

Deutsche Fassung

Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme –
Teil 2: Anforderungen an sicherheitsbezogene elektrische/elektronische/programmierbare elektronische Systeme

Inhalt

	Seite
Einleitung	4
1 Anwendungsbereich	6
2 Normative Verweisungen	9
3 Begriffe und Abkürzungen	9
4 Übereinstimmung mit dieser Norm	9
5 Dokumentation	9
6 Management der funktionalen Sicherheit	10
7 Anforderungen des Sicherheitslebenszyklus des E/E/PE-Systems	10
7.1 Allgemeines	10
7.2 Entwurfsanforderungen des E/E/PE-Systems	14
7.3 Planung der Validierung der Sicherheit des E/E/PE-Systems	17
7.4 Entwurf und Entwicklung des E/E/PE-Systems	17
7.5 Integration des E/E/PE-Systems	39
7.6 Betriebs- und Instandhaltungsverfahren des E/E/PE-Systems	40
7.7 Validierung der Sicherheit des E/E/PE-Systems	42
7.8 Modifikation des E/E/PE-Systems	43
7.9 Verifikation des E/E/PE-Systems	44
8 Beurteilung der funktionalen Sicherheit	45
Anhang A (normativ) Verfahren und Maßnahmen für sicherheitsbezogene E/E/PE-Systeme: Beherrschung von Ausfällen während des Betriebs	46
A.1 Allgemeines	46
A.2 Sicherheitsintegrität der Hardware	47
A.3 Systematische Sicherheitsintegrität	58
Anhang B (normativ) Verfahren und Maßnahmen für sicherheitsbezogene E/E/PE-Systeme: Vermeidung von systematischen Ausfällen während der verschiedenen Phasen des Lebenszyklus	63
Anhang C (normativ) Diagnosedeckungsgrad und Anteil sicherer Ausfälle	73
C.1 Berechnung von Diagnosedeckungsgrad und dem Anteil sicherer Ausfälle eines Hardwareelements	73
C.2 Bestimmung von Diagnosedeckungsfaktoren	74
Anhang D (normativ) Sicherheitshandbuch für konforme Objekte	76

	Seite
D.1 Allgemeines	76
D.2 Inhalte	76
Anhang E (normativ) Besondere Architekturanforderungen für integrierte Schaltkreise (ICs) mit On-Chip-Redundanz	78
E.1 Allgemeines	78
E.2 Zusätzliche Anforderungen für On-Chip-Redundanz in SIL3	80
E.3 β -Faktor.....	80
Anhang F (informativ) Verfahren und Maßnahmen für ASICs: Vermeidung von systematischen Ausfällen	83
Literaturhinweise	92
Bilder	
Bild 1 – Gesamtrahmen dieser Norm.....	8
Bild 2 – Sicherheitslebenszyklus des E/E/PE-Systems (in der Realisierungsphase).....	11
Bild 3 – ASIC-Entwicklungslebenszyklus (V-Modell)	12
Bild 4 – Beziehung zwischen IEC 61508-2 und IEC 61508-3 und ihre Anwendungsbereiche.....	12
Bild 5 (siehe 7.4.4.2.3): Beispiel: Bestimmung des maximalen SIL für eine festgelegte Architektur	25
Bild 6 – Beispiel (siehe 7.4.4.2.4): Bestimmung des maximalen SIL für eine festgelegte Architektur	29
Bild 7 – Architekturen für Datenkommunikation.....	39
Tabellen	
Tabelle 1 – Überblick – Realisierungsphase des Sicherheitslebenszyklus des E/E/PE-Systems	13
Tabelle 2 – Maximal zulässiger Sicherheits-Integritätslevel für eine Sicherheitsfunktion, die von einem sicherheitsbezogenen Typ A-Element ausgeführt wird	24
Tabelle 3 – Maximal zulässiger Sicherheits-Integritätslevel für eine Sicherheitsfunktion, die von einem sicherheitsbezogenen Typ B-Element ausgeführt wird	24
Tabelle A.1 – Fehler oder Ausfälle, die während des Betriebs erkannt oder zur Bestimmung des Anteils sicherer Ausfälle analysiert werden müssen	47
Tabelle A.2 – Elektrische Elemente	50
Tabelle A.3 – Elektronische Elemente	51
Tabelle A.4 – Verarbeitungseinheiten.....	52
Tabelle A.5 – Unveränderliche Speicherbereiche.....	52
Tabelle A.6 – Veränderliche Speicherbereiche.....	53
Tabelle A.7 – E/A-Einheiten und Schnittstellen (externe Kommunikation)	54
Tabelle A.8 – Datenwege (interne Kommunikation)	54
Tabelle A.9 – Energieversorgung	55
Tabelle A.10 – Programmablauf (Watchdog).....	55
Tabelle A.11 – Takt	56
Tabelle A.12 – Kommunikation und Massenspeicher.....	56
Tabelle A.13 – Sensoren.....	57
Tabelle A.14 – Stellglieder (Aktoren)	57

	Seite
Tabelle A.15 – Verfahren und Maßnahmen zur Beherrschung von durch den Hardwareentwurf verursachten systematischen Ausfällen	59
Tabelle A.16 – Verfahren und Maßnahmen zur Beherrschung von durch umgebungsbedingte Beanspruchung oder Einflüsse verursachten systematischen Ausfällen.....	59
Tabelle A.17 – Verfahren und Maßnahmen zur Beherrschung von systematischen Ausfällen während des Betriebs.....	61
Tabelle A.18 – Wirksamkeit von Verfahren und Maßnahmen zur Beherrschung von systematischen Ausfällen.....	61
Tabelle B.1 – Verfahren und Maßnahmen zur Vermeidung von Irrtümern während der Spezifikation von E/E/PE-Entwurfsanforderungen (siehe 7.2)	65
Tabelle B.2 – Verfahren und Maßnahmen zur Vermeidung von Fehlern während Entwurf und Entwicklung des E/E/PE-Systems (siehe 7.4).....	66
Tabelle B.3 – Verfahren und Maßnahmen zur Vermeidung von Fehlern während der Integration des E/E/PE-Systems (siehe 7.5).....	67
Tabelle B.4 – Verfahren und Maßnahmen von Fehlern und Ausfällen während der Betriebs- und Instandhaltungsverfahren des E/E/PE-Systems (siehe 7.6)	68
Tabelle B.5 – Verfahren und Maßnahmen zur Vermeidung von Fehlern während der Validierung der Sicherheit des E/E/PE-Systems (siehe 7.7)	68
Tabelle B.6 – Wirksamkeit von Verfahren und Maßnahmen zur Vermeidung von systematischen Ausfällen.....	70