

Inhaltsverzeichnis

Abstract..... I

Kurzfassung..... III

1 **Einleitung, Aufgabenstellung und Zielsetzung..... 1**

1.1 Aufarbeitung des für das Vorhaben relevanten Standes von
Wissenschaft und Technik (Arbeitspaket 1) 2

1.2 Entwicklung eines Konzeptes zur Untersuchung von Softwarefehlern in
softwarebasierter Leittechnik (Arbeitspaket 2) 3

1.3 Entwicklung eines Konzeptes zur Validierung der Analyseergebnisse
zu den Auswirkungen von Softwarefehlern auf softwarebasierte
Leittechnikssysteme (Arbeitspaket 3)..... 4

2 **Ermittlung und Aufbereitung des für das Vorhaben relevanten
Standes von Wissenschaft und Technik..... 7**

2.1 Modelle zur Beschreibung der Fehlerausbreitung in softwarebasierten
Leittechnikssystemen 7

2.2 Für das Vorhaben relevante Regelwerksanforderungen an
softwarebasierte Leittechnik 10

2.2.1 Anforderungen an die Software in softwarebasierter Leittechnik..... 10

2.2.2 Anforderungen an die Datenkommunikationsnetzwerke
softwarebasierter Leittechnikssysteme 17

2.2.4 Relevante Aspekte der Zuverlässigkeitsuntersuchung
softwarebasierter Leittechnikssysteme 22

2.3 Fehlertoleranz in softwarebasierter Leittechnik 26

2.3.1 Überblick über Fehlertoleranzverfahren 26

2.3.2 Fehlererkennungsverfahren 27

2.3.3 Fehlerbehandlungsverfahren 29

2.4 Zuverlässigkeitsanalysemethoden in softwarebasierter Leittechnik..... 36

2.4.1 Software Failure Modes and Effects Analysis 38

2.4.2 Software Fault Tree Analysis (SFTA)..... 43

2.4.3 Event Tree Analysis (ETA)..... 46

2.4.4	Markov-Modell	47
2.4.5	Petri-Netze.....	49
2.4.6	Software Fault Injection (SFI).....	52
2.4.7	Software HAZOP	57
2.4.9	Softwaresicherheitsanalyse am Beispiel eines vollständig digitalen Reaktorschutzsystems aus Korea.....	64
2.4.10	Zusammenfassung und Schlussfolgerungen für das Vorhaben	72
2.5	Betriebserfahrung zur Ausbreitung von Softwarefehlern in softwarebasierten Leittechniksystemen	76
2.5.1	Fehlerbedingte sekundärseitige Lastabsenkung und nicht erfolgter Stabeinwurf.....	76
2.5.2	Baugruppenfehler in einer Brandmeldezentrale	78
2.5.3	Vorübergehende Unverfügbarkeit der Bedienstationen eines rechnerbasierten Informations- und Steuerungssystems	80
3	Entwicklung eines Konzeptes zur Untersuchung von Softwarefehlern in softwarebasierter Leittechnik	83
3.1	Einleitung.....	83
3.2	Generisches Modell/Generische Beschreibung eines softwarebasierten Leittechniksystems.....	84
3.3	Untersuchungsrahmen für das entwickelte Konzept	86
3.4	Spezifikation der Anwendungssoftware softwarebasierter Leittechniksysteme	87
3.5	Konzept zur Untersuchung von potenziellen Ausfällen in softwarebasierter Leittechnik	90
3.5.1	Überblick über das Analysekonzept.....	90
3.5.2	FMEA auf Ebene der elementaren Funktionsblöcke	92
3.5.3	Anwendungsbeispiele	96

4	Entwicklung eines Konzepts zur Validierung der Analyse- ergebnisse zu den Auswirkungen von Softwarefehlern in softwarebasierten Leitechniksystemen	103
4.1	Einleitung.....	103
4.2	Das Analyse- und Testsystem der GRS.....	104
4.3	Dynamische Simulationen zur Validierung des SFMEA- Analysekonzeptes.....	108
4.3.1	Prinzip der dynamischen Simulationen	108
4.3.2	Automatisierte SFMEA eines AND-EFB.....	109
4.3.3	SFMEA einer Leitechnikfunktion bestehend aus mehreren EFB	113
4.3.4	Ergänzende Aspekte zur Automatisierung des SFMEA-Konzepts	127
4.4	Zusammenfassung	128
5	Zusammenfassung und Schlussfolgerung.....	131
	Literatur.....	137
	Abbildungsverzeichnis.....	147
	Tabellenverzeichnis.....	151
A	Anhang: Ergebnisse von Simulationen weiterer Funktions- bausteine.....	153
A.1	OR-EFB.....	153
A.2	Limiter-EFB.....	154