

## Inhalt

	Seite
Vorwort.....	2
Einleitung .....	6
1 Anwendungsbereich .....	8
2 Normative Verweisungen .....	11
3 Begriffe und Abkürzungen .....	11
4 Übereinstimmung mit dieser Norm .....	11
5 Dokumentation .....	11
6 Management der funktionalen Sicherheit.....	12
7 Anforderungen des Sicherheitslebenszyklus des E/E/PE-Systems.....	12
7.1 Allgemeines .....	12
7.2 Spezifikation der Anforderungen an den Entwurf des E/E/PE-Systems .....	16
7.3 Planung der Validierung der Sicherheit des E/E/PE-Systems .....	19
7.4 Entwurf und Entwicklung des E/E/PE-Systems.....	19
7.5 Integration des E/E/PE-Systems .....	41
7.6 Betriebs- und Instandhaltungsverfahren für das E/E/PE-System .....	42
7.7 Validierung der Sicherheit des E/E/PE-Systems.....	44
7.8 Modifikation des E/E/PE-Systems.....	45
7.9 Verifikation des E/E/PE-Systems .....	46
8 Beurteilung der funktionalen Sicherheit.....	47
Anhang A (normativ) Verfahren und Maßnahmen für sicherheitsbezogene E/E/PE-Systeme – Beherrschung von Ausfällen während des Betriebs .....	48
A.1 Allgemeines .....	48
A.2 Sicherheitsintegrität der Hardware .....	49
A.3 Systematische Sicherheitsintegrität .....	61
Anhang B (normativ) Verfahren und Maßnahmen für sicherheitsbezogene E/E/PE-Systeme – Vermeidung von systematischen Ausfällen während der verschiedenen Phasen des Lebenszyklus.....	66
Anhang C (normativ) Diagnosedeckungsgrad und Anteil sicherer Ausfälle.....	75
C.1 Berechnung des Diagnosedeckungsgrads und des Anteils sicherer Ausfälle eines Hardwareelements .....	75
C.2 Bestimmung von Diagnosedeckungsfaktoren.....	76
Anhang D (normativ) Sicherheitshandbuch für konforme Objekte.....	78
D.1 Allgemeines .....	78
D.2 Inhalte.....	78
Anhang E (normativ) Besondere Architektur Anforderungen an integrierte Schaltkreise (ICs) mit On- Chip-Redundanz.....	80
E.1 Allgemeines .....	80
E.2 Zusätzliche Anforderungen an On-Chip-Redundanz bei SIL 3.....	83

	Seite
E.3 $\beta$ -Faktor.....	83
Anhang F (informativ) Verfahren und Maßnahmen für ASICs – Vermeidung von systematischen Ausfällen .....	86
F.1 Allgemeines .....	86
F.2 Hinweise: Verfahren und Maßnahmen .....	87
Literaturhinweise .....	95
Anhang ZA (normativ) Normative Verweisungen auf internationale Publikationen mit ihren entsprechenden europäischen Publikationen.....	97
<b>Bilder</b>	
Bild 1 – Gesamtrahmen der Normenreihe IEC 61508 .....	10
Bild 2 – Sicherheitslebenszyklus des E/E/PE-Systems (in der Realisierungsphase).....	13
Bild 3 – ASIC-Entwicklungslebenszyklus (V-Modell) .....	14
Bild 4 – Beziehung zwischen und Anwendungsbereich von IEC 61508-2 und IEC 61508-3.....	14
Bild 5 – Bestimmung des maximalen SIL für eine festgelegte Architektur (sicherheitsbezogenes E/E/PE-Teilsystem, das aus einer Anzahl hintereinandergeschalteter Elemente besteht, siehe 7.4.4.2.3) .....	28
Bild 6 – Bestimmung des maximalen SIL für eine festgelegte Architektur (sicherheitsbezogenes E/E/PE-Teilsystem, das aus zwei Teilsystemen X und Y besteht, siehe 7.4.4.2.4).....	30
Bild 7 – Architekturen für Datenkommunikation.....	41
<b>Tabellen</b>	
Tabelle 1 – Überblick – Realisierungsphase des Sicherheitslebenszyklus des E/E/PE-Systems .....	15
Tabelle 2 – Maximal zulässiger Sicherheits-Integritätslevel für eine Sicherheitsfunktion, die von einem sicherheitsbezogenen Typ A-Element oder Teilsystem ausgeführt wird.....	26
Tabelle 3 – Maximal zulässiger Sicherheits-Integritätslevel für eine Sicherheitsfunktion, die von einem sicherheitsbezogenen Typ B-Element oder Teilsystem ausgeführt wird.....	27
Tabelle A.1 – Fehler oder Ausfälle, die bei der Quantifizierung der Auswirkungen zufälliger Hardwareausfälle angenommen werden müssen oder bei der Bestimmung des Anteils sicherer Ausfälle berücksichtigt werden müssen.....	49
Tabelle A.2 – Elektrische Bauteile .....	52
Tabelle A.3 – Elektronische Bauteile .....	53
Tabelle A.4 – Verarbeitungseinheiten.....	54
Tabelle A.5 – Unveränderliche Speicherbereiche.....	55
Tabelle A.6 – Veränderliche Speicherbereiche.....	56
Tabelle A.7 – E/A-Einheiten und Schnittstellen (externe Kommunikation).....	57
Tabelle A.8 – Datenwege (interne Kommunikation) .....	57
Tabelle A.9 – Energieversorgung .....	58
Tabelle A.10 – Programmablauf (Watchdog).....	58
Tabelle A.11 – Takt .....	59
Tabelle A.12 – Kommunikation und Massenspeicher.....	59
Tabelle A.13 – Sensoren.....	60
Tabelle A.14 – Stellglieder (Aktoren) .....	60

	Seite
Tabelle A.15 – Verfahren und Maßnahmen zur Beherrschung von durch den Hardwareentwurf verursachten systematischen Ausfällen .....	62
Tabelle A.16 – Verfahren und Maßnahmen zur Beherrschung von durch umgebungsbedingte Beanspruchung oder Einflüsse verursachten systematischen Ausfällen.....	62
Tabelle A.17 – Verfahren und Maßnahmen zur Beherrschung von systematischen Ausfällen während des Betriebs.....	64
Tabelle A.18 – Wirksamkeit von Verfahren und Maßnahmen zur Beherrschung von systematischen Ausfällen.....	64
Tabelle B.1 – Verfahren und Maßnahmen zur Vermeidung von Irrtümern während der Spezifikation der Anforderungen an den Entwurf des E/E/PE-Systems (siehe 7.2).....	67
Tabelle B.2 – Verfahren und Maßnahmen zur Vermeidung von Fehlern während Entwurf und Entwicklung des E/E/PE-Systems (siehe 7.4).....	68
Tabelle B.3 – Verfahren und Maßnahmen zur Vermeidung von Fehlern während der Integration des E/E/PE-Systems (siehe 7.5).....	69
Tabelle B.4 – Verfahren und Maßnahmen zur Vermeidung von Fehlern und Ausfällen während der Betriebs- und Instandhaltungsverfahren für das E/E/PE-System (siehe 7.6) .....	70
Tabelle B.5 – Verfahren und Maßnahmen zur Vermeidung von Fehlern während der Validierung der Sicherheit des E/E/PE-Systems (siehe 7.7) .....	70
Tabelle B.6 – Wirksamkeit von Verfahren und Maßnahmen zur Vermeidung von systematischen Ausfällen.....	72