Inhalt

Seite

Vorwort ... 2
Einleitung ... 8
1 Anwendungsbereich ... 10
2 Normative Verweisungen ... 12
3 Begriffe und Abkürzungen ... 12
Anhang A (informativ) Anwendung der IEC 61508-2 und der IEC 61508-3 ... 13
A.1 Allgemeines ... 13
A.2 Funktionale Schritte bei der Anwendung der IEC 61508-2 ... 15
A.3 Funktionale Schritte bei der Anwendung der IEC 61508-3 ... 19
Anhang B (informativ) Beispielverfahren für die Bewertung von Ausfallwahrscheinlichkeiten der Hardware ... 21
B.1 Allgemeines ... 21
B.2 Betrachtungen zu grundlegenden Wahrscheinlichkeitsberechnungen ... 22
B.2.1 Einleitung ... 22
B.2.2 Sicherheitsbezogenes E/E/PE-System mit niedriger Anforderungsrate ... 22
B.2.3 Sicherheitsbezogenes E/E/PE-System mit hoher Anforderungsrate oder kontinuierlicher Anforderung ... 23
B.3 Zuverlässigkeitsblockdiagramm-Ansatz mit angenommener konstanter Ausfallrate ... 25
B.3.1 Grundlegende Hypothese ... 25
B.3.2 Mittlere Ausfallwahrscheinlichkeit bei Anforderung (für die Betriebsart mit niedriger Anforderungsrate) ... 29
B.3.3 Mittlere Häufigkeit eines gefahrbringenden Ausfalls (für die Betriebsart mit hoher Anforderungsrate oder kontinuierlicher Anforderung) ... 43
B.4 Boolescher Ansatz ... 52
B.4.1 Allgemeines ... 52
B.4.2 Modell des Zuverlässigkeitsblockdiagramms ... 52
B.4.3 Fehlerbaummodell ... 53
B.4.4 *PFD*-Berechnungen ... 53
B.5 Zustands-/Übergangs-Ansätze ... 58
B.5.1 Allgemeines ... 58
B.5.2 Markov-Ansatz ... 59
B.5.3 Ansätze basierend auf Petri-Netzen und Monte-Carlo-Simulation ... 67
B.5.4 Andere Ansätze ... 73
B.6 Behandlung von Unsicherheiten ... 75
B.7 Verweise ... 76
Anhang C (informativ) Ausgearbeitetes Beispiel für die Berechnung des Diagnosedeckungsgrads und des Anteils sicherer Ausfälle ... 77
Anhang D (informativ) Eine Methode zur Quantifizierung der Auswirkungen von hardwarebedingten Ausfällen infolge gemeinsamer Ursache in E/E/PE-Systemen ... 80
D.1 Allgemeines ... 80

Seite

D.1.1 Einleitung ... 80
D.1.2 Kurzübersicht ... 80
D.1.3 Schutz gegen Ausfälle infolge gemeinsamer Ursache ... 81
D.1.4 In der Normenreihe IEC 61508 gewählter Ansatz ... 83
D.2 Anwendungsbereich der Methode ... 84
D.3 Durch die Methode berücksichtigte Punkte ... 85
D.4 Verwendung des β-Faktors, um die Wahrscheinlichkeit eines Ausfalls eines sicherheitsbezogenen E/E/PE-Systems durch Ausfälle infolge gemeinsamer Ursache zu berechnen ... 86
D.5 Schätzung von β unter Verwendung der Tabellen ... 87
D.6 Beispiele für die Anwendung der β-Faktor-Methode ... 92
D.7 Binomialverteilte Ausfallrate (Schockmodell) – CCF-Ansatz ... 93
D.8 Literaturhinweise ... 95
Anhang E (informativ) Beispiele für die Anwendung der Tabellen zur Sicherheitsintegrität der Software aus IEC 61508-3 ... 96
E.1 Allgemeines ... 96
E.2 Beispiel für den Sicherheits-Integritätslevel 2 ... 96
E.3 Beispiel für den Sicherheits-Integritätslevel 3 ... 105
Literaturhinweise ... 114
Anhang ZA (normativ) Normative Verweisungen auf internationale Publikationen mit ihren entsprechenden europäischen Publikationen ... 117

Bilder

Bild 1 – Gesamtrahmen der Normenreihe IEC 61508 ... 11
Bild A.1 – Anwendung der IEC 61508-2 ... 17
Bild A.2 – Anwendung der IEC 61508-2 (Fortsetzung von Bild A.1) ... 18
Bild A.3 – Anwendung der IEC 61508-3 ... 20
Bild B.1 – Zuverlässigkeitsblockdiagramm einer vollständigen PLT-Schutzeinrichtung ... 22
Bild B.2 – Beispielkonfiguration für zwei Kanäle mit Sensoren ... 27
Bild B.3 – Struktur mit Teilsystemen ... 29
Bild B.4 – Blockschaltbild für 1oo1 ... 31
Bild B.5 – Zuverlässigkeitsblockdiagramm für 1oo1 ... 31
Bild B.6 – Blockschaltbild für 1oo2 ... 32
Bild B.7 – Zuverlässigkeitsblockdiagramm für 1oo2 ... 32
Bild B.8 – Blockschaltbild für 2oo2 ... 32
Bild B.9 – Zuverlässigkeitsblockdiagramm für 2oo2 ... 33
Bild B.10 – Blockschaltbild für 1oo2D ... 33
Bild B.11 – Zuverlässigkeitsblockdiagramm für 1oo2D ... 33
Bild B.12 – Blockschaltbild für 2oo3 ... 34
Bild B.13 – Zuverlässigkeitsblockdiagramm für 2oo3 ... 34
Bild B.14 – Architektur eines Beispiels für die Betriebsart mit niedriger Anforderungsrate ... 40

Seite

Bild B.15 – Architektur des Beispiels für die Betriebsart mit hoher Anforderungsrate oder kontinuierlicher Anforderung ... 50
Bild B.16 – Zuverlässigkeitsblockdiagramm einer einfachen vollständigen Schleife mit Sensoren als 2oo3-Logik ... 52
Bild B.17 – Einfacher Fehlerbaum entsprechend dem in Bild B.1 dargestellten Zuverlässigkeitsblockdiagramm ... 53
Bild B.18 – Gleichartigkeit von Fehlerbaum und Zuverlässigkeitsblockdiagramm ... 54
Bild B.19 – Augenblickliche Nichtverfügbarkeit $U(t)$ einzelner, periodisch getesteter Komponenten ... 55
Bild B.20 – Prinzip der Berechnung von PFD_{avg} bei Verwendung von Fehlerbäumen ... 56
Bild B.21 – Auswirkung von versetzten Tests ... 57
Bild B.22 – Beispiel eines komplexen Testmusters ... 58
Bild B.23 – Markov-Graph, der das Verhalten eines Systems mit zwei Komponenten modelliert ... 59
Bild B.24 – Prinzip der Modellierung eines mehrphasigen Markov-Prozesses ... 60
Bild B.25 – Sägezahnkurve bei mehrphasigem Markov-Ansatz ... 62
Bild B.26 – Angenähertes Markov-Modell ... 62
Bild B.27 – Auswirkungen von Ausfälle durch die Anforderung selbst ... 62
Bild B.28 – Modellierung des Einflusses der Testdauer ... 63
Bild B.29 – Mehrphasiges Markov-Modell mit DD- und DU-Ausfällen ... 63
Bild B.30 – Logikänderung (2oo3 nach 1oo2) anstelle einer Reparatur des ersten Ausfalls ... 64
Bild B.31 – Markov-Graphen für die „Zuverlässigkeit“ mit einem absorbierenden Zustand ... 65
Bild B.32 – Markov-Graphen für die „Verfügbarkeit“ ohne absorbierende Zustände ... 66
Bild B.33 – Petri-Netz für die Modellierung einer einzelnen periodisch getesteten Komponente ... 68
Bild B.34 – Petri-Netze zur Modellierung von Ausfällen infolge gemeinsamer Ursache und Reparaturressourcen ... 71
Bild B.35 – Verwendung von Zuverlässigkeitsblockdiagrammen zur Aufstellung von Petri-Netzen und Auxiliary-Petri-Netzen für die *PFD*- und *PFH*-Berechnungen ... 71
Bild B.36 – Einfaches Petri-Netz für eine einzelne Komponente mit entdeckten Ausfällen und Reparaturen ... 72
Bild B.37 – Beispiel einer funktionalen und dysfunktionalen Modellierung mit einer formalen Sprache ... 74
Bild B.38 – Prinzip der Fortpflanzung von Unsicherheiten ... 75
Bild D.1 – Beziehung zwischen Ausfällen infolge gemeinsamer Ursache und Ausfällen einzelner Kanäle ... 83
Bild D.2 – Umsetzung des Schockmodells anhand von Fehlerbäumen ... 94

Tabellen

Tabelle B.1 – In diesem Anhang verwendete Benennungen und ihre zugehörigen Parameterbereiche ... 27
Tabelle B.2 – Mittlere Wahrscheinlichkeit eines Ausfalls bei Anforderung für ein Wiederholungsprüfungsintervall von sechs Monaten und eine mittlere Dauer bis zur Wiederherstellung von 8 h ... 36
Tabelle B.3 – Mittlere Wahrscheinlichkeit eines Ausfalls bei Anforderung für ein Wiederholungsprüfungsintervall von einem Jahr und eine mittlere Dauer bis zur Wiederherstellung von 8 h ... 37

Seite

Tabelle B.4 – Mittlere Wahrscheinlichkeit eines Ausfalls bei Anforderung für ein Wiederholungsprüfungsintervall von zwei Jahren und eine mittlere Dauer bis zur Wiederherstellung von 8 h 38

Tabelle B.5 – Mittlere Wahrscheinlichkeit eines Ausfalls bei Anforderung für ein Wiederholungsprüfungsintervall von zehn Jahren und eine mittlere Dauer bis zur Wiederherstellung von 8 h 39

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 *MTTR*) 40

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 *MTTR*) 41

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 *MTTR*) 41

Tabelle B.9 – Beispiel für eine unvollständige Wiederholungsprüfung 43

Tabelle B.10 – Mittlere Häufigkeit eines gefahrbringenden Ausfalls (in der Betriebsart mit hoher Anforderungsrate oder kontinuierlicher Anforderung) für ein Wiederholungsprüfungsintervall von einem Monat und eine mittlere Dauer bis zur Wiederherstellung von 8 h 46

Tabelle B.11 – Mittlere Häufigkeit eines gefahrbringenden Ausfalls (in der Betriebsart mit hoher oder Anforderungsrate kontinuierlicher Anforderung) für ein Wiederholungsprüfungsintervall von drei Monaten und eine mittlere Dauer bis zur Wiederherstellung von 8 h 47

Tabelle B.12 – Mittlere Häufigkeit eines gefahrbringenden Ausfalls (in der Betriebsart mit hoher Anforderungsrate oder kontinuierlicher Anforderung) für ein Wiederholungsprüfungsintervall von sechs Monaten und eine mittlere Dauer bis zur Wiederherstellung von 8 h 48

Tabelle B.13 – Mittlere Häufigkeit eines gefahrbringenden Ausfalls (in der Betriebsart mit hoher Anforderungsrate oder kontinuierlicher Anforderung) für ein Wiederholungsprüfungsintervall von einem Jahr und eine mittlere Dauer bis zur Wiederherstellung von 8 h 49

Tabelle B.14 – Mittlere Häufigkeit eines gefahrbringenden Ausfalls für das Sensor-Teilsystem in dem Beispiel für die Betriebsart mit hoher Anforderungsrate oder kontinuierlicher Anforderung (sechs Monate Wiederholungsprüfungsintervall und 8 h *MTTR)* 50

Tabelle B.15 – Mittlere Häufigkeit eines gefahrbringenden Ausfalls für das Logik-Teilsystem in dem Beispiel für die Betriebsart mit hoher Anforderungsrate oder kontinuierlicher Anforderung (sechs Monate Wiederholungsprüfungsintervall und 8 h *MTTR*) 51

Tabelle B.16 – Mittlere Häufigkeit eines gefahrbringenden Ausfalls für das Stellglied-Teilsystem in dem Beispiel für die Betriebsart mit hoher Anforderungsrate oder kontinuierlicher Anforderung (sechs Monate Wiederholungsprüfungsintervall und 8 h *MTTR*) 51

Tabelle C.1 – Beispielberechnung für den Diagnosedeckungsgrad und den Anteil sicherer Ausfälle 78

Tabelle C.2 – Diagnosedeckungsgrad und Wirksamkeit für verschiedene Teilsysteme 79

Tabelle D.1 – Bewertung programmierbarer Elektronik oder Sensoren/Stellglieder 88

Tabelle D.2 – Werte für Z – programmierbare Elektronik 90

Tabelle D.3 – Werte für Z – Sensoren oder Stellglieder 90

Tabelle D.4 – Berechnung von β_{int} oder $\beta_{D\,int}$ 91

Tabelle D.5 – Berechnung von β für Redundanzsysteme größer als 1oo2 91

Tabelle D.6 – Beispielwerte für programmierbare Elektroniken 93

Tabelle E.1 – Spezifikation der Anforderungen an die Sicherheit der Software 97

Tabelle E.2 – Softwareentwurf und Softwareentwicklung – Entwurf der Softwarearchitektur 98

Seite

Tabelle E.3 – Softwareentwurf und Softwareentwicklung – Werkzeuge und Programmiersprache 99
Tabelle E.4 – Softwareentwurf und Softwareentwicklung – Detaillierter Entwurf 100
Tabelle E.5 – Softwareentwurf und Softwareentwicklung – Test der Softwaremodule und Integration 101
Tabelle E.6 – Integration der programmierbaren Elektronik (Hardware und Software) 101
Tabelle E.7 – Softwareaspekte bezüglich der Validierung der Sicherheit des Systems 102
Tabelle E.8 – Softwaremodifikation 103
Tabelle E.9 – Softwareverifikation 104
Tabelle E.10 – Beurteilung der funktionalen Sicherheit 104
Tabelle E.11 – Spezifikation der Anforderungen an die Sicherheit der Software 106
Tabelle E.12 – Softwareentwurf und Softwareentwicklung – Entwurf der Softwarearchitektur 106
Tabelle E.13 – Softwareentwurf und Softwareentwicklung – Werkzeuge und Programmiersprache 108
Tabelle E.14 – Softwareentwurf und Softwareentwicklung – Detaillierter Entwurf 108
Tabelle E.15 – Softwareentwurf und Softwareentwicklung – Test der Softwaremodule und Integration 109
Tabelle E.16 – Integration der programmierbaren Elektronik (Hardware und Software) 110
Tabelle E.17 – Softwareaspekte bezüglich der Validierung der Sicherheit des Systems 110
Tabelle E.18 – Modifikation 111
Tabelle E.19 – Softwareverifikation 112
Tabelle E.20 – Beurteilung der funktionalen Sicherheit 112