1 | Allgemeines..... | 80 |
| 10.1.2 | Validierungsplan | 83 |
| 10.1.3 | Allgemeine Fehlerlisten | 83 |
| 10.1.4 | Spezielle Fehlerlisten..... | 83 |
| 10.1.5 | Angaben zur Validierung..... | 84 |
| 10.2 | Validierung der Spezifikation der Sicherheitsanforderungen (SRS) | 85 |
| 10.3 | Validierung durch Analyse..... | 85 |
| 10.3.1 | Allgemeines..... | 85 |
| 10.3.2 | Analysetechniken..... | 86 |
| 10.4 | Validierung durch Prüfung | 86 |
| 10.4.1 | Allgemeines..... | 86 |
| 10.4.2 | Messgenauigkeit..... | 87 |
| 10.4.3 | Zusätzliche Prüfanforderungen..... | 87 |
| 10.4.4 | Anzahl der Prüflinge | 87 |
| 10.4.5 | Prüfverfahren..... | 88 |
| 10.5 | Validierung der Sicherheitsfunktionen | 88 |
| 10.6 | Validierung der Sicherheitsintegrität des SRP/CS | 89 |
| 10.6.1 | Validierung von Teilsystem(en)..... | 89 |
| 10.6.2 | Validierung der Maßnahmen zur Vermeidung systematischer Ausfälle | 90 |
| 10.6.3 | Validierung der sicherheitsbezogenen Software..... | 91 |
| 10.6.4 | Validierung der Kombination von Teilsystemen..... | 92 |
| 10.6.5 | Gesamtvalidierung der Sicherheitsintegrität | 92 |
| 10.7 | Validierung der Umgebungsanforderungen | 92 |
| 10.8 | Aufzeichnung der Validierung | 93 |
| 10.9 | Validierung der Instandhaltungsanforderungen..... | 93 |

| | | |
|---------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------|------------|
| 11 | Wartungsfreundlichkeit von SRP/CS | 94 |
| 12 | Technische Dokumentation | 94 |
| 13 | Benutzerinformation | 95 |
| 13.1 | Allgemeines | 95 |
| 13.2 | Informationen für die Integration des SRP/CS | 95 |
| 13.3 | Informationen für den Benutzer | 96 |
| Anhang A (informativ) Leitlinien für die Bestimmung des erforderlichen Performance Levels (PL_r) | | 98 |
| A.1 | Allgemeines | 98 |
| A.2 | Auswahl des erforderlichen Performance Levels (PL _r) | 98 |
| A.3 | Anleitung für die Auswahl der Parameter S, F und P zur Einschätzung des Risikos | 99 |
| A.3.1 | Schwere der Verletzung S1 und S2 | 99 |
| A.3.2 | Häufigkeit und/oder Dauer der Gefährdungsexposition F1 und F2 | 99 |
| A.3.3 | Möglichkeit zur Vermeidung oder Begrenzung eines Schadens, P1 und P2 | 100 |
| A.4 | Überlagerte Gefährdungen | 102 |
| Anhang B (informativ) Blockmethode und sicherheitsbezogenes Blockdiagramm | | 103 |
| B.1 | Blockmethode | 103 |
| B.2 | Sicherheitsbezogenes Blockdiagramm | 103 |
| Anhang C (informativ) Berechnung oder Bewertung von MTTF_D-Werten für einzelne Bauteile | | 105 |
| C.1 | Allgemeines | 105 |
| C.2 | Verfahren guter ingenieurmäßiger Praxis | 105 |
| C.3 | Hydraulische Bauteile | 107 |
| C.4 | MTTF _D von pneumatischen, mechanischen und elektromechanischen Bauteilen | 107 |
| C.4.1 | Allgemeines | 107 |
| C.4.2 | Berechnung der MTTF _D für Bauteile aus B _{10D} | 108 |
| C.4.3 | Erläuterung der Gleichungen | 109 |
| C.4.4 | Beispiel | 109 |
| C.5 | MTTF _D -Daten für elektronische Bauteile | 110 |
| C.5.1 | Allgemeines | 110 |
| C.5.2 | Halbleiter | 110 |
| C.5.3 | Passive Bauteile | 111 |
| Anhang D (informativ) Vereinfachtes Verfahren zur Abschätzung der MTTF_D für jeden Kanal | | 113 |
| D.1 | Parts-Count-Verfahren | 113 |
| D.2 | MTTF _D für unterschiedliche Kanäle, Symmetrisierung der MTTF _D für jeden Kanal | 114 |
| Anhang E (informativ) Abschätzungen des Diagnosedeckungsgrades (DC) für Funktionen und Teilsysteme | | 115 |
| E.1 | Beispiele für den Diagnosedeckungsgrad (DC) | 115 |
| E.2 | Abschätzung des durchschnittlichen Diagnosedeckungsgrads | 118 |
| Anhang F (informativ) Verfahren zur Quantifizierung von Maßnahmen gegen Ausfälle infolge gemeinsamer Ursache (CCF) | | 119 |
| F.1 | Allgemeines | 119 |
| F.2 | Abschätzung der Auswirkung der Maßnahmen gegen CCF | 119 |
| F.3 | Beschreibung der Maßnahmen von Tabelle F.1 gegen Ausfälle infolge gemeinsamer Ursache (CCF) | 120 |
| F.3.1 | Trennung/Abtrennung | 120 |
| F.3.2 | Diversität | 121 |
| F.3.3 | Gestaltung/Anwendung/Erfahrung | 121 |
| F.3.4 | Beurteilung/Analyse | 121 |
| F.3.5 | Ausbildung | 122 |
| F.3.6 | Umgebung | 122 |
| F.4 | Maßnahmen gegen Ausfälle infolge gemeinsamer Ursache (CCF) und weitere zutreffende Normen | 122 |

| | |
|---------------------------------------------------------------------------------------------------------------------------------------------------------|------------|
| Anhang G (informativ) Systematischer Ausfall | 123 |
| G.1 Allgemeines..... | 123 |
| G.2 Maßnahmen zur Beherrschung systematischer Ausfälle..... | 123 |
| G.3 Maßnahmen zur Vermeidung systematischer Ausfälle während des SRP/CS-Entwurfs | 124 |
| G.4 Maßnahmen zur Vermeidung systematischer Ausfälle während der Integration des SRP/CS | 125 |
| G.5 Management der funktionalen Sicherheit | 125 |
| Anhang H (informativ) Beispiel für eine Kombination von mehreren Teilsystemen | 127 |
| Anhang I (informativ) Beispiele für das vereinfachte Verfahren zur Abschätzung des PL von Teilsystemen | 130 |
| I.1 Allgemeines..... | 130 |
| I.2 Sicherheitsfunktion und erforderlicher Performance Level (PL_T) | 130 |
| I.3 Beispiel A — Einkanaliges System..... | 131 |
| I.3.1 Identifizierung der sicherheitsbezogenen Teile | 131 |
| I.3.2 Quantifizierung von $MTTF_D$, DC_{avg} , Maßnahmen gegen CCF, Kategorie und Performance Level | 132 |
| I.4 Beispiel B — Redundantes System | 133 |
| I.4.1 Identifizierung der sicherheitsbezogenen Teile | 133 |
| I.4.2 Quantifizierung von $MTTF_D$ für jeden Kanal, durchschnittlichem Diagnosedeckungsgrad, Maßnahmen gegen CCF, Kategorie und Performance Level | 135 |
| Anhang J (informativ) Beispiel für die Ausführung einer SRESW | 140 |
| J.1 Beschreibung des Beispiels | 140 |
| J.2 Anwendung des V-Modells des Software-Sicherheitslebenszyklus | 141 |
| J.3 Verifizierung der Softwarespezifikation auf verschiedenen Ebenen (d. h. SDS, SSDS, MDS).. | 142 |
| J.4 Beispiel für Programmierregeln | 143 |
| Anhang K (informativ) Numerische Darstellung von Bild 12 | 145 |
| Anhang L (informativ) Elektromagnetische Störfestigkeit (EMI) | 149 |
| Anhang M (informativ) Ergänzende Informationen zur Spezifikation der Sicherheitsanforderungen (SRS) | 153 |
| Anhang N (informativ) Vermeiden eines systematischen Ausfalls durch den Entwurf von Software | 155 |
| N.1 Auswahl von Maßnahmen zur Fehlervermeidung für den Entwurf von sicherheitsbezogener Software | 155 |
| N.2 Beispiel für eine Software-Validierung..... | 160 |
| N.2.1 Allgemeines..... | 160 |
| N.2.2 Codierungsrichtlinien..... | 160 |
| N.2.3 Spezifikation der Sicherheitsfunktionen..... | 160 |
| N.2.4 Eingangsinformationen aus der Spezifikation des Hardware-Entwurfs..... | 161 |
| N.2.5 Anwendungsprogramm | 164 |
| N.2.6 Validierung der eingesetzten SRASW | 164 |
| Anhang O (informativ) Sicherheitsbezogene Werte von Bauteilen oder Komponenten der Steuerungen | 175 |
| O.1 Definition der Gerätetypen | 175 |
| O.1.1 Allgemeines..... | 175 |
| O.1.2 Gerätetyp 1 | 176 |
| O.1.3 Gerätetyp 2 | 176 |
| O.1.4 Gerätetyp 3 | 177 |
| O.1.5 Gerätetyp 4 | 177 |
| O.2 Zusätzliche Informationen..... | 177 |
| O.2.1 Software | 177 |
| O.2.2 Grundlegende Sicherheitsprinzipien..... | 177 |
| O.2.3 Bewährte Sicherheitsprinzipien | 177 |
| Literaturhinweise | 178 |