

Inhalt

1	Verkehrssicherheit	9
1.1	Begriffe	9
1.1.1	Verkehr	9
1.1.2	Sicherheit	12
1.1.3	Gefahr	14
1.1.4	Schaden	15
1.1.5	Risiko	15
1.2	Psychologische Grundlagen	17
1.2.1	Grundlebensrisiko	17
1.2.2	Zusätzliche Lebensrisiken	18
1.2.3	Risikoakzeptanz	20
1.3	Rechtliche Grundlagen	23
1.3.1	Sicherheitsbestimmungen	29
1.3.1.1	Sicherheitsregeln für Schienenbahnen	31
1.3.1.2	Sicherheitsregeln für die übrigen Verkehrsmittel	34
1.3.2	Schutzbestimmungen	35
1.3.3	Schadensersatzbestimmungen	38
1.3.3.1	Verschuldenshaftung	38
1.3.3.2	Gefährdungshaftung	39
1.3.4	Sicherheitsorganisation	41
1.3.4.1	Sicherheitsorganisation nach dem Personenbeförderungsgesetz für Straßen- und U-Bahnen	43
1.3.4.2	Sicherheitsorganisation nach dem Bundesbahngesetz	46
1.3.5	Sicherheitsverantwortung	49
1.3.5.1	Sicherheit und Zuverlässigkeit	49
1.3.5.2	Produkthaftung	52
1.4	Technische Grundlagen	58
1.4.1	Fehler	58
1.4.1.1	Fehlereintritt	58
1.4.1.2	Fehlerursache	58
1.4.2	Fehlerauswirkungen	58
1.4.3	Ausfälle und Störungen	60
1.4.3.1	Ausfalleintritt	61
1.4.3.2	Ausfallursachen	62
1.4.3.3	Ausfallarten	62
1.4.4	Ausfallauswirkungen	62
1.4.4.1	Systeme mit nur einem sicheren Systemzustand	63

1.4.4.2	Systeme mit mehreren sicheren Systemzuständen	63
1.4.5	Ereignisverkettung	65
2	Sicherungsmethoden	69
2.1	Sicherungsmethoden gegen Fehler	71
2.1.1	Fehlerausschluß	72
2.1.1.1	Systemübergreifende Maßnahmen	72
2.1.1.2	Einzelmaßnahmen des Fehlerausschlusses	72
2.1.1.3	Beispiele für Einzelmaßnahmen des Fehlerausschlusses	75
2.1.2	Fehlerabwehr	86
2.1.2.1	Fehlerabwehr gegen Unterlassungen	86
2.1.2.2	Fehlerabwehr gegen Falschhandeln	89
2.1.3	Fehleroffenbarung	91
2.1.3.1	Fehleroffenbarung durch nachvollziehende Prüfung	91
2.1.3.2	Fehleroffenbarung durch Testverfahren	95
2.1.3.3	Fehleroffenbarung durch Beweisverfahren	100
2.1.4	Rechnergestützte Anwendung der Sicherungsmethoden gegen Fehler im spurgeführten Verkehr als Nachweis der Software-Sicherheit	101
2.1.4.1	Grundlagen	102
2.1.4.2	Allgemeine Nachweisanforderungen	103
2.1.4.3	Einzel-Nachweisanforderungen	104
2.1.4.4	Prinzipbeschreibung eines rechnergestützten Prüf- und Nachweissystems am Beispiel des Systems „ProTest“	109
2.1.4.5	Elemente eines rechnergestützten Prüf- und Nachweissystems	111
2.2	Sicherungsmethoden gegen Ausfälle	117
2.2.1	Ausfallausschluß	119
2.2.2	Begrenzung der Ausfallwahrscheinlichkeit	119
2.3	Sicherungsmethoden gegen Gefahren	121
2.3.1	Gefahrenausschluß	122
2.3.1.1	Direkter Gefahrenausschluß (einkanalige Fail-Safe-Technik)	122
	2.3.1.1.1 Ruhestromprinzip. 2.3.1.1.2 Sicherheitsschaltungen	
2.3.1.2	Signaltechnischer sicherer indirekter Gefahrenausschluß	162
	2.3.1.2.1 Einkanalig mit Fail-Safe-Überwachung der Nutzfunktion. 2.3.1.2.2 Zweikanalig mit Fail-Safe-Vergleicher paralleler Nutzfunktionen	
2.3.2	Begrenzung der Gefährdungswahrscheinlichkeit	177
2.3.2.1	Parallelredundante Schaltwerke gleichen Aufbaus	177
	2.3.2.1.1 Vergleicher-Systeme (nvn-Systeme)	
	2.3.2.1.2 Mehrheitsentscheidungssysteme (mvn-Systeme)	

2.3.2.2	Parallelredundante Schaltwerke mit Diversität	185
2.3.2.2.1	Diversität durch Aufbau. 2.3.2.2.2 Diversität durch Programm	
2.3.2.3	Prüffunktion mittels Testprogramm	189
2.3.2.3.1	Zeitmultiplexe Unterbrechung des Programmablaufes	
2.3.2.3.2	Ausführungsbeispiel für mitlaufende Prüfprogramme	
2.3.2.4	Software-Sicherheit	190
2.4	Sicherungsmethoden gegen Schäden	191
3	Sicherheitsbewertung	193
3.1	Kennwertebenen	193
3.1.1	Kennwertebene Fehler	194
3.1.2	Kennwertebene Ausfall	194
3.1.3	Kennwertebene Gefahr	197
3.1.4	Kennwertebene Unfall	198
3.1.5	Kennwertebene Unfallfolgen	200
3.2	Bewertungsverfahren	201
3.2.1	Ereigniswahrscheinlichkeit	201
3.2.2	Verhältnis von Aufwand und Ereigniswahrscheinlichkeit	202
3.2.3	Sicherheitsarbeit	207
3.2.3.1	Stochastisch-empirische Sicherheitsarbeit	207
3.2.3.2	Systematisch-prognostische Sicherheitsarbeit	208
3.2.3.3	Praktisch-aktuelle Sicherheitsarbeit	209
3.3	Wirtschaftlichkeit von Sicherheitsmaßnahmen	210
3.3.1	Voraussetzungen	210
3.3.2	Gesetzmäßigkeiten	211
3.3.3	Grenzen der wirtschaftlichen Bewertung	213
3.3.4	Zumutbarkeitsgrenzen für Sicherheitsmaßnahmen	217
Literatur	225
Sachverzeichnis	235