Anwendungsbeginn

Anwendungsbeginn dieser Norm ist ... .

Inhalt

Seite

Einleitung ... 13
1 Anwendungsbereich ... 15
2 Normative Verweisungen ... 16
3 Begriffe ... 17
4 Festgelegte *Sicherheitsfunktionen* ... 22
4.1 Allgemeines ... 22
4.2 *Sicherheitsfunktionen* ... 23
4.2.1 Grenzwerte ... 23
4.2.2 Stoppfunktionen ... 23
4.2.3 Weitere *Sicherheitsfunktionen* ... 24
5 Management der *funktionalen Sicherheit* ... 26
5.1 Zweck ... 26
5.2 Anforderungen für das Management der *funktionalen Sicherheit* ... 26
5.3 Entwicklungslebenszyklus eines *PDS(SR)* ... 26
5.4 Planung des Managements der *funktionalen Sicherheit* ... 27
5.5 *Spezifikation der Anforderungen an die Sicherheit* (*SRS*) für ein *PDS(SR)* ... 29
5.5.1 Allgemeines ... 29
5.5.2 Spezifikation der Anforderungen an die *Sicherheitsfunktionen* ... 29
5.5.3 Spezifikation der Anforderungen an die *Sicherheitsintegrität* ... 30
5.6 Architektur des Sicherheitssystems des *PDS(SR)* ... 31
5.6.1 Allgemeines ... 31
5.6.2 Anforderungen an die Architektur des Sicherheitssystems ... 31
6 Anforderungen an Entwurf und Entwicklung des *PDS(SR)* ... 33
6.1 Allgemeine Anforderungen ... 33
6.1.1 Wechsel des Betriebszustands ... 33
6.1.2 Entwurfsnormen ... 33
6.1.3 Realisierung ... 33
6.1.4 *Sicherheitsintegrität* und Fehlererkennung ... 33
6.1.5 *Sicherheitsfunktionen* und nicht sicherheitsbezogene Funktionen ... 33
6.1.6 *SIL* für mehrere *Sicherheitsfunktionen* innerhalb eines *PDS(SR)* ... 33
6.1.7 Integrierte Schaltkreise mit On-Chip-Redundanz ... 34
6.1.8 Anforderungen an die Software ... 34
6.1.9 Überprüfung der Anforderungen ... 34
6.1.10 Dokumentation des Entwurfs ... 35
6.2 Anforderungen an den *PDS(SR)*-Entwurf ... 35

Seite

6.2.1 Wesentliche und bewährte Sicherheitsgrundsätze ... 35
6.2.2 Anforderungen für die Abschätzung der Wahrscheinlichkeit von gefahrbringenden zufälligen Hardwareausfällen je Stunde (*PFH*) ... 35
6.2.3 Abschätzung des PFD-Werts mit einem gegebenen *PFH*-Wert ... 38
6.2.4 Strukturelle Einschränkungen ... 38
6.2.5 Abschätzung des *Anteils ungefährlicher Ausfälle (SFF)* ... 40
6.2.6 Anforderungen an die *systematische Sicherheitsintegrität* eines *PDS(SR)* und von *PDS(SR)-Teilsystemen* ... 41
6.2.7 Anforderungen an die elektromagnetische Störfestigkeit eines *PDS(SR)* ... 44
6.3 Verhalten bei der Erkennung von Fehlern ... 45
6.3.1 Fehlererkennung ... 45
6.3.2 Fehlertoleranz größer Null ... 45
6.3.3 Fehlertoleranz von Null ... 45
6.4 Zusätzliche Anforderungen für die Datenkommunikation ... 45
6.5 Anforderungen an Integration und Prüfung des *PDS(SR)* ... 46
6.5.1 Integration der Hardware ... 46
6.5.2 Integration der Software ... 46
6.5.3 Modifikationen bei der Integration ... 46
6.5.4 Durchzuführende Integrationsprüfungen ... 46
6.5.5 Prüfprotokoll ... 46
7 Anwenderdokumentation ... 46
7.1 Informationen und Anweisungen für eine sichere Anwendung eines *PDS(SR)* ... 47
8 *Verifikation* und *Validierung* ... 48
8.1 Allgemeines ... 48
8.2 *Verifikation* ... 48
8.3 *Validierung* ... 49
8.4 Dokumentation ... 49
9 Prüfanforderungen ... 49
9.1 Prüfplanung ... 49
9.2 Prüfdokumentation ... 49
10 Modifikation ... 50
10.1 Ziel ... 50
10.2 Anforderungen ... 50
10.2.1 Anforderungen an die Modifikation ... 50
10.2.2 Einflussanalyse ... 50
10.2.3 Berechtigung ... 50
10.2.4 Dokumentation ... 50
Anhang A (informativ) Aufgabenablaufplan ... 51
Anhang B (informativ) Beispiel für die Bestimmung der *PFH* ... 55
B.1 Allgemeines ... 55

Seite

B.2 Aufbau des Beispiel-*PDS(SR)* ... 55
B.2.1 Allgemeines ... 55
B.2.2 *Teilsystem* A/B ... 56
B.2.3 *Teilsystem* PS/VM ... 56
B.3 Bestimmung des *PFH*-Werts für das Beispiel-*PDS(SR)* ... 57
B.3.1 *Teilsystem* „A/B“ (Haupt-*Teilsystem*) ... 57
B.3.1.1 Zerlegung in Funktionsblöcke ... 57
B.3.1.2 Bestimmung der Ausfallraten der Funktionsblöcke ... 57
B.3.1.3 *Anteil ungefährlicher Ausfälle* ... 58
B.3.1.4 Faktor der *Ausfälle infolge gemeinsamer Ursache* $\beta_{A/B}$ ... 60
B.3.1.5 Zuverlässigkeitsmodell (Markov) ... 60
B.3.1.6 Berechnung des *PFH*-Werts ... 61
B.3.2 *Teilsystem* „PS/VM“ ... 62
B.3.2.1 Zerlegung in Funktionsblöcke ... 62
B.3.2.2 Ausfallraten der Funktionsblöcke ... 63
B.3.2.3 *Anteil ungefährlicher Ausfälle* ... 63
B.3.2.4 Faktor der *Ausfälle infolge gemeinsamer Ursache* $\beta_{PS/VM}$ ... 63
B.3.2.5 Zuverlässigkeitsmodell (Markov) ... 64
B.3.2.6 Berechnung des *PFH*-Werts ... 65
B.3.3 *PFH*-Wert der Sicherheitsfunktion STO des *PDS(SR)* ... 65
Anhang C (informativ) Verfügbare Datenbanken für Ausfallraten ... 66
C.1 Datenbanken ... 66
C.2 Hilfreiche Normen für den Bauelementeausfall ... 66
Anhang D (informativ) Fehlerlisten und Fehlerausschlüsse ... 68
D.1 Allgemeines ... 68
D.2 Anmerkungen zu Fehlerausschlüssen ... 68
D.2.1 Gültigkeit von Ausschlüssen ... 68
D.2.2 Zinn-Whisker-Wachstum ... 68
D.2.3 Kurzschlüsse von Teilen, die auf Leiterplatten montiert sind ... 69
D.3 Fehlermodelle ... 69
D.3.1 Leiter/Kabel ... 69
D.3.2 Leiterplatten/Baugruppen ... 69
D.3.3 Reihenklemmen ... 70
D.3.4 Mehrpoliger Steckverbinder ... 70
D.3.5 Elektromechanische Bauelemente ... 71
D.3.6 Transformatoren ... 71
D.3.7 Induktivitäten ... 71
D.3.8 Widerstände ... 71
D.3.9 Widerstandsnetzwerke ... 72

Seite

D.3.10 Potentiometer 72
D.3.11 Kondensatoren 72
D.3.12 Diskrete Halbleiter 72
D.3.13 Optokoppler 72
D.3.14 Nicht programmierbare integrierte Schaltkreise 73
D.3.15 Programmierbare und/oder komplexe integrierte Schaltkreise 73
D.3.16 Bewegungs- und Lagesensoren 74
Anhang E (informativ) Empfehlungen für die Verwendung der SMT-*Sicherheitsfunktion* in Anwendungen in explosionsfähigen Atmosphären 77
E.1 Allgemeines 77
E.1.1 Beispiel für die Einstufung und Definition von explosionsfähigen Atmosphären 77
E.1.2 Normen und Motorschutz in den Zonen explosionsfähiger Atmosphären 78
E.1.3 Anforderungen an den *Sicherheits-Integritätslevel* und die Fehlertoleranz der SMT-*Sicherheitsfunktion* 79
E.2 Nutzung der SMT-Sicherheitsfunktion für den Motorschutz durch Überwachung der Motorbelastung 80
E.2.1 Allgemeines 80
E.2.2 Beispiel für die *PDS(SR)*-Architektur für den Schutz eines Motors, der in einer explosionsfähigen Gasatmosphäre eingesetzt wird 81
E.2.3 Anforderungen für die Überwachung der Motorbelastung 81
E.3 Nutzung der SMT-*Sicherheitsfunktion* für die Motorschutzbetriebsart „d“ durch Überwachung der Motortemperatur 82
Anhang F (normativ) Anforderungen an die elektromagnetische Störfestigkeit eines *PDS(SR)* 84
F.1 Störfestigkeitsanforderungen – niederfrequente Störungen 84
F.2 Störfestigkeitsanforderungen – hochfrequente Störungen 86
Literaturhinweise 89

Bilder

Bild 1 – Funktionselemente eines *PDS(SR)* 16
Bild 2 – Entwicklungslebenszyklus eines *PDS(SR)* 27
Bild B.1 – Beispiel-*PDS(SR)* 55
Bild B.2 – *Teilsysteme* des *PDS(SR)* 56
Bild B.3 – Funktionsblöcke des *Teilsystems* A/B 57
Bild B.4 – Zuverlässigkeitsmodell (Markov) des Teilsystems A/B 60
Bild B.5 – Funktionsblöcke des *Teilsystems* PS/VM 62
Bild B.6 – Zuverlässigkeitsmodell (Markov) des *Teilsystems* PS/VM 64
Bild E.1 – *PDS(SR)* mit dem CDM im sicheren Bereich und mit der Motorschutzbetriebsart „e“ 81
Bild E.2 – *PDS(SR)* mit dem CDM in der Gefahrenzone und mit der Motorschutzbetriebsart „e“ 81
Bild E.3 – Mindestwerte für die Zeit t_E des Motors als Funktion des Anzugsstromverhältnisses I_A/I_N 82
Bild E.4 – Beispiel für ein Belastungs-/Drehzahlprofil, das bei einer Prüfung für einen Induktionsmotor eines *PDS(SR)* mit der SMT-*Sicherheitsfunktion* aufgestellt wurde 82

Seite

Bild E.5 – *PDS(SR)* mit dem CDM in sicheren Bereich und mit der Motorschutzbetriebsart „d“ 83

Bild E.6 – *PDS(SR)* mit dem CDM in der Gefahrenzone und mit der Motorschutzbetriebsart „d“ 83

Tabellen

Tabelle 3-1 – Alphabetisches Verzeichnis der Begriffe 17

Tabelle 6-1 – *Sicherheits-Integritätslevel*: Ausfallgrenzwerte für eine *Sicherheitsfunktion* eines *PDS(SR)* 35

Tabelle 6-2 – Hardware-*Sicherheitsintegrität*: Strukturelle Einschränkungen für sicherheitsbezogene *Teilsysteme* des Typs A 40

Tabelle 6-3 – Hardware-*Sicherheitsintegrität*: Strukturelle Einschränkungen für sicherheitsbezogene *Teilsysteme* des Typs B 40

Tabelle B.1 – Bestimmung des *DC*-Faktors des *Teilsystems* A/B 59

Tabelle B.2 – Ergebnisse der Berechnung der *PFH*-Werte für *Teilsystem* A/B 62

Tabelle B.3 – Bestimmung des *DC*-Faktors des *Teilsystems* PS/VM 63

Tabelle B.4 – Ergebnisse der Berechnung der *PFH*-Werte für *Teilsystem* PS/VM 65

Tabelle D.1 – Leiterplatten/Baugruppen 69

Tabelle D.2 – Reihenklemme 70

Tabelle D.3 – Mehrpoliger Steckverbinder 70

Tabelle D.4 – Elektromechanische Bauelemente (z. B. Relais, Schaltrelais) 71

Tabelle D.5 – Optokoppler 72

Tabelle D.6 – Nicht programmierbare integrierte Schaltkreise 73

Tabelle D.7 – Programmierbare und/oder komplexe integrierte Schaltkreise 73

Tabelle D.8 – Bewegungs- und Lagesensoren 74

Tabelle D.9 – Bewegungs- und Lagesensoren 76

Tabelle E.1 – Einstufung und Definition von explosionsfähigen Atmosphären 78

Tabelle E.2 – Normen und Motorschutz in explosionsfähiger Atmosphäre 78

Tabelle E.3 – Anforderungen an den *Sicherheits-Integritätslevel* und die Fehlertoleranz der SMT-*Sicherheitsfunktion* 80

Tabelle F.1 – Mindestanforderungen an die Störfestigkeit für Spannungsabweichungen, Spannungseinbrüche und kurzzeitige Unterbrechungen 84

Tabelle F.2 – Mindestanforderungen an die Störfestigkeit für Spannungsabweichungen, Spannungseinbrüche und kurzzeitige Unterbrechungen an Netzspannungsanschlüssen mit einer Bemessungsspannung über 1 000 V eines *PDS(SR)* 85

Tabelle F.3 – Störfestigkeitsanforderungen – hochfrequente Störungen 86

Tabelle F.4 – Allgemeine Frequenzbereiche für ortsveränderliche Sender und ISM für die Prüfung abgestrahlter Störgrößen 87

Tabelle F.5 – Allgemeine Frequenzbereiche für ortsveränderliche Sender und ISM für die Prüfung leitungsgeführter Störgrößen 88