

Inhaltsverzeichnis

1	Einleitung	1
2	Stand von Wissenschaft und Technik.....	5
2.1	Definition verwendeter Begriffe	5
2.2	Bisherige Arbeiten der GRS.....	12
2.3	Stellungnahme der RSK zum Einsatz rechnerbasierter Leittechnik.....	16
2.4	Fachvorträge	19
2.5	Fachliteratur.....	20
3	Überblick über nationale und internationale Normen und Standards.....	23
3.1	Allgemeine Standards und Normen	23
3.2	Nukleare Standards und Normen.....	24
3.2.1	Nationale Regelwerke, Standards und Normen	24
3.2.2	Internationale Standards und Normen	26
3.3	Nicht-nukleare Standards und Normen	28
4	Auswertung der relevanten Standards und Normen.....	31
4.1	System-Sicherheitslebenszyklus.....	31
4.1.1	Konzept	33
4.1.2	Definition des Anwendungsbereichs des Gesamtsystems	35
4.1.3	Gefährdungs- und Risikoanalyse	35
4.1.4	Zuordnung der Sicherheitsanforderungen.....	36
4.1.5	Gesamtplanung	38
4.1.6	Realisierung.....	38
4.1.7	Installation und Inbetriebnahme des Gesamtsystems	39
4.1.8	Validierung der Sicherheit des Gesamtsystems.....	41
4.1.9	Betrieb, Instandhaltung und Reparatur des Gesamtsystems	42
4.1.10	Modifikation und Nachrüstung des Gesamtsystems.....	43
4.1.11	Stilllegung und Entsorgung	44
4.2	Software-Sicherheitslebenszyklus	44
4.2.1	Management und Organisationsstruktur	47
4.2.2	Lebenszyklus, allgemeine Anforderungen	47
4.2.3	Software-Anforderungsspezifikation	48
4.2.4	Entwurf, Architektur, Entwicklung und Implementierung.....	48

4.2.5	Integration.....	50
4.2.6	Verifizierung.....	52
4.2.7	Validierung.....	52
4.3	Anforderungen an die Software	53
4.3.1	Personal und Management.....	57
4.3.2	Lebenszyklus.....	58
4.3.3	Sonstige Themen.....	63
4.4	Fazit.....	67
4.4.1	System-Sicherheitslebenszyklus.....	67
4.4.2	Software-Sicherheitslebenszyklus	68
4.4.3	Anforderungen an die Software	69
4.5	Vergleich kerntechnischer Kategorien und SIL	69
4.5.1	Beziehung zwischen Sicherheitsanforderungsstufe (SIL), Performance Level (PL) und Leittechnikategorien des übergeordneten deutschen Regelwerks.....	70
4.5.2	Herleitung einer Beziehung aufgrund der Klassifizierung nach verschiedenen Regelwerken.....	70
4.5.3	In den Normen angegebene Beziehung.....	74
4.5.4	Herleitung einer Beziehung aufgrund quantitativer Zuverlässigkeitswerte	75
4.5.5	Vergleich SIL und ASIL basierend auf in den Normen genannten Vorgehensweisen	80
4.5.6	Zusammenfassung	84
5	Qualifizierung.....	85
5.1	Anforderungen aus allgemeinen Normen.....	86
5.2	Anforderungen in der Kerntechnik	88
5.3	Anforderungen in der Automobilindustrie	89
5.4	Anforderungen beim Schienenverkehr.....	91
5.5	Anforderungen in der Wehrtechnik	94
5.6	Anforderungen in der Luftfahrt	95
5.7	Fazit.....	96
6	Zuverlässigkeitsbewertung.....	99
6.1	Qualitative Methoden.....	99
6.2	Quantitative Methoden.....	101

6.2.1	Metrik-Modelle auf Grundlage von Softwareeigenschaften	102
6.2.2	Stochastische Modelle auf Grundlage von Ausfalldaten.....	108
6.3	Anwendungsbeispiele	111
6.3.1	Einsatz von Software-Metriken und stochastischen Modellen für die Zuverlässigkeitsbewertung (ISTec)	111
6.3.2	Einsatz von Bayesschen Netzen zur Zuverlässigkeitsbewertung (STUK)	113
6.4	Diskussion der Zuverlässigkeitsbewertung	115
6.4.1	Nicht-nuklear	115
6.4.2	Übertragbarkeit der Methoden und Anforderungen auf die Kerntechnik	120
6.4.3	Fazit.....	123
7	Fazit	125
	Literaturverzeichnis.....	129
	Abbildungsverzeichnis.....	139
	Tabellenverzeichnis.....	141
	Abkürzungsverzeichnis.....	143
A	Definition verwendeter Begriffe.....	147
B	Beschreibung von Standards und Normen	173
B.1	Allgemeine Standards und Normen	173
B.2	Nukleare Regelwerke, Standards und Normen	186
B.3	Nicht-Nukleare Standards und Normen	216
C	Modelle zur Software-Entwicklung.....	237
C.1	Wasserfallmodell	237
C.2	V-Modell	238
C.3	Agil Scrum	239
D	Beschreibung von Methoden zur Zuverlässigkeitsbewertung	241
D.1	Software Failure Modes and Effects Analysis (SFMEA).....	241
D.2	Software Failure Modes, Effects and Criticality Analysis (SFMECA)	242

D.3	Software Fault Tree Analysis (SFTA).....	244
D.4	Software Common Cause Analysis (SCCA).....	246
D.5	Dynamic Flowgraph Methodology (DFM).....	250
D.6	Stochastische Modelle auf Grundlage von Ausfalldaten.....	251
E	Hauptkomponentenanalyse	263
F	Einsatz von Software-Metriken und stochastischen Modellen zur Zuverlässigkeitsbewertung (ISTec)	269
F.1	TELEPERM XS	269
F.2	Quantitative Bestimmung der Komplexität der Funktionsbausteine.....	270
F.3	Bestimmung des Komplexitätsvektors	274
F.4	Bestimmung der Zuverlässigkeit auf Grundlage der Komplexität	279
G	Einsatz von Bayesschen Netzen zur Zuverlässigkeitsbewertung (STUK)	283