

Inhaltsverzeichnis

1	Einleitung	9
1.1	Motivation	9
1.2	Zielsetzung	11
1.3	Aufbau	12
2	Stand der Technik	15
2.1	Sicherheitstechnische Grundlagenbetrachtungen für integrierte Schaltungen	15
2.2	FPGAs und ihr Einsatz in sicherheitsgerichteten Systemen	25
2.2.1	Aufbau eines FPGA	25
2.2.2	FPGA-Designmethodik	27
2.2.3	FPGA für sicherheitsgerichtete Anwendungen	27
2.3	Thermodynamische Grundlagen für integrierte Schaltungen	32
3	Konzept	37
3.1	Konzeptuelles Modell für ein komplettes auf CFv2SPP basierendes Rechnersystem	38
3.2	Systemarchitektur	39
3.2.1	Redundantes CFv2SPP-System	40
3.2.2	DistributedInputs	41
3.2.3	SafeMultiplexer	42
3.3	Isolierung einzelner OCR-Komponenten	43
3.4	Warme Redundanz	44
3.5	CCF-Vermeidungskonzept und SIL-Berechnungsmodell	46
4	Strukturelle Maßnahmen und Modelle zur Betrachtung von Fehlervermeidungs- und Fehlerbeherrschungsaspekten	49
4.1	I/Os-Trennung	50
4.2	Trennung des Taktmanagements	51
4.3	Trennung der Spannungsversorgung	53
4.4	Überwachung des Konfigurationsspeichers	54
4.5	Erhöhung des DC	57
4.5.1	Selbst-Tests	57
4.5.2	Implementierung der warmen Redundanz	58
4.5.3	Sicherer Multiplexer	60
4.5.4	Überwachung der Inputs	63

5	Ergebnisse und Evaluierung	65
5.1	Modellwertung	65
5.2	Thermodynamische Analyse	83
6	Wertung, Abgrenzung und Ausblick	95
7	Zusammenfassung	111
A	Anhang	113
A.1	Designverifikation	113
A.1.1	Verifikation der Isolierung auf dem Spartan 6	113
A.1.2	Verifikation der Isolierung auf dem Artix 7	114
A.2	β_{IC} -Faktor	116
A.3	λ -Berechnung gemäß dem MIL-HDBK-217F	119
A.4	λ -Berechnung gemäß dem Ansatz aus [HD12]	120
B	Literaturverzeichnis	123
	Eigene Publikationen	133