

# Inhaltsverzeichnis

<b>1</b>	<b>Funktionale Sicherheit – Was ist das? .....</b>	<b>1</b>
<b>2</b>	<b>Normungssituation „funktionale Sicherheit“ .....</b>	<b>3</b>
2.1	Europa .....	3
2.2	USA .....	4
2.3	China .....	4
2.4	Japan .....	5
<b>3</b>	<b>Risikobeurteilung und Risikoreduzierung .....</b>	<b>7</b>
3.1	Risikoreduzierung durch „Inhärentes Design“ .....	10
3.2	Risikoreduzierung durch „Technische Schutzmaßnahmen“ .....	11
3.2.1	Trennende Schutzeinrichtungen .....	11
3.2.2	Nicht-trennende Schutzeinrichtungen .....	12
3.2.3	Not-Halt-Einrichtung als ergänzende Schutzmaßnahme .....	13
3.3	Risikoreduzierung durch „Benutzerinformation“ .....	14
<b>4</b>	<b>Sichere Steuerungstechnik .....</b>	<b>15</b>
4.1	Erfassung von Signalen .....	15
4.1.1	Schutztürverriegelung mit und ohne Zuhaltung .....	15
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 .....	22
4.2	Verarbeitung von Signalen .....	22
4.2.1	Sicherheitsrelais .....	22
4.2.2	Sicherheitsschaltgeräte .....	23
4.2.3	Sicherheitssteuerungen .....	24
4.2.4	Sichere Kommunikation und Netzwerke .....	25
4.3	Aktorik .....	26
4.3.1	Schütze .....	26
4.3.2	Drehzahlgeregelte Antriebssysteme .....	27
4.3.3	Fluidtechnik .....	30
<b>5</b>	<b>Beurteilung der funktionalen Sicherheit .....</b>	<b>31</b>
5.1	Von der Risikobeurteilung zur Sicherheitsfunktion .....	31
5.2	Von der Sicherheitsfunktion zum PL <sub>r</sub> .....	32
5.2.1	Schwere der Verletzung – S .....	32

5.2.2	Häufigkeit und Dauer der Gefährdungsexposition – F .....	33
5.2.3	Möglichkeit zur Vermeidung der Gefährdungsereignisse – P .....	33
5.3	Technische Realisierung .....	34
5.4	Identifizierung der sicherheitsrelevanten Steuerungsteile .....	35
5.5	Zuweisung zu Teilsystemen .....	35
5.6	Bestimmung des erreichten PL .....	36
5.6.1	Grundlegende und bewährte Sicherheitsprinzipien .....	36
5.6.2	Bewährte Bauteile .....	36
5.6.3	MTTF <sub>D</sub> – Mean Time to Failure, dangerous .....	37
5.6.4	Diagnosedeckungsgrad .....	39
5.6.5	Fehler gemeinsamer Ursache .....	41
5.6.6	Kategorien .....	43
5.6.7	Bestimmung des PL für ein Teilsystem .....	51
5.6.8	Wenn die Zuverlässigkeitsskennwerte fehlen .....	53
5.7	Bestimmung des PL für die gesamte Sicherheitsfunktion .....	54
5.8	Ist erreichter PL mindestens dem erforderlichen PL <sub>r</sub> ? .....	55
<b>6</b>	<b>Verifikation und Validierung</b> .....	57
6.1	Zufällige und systematische Fehler .....	58
6.2	Fehlerannahmen und Fehlerausschlüsse .....	59
6.3	Fehlerarten- und Auswirkungsanalyse .....	61
6.4	Sicherheitsrelevante Software und V-Modell .....	63
6.4.1	Sicherheitsrelevante Embedded-Software (SRESW) .....	64
6.4.2	Sicherheitsrelevante Applikations-Software (SRASW) .....	66
6.4.3	Softwarebasiertes Parametrieren .....	68
<b>7</b>	<b>Häufig gestellte Fragen</b> .....	71
7.1	Testeinrichtungen bei Kategorie 2 .....	71
7.2	EMV-Maßnahmen bei CCF .....	71
7.3	Muting als Sicherheitsfunktion .....	72
7.4	Bedingungen zur Ermittlung von MTTF-Kennwerten .....	72
7.5	Mehrheitsentscheider in 2oo3-Struktur .....	73
7.6	Abschätzung des DC .....	73
7.7	FIT vs. PFH und MTTF .....	74
7.8	Serienschaltung von Schutztürschaltern .....	74
7.9	EN ISO 13849 oder EN IEC 62061? .....	75
7.10	Kann man auf die Kennwert-Angaben der Hersteller vertrauen? ..	76

7.11	Anwendungsbereich Risikobewertung .....	76
7.12	Manuelle Rückstelleinrichtung .....	77
7.13	Verwendung von Standardkomponenten .....	77
7.14	Not-Halt-Einrichtungen bei komplexen Anlagen .....	78
7.15	Vereinfachter Ansatz in EN ISO 13849 .....	79
7.16	Testrate bei Kategorie 2 .....	79
7.17	Einkanalige Architekturen in Kategorie 3 zulässig? .....	80
7.18	Relais mit Zwangsführung .....	81
7.19	Verwendung von low-demand-Komponenten gemäß EN ISO 13849 .....	81
7.20	Not-Halt-Einrichtungen mit antivalenten Kontakten .....	82
7.21	Bewertung unterschiedlicher Betriebsarten .....	82
<b>Literaturverzeichnis .....</b>		83
<b>Stichwortverzeichnis .....</b>		85