Inhalt

Seite

Vorwort ... 2

Einleitung ... 5

1 Anwendungsbereich ... 7

2 Normative Verweisungen ... 10

3 Begriffe und Abkürzungen ... 10

4 Übereinstimmung mit dieser Norm ... 10

5 Dokumentation ... 11

6 Management der funktionalen Sicherheit ... 11

7 Anforderungen zum E/E/PES-Sicherheitslebenszyklus ... 11

7.1 Allgemeines ... 11

7.2 Spezifikation der E/E/PES-Sicherheitsanforderungen ... 15

7.3 Planung der Validierung der sicherheitsbezogenen E/E/PE-Systeme bezüglich der Sicherheit ... 18

7.4 E/E/PES-Entwurf und Entwicklung ... 18

7.5 E/E/PES-Integration ... 36

7.6 E/E/PES-Betriebs- und Instandhaltungsverfahren ... 37

7.7 Validierung der E/E/PES bezüglich der Sicherheit ... 38

7.8 E/E/PES-Modifikation ... 40

7.9 E/E/PES-Verifikation ... 40

8 Beurteilung der funktionalen Sicherheit ... 42

Anhang A (normativ) Verfahren und Maßnahmen für sicherheitsbezogene E/E/PE-Systeme: Beherrschung von Ausfällen während des Betriebs ... 43

A.1 Allgemeines ... 43

A.2 Sicherheitsintegrität der Hardware ... 44

A.3 Systematische Sicherheitsintegrität ... 54

Anhang B (normativ) Verfahren und Maßnahmen für sicherheitsbezogene E/E/PE-Systeme: Vermeidung von systematischen Ausfällen während der verschiedenen Phasen des Lebenszyklus ... 59

Anhang C (normativ) Diagnosedeckungsgrad und Anteil ungefährlicher Ausfälle ... 69

C.1 Berechnung von Diagnosedeckungsgrad und dem Anteil ungefährlicher Ausfälle eines Teilsystems ... 69

C.2 Bestimmung von Diagnosedeckungsfaktoren ... 70

Literaturhinweise ... 72

Anhang ZA (normativ) Normative Verweisungen auf internationale Publikationen mit ihren entsprechenden europäischen Publikationen ... 73

Bilder

Bild 1 – Gesamtrahmen dieser Norm ... 9

Bild 2 – E/E/PES-Sicherheitslebenszyklus (in der Realisierungsphase) ... 12

Bild 3 – Beziehung zwischen der IEC 61508-2 und IEC 61508-3 und ihrer Anwendungsbereiche ... 13

Bild 4 – Beziehung zwischen den Hardware- und Software-Architekturen von programmierbarer Elektronik ... 20

Bild 5 – Beispiel der Begrenzung der Sicherheitsintegrität der Hardware für eine einkanalige

Seite
Sicherheitsfunktion 25
Bild 6 – Beispiel der Begrenzung der Sicherheitsintegrität der Hardware für eine mehrkanalige Sicherheitsfunktion 27

Tabellen

Tabelle 1 – Überblick – Realisierungsphase des E/E/PES-Sicherheitslebenszyklus 14
Tabelle 2 – Sicherheitsintegrität der Hardware: Einschränkungen aufgrund der Architektur für sicherheitsbezogene Typ A-Teilsysteme 24
Tabelle 3 – Sicherheitsintegrität der Hardware: Einschränkungen aufgrund der Architektur für sicherheitsbezogene Typ B-Teilsysteme 24
Tabelle A.1 – Fehler oder Ausfälle, die während des Betriebs erkannt oder zur Bestimmung des Anteils ungefährlicher Ausfälle analysiert werden müssen 45
Tabelle A.2 – Elektrische Teilsysteme 47
Tabelle A.3 – Elektronische Teilsysteme 47
Tabelle A.4 – Verarbeitungseinheiten 48
Tabelle A.5 – Unveränderliche Speicherbereiche 48
Tabelle A.6 – Veränderliche Speicherbereiche 49
Tabelle A.7 – E/A-Einheiten und Schnittstellen (externe Kommunikation) 49
Tabelle A.8 – Datenwege (interne Kommunikation) 50
Tabelle A.9 – Energieversorgung 50
Tabelle A.10 – Programmablauf (Watchdog) 51
Tabelle A.11 – Lüftung und Beheizungssystem (falls notwendig) 51
Tabelle A.12 – Takt 52
Tabelle A.13 – Kommunikation und Massenspeicher 52
Tabelle A.14 – Sensoren 53
Tabelle A.15 – Stellglieder (Aktoren) 53
Tabelle A.16 – Verfahren und Maßnahmen zur Beherrschung von durch den Hardwareentwurf und den Softwareentwurf verursachten systematischen Ausfällen 55
Tabelle A.17 – Verfahren und Maßnahmen zur Beherrschung von durch umgebungsbedingte Beanspruchung oder Einflüsse verursachten systematischen Ausfällen 56
Tabelle A.18 – Verfahren und Maßnahmen zur Beherrschung von systematischen Ausfällen während des Betriebs 57
Tabelle A.19 – Wirksamkeit von Verfahren und Maßnahmen zur Beherrschung von systematischen Ausfällen 58
Tabelle B.1 – Empfehlungen zur Vermeidung von Irrtümern während der Spezifikation der E/E/PES-Anforderungen (siehe 7.2) 61
Tabelle B.2 – Empfehlungen zur Vermeidung von Fehlern während des E/E/PES-Entwurfs und der Entwicklung (siehe 7.4) 62
Tabelle B.3 – Empfehlungen zur Vermeidung von Fehlern während der E/E/PES-Integration (siehe 7.5) 63
Tabelle B.4 – Empfehlungen zur Vermeidung von Fehlern und Ausfällen während der E/E/PES-Betriebs- und Instandhaltungsverfahren (siehe 7.6) 64
Tabelle B.5 – Empfehlungen zur Vermeidung von Fehlern während der Validierung der E/E/PES bezüglich der Sicherheit (siehe 7.7) 65
Tabelle B.6 – Wirksamkeit von Verfahren und Maßnahmen zur Vermeidung von systematischen Ausfällen 66