

Inhalt

	Seite
Europäisches Vorwort.....	2
Einleitung	9
1 Anwendungsbereich	10
2 Normative Verweisungen	11
3 Begriffe	13
4 Festgelegte <i>Sicherheits-Teilfunktionen</i>	20
4.1 Allgemeines	20
4.2 <i>Sicherheits-Teilfunktionen</i>	21
4.2.1 Allgemeines	21
4.2.2 Grenzwerte	22
4.2.3 Stopp-Funktionen	22
4.2.4 Überwachungsfunktionen	24
4.2.5 Ausgangsfunktionen – Sichere Bremsenansteuerung (en: safe brake control, SBC)	25
5 Management der <i>funktionalen Sicherheit</i>	25
5.1 Zweck	25
5.2 Anforderungen für das Management der <i>funktionalen Sicherheit</i>	26
5.3 Entwicklungslebenszyklus eines <i>PDS(SR)</i>	26
5.4 Planung des Managements der <i>funktionalen Sicherheit</i> des <i>PDS(SR)</i>	27
5.5 <i>Spezifikation der Anforderungen an die Sicherheit (SRS) für ein PDS(SR)</i>	29
5.5.1 Allgemeines	29
5.5.2 <i>Spezifikation der Anforderungen an die Sicherheits-Teilfunktionen</i>	29
5.5.3 <i>Spezifikation der Anforderungen an die Sicherheitsintegrität</i>	30
5.6 Architekturspezifikation des Sicherheitssystems des <i>PDS(SR)</i>	31
5.6.1 Allgemeines	31
5.6.2 Anforderungen an die Architekturspezifikation des Sicherheitssystems.....	31
6 Anforderungen an Entwurf und Entwicklung eines <i>PDS(SR)</i>	32
6.1 Allgemeine Anforderungen	32
6.1.1 Wechsel des Betriebszustands	32
6.1.2 Entwurfsnormen	32
6.1.3 Realisierung.....	32
6.1.4 <i>Sicherheitsintegrität</i> und Fehlererkennung	32
6.1.5 <i>Sicherheits-Teilfunktionen</i> und nicht sicherheitsbezogene Teilfunktionen.....	33
6.1.6 <i>SIL</i> für mehrere <i>Sicherheits-Teilfunktionen</i> innerhalb eines <i>PDS(SR)</i>	33
6.1.7 Integrierte Schaltkreise mit On-Chip-Redundanz.....	34
6.1.8 Anforderungen an die Software.....	34
6.1.9 Dokumentation des Entwurfs	34
6.2 Anforderungen an den Entwurf des <i>PDS(SR)</i>	34
6.2.1 Wesentliche und bewährte Sicherheitsgrundsätze	34
6.2.2 Anforderungen für die Abschätzung der Wahrscheinlichkeit von gefahrbringenden zufälligen Hardwareausfällen je Stunde (<i>PFH</i>)	34
6.2.3 Strukturelle Einschränkungen	37
6.2.4 Abschätzung des <i>Anteils ungefährlicher Ausfälle (SFF)</i>	39

6.2.5	Anforderungen an die <i>systematische Sicherheitsintegrität</i> eines PDS(SR) und von PDS(SR)-Teilsystemen	39
6.2.6	Entwurfsanforderungen an die elektromagnetische Störfestigkeit eines PDS(SR)	42
6.2.7	Entwurfsanforderungen für die Wärmeunempfindlichkeit eines PDS(SR)	43
6.2.8	Entwurfsanforderungen für die mechanische Unempfindlichkeit eines PDS(SR)	43
6.3	Verhalten bei der Erkennung von Fehlern	43
6.3.1	Fehlererkennung	43
6.3.2	Fehlertoleranz größer null	43
6.3.3	Fehlertoleranz von null	43
6.4	Zusätzliche Anforderungen für die Datenkommunikation	43
6.5	Anforderungen an Integration und Prüfung des PDS(SR)	44
6.5.1	Integration der Hardware	44
6.5.2	Integration der Software	44
6.5.3	Modifikationen während der Integration	44
6.5.4	Durchzuführende Integrationsprüfungen	44
6.5.5	Prüfprotokoll	44
7	Anwenderdokumentation	44
7.1	Allgemeines	44
7.2	Informationen und Anweisungen für eine sichere Anwendung eines PDS(SR)	45
8	<i>Verifikation</i> und <i>Validierung</i>	46
8.1	Allgemeines	46
8.2	<i>Verifikation</i>	47
8.3	<i>Validierung</i>	47
8.4	Dokumentation	47
9	Prüfanforderungen	47
9.1	Prüfplanung	47
9.2	Funktionsprüfungen	47
9.3	Prüfung der elektromagnetischen Störfestigkeit	48
9.3.1	Allgemeines	48
9.3.2	Vorgesehene elektromagnetische Umgebung	48
9.3.3	Leistungskriterium (<i>Fail-safe-Zustand – FS</i>)	48
9.4	Prüfung der Wärmeunempfindlichkeit	49
9.4.1	Allgemeines	49
9.4.2	Thermische Funktionsprüfung	49
9.4.3	Thermische Bauteilprüfung	49
9.5	Prüfung der mechanischen Unempfindlichkeit	49
9.5.1	Allgemeines	49
9.5.2	Schwingprüfung	49
9.5.3	Schockprüfung	49
9.5.4	Leistungskriterium für Prüfungen der mechanischen Unempfindlichkeit (<i>Fail-safe-Zustand – FS</i>)	49
9.6	Prüfdokumentation	50
10	Modifikation	50
10.1	Ziel	50

	Seite
10.2 Anforderungen	50
10.2.1 Allgemeines	50
10.2.2 Anforderung einer Modifikation	50
10.2.3 Einflussanalyse.....	50
10.2.4 Berechtigung	50
10.2.5 Dokumentation	51
Anhang A (informativ) Aufgabenablaufplan	52
Anhang B (informativ) Beispiel für die Abschätzung der <i>PFH</i>	57
B.1 Allgemeines	57
B.2 Aufbau des Beispiel- <i>PDS(SR)</i>	57
B.2.1 Allgemeines	57
B.2.2 <i>Teilsystem A/B</i>	58
B.2.3 <i>Teilsystem PS/VM</i>	59
B.3 Bestimmung des <i>PFH</i> -Werts für das Beispiel- <i>PDS(SR)</i>	59
B.3.1 <i>Teilsystem „A/B“ (Haupt-Teilsystem)</i>	59
B.3.1.1 Zerlegung in Funktionsblöcke	59
B.3.1.2 Bestimmung der Ausfallraten der Funktionsblöcke	60
B.3.1.3 <i>Anteil ungefährlicher Ausfälle</i>	61
B.3.1.4 Faktor der <i>Ausfälle infolge gemeinsamer Ursache</i> $\beta_{A/B}$	62
B.3.1.5 Zuverlässigkeitsmodell (Markov).....	62
B.3.1.6 Berechnung des <i>PFH</i> -Werts	64
B.3.2 <i>Teilsystem „PS/VM“</i>	65
B.3.2.1 Zerlegung in Funktionsblöcke	65
B.3.2.2 Ausfallraten der Funktionsblöcke	66
B.3.2.3 <i>Anteil ungefährlicher Ausfälle</i>	66
B.3.2.4 Faktor der <i>Ausfälle infolge gemeinsamer Ursache</i> $\beta_{PS/VM}$	67
B.3.2.5 Zuverlässigkeitsmodell (Markov).....	67
B.3.2.6 Berechnung des <i>PFH</i> -Werts	69
B.3.3 <i>PFH</i> -Wert der <i>Sicherheits-Teilfunktion STO</i> des <i>PDS(SR)</i>	69
B.4 Verringerung von <i>DC</i> und <i>SFF</i> in Abhängigkeit vom Prüfintervall	70
Anhang C (informativ) Verfügbare Datenbanken für Ausfallraten	71
C.1 Datenbanken	71
C.2 Hilfreiche Normen für den Bauelementeausfall.....	71
Anhang D (informativ) Fehlerlisten und Fehlerausschlüsse	73
D.1 Allgemeines	73
D.2 Anmerkungen zu Fehlerausschlüssen	73
D.2.1 Gültigkeit von Ausschlüssen	73
D.2.2 Zinn-Whisker-Wachstum	73
D.2.3 Kurzschlüsse von Teilen, die auf Leiterplatten montiert sind	74
D.3 Fehlermodelle	74
D.3.1 Leiter/Kabel	74
D.3.2 Leiterplatten/Baugruppen	74
D.3.3 Reihenklempen.....	75

	Seite
D.3.4 Mehrpoliger Steckverbinder	75
D.3.5 Elektromechanische Bauelemente.....	76
D.3.6 Transformatoren.....	76
D.3.7 Induktivitäten	76
D.3.8 Widerstände	76
D.3.9 Widerstandsnetzwerke	76
D.3.10 Potentiometer	77
D.3.11 Kondensatoren.....	77
D.3.12 Diskrete Halbleiter	77
D.3.13 Signalisierbauteile	77
D.3.14 Nicht programmierbare integrierte Schaltkreise.....	78
D.3.15 Programmierbare und/oder komplexe integrierte Schaltkreise.....	78
D.3.16 Bewegungs- und Lagerückführungssensoren	79
Anhang E (normativ) Anforderungen an die elektromagnetische Störfestigkeit eines <i>PDS(SR)</i>	83
E.1 Allgemeines.....	83
E.2 Anforderungen an die Störfestigkeit – niederfrequente Störungen.....	83
E.3 Anforderungen an die Störfestigkeit – hochfrequente Störungen.....	86
Anhang F (informativ) Abschätzung des PFD_{avg} -Werts für Anwendungen mit niedriger Anforderungsrate aus einem vorgegebenen <i>PFH</i> -Wert	90
F.1 Allgemeines.....	90
F.2 Abschätzung des PFD_{avg} -Werts für Anwendungen mit niedriger Anforderungsrate aus einem vorgegebenen <i>PFH</i> -Wert	90
Literaturhinweise	91
Anhang ZA (normativ) Normative Verweisungen auf internationale Publikationen mit ihren entsprechenden europäischen Publikationen	93
Bilder	
Bild 1 – Anlagen- und Funktionsteile eines <i>PDS(SR)</i>	11
Bild 2 – Aus <i>Sicherheits-Teilfunktionen</i> bestehende <i>Sicherheitsfunktion</i>	22
Bild 3 – Entwicklungslebenszyklus eines <i>PDS(SR)</i>	26
Bild B.1 – Beispiel- <i>PDS(SR)</i>	57
Bild B.2 – <i>Teilsysteme</i> des <i>PDS(SR)</i>	58
Bild B.3 – Funktionsblöcke des <i>Teilsystems A/B</i>	60
Bild B.4 – Zuverlässigkeitsmodell (Markov) des <i>Teilsystems A/B</i>	63
Bild B.5 – Funktionsblöcke des <i>Teilsystems PS/VM</i>	66
Bild B.6 – Zuverlässigkeitsmodell (Markov) des <i>Teilsystems PS/VM</i>	68
Tabellen	
Tabelle 1 – Verzeichnis der Begriffe	13
Tabelle 2 – Beispiel für die Bestimmung des <i>SIL</i> aus der Hardware- und Software-Unabhängigkeit.....	33
Tabelle 3 – <i>Sicherheits-Integritätslevel</i> : Ausfallgrenzwerte für eine <i>Sicherheits-Teilfunktion</i> eines <i>PDS(SR)</i>	35
Tabelle 4 – Höchster zulässiger <i>Sicherheits-Integritätslevel</i> für eine <i>Sicherheits-Teilfunktion</i> , die von einem sicherheitsbezogenen <i>Teilsystem</i> des Typs A ausgeführt wird	38
Tabelle 5 – Höchster zulässiger <i>Sicherheits-Integritätslevel</i> für eine <i>Sicherheits-Teilfunktion</i> , die von einem sicherheitsbezogenen <i>Teilsystem</i> des Typs B ausgeführt wird	39
Tabelle A.1 – Entwurfs- und Entwicklungsverfahren für <i>PDS(SR)</i>	52

	Seite
Tabelle B.1 – Bestimmung des <i>DC</i> -Faktors des <i>Teilsystems A/B</i>	61
Tabelle B.2 – Ergebnisse der Berechnung der <i>PFH</i> -Werte für <i>Teilsystem A/B</i>	65
Tabelle B.3 – Bestimmung des <i>DC</i> -Faktors des <i>Teilsystems A/B</i>	66
Tabelle B.4 – Ergebnisse der Berechnung der <i>PFH</i> -Werte für <i>Teilsystem PS/VM</i>	69
Tabelle D.1 – Leiterplatten/Baugruppen	74
Tabelle D.2 – Reihenklemme	75
Tabelle D.3 – Mehrpoliger Steckverbinder	75
Tabelle D.4 – Elektromechanische Bauelemente (z. B. Relais, Schaltrelais)	76
Tabelle D.5 – Signalisierbauteile	77
Tabelle D.6 – Nicht programmierbare integrierte Schaltkreise	78
Tabelle D.7 – Programmierbare und/oder komplexe integrierte Schaltkreise.....	78
Tabelle D.8 – Bewegungs- und Lagerückführungssensoren	79
Tabelle E.1 – Mindestanforderungen an die Störfestigkeit für Spannungsabweichungen, Spannungseinbrüche und kurzzeitige Unterbrechungen	84
Tabelle E.2 – Mindestanforderungen an die Störfestigkeit von <i>PDS(SR)</i> für Spannungsabweichungen, Spannungseinbrüche und kurzzeitige Unterbrechungen an Netzspannungsanschlüssen mit einer Bemessungsspannung über 1 000 V	85
Tabelle E.3 – Anforderungen an die Störfestigkeit – hochfrequente Störungen	86
Tabelle E.4 – Allgemeine Frequenzbereiche für ortsveränderliche Sender und ISM für die Prüfung abgestrahlter Störgrößen.....	88
Tabelle E.5 – Allgemeine Frequenzbereiche für ortsveränderliche Sender und ISM für die Prüfung leitungsführter Störgrößen.....	89