

Inhalt

	Seite
Europäisches Vorwort.....	6
Einleitung	8
1 Anwendungsbereich	9
2 Normative Verweisungen	10
3 Begriffe und Abkürzungen	10
3.1 Begriffe	10
3.2 Abkürzungen	21
4 Übergeordnete Rahmenbedingungen dieses Dokuments	22
5 Anforderungen an die Entwicklung sicherheitsbezogener elektronischer Systeme	24
5.1 Einleitung	24
5.2 Der Qualitätsmanagementprozess	24
5.3 Der Sicherheitsmanagementprozess	27
6 Anforderungen an Elemente mit anderem Lebenszyklus	37
6.1 Einleitung	37
6.2 Verwendung bereits existierender Betrachtungseinheiten	38
6.3 Sicherheitsbezogene Tools für elektronische Systeme	40
6.4 Physische Sicherheit und IT-Sicherheit.....	42
7 Der Sicherheitsnachweis: Struktur und Inhalt	43
7.1 Struktur des Sicherheitsnachweises	43
7.2 Der Technische Sicherheitsbericht.....	44
7.3 Generische und spezifische Sicherheitsnachweise	54
7.4 Festlegungen für den Sicherheitsnachweis für eine spezifische Anwendung	54
7.5 Beziehungen zu anderen Sicherheitsnachweisen	55
8 Systemsicherheitsanerkennung und folgende Phasen	56
8.1 Prozess der Systemsicherheitsanerkennung	56
8.2 Betrieb, Instandhaltung und Leistungsüberwachung	60
8.3 Veränderung und Umrüstung	60
8.4 Stilllegung und Entsorgung	60
Anhang A (normativ) Sicherheits-Integritätslevel	61
A.1 Einleitung	61
A.2 Sicherheitsanforderungen	61
A.3 Sicherheitsintegrität	62
A.4 Bestimmung der Anforderungen an die Sicherheitsintegrität.....	63
A.4.1 Allgemeines	63
A.4.2 Risikobewertung	64
A.4.3 Gefährdungsbeherrschung.....	67
A.4.4 Bestimmung und Behandlung neuer aus dem Entwurf hervorgegangener Fehler	72
A.5 Zuweisung von SILs	72
A.5.1 Allgemeine Aspekte	72
A.5.2 Beziehung zwischen SIL und zugehöriger TFFR.....	74

	Seite
Anhang B (normativ) Management von Fehlzuständen für sicherheitsbezogene Funktionen	76
B.1 Einleitung.....	76
B.2 Allgemeine Konzepte	76
B.2.1 Offenbarungszeit und Ausfallreaktionszeit.....	76
B.2.2 Kombination zweier unabhängiger Betrachtungseinheiten.....	78
B.3 Ausfallauswirkungen	78
B.3.1 Auswirkungen von Einzelausfällen.....	78
B.3.2 Einflüsse zwischen Betrachtungseinheiten.....	80
B.3.3 Offenbarung von Einzelausfällen	85
B.3.4 Aktion nach Offenbarung (Beibehalten des sicheren Zustands)	87
B.3.5 Auswirkungen von Mehrfachausfällen	89
B.3.6 Schutz gegen systematische Fehler	92
Anhang C (normativ) Identifizierung der Fehlzustandsarten von Hardware-Bauteilen	93
C.1 Einleitung.....	93
C.2 Allgemeines Verfahren.....	93
C.3 Das Verfahren für integrierte Schaltkreise	93
C.4 Das Verfahren für Bauteile mit unverlierbaren physischen Eigenschaften.....	94
C.5 Allgemeine Vorkehrungen zu den Bauteil-Fehlzustandsarten.....	94
Anhang D (informativ) Beispiel für die THR/TFFR/FR-Aufteilung und SIL-Zuweisung.....	113
Anhang E (normativ) Techniken und Maßnahmen für die Vermeidung von systematischen Fehlern und die Beherrschung von zufälligen Ausfällen und systematischen Fehlern.....	115
E.1 Einleitung.....	115
E.2 Tabellen der Techniken und Maßnahmen	117
Anhang F (informativ) Anleitungen für anwenderprogrammierbare integrierte Schaltungen.....	124
F.1 Einleitung.....	124
F.1.1 Zweck.....	124
F.1.2 Terminologie und Kontext	124
F.2 UPIC-Lebenszyklus.....	125
F.2.1 Allgemeines.....	125
F.2.2 Organisation, Rollen, Verantwortlichkeiten und Kompetenzen des Personals.....	128
F.2.3 UPIC-Anforderungen.....	128
F.2.4 UPIC-Architektur und -Entwurf.....	128
F.2.5 Entwurf der Logik-Komponenten.....	129
F.2.6 Kodierung der Logik-Komponenten	129
F.2.7 Verifikation der Logik-Komponenten.....	129
F.2.8 Physische Implementierung des UPIC	129
F.2.9 UPIC-Integration.....	130
F.2.10 UPIC-Validierung.....	130
F.2.11 Anforderungen für die Verwendung von bereits existierenden Logik-Komponenten	130
F.3 Detaillierte technische Anforderungen für UPICs	130
F.3.1 Anleitung für die Sicherheitsarchitektur	130

	Seite
F.3.2 Schutz gegen zufällige Fehlzustände – Architekturprinzipien	130
F.3.3 Schutz gegen systematische Fehler (Techniken/Maßnahmen)	131
Anhang G (informativ) Änderungen in diesem Dokument im Vergleich zu EN 50129:2003	141
Anhang ZZ (informativ) Zusammenhang zwischen dieser Europäischen Norm und den grundlegenden Anforderungen der Richtlinie EU 2008/57/EG [2008 ABI. L191].....	145
Literaturhinweise	146
Bilder	
Bild 1 – Anwendungsbereich der wichtigsten CENELEC-Normen für Bahnanwendungen	10
Bild 2 – Struktur der EN 50129	23
Bild 3 – Beispiel des Systemlebenszyklus (aus EN 50126-1:2017)	26
Bild 4 – Beispiel der Anteile Entwurf und Validierung im Systemlebenszyklus	28
Bild 5 – Unabhängigkeit der Rollen für unterschiedliche SILs	30
Bild 6 – Struktur des Sicherheitsnachweises	43
Bild 7 – Struktur des Technischen Sicherheitsberichts	45
Bild 8 – Beispiele für die unterschiedliche Verwendung von Sicherheitsnachweisen	56
Bild 9 – Beispiele verschiedener Prozesse für die Sicherheitsanerkennung	59
Bild A.1 – Sicherheitsanforderungen und Sicherheitsintegrität	61
Bild A.2 – Übersicht über den Gesamtprozess	64
Bild A.3 – Definition von Gefährdungen in Bezug auf Systemgrenzen	66
Bild A.4 – Beispiel eines Gefährdungsbeherrschungsprozesses	68
Bild A.5 – Behandlung von CCFs durch FTA	70
Bild A.6 – Beziehung zwischen SILs und Techniken	74
Bild B.1 – Offenbarungszeit und Ausfallreaktionszeit	76
Bild B.2 – Beherrschung von Einzel- und Mehrfachausfällen	80
Bild B.3 – Die Unabhängigkeit beeinträchtigende Einflussfaktoren	84
Bild B.4 – Offenbarung und sicherheitsgerichtete Ausfallreaktion von Einzelausfällen – „fail-safety“ durch mindestens zwei Betrachtungseinheiten	88
Bild B.5 – Offenbarung und sicherheitsgerichtete Ausfallreaktion von Einzelausfällen – „fail-safety“ durch sicherheitsgerichtete Ausfallreaktion	88
Bild C.1 – Fehlzustand in einem Vierpolwiderstand	96
Bild D.1 – Beispiel für THR/TFFR/FR-Aufgliederung und zugehöriger SIL-Zuweisung	113
Bild F.1 – UPIC-Architektur	125
Bild F.2 – UPIC-Entwicklungskontext	125
Bild F.3 – Beispiel für einen UPIC-Entwicklungslebenszyklus	126
Bild F.4 – Beispiel für einen UPIC-Entwicklungslebenszyklus mit bereits existierenden Komponenten	127
Bild F.5 – UPIC-Entwicklungstechniken/-maßnahmen	132
Tabellen	
Tabelle 1 – Beispiel SRAC-Vorlage	36
Tabelle A.1 – SIL-Tabelle	74
Tabelle B.1 – Maßnahmen zur Offenbarung von Ausfällen in integrierten Schaltkreisen durch zyklische Online-Prüfungen	90

	Seite
Tabelle C.1 – Widerstände	95
Tabelle C.2 – Kondensatoren.....	96
Tabelle C.3 – Elektromagnetische Bauteile	97
Tabelle C.4 – Dioden.....	101
Tabelle C.5 – Transistoren	102
Tabelle C.6 – Gesteuerte Gleichrichter	104
Tabelle C.7 – Überspannungsschutz	105
Tabelle C.8 – Optoelektronische Bauelemente	106
Tabelle C.9 – Filter	108
Tabelle C.10 – Verbindungszubehör.....	109
Tabelle C.11 – Sicherungen	110
Tabelle C.12 – Schalter und Taster.....	110
Tabelle C.13 – Lampen	111
Tabelle C.14 – Batterien.....	111
Tabelle C.15 – Wandler (Transducer)/Sensoren (nicht solche mit internen elektronischen Schaltungen)	112
Tabelle E.1 – Sicherheitsplanung und Qualitätssicherungstätigkeiten	117
Tabelle E.2 – Sicherheitsanforderungsspezifikation	117
Tabelle E.3 – Sicherheitsorganisation.....	118
Tabelle E.4 – Architektur des Systems, des Subsystems oder der Einrichtung	118
Tabelle E.5 – Entwurfsmerkmale	120
Tabelle E.6 – Ausfall- und Gefährdungsanalysemethoden.....	121
Tabelle E.7 – Entwurf und Entwicklung des Systems, des Subsystems oder der Einrichtung.....	122
Tabelle E.8 – Sicherheitsverifizierung und -validierung des Systems, des Subsystems und der Einrichtung	122
Tabelle E.9 – Anwendung, Betrieb und Instandhaltung	123
Tabelle F.1 – Beispiel für die in jeder Phase zu erstellende Dokumentation.....	127
Tabelle F.2 – Vereinfachte Techniken/Maßnahmen zum Schutz gegen systematische Fehler.....	132
Tabelle F.3 – Entwurf und Verifizierung (einschließlich aller Aktivitäten vor der Synthese).....	133
Tabelle F.4 – Synthese.....	133
Tabelle F.5 – Platzierung, Verfolgung und Generierung des Layouts	134
Tabelle F.6 – Beschreibung der Techniken für den Entwurf.....	134
Tabelle F.7 – Beschreibung der Techniken für die Synthese	138
Tabelle F.8 – Beschreibung der Techniken für Platzierung, Verfolgung und Generierung des Layout.....	139
Tabelle G.1 – Abschnitte und Unterabschnitte – Entsprechung zu EN 50129:2003	141
Tabelle G.2 – Bilder und Tabellen – Entsprechung zu EN 50129:2003	144
Tabelle ZZ.1 – Zusammenhang zwischen dieser Europäischen Norm, der TSI ZZS (VERORDNUNG (EU) Nr. 2016/919 vom 27. Mai 2016) und der Richtlinie 2008/57/EG	145