

Deutsche Fassung

Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme –
Teil 5: Beispiele von Methoden für die Bestimmung von Sicherheits-Integritätsleveln

Inhalt

	Seite
Einleitung	4
2 Normative Verweisungen.....	8
3 Begriffe und Abkürzungen	8
Anhang A (informativ) Risiko und Sicherheitsintegrität – Allgemeine Konzepte	9
A.1 Allgemeines	9
A.2 Notwendige Risikominderung	9
A.2.1 Individuelles Risiko	10
A.2.2 Gesellschaftliche Risiken.....	10
A.2.3 Kontinuierliche Verbesserung.....	10
A.2.4 Risikoprofil	11
A.3 Die Rolle der sicherheitsbezogenen E/E/PE-Systeme	11
A.4 Sicherheitsintegrität	11
A.5 Betriebsarten und Bestimmung des SIL	12
A.5.1 Sicherheitsintegrität und Risikominderung für Anwendungen mit niedriger Anforderungsrate.....	12
A.5.2 Sicherheitsintegrität für Anwendungen in der Betriebsart mit hoher Anforderungsrate	14
A.5.3 Sicherheitsintegrität für Anwendungen in der Betriebsart mit kontinuierlicher Anforderung	15
A.5.4 Ausfälle infolge gemeinsamer und abhängiger Ursache.....	16
A.5.5 Sicherheits-Integritätslevel, bei Verwendung mehrerer Schichten eines Schutzes	17
A.6 Risiko und Sicherheitsintegrität	18
A.7 Sicherheits-Integritätslevel und Software-Sicherheits-Integritätslevel	18
A.8 Zuordnung von Sicherheitsanforderungen	19
A.9 Systeme zur Schadensbegrenzung.....	21
Anhang B (informativ) Auswahl von Methoden zur Bestimmung der Sicherheits-Integritätslevel.....	22
B.1 Allgemeines	22
B.2 Quantitative Methode der SIL-Bestimmung.....	22
B.3 Die Risikograph-Methode	23
B.4 Analyse der Schutzebenen (en.: Layer of Protection Analysis (LOPA))	23
Anhang C (informativ) Konzepte für ALARP und tolerierbares Risiko.....	25
C.1 Allgemeines	25
C.2 ALARP-Modell	25
C.2.1 Einleitung	25

	Seite
C.2.2 Grenzwert für das tolerierbare Risiko	26
Anhang D (informativ) Festlegung der Sicherheits-Integritätslevel: Eine quantitative Methode.....	28
D.1 Allgemeines	28
D.2 Allgemeine Methode	28
D.3 Beispielrechnung	29
Anhang E (informativ) Bestimmung der Sicherheits-Integritätslevel Risikograph-Methoden	31
E.1 Allgemeines	31
E.2 Aufbau des Risikographen.....	31
E.3 Kalibrierung.....	32
E.4 Mögliche andere Risikoparameter	33
E.5 Anwendung des Risikographen: allgemeines Schema	33
E.6 Beispiel eines Risikographen.....	34
Anhang F (informativ) Semi-quantitative Methode, Verwendung einer Analyse der Schutzebenen (LOPA)	38
F.1 Allgemeines	38
F.1.1 Beschreibung	38
F.1.2 Anhang Verweis.....	38
F.1.3 Beschreibung der Methode.....	38
F.2 Schadensereignis	38
F.3 Schweregrad.....	38
F.4 Auslösende Ursache.....	39
F.5 Eintrittswahrscheinlichkeit.....	39
F.6 Schutzebenen (PLs)	42
F.6.1 Allgemeines	42
F.6.2 Grundlegendes Steuerungssystem	42
F.6.3 Alarmer.....	42
F.7 Zusätzliche Schadensbegrenzungsmaßnahmen	43
F.8 Vorläufige Wahrscheinlichkeit für das Ereignis	43
F.9 Sicherheits-Integritätslevel (SILs).....	43
Anhang G (informativ) Festlegung der Sicherheits-Integritätslevel – Eine qualitative Vorgehensweise: Matrix des Ausmaßes des gefährlichen Vorfalls.....	45
Anhang G (informativ) Festlegung der Sicherheits-Integritätslevel – Eine qualitative Vorgehensweise: Matrix des Ausmaßes des gefährlichen Vorfalls.....	45
G.1 Allgemeines	45
G.2 Matrix des Ausmaßes des gefährlichen Vorfalls	45
Literaturhinweise	47
Bilder	
Bild 1 – Gesamtrahmen der Betrachtung dieser Norm.....	7
Bild A.1 – Risikominderung: allgemeine Konzepte (Betriebsart mit niedriger Anforderungsrate)	13
Bild A.2 – Risiko- und Sicherheitsintegritätskonzepte	13

Bild A.3 – Risikodarstellung zu Anwendungen mit hoher Anforderungsrate	15
Bild A.4 – Risikodarstellung zu Anwendungen mit kontinuierlichen Anforderungsrate	16
Bild A.5 – Darstellung von Ausfällen infolge gemeinsamer Ursache (CCFs) von Elementen im EUC- Leit- oder Steuerungssystem und Elementen im sicherheitsbezogenen E/E/PE-System	17
Bild A.6 – Gemeinsame Ursache zwischen zwei sicherheitsbezogenen E/E/PE-Systemen	18
Bild A.7 – Zuordnung der Sicherheitsanforderungen zu den sicherheitsbezogenen E/E/PE- Systemen, sicherheitsbezogenen Systemen anderer Technologie und externen Einrichtungen zur Risikominderung	20
Bild C.1 – Tolerierbares Risiko und ALARP	26
Bild D.1 – Zuordnung der Sicherheitsintegrität: Beispiel für eine sicherheitsbezogene Schutzeinrichtung	30
Bild E.1 – Risikograph: Allgemeine Darstellung	34
Bild E.2 – Risikograph: Beispiel (zeigt nur allgemeine Prinzipien auf)	34
Bild G.1 – Matrix des Ausmaßes des gefährlichen Vorfalls: Beispiel (stellt nur die allgemeinen Prinzipien dar).....	46
Tabellen	
Tabelle C.1 – Beispiel für die Risikoklassifizierung von Unfällen	27
Tabelle C.2 – Interpretation der Risikoklassen	27
Tabelle E.1 – Beispieldaten, die sich auf das Beispiel des Risikographen (Bild E.2) beziehen.....	35
Tabelle E.2 – Beispielkalibrierung eines allgemeinen Risikographen	36