

## Deutsche Fassung

Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme –  
Teil 6: Anwendungsrichtlinie für IEC 61508-2 und IEC 61508-3

### Inhalt

	Seite
Einleitung .....	6
1 Anwendungsbereich .....	8
2 Normative Verweisungen .....	10
3 Begriffe und Abkürzungen .....	10
Anhang A (informativ) Anwendung der IEC 61508-2 und der IEC 61508-3.....	11
A.1 Allgemeines .....	11
A.2 Funktionale Schritte in der Anwendung der IEC 61508-2 .....	13
A.3 Funktionale Schritte in der Anwendung der IEC 61508-3 .....	17
Anhang B (informativ) Beispiel eines Verfahrens für die Bewertung von Ausfallwahrscheinlichkeiten der Hardware .....	19
B.1 Allgemeines .....	19
B.2 Grundsätzliche Betrachtungen zu Wahrscheinlichkeitsberechnungen .....	20
B.2.1 Einleitung .....	20
B.2.2 Sicherheitsbezogenes E/E/PE-System mit niedriger Anforderungsrate .....	20
B.2.3 Sicherheitsbezogenes E/E/PE-System mit hoher Anforderungsrate oder kontinuierlicher Anforderung .....	21
B.3 RBD-Ansatz mit angenommener konstanter Ausfallrate.....	23
B.3.1 Grundlegende Hypothese.....	23
B.3.2 Mittlere Ausfallwahrscheinlichkeit bei Anforderung (für die Betriebsart mit niedriger Anforderungsrate).....	27
B.3.3 Wahrscheinlichkeit eines Ausfalls je Stunde (für die Betriebsart mit hoher Anforderungsrate oder kontinuierlicher Anforderung) .....	42
B.4 Boolescher Ansatz.....	51
B.4.1 Einleitung .....	51
B.4.2 Modell des Zuverlässigkeits-Blockdiagramms .....	51
B.4.3 Fehlzustandsbaumanalysen-Modell.....	52
B.4.4 <i>PF</i> D-Berechnungen .....	52
B.5 Zustand/Übergangs-Ansätze.....	57
B.5.1 Einleitung .....	57
B.5.2 Markov-Ansatz.....	57
B.5.3 Auf Petri-Netze und Monte Carlo-Simulation basierte Ansätze .....	66
B.5.4 Weitere Ansätze .....	71

	Seite
B.6 Unsicherheitenbehandlung .....	73
B.7 Verweise .....	74
Anhang C (informativ) Ausgearbeitetes Beispiel für die Berechnung des Diagnosedeckungsgrads und des Anteils sicherer Ausfälle.....	75
Anhang D (informativ) Eine Methode zur Quantifizierung der Auswirkungen von hardwarebedingten Ausfällen infolge gemeinsamer Ursache in E/E/PE-Systemen .....	78
D.1 Allgemeines .....	78
D.2 Anwendungsbereich der Methode .....	82
D.3 Durch die Methode berücksichtigte Punkte .....	82
D.4 Verwendung des $\beta$ -Faktor, um die Wahrscheinlichkeit eines Ausfalls eines sicherheitsbezogenen E/E/PE-Systems durch Ausfälle infolge gemeinsamer Ursache zu berechnen .....	83
D.5 Schätzung von $\beta$ unter Verwendung der Tabellen .....	84
D.6 Beispiele für die Anwendung der $\beta$ -Faktor-Methode .....	89
D.7 CCF-Ansatz mit Binomial-Ausfallraten Modell (Modell mit Zufallsstörungen) .....	90
D.8 Literaturhinweise.....	92
Anhang E (informativ) Beispiele für die Anwendung der Tabellen zur Sicherheitsintegrität der Software aus der IEC 61508-3 .....	93
E.1 Allgemeines .....	93
E.2 Beispiel für den Sicherheits-Integritätslevel 2.....	93
E.3 Beispiel für den Sicherheits-Integritätslevel 3.....	98
Literaturhinweise .....	103
<b>Bilder</b>	
Bild 1 – Gesamtrahmen der IEC 61508 .....	9
Bild A.1 – Anwendung der IEC 61508-2 .....	15
Bild A.2 – Anwendung der IEC 61508-2 .....	16
Bild A.3 – Anwendung der IEC 61508-3 .....	18
Bild B.1 – Zuverlässigkeits-Blockdiagramm einer vollständigen Sicherheitsschleife .....	20
Bild B.2 – Beispielkonfiguration für zwei Kanäle mit Sensoren .....	25
Bild B.3 – Struktur mit Teilsystemen .....	27
Bild B.4 – Blockschaltbild für 1oo1 .....	29
Bild B.5 – Zuverlässigkeits-Blockdiagramm für 1oo1.....	29
Bild B.6 – Blockschaltbild für 1oo2.....	30
Bild B.7 – Zuverlässigkeits-Blockdiagramm für 1oo2.....	30
Bild B.8 – Blockschaltbild für 2oo2.....	31
Bild B.9 – Zuverlässigkeits-Blockdiagramm für 2oo2.....	31
Bild B.10 – Blockschaltbild für 1oo2D .....	31
Bild B.11 – Zuverlässigkeits-Blockdiagramm für 1oo2D.....	32
Bild B.12 – Blockschaltbild für 2oo3.....	32
Bild B.13 – Zuverlässigkeits-Blockdiagramm für 2oo3 .....	33

	Seite
Bild B.14 – Architektur des Beispiels für die Betriebsart mit niedriger Anforderungsrate .....	39
Bild B.15 – Architektur des Beispiels für die Betriebsart mit hoher Anforderungsrate oder kontinuierlicher Anforderung.....	49
Bild B.16 – RBD einer einfachen vollständigen Schleife mit Sensoren und 2oo3-Architektur .....	52
Bild B.17 – Einfache Fehlzustandsbaumanalyse, entsprechend dem in Bild B.1 dargestellten RBD.....	52
Bild B.18 – Äquivalenz von Fehlzustandsbaum und Zuverlässigkeits-Blockdiagramm .....	53
Bild B.19 – Augenblickliche Nichtverfügbarkeit $U(t)$ einzelner periodisch getesteter Bauteile.....	54
Bild B.20 – Prinzip der Berechnung von $PF_{D,avg}$ durch Fehlzustandsbaumanalysen.....	55
Bild B.21 – Auswirkung von versetzten Tests .....	56
Bild B.22 – Beispiel einer komplexen Teststruktur .....	56
Bild B.23 – Markov-Graph, der das Verhalten eines Zwei-Komponenten-Systems modelliert.....	58
Bild B.24 – Prinzip der Modellierung eines mehrphasigen Markov-Prozesses .....	59
Bild B.25 – Sägezahnprofil für den mehrphasigen Markov-Ansatz .....	60
Bild B.26 – Markov-Modell-Approximation.....	60
Bild B.27 – Auswirkung der Ausfälle durch die Anforderung selbst .....	61
Bild B.28 – Modellierung der Auswirkung der Testdauer .....	61
Bild B.29 – Mehrphasiges Markov-Modell mit DD- und auch DU-Ausfällen.....	61
Bild B.30 – Logikänderung (2oo3 nach 1oo2) anstelle einer Reparatur des ersten Ausfalls .....	62
Bild B.31 – Markov-Graphen für die „Zuverlässigkeit“ mit einem absorbierenden Zustand.....	63
Bild B.32 – Markov-Graphen für die „Verfügbarkeit“ ohne absorbierende Zustände .....	64
Bild B.33 – Petri-Netz für die Modellierung einer einzelnes periodisch getestetes Bauteil .....	66
Bild B.34 – PN zur Modellierung von CCF und der Reparaturressourcen .....	69
Bild B.35 – RBD für die PN-Modellbildung und Zusatz-PN für die $PF_{D-}$ und $PF_{FH}$ -Berechnungen .....	69
Bild B.36 – Einfaches PN für ein Einzelbauteil und entdeckten Ausfällen und Reparaturen .....	70
Bild B.37 – Beispiel der funktionalen und dysfunktionalen Modellierung mit einer formalen Sprache.....	72
Bild B.38 – Prinzip der Unsicherheitsverteilung.....	73
Bild D.1 – Beziehung zwischen Ausfällen infolge gemeinsamer Ursache und Ausfällen einzelner Kanäle.....	80
Bild D.2 – Umsetzung des Modells mit Zufallsstörungen anhand von Fehlzustandsbäumen.....	91
<b>Tabellen</b>	
Tabelle B.1 – In diesem Anhang verwendete Benennungen und ihre zugehörigen Parameterbereiche .....	26
Tabelle B.2 – Mittlere Wahrscheinlichkeit eines Ausfalls bei Anforderung für ein Wiederholungsprüfungsintervall von 6 Monaten und eine mittlere Zeit zur Wiederherstellung von 8 h .....	34
Tabelle B.3 – Mittlere Wahrscheinlichkeit eines Ausfalls bei Anforderung für ein Wiederholungsprüfungsintervall von einem Jahr und eine mittlere Zeit zur Wiederherstellung von 8 h .....	35
Tabelle B.4 – Mittlere Wahrscheinlichkeit eines Ausfalls bei Anforderung für ein Wiederholungsprüfungsintervall von zwei Jahren und eine mittlere Zeit zur Wiederherstellung von 8 h.....	37

	Seite
Tabelle B.5 – Mittlere Wahrscheinlichkeit eines Ausfalls bei Anforderung für ein Wiederholungsprüfungsintervall von 10 Jahren und eine mittlere Zeit zur Wiederherstellung von 8 h .....	38
Tabelle B.6 – Mittlere Wahrscheinlichkeit eines Ausfalls bei Anforderung für das Sensor-Teilsystem in dem Beispiel für die Betriebsart mit niedriger Anforderungsrate (ein Jahr Wiederholungsprüfungsintervall und 8 h <i>MTTR</i> ) .....	39
Tabelle B.7 – Mittlere Wahrscheinlichkeit eines Ausfalls bei Anforderung für das Logik-Teilsystem in dem Beispiel für die Betriebsart mit niedriger Anforderungsrate (ein Jahr Wiederholungsprüfungsintervall und 8 h <i>MTTR</i> ) .....	40
Tabelle B.8 – Mittlere Wahrscheinlichkeit eines Ausfalls bei Anforderung für das Stellglied-Teilsystem in dem Beispiel für die Betriebsart mit niedriger Anforderungsrate (ein Jahr Wiederholungsprüfungsintervall und 8 h <i>MTTR</i> ) .....	40
Tabelle B.9 – Beispiel für eine nicht ausreichende Wiederholungsprüfung .....	42
Tabelle B.10 – Wahrscheinlichkeit eines Ausfalls je Stunde (für die Betriebsart mit hoher Anforderungsrate oder kontinuierlicher Anforderung) für ein Wiederholungsprüfungsintervall von einem Monat und eine mittlere Zeit zur Wiederherstellung von 8 h .....	44
Tabelle B.11 – Wahrscheinlichkeit eines Ausfalls je Stunde (für die Betriebsart mit hoher oder Anforderungsrate kontinuierlicher Anforderung) für ein Wiederholungsprüfungsintervall von drei Monaten und eine mittlere Zeit zur Wiederherstellung von 8 h .....	45
Tabelle B.12 – Wahrscheinlichkeit eines Ausfalls je Stunde (für die Betriebsart mit hoher Anforderungsrate oder kontinuierlicher Anforderung) für ein Wiederholungsprüfungsintervall von 6 Monaten und eine mittlere Zeit zur Wiederherstellung von 8 h .....	47
Tabelle B.13 – Wahrscheinlichkeit eines Ausfalls je Stunde (für die Betriebsart mit hoher Anforderungsrate oder kontinuierlicher Anforderung) für ein Wiederholungsprüfungsintervall von einem Jahr und eine mittlere Zeit zur Wiederherstellung von 8 h .....	48
Tabelle B.14 – Wahrscheinlichkeit des Ausfalls je Stunde für das Sensor-Teilsystem in dem Beispiel für die Betriebsart mit hoher Anforderungsrate oder kontinuierlicher Anforderung (sechs Monate Wiederholungsprüfungsintervall und 8 h <i>MTTR</i> ) .....	49
Tabelle B.15 – Wahrscheinlichkeit eines Ausfalls je Stunde für das Logik-Teilsystem in dem Beispiel für die Betriebsart mit hoher Anforderungsrate oder kontinuierlicher Anforderung (sechs Monate Wiederholungsprüfungsintervall und 8 h <i>MTTR</i> ) .....	50
Tabelle B.16 – Wahrscheinlichkeit eines Ausfalls je Stunde für das Stellglied-Teilsystem in dem Beispiel für die Betriebsart mit hoher Anforderungsrate oder kontinuierlicher Anforderung (sechs Monate Wiederholungsprüfungsintervall und 8 h <i>MTTR</i> ) .....	50
Tabelle C.1 – Beispielberechnung für den Diagnosedeckungsgrad und den Anteil sicherer Ausfälle .....	76
Tabelle C.2 – Diagnosedeckungsgrad und Wirksamkeit für verschiedene Teilsysteme .....	77
Tabelle D.1 – Anrechnung programmierbarer Elektronik oder Sensoren/Stellglieder .....	86
Tabelle D.2 – Werte für <i>Z</i> : programmierbare Elektronik .....	88
Tabelle D.3 – Werte für <i>Z</i> : Sensoren oder Stellglieder .....	88
Tabelle D.4 – Berechnung von $\beta$ oder $\beta_p$ .....	89
Tabelle D.5 – Berechnung von $\beta$ für Redundanzsysteme größer als 1oo2 .....	89
Tabelle D.6 – Beispielwerte für programmierbare Elektroniken .....	90
Tabelle E.1 – Spezifikation der Software-Sicherheitsanforderungen (siehe IEC 61508-3, 7.2) .....	94
Tabelle E.2 – Software-Entwurf und -Entwicklung: Entwurf der Software-Architektur (siehe IEC 61508-3, 7.4.3) .....	95
Tabelle E.3 – Software-Entwurf und -Entwicklung: Hilfswerkzeuge und Programmiersprachen (siehe IEC 61508-3, 7.4.4) .....	96

	Seite
Tabelle E.4 – Software-Entwurf und -Entwicklung: Detaillierter Entwurf (siehe IEC 61508-3, 7.4.5 und 7.4.6).....	96
Tabelle E.5 – Software-Entwurf und -Entwicklung: Test der Software-Module und der Integration der Software (siehe IEC 61508-3, 7.4.7 und 7.4.8).....	96
Tabelle E.6 – Integration der programmierbaren Elektronik (Hardware und Software) (siehe IEC 61508-3, 7.5) .....	97
Tabelle E.7 – Validierung der Software bezüglich der Sicherheit (siehe IEC 61508-3, 7.7) .....	97
Tabelle E.8 – Software-Modifikation (siehe IEC 61508-3, 7.8).....	97
Tabelle E.9 – Software-Verifikation (siehe IEC 61508-3, 7.9).....	97
Tabelle E.10 – Beurteilung der funktionalen Sicherheit (siehe IEC 61508-3, Abschnitt 8) .....	98
Tabelle E.11 – Spezifikation der Software-Sicherheitsanforderungen (siehe IEC 61508-3, 7.2).....	99
Tabelle E.12 – Software-Entwurf und -Entwicklung: Entwurf der Software-Architektur (siehe IEC 61508-3, 7.4.3) .....	99
Tabelle E.13 – Software-Entwurf und -Entwicklung: Hilfswerkzeuge und Programmiersprachen (siehe IEC 61508-3, 7.4.4) .....	100
Tabelle E.14 – Software-Entwurf und -Entwicklung: Detaillierter Entwurf (siehe IEC 61508-3, 7.4.5 und 7.4.6).....	100
Tabelle E.15 – Software-Entwurf und -Entwicklung: Test der Software-Module und -Integration (siehe IEC 61508-3, 7.4.7 und 7.4.8) .....	101
Tabelle E.16 – Integration der programmierbaren Elektronik (Hardware und Software) (siehe IEC 61508-3, 7.5) .....	101
Tabelle E.17 – Validierung der Softwaresicherheit (siehe IEC 61508-3, 7.7) .....	101
Tabelle E.18 – Software-Modifikation (siehe IEC 61508-3, 7.8) .....	102
Tabelle E.19 – Software-Verifikation (siehe IEC 61508-3, 7.9).....	102
Tabelle E.20 – Beurteilung der funktionalen Sicherheit (siehe IEC 61508-3, Abschnitt 8) .....	102