Inhalt

Seite

Vorwort ... 2
Einleitung ... 6
1 Anwendungsbereich ... 7
2 Normative Verweisungen ... 8
3 Begriffe ... 9
4 Festgelegte *Sicherheitsfunktionen* ... 14
4.1 Allgemeines ... 14
4.2 *Sicherheitsfunktionen* ... 14
4.2.1 Grenzwerte ... 14
4.2.2 Stoppfunktionen ... 15
4.2.3 Andere *Sicherheitsfunktionen* ... 16
5 Management der *funktionalen Sicherheit* ... 17
5.1 Ziel ... 17
5.2 Sicherheitslebenszyklus eines *PDS(SR)* ... 17
5.3 Planung der *funktionalen Sicherheit* ... 18
5.4 *Spezifikation der Sicherheitsanforderungen* (SRS) für ein *PDS(SR)* ... 20
5.4.1 Allgemeines ... 20
5.4.2 Spezifikation der Anforderungen an die *Sicherheitsfunktionen* ... 20
5.4.3 Spezifikation der Anforderungen zur *Sicherheitsintegrität* ... 21
6 Anforderungen an Entwurf und Entwicklung eines *PDS(SR)* ... 21
6.1 Allgemeine Anforderungen ... 21
6.1.1 Wechsel des Betriebszustandes ... 21
6.1.2 Normen ... 22
6.1.3 Realisierung ... 22
6.1.4 *Sicherheitsintegrität* und Fehlererkennung ... 22
6.1.5 *Sicherheitsfunktionen* und nicht sicherheitsbezogene Funktionen ... 22
6.1.6 Anzuwendender *SIL* ... 22
6.1.7 Anforderungen an die Software ... 22
6.1.8 Überprüfung der Anforderungen ... 23
6.1.9 Dokumentation von Entwurf und Entwicklung ... 23
6.2 Anforderungen an den *PDS(SR)*-Entwurf ... 23
6.2.1 Anforderungen an die Wahrscheinlichkeit von gefahrbringenden zufälligen Hardwareausfällen je Stunde (PFH) ... 23
6.2.2 Strukturelle Einschränkungen ... 25
6.2.3 Abschätzung des *Anteils sicherer Ausfälle (SFF)* ... 27
6.2.4 Anforderungen an die systematische *Sicherheitsintegrität* eines *PDS(SR)* und von *PDS(SR)-Teilsystemen* ... 28
6.2.5 Anforderungen an die elektromagnetische Störfestigkeit eines *PDS(SR)* ... 30
6.3 Verhalten bei der Erkennung von Fehlern ... 31

Seite

6.3.1 Fehlererkennung ... 31
6.3.2 Fehlertoleranz größer Null ... 31
6.3.3 Fehlertoleranz von Null ... 31
6.4 Zusätzliche Anforderungen an die Datenkommunikation ... 31
6.5 Anforderungen an Integration und Prüfung des *PDS(SR)* ... 32
6.5.1 Integration der Hardware ... 32
6.5.2 Integration der Software ... 32
6.5.3 Modifikationen bei der Integration ... 33
6.5.4 Durchzuführende Integrationsprüfungen ... 33
6.5.5 Prüfprotokoll ... 33
7 Anwenderdokumentation ... 33
7.1 Informationen und Anweisungen für eine sichere Anwendung eines *PDS(SR)* ... 33
8 *Verifikation* und *Validierung* ... 35
8.1 Allgemeines ... 35
8.2 *Verifikation* ... 35
8.3 *Validierung* ... 35
8.4 Dokumentation ... 35
9 Prüfanforderungen ... 35
9.1 Prüfplanung ... 35
9.2 Prüfdokumentation ... 36
10 Modifikation ... 36
10.1 Ziel ... 36
10.2 Anforderungen ... 36
10.2.1 Anforderungen an die Modifikation ... 36
10.2.2 Einflussanalyse ... 36
10.2.3 Berechtigung ... 37
10.2.4 Dokumentation ... 37

Anhang A (informativ) Aufgabenablaufplan ... 38
Anhang B (informativ) Beispiel für die Bestimmung der *PFH* ... 42
Anhang C (informativ) Verfügbare Datenbanken für Ausfallraten ... 53
Anhang D (informativ) Fehlerlisten und Fehlerausschlüsse ... 55
Literaturhinweise ... 65
Anhang ZA (normativ) Normative Verweisungen auf internationale Publikationen mit ihren entsprechenden europäischen Publikationen ... 67
Anhang ZZ (informativ) Zusammenhang mit grundlegenden Anforderungen von EG-Richtlinien ... 69
Anhang ZZA (informativ) Zusammenhang mit grundlegenden Anforderungen von Richtlinie 98/37/EG ... 69
Anhang ZZB (informativ) Zusammenhang mit grundlegenden Anforderungen von Richtlinie 2006/42/EG ... 69

Seite

Bild 1 – Funktionselemente eines *PDS(SR)* ... 8
Bild 2 – Entwicklungslebenszyklus eines *PDS(SR)* ... 18
Bild 3 – Architekturen der Datenkommunikation: a) Weißer Kanal, b) Schwarzer Kanal ... 32
Bild B.1 – Beispiel-*PDS(SR)* ... 42
Bild B.2 – *Teilsysteme* des *PDS(SR)* ... 43
Bild B.3 – Funktionsblöcke des *Teilsystems* A/B ... 44
Bild B.4 – Zuverlässigkeitsmodell (Markov) des Teilsystems A/B ... 47
Bild B.5 – Funktionsblöcke des *Teilsystems* PS/VM ... 49
Bild B.6 – Zuverlässigkeitsmodell (Markov) des Teilsystems PS/VM ... 51

Tabelle 1 – Alphabetisches Verzeichnis der Begriffe ... 9
Tabelle 2 – *Sicherheits-Integritätslevel*: Ausfallgrenzwerte für eine *Sicherheitsfunktion* eines *PDS(SR)* ... 23
Tabelle 3 – Hardware-*Sicherheitsintegrität*: Strukturelle Einschränkungen der Architektur für sicherheitsbezogene *Teilsysteme* des Typs A ... 27
Tabelle 4 – Hardware-*Sicherheitsintegrität*: Strukturelle Einschränkungen der Architektur für sicherheitsbezogene *Teilsysteme* des Typs B ... 27
Tabelle B.1 – Bestimmung des *DC*-Faktors des *Teilsystems* A/B ... 46
Tabelle B.2 – Ergebnisse der Berechnung der *PFH*-Werte für *Teilsystem* A/B ... 49
Tabelle B.3 – Bestimmung des *DC*-Faktors des *Teilsystems* PS/VM ... 50
Tabelle B.4 – Ergebnisse der Berechnung der *PFH*-Werte für *Teilsystem* PS/VM ... 52
Tabelle D.1 – Leiter/Kabel ... 56
Tabelle D.2 – Leiterplatten/Baugruppen ... 56
Tabelle D.3 – Reihenklemme ... 57
Tabelle D.4 – Mehrpoliger Steckverbinder ... 57
Tabelle D.5 – Elektromagnetische Bauelemente (z. B. Relais, Schaltrelais) ... 58
Tabelle D.6 – Transformatoren ... 58
Tabelle D.7 – Induktivitäten ... 59
Tabelle D.8 – Widerstände ... 59
Tabelle D.9 – Widerstandsnetzwerke ... 59
Tabelle D.10 – Potentiometer ... 60
Tabelle D.11 – Kondensatoren ... 60
Tabelle D.12 – Diskrete Halbleiter (z. B. Dioden, Zener-Dioden, Transistoren, Triacs, GTO-Thyristoren, IGBTs, Spannungsregler, Schwingquarze, Fototransistoren, Leuchtdioden (LEDs)) ... 60
Tabelle D.13 – Optokoppler ... 61
Tabelle D.14 – Nicht programmierbare integrierte Schaltkreise ... 61
Tabelle D.15 – Programmierbare und/oder komplexe integrierte Schaltkreise ... 62
Tabelle D.16 – Bewegungs- und Lagesensoren ... 62