

## **Inhalt**

	Seite
Europäisches Vorwort.....	7
Einleitung .....	8
1 Anwendungsbereich .....	10
2 Normative Verweisungen .....	11
3 Begriffe .....	11
4 Abkürzungen .....	11
5 Sicherheitsprozess .....	12
5.1 Risikobewertung und Gefährdungsbeherrschung.....	12
5.2 A. Risikobewertung.....	13
5.2.1 Allgemeines .....	13
5.2.2 Durchführen der Risikobewertung.....	14
5.3 B. Ergebnis der Risikobewertung .....	14
5.4 C. Gefährdungsbeherrschung .....	14
5.5 D. Überprüfung der Risikobewertung .....	16
5.6 Verantwortlichkeiten .....	16
6 Nachweis der Sicherheit und der Sicherheitsabnahme .....	16
6.1 Einleitung.....	16
6.2 Prozess zum Nachweis der Sicherheit und zur Sicherheitsabnahme.....	17
6.3 Verantwortung für das Management des Sicherheitsnachweises .....	20
6.4 Modifikationen nach einer Sicherheitsabnahme .....	20
6.5 Abhängigkeiten zwischen Sicherheitsnachweisen.....	20
6.6 Beziehung zwischen Sicherheitsnachweisen und Systemarchitektur.....	21
7 Organisation und Unabhängigkeit Rollen.....	22
7.1 Allgemeines .....	22
7.2 Frühe Phasen des Lebenszyklus (Phasen 1 bis 4).....	23
7.3 Spätere Phasen des Lebenszyklus (ab Phase 5) .....	24
7.4 Kompetenz der Mitarbeiter .....	26
8 Risikobewertung .....	27
8.1 Einleitung.....	27
8.2 Risikoanalyse .....	27
8.2.1 Allgemeines .....	27
8.2.2 Das Risikomodell.....	27
8.2.3 Methoden der Auswirkungsanalyse .....	30
8.2.4 Expertenurteil .....	30
8.3 Risikoakzeptanzprinzipien und Risikobeurteilung .....	31
8.3.1 Anwenden der Regelwerke .....	31
8.3.2 Anwenden eines Referenzsystems .....	31
8.3.3 Anwenden der expliziten Risikoeinschätzung .....	32

	Seite
8.4 Anwenden der expliziten Risikoeinschätzung.....	33
8.4.1 Quantitativer Ansatz.....	33
8.4.1.1 Allgemeines.....	33
8.4.1.2 Für Unfälle geltende Sicherheitsziele .....	35
8.4.1.3 Tolerierbare Gefährdungsrate (THR).....	35
8.4.1.4 Verantwortlichkeiten.....	36
8.4.2 Variabilität bei der Anwendung von quantitativen Risikoeinschätzungen.....	36
8.4.2.1 Allgemeines.....	36
8.4.2.2 „Ungünstigstes Szenario“ .....	37
8.4.2.3 „Angemessene Einschätzungen“ .....	37
8.4.2.4 „Angemessene ungünstigster Fall“ .....	37
8.4.3 Qualitative und semi-quantitative Ansätze.....	38
9 Festlegung von Systemsicherheitsanforderungen.....	38
9.1 Allgemeines.....	38
9.2 Sicherheitsanforderungen .....	38
9.3 Kategorisierung von Sicherheitsanforderungen.....	39
9.3.1 Allgemeines.....	39
9.3.2 Funktionale Sicherheitsanforderungen .....	39
9.3.3 Technische Sicherheitsanforderungen .....	40
9.3.4 Kontextuelle Sicherheitsanforderungen.....	40
10 Aufteilung der funktionalen Sicherheitsintegritätsanforderungen .....	41
10.1 Ableitung und Aufteilung von Systemsicherheitsanforderungen .....	41
10.2 Funktionale Sicherheitsintegrität bei elektronischen Systemen.....	41
10.2.1 Ableitung von funktionalen Sicherheitsanforderungen für elektronische Systeme.....	41
10.2.2 Aufteilung von Sicherheitsanforderungen .....	41
10.2.3 Sicherheitsintegritätsfaktoren.....	44
10.2.4 Funktionale Sicherheitsintegrität und zufällige Fehler .....	44
10.2.5 Systematischer Aspekt der funktionalen Sicherheitsintegrität.....	45
10.2.6 Ausgewogene Anforderungen zur Beherrschung zufälliger und systematischer Fehler.....	45
10.2.7 SIL-Tabelle.....	46
10.2.8 SIL-Zuordnung .....	47
10.2.9 Aufteilung von TFFR nach der SIL-Zuordnung.....	47
10.2.10 Nachweis von quantifizierten Zielen .....	47
10.2.11 Anforderungen an die Basisintegrität.....	47
10.2.12 Verhinderung der falschen Verwendung von SIL .....	49
10.3 Sicherheitsintegrität bei nicht-elektronischen Systemen – Anwenden der Regelwerke.....	49
11 Entwurf und Implementierung .....	50
11.1 Einleitung.....	50
11.2 Ursachenanalyse.....	50

	Seite
11.3 Gefährdungsermittlung (detailliert).....	51
11.4 Analyse gemeinsamer Ursachen .....	51
Anhang A (informativ) ALARP, GAME, MEM .....	53
A.1 ALARP, GAME und MEM als Verfahren für die Festlegung von Risikoakzeptanzkriterien .....	53
A.2 ALARP (so niedrig wie vernünftigerweise in der Praxis praktikabel) .....	54
A.2.1 Allgemeines .....	54
A.2.2 Vertretbarkeit und ALARP .....	55
A.3 Globalement au Moins Equivalent (GAME)-Grundsatz.....	55
A.3.1 Kurzbeschreibung.....	55
A.3.2 Anwendung von GAME .....	56
A.3.2.1 Allgemeines .....	56
A.3.2.2 Grundlagen.....	56
A.3.2.3 Anwendung von GAME zur Entwicklung eines qualitativen Sicherheitsarguments.....	57
A.3.2.4 GAME mit Nutzung von quantitativen Risikozielen .....	57
A.4 Minimale endogene Mortalität (MEM) .....	57
Anhang B (informativ) Anwendung von Ausfall- und Unfallstatistiken für die Ableitung einer THR.....	59
Anhang C (informativ) Anleitung für die SIL-Zuordnung.....	61
Anhang D (informativ) Verfahren für die Aufteilung von Sicherheitszielen.....	63
D.1 Analyse des Systems und der Verfahren .....	63
D.2 Beispiel für ein qualitatives Aufteilungsverfahren.....	63
D.2.1 Allgemeines .....	63
D.2.2 Beispiel für ein qualitatives Verfahren für die Effizienz der Barriere .....	64
D.3 Beispiel für ein quantitatives Zuteilungsverfahren.....	66
D.3.1 Einleitung.....	66
D.3.2 Funktionen mit unabhängigen Mechanismen für die Fehlererkennung und sicherheitsgerichtete Ausfallreaktion .....	68
D.3.3 Funktion und unabhängige Barriere, die zusammen als Mechanismus der Fehlererkennung und sicherheitsgerichteten Ausfallreaktion wirken .....	70
D.3.4 Aufteilen eines als Wahrscheinlichkeit gegebenen Sicherheitszieles .....	71
D.3.5 Aufteilen eines „zeitbezogenen“ Sicherheitsziels .....	71
Anhang E (informativ) Häufige Fehler bei der Quantifizierung.....	73
E.1 Häufige Fehlanwendungen .....	73
E.2 Vermischen von Ausfallraten mit Wahrscheinlichkeiten.....	73
E.3 Verwendung von Formeln außerhalb ihres Anwendbarkeitsbereichs.....	74
Anhang F (informativ) Techniken/Methoden der Sicherheitsanalyse.....	75
Anhang G (informativ) Für die Systemsicherheit entscheidende Funktionen und Verantwortlichkeiten .....	78
Anhang ZZ (informativ) Zusammenhang zwischen dieser Europäischen Norm und den grundlegenden Anforderungen der EU-Richtlinie 2008/57/EG .....	83
Literaturhinweise.....	89

**Bilder**

Bild 1 – Das Sanduhrmodell .....	13
Bild 2 – Darstellung der Gefährdungen in Bezug auf die Systemgrenzen .....	15
Bild 3 – Beispiel für Sicherheitsabnahmeprozesse .....	19
Bild 4 – Beispiele für Abhängigkeiten zwischen Sicherheitsnachweisen .....	21
Bild 5 – Unabhängigkeit von Rollen in den frühen Phasen (Phasen 1 bis 4) des Lebenszyklus .....	24
Bild 6 – Unabhängigkeit der Rollen in den späteren Phasen des Lebenszyklus (ab Phase 5) .....	26
Bild 7 – Ein Beispiel eines Risikomodells .....	28
Bild 8 – Tolerierbare Raten in einem Risikomodellbeispiel .....	34
Bild 9 – Klassifikation von Anforderungen .....	39
Bild 10 – Zuteilung von funktionalen Sicherheitsanforderungen .....	42
Bild 11 – Kategorisierung von Sicherheitsintegritätsmaßnahmen .....	46
Bild 12 – Auswirkungen funktionaler Abhängigkeiten in einer Fehlerbaumanalyse .....	52
Bild A.1 – Differentielle Risikoaversion .....	58
Bild D.1 – Beispiel für ein qualitatives Aufteilungsverfahren .....	64
Bild D.2 – Interpretation von Ausfall- und Reparaturzeiten .....	67
Bild D.3 – Kombination von zwei Funktionen mit unabhängigen Mechanismen für die Fehlererkennung und sicherheitsgerichtete Ausfallreaktion .....	68
Bild D.4 – Zuordnung von Sicherheitsintegritätsanforderungen .....	69
Bild D.5 – Kombination von Funktion und unabhängiger Barriere, die zusammen als Mechanismus der Fehlererkennung und sicherheitsgerichteten Ausfallreaktion wirken .....	70
Bild D.6 – Beispiel für eine quantifizierte Aufteilung .....	72
Bild E.1 .....	73

**Tabellen**

Tabelle 1 – Beispiele für Gefährdungen .....	29
Tabelle 2 – SIL-bezogene quantitative und qualitative Maßnahmen .....	46
Tabelle A.1 – Übersicht über ALARP, GAME, MEM .....	53
Tabelle D.1 – Effizienz basierend auf den Ausfällen der Komponente .....	65
Tabelle D.2 – Effizienz basierend auf dem Wissen der Komponente .....	65
Tabelle D.3 – Effizienz basierend auf der Verwendung der Komponente .....	65
Tabelle D.4 – Effizienz basierend auf der Instandhaltung der Komponente .....	66
Tabelle F.1 – Techniken/Methoden der Sicherheitsanalyse .....	75
Tabelle F.2 – Verfahren/Methoden für BI und SIL .....	76
Tabelle G.1 – Funktionsspezifikation für Entwerfer .....	78
Tabelle G.2 – Funktionsspezifikation für Verifizierer .....	79
Tabelle G.3 – Funktionsspezifikation für Validierer .....	80
Tabelle G.4 – Funktionsspezifikation für den unabhängigen Sicherheitsbewerter .....	81
Tabelle G.5 – Funktionsspezifikation für Projektmanager .....	82

Tabelle ZZ.1 – Zusammenhang zwischen dieser Europäischen Norm, der TSI „Zugsteuerung, Zugsicherung und Signalgebung“ (KOMMISSION VERORDNUNG (EU) 2016/919 vom 24. Mai 2016) und der Richtlinie 2008/57/EG .....	83
Tabelle ZZ.2 – Zusammenhang zwischen dieser Europäischen Norm, der TSI „Lokomotiven und Personenwagen“ (VERORDNUNG (EU) Nr. 1302/2014 vom 18. November 2014) und der Richtlinie 2008/57/EG .....	86
Tabelle ZZ.3 – Zusammenhang zwischen dieser Europäischen Norm, der TSI „Energie“ (VERORDNUNG (EU) Nr. 1301/2014 vom 18. November 2014) und der Richtlinie 2008/57/EG.....	87
Tabelle ZZ.4 – Zusammenhang zwischen dieser Europäischen Norm, der TSI „Infrastruktur“ (VERORDNUNG (EU) Nr. 1299/2014 vom 18. November 2014) und der Richtlinie 2008/57/EG.....	88