

# Inhaltsverzeichnis

|  |          |
|--|----------|
| <b>Autorenporträt</b> . . . . .  | <b>V</b> |
| <b>1</b> <b>Funktionale Sicherheit – Was ist das?</b> . . . . .              | 1        |
| <b>2</b> <b>Normungssituation zum Thema funktionale Sicherheit</b> . . . . . | 3        |
| 2.1      Europa . . . . .  | 4        |
| 2.2      USA . . . . .   | 4        |
| 2.3      China . . . . .   | 5        |
| 2.4      Japan . . . . .   | 5        |
| <b>3</b> <b>Risikobeurteilung und Risikoreduzierung</b> . . . . .            | 6        |
| 3.1      Risikoreduzierung durch „Inhärentes Design“ . . . . .               | 9        |
| 3.2      Risikoreduzierung durch „Technische Schutzmaßnahmen“ . . . . .      | 10       |
| 3.2.1      Trennende Schutzeinrichtungen . . . . .                           | 10       |
| 3.2.2      Nicht trennende Schutzeinrichtungen . . . . .                     | 11       |
| 3.2.3      Not-Halt-Einrichtung als ergänzende Schutzmaßnahme . . . . .      | 12       |
| 3.3      Risikoreduzierung durch „Benutzerinformation“ . . . . .             | 13       |
| <b>4</b> <b>Sichere Steuerungstechnik</b> . . . . .                          | 14       |
| 4.1      Erfassung von Signalen . . . . .                                    | 14       |
| 4.1.1      Schutztürverriegelung mit und ohne Zuhaltung . . . . .            | 14       |
| 4.1.2      Berührungslos wirkende Schutzeinrichtungen . . . . .              | 17       |
| 4.1.3      Not-Halt-Einrichtungen . . . . .                                  | 20       |
| 4.1.4      Schaltmatten, Schaltleisten . . . . .                             | 21       |
| 4.1.5      Zwei-Hand-Bedienung . . . . .                                     | 23       |
| 4.2      Verarbeitung von Signalen . . . . .                                 | 24       |
| 4.2.1      Sicherheitsrelais . . . . .                                       | 24       |
| 4.2.2      Sicherheitsschaltgeräte . . . . .                                 | 26       |
| 4.2.3      Sicherheitssteuerungen . . . . .                                  | 27       |
| 4.2.4      Sichere Kommunikation und Netzwerke . . . . .                     | 28       |
| 4.3      Aktorik . . . . .   | 29       |
| 4.3.1      Schütze . . . . .   | 29       |
| 4.3.2      Drehzahlgeregelte Antriebssysteme . . . . .                       | 30       |
| 4.3.3      Fluidtechnik . . . . .  | 35       |
| <b>5</b> <b>Beurteilung der funktionalen Sicherheit</b> . . . . .            | 36       |
| 5.1      Von der Risikobeurteilung zur Sicherheitsfunktion . . . . .         | 36       |
| 5.2      Von der Sicherheitsfunktion zum PLr . . . . .                       | 37       |
| 5.2.1      Schwere der Verletzung – S . . . . .                              | 38       |

|          |   |           |
|----------|---|-----------|
| 5.2.2    | Häufigkeit und Dauer der Gefährdungsexposition – F . . . . .        | 39        |
| 5.2.3    | Möglichkeit zur Vermeidung der Gefährdungsereignisse – P . . . . .  | 39        |
| 5.3      | Technische Realisierung . . . . .                                   | 42        |
| 5.4      | Identifizierung der sicherheitsrelevanten Steuerungsteile . . . . . | 42        |
| 5.5      | Zuweisung zu Teilsystemen . . . . .                                 | 43        |
| 5.6      | Bestimmung des erreichten PL . . . . .                              | 43        |
| 5.6.1    | Grundlegende und bewährte Sicherheitsprinzipien . . . . .           | 43        |
| 5.6.2    | Bewährte Bauteile . . . . .   | 44        |
| 5.6.3    | Mean Time to Failure (MTTFD) – dangerous . . . . .                  | 44        |
| 5.6.4    | Diagnosedeckungsgrad . . . . .                                      | 47        |
| 5.6.5    | Fehler gemeinsamer Ursache . . . . .                                | 49        |
| 5.6.6    | Kategorien . . . . .  | 53        |
| 5.6.7    | Bestimmung des PL für ein Teilsystem . . . . .                      | 61        |
| 5.6.8    | Gerätetypen gemäß VDMA 66413 . . . . .                              | 62        |
| 5.6.9    | Wenn die Zuverlässigkeitsskennwerte fehlen . . . . .                | 64        |
| 5.7      | Bestimmung des PL für die gesamte Sicherheitsfunktion . . . . .     | 66        |
| 5.8      | Ist erreichter PL mindestens dem erforderlichen PLr? . . . . .      | 67        |
| <b>6</b> | <b>Verifikation und Validierung . . . . .</b>                       | <b>68</b> |
| 6.1      | Zufällige und systematische Fehler . . . . .                        | 70        |
| 6.2      | Fehlerannahmen und Fehlerausschlüsse . . . . .                      | 71        |
| 6.3      | Fehlermöglichkeits- und Auswirkungsanalyse . . . . .                | 73        |
| 6.4      | Sicherheitsrelevante Software und V-Modell . . . . .                | 75        |
| 6.4.1    | Sicherheitsrelevante Embedded-Software . . . . .                    | 77        |
| 6.4.2    | Sicherheitsrelevante Applikations-Software . . . . .                | 79        |
| 6.4.3    | Softwarebasiertes Parametrieren . . . . .                           | 82        |
| 6.4.4    | Beispiele für Programmierregeln . . . . .                           | 83        |
| <b>7</b> | <b>Funktionale Sicherheit und Security . . . . .</b>                | <b>85</b> |
| <b>8</b> | <b>Häufig gestellte Fragen . . . . .</b>                            | <b>86</b> |
| 8.1      | Testeinrichtungen bei Kategorie 2 . . . . .                         | 86        |
| 8.2      | EMV-Maßnahmen bei CCF . . . . .                                     | 86        |
| 8.3      | Muting als Sicherheitsfunktion . . . . .                            | 87        |
| 8.4      | Bedingungen zur Ermittlung von MTTF-Kennwerten . . . . .            | 87        |
| 8.5      | Mehrheitsentscheider in 2003-Struktur . . . . .                     | 88        |
| 8.6      | Abschätzung des DC . . . . .  | 88        |
| 8.7      | FIT vs. PFH <sub>D</sub> und MTTF . . . . .                         | 89        |
| 8.8      | Serienschaltung von Schutztürschaltern . . . . .                    | 89        |

|      |   |           |
|------|---|-----------|
| 8.9  | DIN EN ISO 13849 oder EN IEC 62061?.....                              | 91        |
| 8.10 | Kann man auf die Kennwert-Angaben der Hersteller vertrauen?..         | 91        |
| 8.11 | Anwendungsbereich Risikobewertung.....                                | 92        |
| 8.12 | Manuelle Rückstelleinrichtung .....                                   | 92        |
| 8.13 | Verwendung von Standardkomponenten .....                              | 93        |
| 8.14 | Not-Halt-Einrichtungen bei komplexen Anlagen .....                    | 94        |
| 8.15 | Vereinfachter Ansatz in DIN EN ISO 13849.....                         | 94        |
| 8.16 | Testrate bei Kategorie 2 .....  | 95        |
| 8.17 | Einkanalige Architekturen in Kategorie 3 zulässig?.....               | 95        |
| 8.18 | Relais mit Zwangsführung.....   | 96        |
| 8.19 | Verwendung von Low-demand-Komponenten gemäß<br>DIN EN ISO 13849 ..... | 96        |
| 8.20 | Not-Halt-Einrichtungen mit antivalenten Kontakten .....               | 97        |
| 8.21 | Bewertung unterschiedlicher Betriebsarten .....                       | 97        |
|      | <b>Literaturverzeichnis .....</b>                                     | <b>98</b> |
|      | <b>Bildquellen.....</b>   | <b>98</b> |