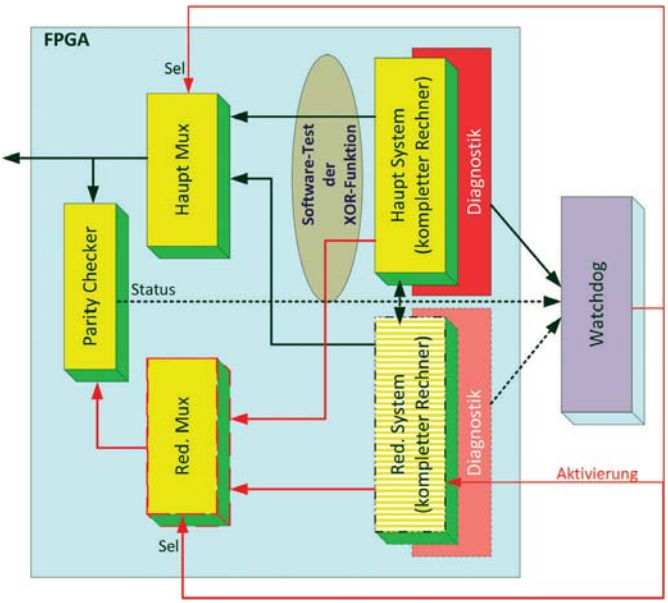
Emil Gracić

Beitrag zur Integration und Analyse sicherheitstechnischer Maßnahmen bei der Entwicklung eines kompletten Rechners auf FPGA-Basis



kassel university press

Emil Gracić

Beitrag zur Integration und Analyse sicherheitstechnischer Maßnahmen bei der Entwicklung eines kompletten Rechners auf FPGA-Basis

kassel university press

Die vorliegende Arbeit wurde vom Fachbereich Elektrotechnik / Informatik der Universität Kassel als Dissertation zur Erlangung des akademischen Grades eines Doktors der Ingenieurwissenschaften (Dr.-Ing.) angenommen.

Gutachter: Prof. Dr.-Ing. habil. Josef Börcsök, Universität Kassel
Prof. Dr.-Ing. David Schepers, Hochschule Ruhr-West

Tag der mündlichen Prüfung: 2. Juni 2020

Bibliografische Information der Deutschen Nationalbibliothek
Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über http://dnb.dnb.de abrufbar.

Zugl.: Kassel, Univ., Diss. 2020
ISBN 978-3-7376-0873-2
DOI: https://dx.doi.org/doi:10.17170/kobra-202008101548

http://kup.uni-kassel.de

Printed in Germany

„Bist Du nicht gewahr, wie Gott das Gleichnis eines guten Wortes darlegt?
Es is wie ein guter Baum, der fest verwurzelt ist und
dessen Zweige zum Himmel ragen,

zu jeder Zeit seine Frucht bringend mit der Erlaubnis seines Erhalters…“

(Koran, 24-25, 14)

Meiner Familie. Denen, die mit uns sind und Denen, die uns verlassen haben.

„Zar ne vidiš kako Bog navodi primjer -
lijepa riječ kao lijepo drvo: korijen mu je čvrsto u zemlji
a grane prema nebu,

ono plod svoj daje u svako doba koje Gospodar njegov odredi…“

(Kur'an, 24-25, 14)

Mojoj porodici. Onima, koji su sa nama i Onima, koji su nas napustili.

Danksagung

Die vorliegende Arbeit entstand während meiner Tätigkeit als wissenschaftlicher Mitarbeiter am Lehrstuhl für Rechnerarchitektur und Systemprogrammierung der Universität Kassel unter der wissenschaftlichen Leitung von Herrn Professor Dr.-Ing. habil. Josef Börcsök. Ihm danke ich recht herzlich für ein spannendes Thema sowie für eine zuverlässige fachliche Lenkung.

Herrn Professor Dr.-Ing. David Schepers danke ich für die Übernahme des zweiten Gutachtens

Weiterhin möchte ich Herrn Dr.-Ing. Ali Hayek für die berechtigte, aber immer wieder konstruktive fachliche Kritik danken, sowie für seine ständige Ansprechbarkeit und Offenheit.

Bei den Kollegen aus dem ehemaligen ASIC-Team des Fachgebiets Rechnerarchitektur und Systemprogrammierung bedanke ich mich für die tolle Zusammenarbeit. Herrn Manuel Matthias Milde danke ich besonders für motivierende fachliche Diskussionen!

Ein ganz herzlicher Dank geht auch an Frau Maida Kasumovic. Ihr Engagement bei den Reviews meiner wissenschaftlichen Publikationen hat diesen ein anderes Niveau verliehen.

Am Ende bedanke ich mich bei meiner Familie, den Säulen meines privaten und fachlichen Lebens, für die gesamte Unterstützung! Dem lieben Gott danke ich für alles, was Er mir gegeben hat, ohne dass ich es verdient habe.

Kurzfassung

Die enorm große Marktnachfrage nach Managern für funktionale Sicherheit reflektiert, in welchem Maße die funktionale Sicherheit in den letzten Jahren an Bedeutung gewonnen hat. Wird zwei Dekaden zurückgeschaut, dann ist zu sehen, dass diese Wissenschaft für die Luftfahrt- und Prozessindustrie reserviert war. Heute findet sie den Einsatz in fast allen Industriebranchen. Ihren systematischen und rigorosen Charakter hat die funktionale Sicherheit trotz der signifikanten Modifikationen und Anpassungen nicht verloren. Das universelle Einsatzpotenzial manifestiert sich im generischen Aufbau des weltweit etablierten Sicherheitsstandards IEC 61508, aus dem Derivate für den Automotive-Bereich, die Medizin, Bahnanwendungen etc. entstanden.
Beim Blick auf die Entwicklung von FPGAs kann eine ähnliche Laufbahn erkannt werden: eng spezifische Einsatzbereiche am Anfang, Verwendung meistens für den Test von Prototypen, während sie heute zu einem festen Bestandteil des Alltags geworden sind.

Obwohl die FPGAs als Designplattform sehr effektive und zeitlich betrachtet sehr pragmatische Entwicklungsmöglichkeiten anbieten, sind diese Aspekte nicht trivial in sicherheitsgerichtete Anwendungen zu überführen. Die vorliegende Studie befasst sich mit dieser Relation und untersucht anhand einer detaillierten Analyse der neuartigen Designflüsse von führenden FPGA-Herstellern, ob die aktuellen FPGA-Strukturen für den Einsatz in Bereich der funktionalen Sicherheit geeignet sind. Der Fokus liegt auch auf der Implementierung und Evaluierung des Konzeptes der On-Chip-Redundanz mit der Zielsetzung der Umsetzung eines SIL2 konformen Systems.
Der Startpunkt dieser Dissertation ist die Entwicklung eines kompletten Rechners auf dem FPGA basierend auf einem Softcore 32-Bit Mikrocontroller. Nach der erfolgreichen Implementierung werden diverse interne und externe Sicherheitsmaßnahmen integriert, die dazu führen, dass die Auswirkungen von Fehlern infolge gemeinsamer Ursache auf ein akzeptables Niveau reduziert werden und dass der Diagnosedeckungsgrad gefährlicher Ausfälle steigt.
Für die Bewertung der Sicherheit wird die Ausfallrate einzelner Systemkomponenten über zwei verschiedene Methoden, die Gatter-Äquivalenz und den Zuverlässigkeitskalkulator von Xilinx, berechnet und durch die Bildung des Mittelwertes validiert. Im Kontext der Sicherheitsevaluierung wird auch eine intensive thermodynamische Analyse in Form einer komplexen und aussagekräftigen Simulation durchgeführt, deren Ergebnisse sehr stark mit denen der praktischen Untersuchungen korrelieren.

Schlüsselwörter: funktionale Sicherheit, FPGA, On-Chip-Redundanz, SIL2, thermodynamische Analyse

Abstract

A frequent market demand for functional safety managers reflected the grade of the importance the functional safety won in last few years. Analyzing the past two decades we could see that this science was reserved for aviation and process industry. Today, it is present in mostly industrial sectors. It did not lose its systematical and rigorous character despite significant modifications and changes. The capability of universal use becomes the manifest in generic concept of the world wide established safety standard IEC 61508. It derivates the instances for various branches as automotive, medicine, railway etc.
In parallel to FPGA a similar progress path can be recognized - specialized applications at the beginning, then frequent use for testing purposes and prototyping, while today it is an integral part of daily life. As a design platform, FPGA provides very efficient and timing pragmatic development capabilities. But these aspects cannot be trivially transferred in a domain of the safety relevant applications. The presented study focusses on this relation and provides a detailed analysis of the novel design flows of the leading FPGA manufacturers with the intention to evaluate whether the current FPGA structures are appropriate for the functional safety field. The primary scope is related to the implementation and evaluation of the On-Chip-Redundancy concept by implementing a SIL2 conform system.

The initial phase of this study was the development of complete computer architecture on the FPGA-based softcore 32-bit microcontroller. After successful system implementation, various internal and external safety measures that implicated a reduction of the common cause failures on an acceptable level, as well as an increase of the diagnostic coverage, have been integrated.

In order to evaluate the safety of the system, the failure rate of each system component will be calculated using two different methods - gate equivalency and Xilinx reliability calculator. Validation of this concept is done by calculating the mean value of these two methods. In the context of the safety evaluation, we carried out an intense thermodynamic analysis in the form of a complex and reliable simulation whose results significantly correlate with practical results.

Keywords: functional safety, FPGA, On-Chip-Redundancy, SIL2, thermodynamical analysis

Inhaltsverzeichnis

Abkürzungsverzeichnis

1oo2	One Out Of Two
ALU	Arithmetic Logic Unit
AHB	Advanced High-performance Bus
ASIC	Application Specific Integrated Circuit
BUFGMUX	Global Clock Multiplexer
CAN	Controller Area Network
CCF	Common Cause Failures
CFv2SPP	ColdFire Version 2 Standard Product Platform
CLB	Configurable Logic Block
CRC	Cyclic Redundancy Check
DC	Diagnostic Coverage
DCM	Digital Clock Manager
DMR	Dual Modular Redundancy
DSP	Digital Signal Processor
ECC	Error Code Corection
EMA	Enhanced Multiply Accumulate
EUC	Equipment Under Control
FF	Flipflop
FIT	Failure In Time
FMEA	Failure Mode and Effects Analysis
FPAA	Field Programmable Analog Array
FPGA	Field Programmable Gate Array
HDL	Hardware Description Language
I2C	Inter-Integrated Circuit

ICAP	Internal Configuration Access Port
IDF	Isolation Design Flow
IEC	International Electrotechnical Commission
IOB	Input/Output Block
IoT	Internet Of Things
IP	Intellectual Property
ISO	International Organization for Standardization
LCD	Liquid Crystal Display
LUT	Look Up Table
MCM	Miscellaneous Control Module
MTBF	Mean Time Between Failures
MTTF	Mean Time To Failure
MTTR	Mean Time To Repair
OCR	On-Chip-Redundanz
PD	Power-Domäne
PFD	Probability of Failure on Demand
PFH	Probability of Failure per Hour
PLL	Phased-Locked-Loop
SATA	Serial AT Attachment
SDF	Separation Design Flow
SEM	Soft Error Mitigation
SIL	Sicherheitsintegritätslevel
SFF	Safety Failure Fraction
SOC	System-On-Chip
SPI	Serial Peripheral Interface
TMR	Triple Modular Redundancy
UART	Universal Asynchronous Receiver Transmitter
VCD	Value Change Dump

Abbildungsverzeichnis

Tabellenverzeichnis

Symbolverzeichnis

A	Availability
	Verfügbarkeitsfunktion einer Betrachtungseinheit
DC	Diagnostic Coverage
	Gesamtrate aller durch Diagnosetests aufgedeckten gefahrbringenden Ausfälle und solcher, die nicht erkannt werden können
$F(t)$	Ausfallwahrscheinlichkeit einer Betrachtungseinheit
H	Auftrittswahrscheinlichkeit eines Unfalls
$MTBF$	Mean Time Between Failures
	Mittlere Brauchbarkeitsdauer einer Betrachtungseinheit
$MTTF$	Mean Time To Failure
	Mittlere Lebensdauer einer Betrachtungseinheit
$MTTR$	Mean Time To Repair
	Mittlere Instandsetzungszeit einer Betrachtungseinheit
$P(t)$	Fehlerwahrscheinlichkeit einer Betrachtungseinheit
$Pfad1_H$	Hardware-Integrität basierend auf der Implementierung der Hardwarefehlertoleranz und dem Anteil sicherer Ausfälle
$Pfad2_H$	Hardware-Integrität basierend auf etablierten Zuverlässigkeitsdaten verschiedener Bauteile
$Pfad1_S$	Systematische Integrität - Vermeidung von systematischen Fehlern
$Pfad2_S$	Systematische Integrität - Nachweis über den Einsatz betriebsbewährter Komponenten
$Pfad3_S$	Systematische Integrität - Anforderungen an die existierenden Softwarekomponenten
PFD_{avg}	Probability of Failure on Demand
	Mittlere Wahrscheinlichkeit eines gefahrbringenden Ausfalls bei Anforderung der Sicherheitsfunktion

R	Risikofunktion einer Betrachtungseinheit
$R(t)$	Zuverlässigkeitsfunktion einer Betrachtungseinheit
S	Schwere eines Unfalls
SFF	Safety Failure Fraction
	Anteil der sicheren Ausfälle, dieser setzt sich aus gefährlichen und ungefährlichen Ausfällen (entdeckbaren und nicht entdeckbaren) zusammen
β_{ic}	Beta Factor of Integrated Circuit
	Größe, die sich auf die Vermeidung der Fehler infolge gemeinsamer Ursache bezieht
$\lambda(t)$	Ausfallrate einer Betrachtungseinheit

1 Einleitung

Die Prognose von 2008, dass sicherheitstechnische Systeme immer mehr an Bedeutung gewinnen werden und ihr Einsatzfeld immer breiter und komplexer sein wird, hat sich als vollkommen korrekt erwiesen[1]. Die Fortentwicklungen aus der Automobilindustrie und die aktuellen Trends zu einer partiellen Implementierung des autonomen Fahrens rufen hervor, dass die funktionale Sicherheit ein hoch priorisierter Parameter geworden ist. Andererseits werden die Konzepte der Industrie 4.0[2] und des InternetOfThings immer aktueller und bedeutender[3]. Diese komplexe Vernetzung der Elektronik aller Art schafft einerseits den Raum für herausragende Innovationen und führt andererseits zu unvorhersehbaren Gefahren. Denn, es sind nicht nur die Daten, die geschützt werden sollen, sondern auch die Systeme und Netzwerke, welche die Funktion der Bearbeitung und Übertragung der Daten übernehmen. Demzufolge ist zu behaupten, dass der Einsatz von sicherheitsgerichteten Systemen weiter intensiviert werden wird. Betrachtet aus der Perspektive der Komplexität scheint sehr realistisch, dass die Aspekte der funktionalen Sicherheit nicht zum ersten Mal vor einer Reform stehen.

1.1 Motivation

Obwohl ursprünglich als sehr konservativ und geschlossen gekennzeichnet, hat sich die Sicherheitstechnik in den letzten zwei Dekaden signifikant fortentwickelt und modifiziert. Mit der Einführung der Mikrocontrollersysteme in Bereichen, in denen Zuverlässigkeit und Sicherheit eine bedeutende Rolle spielen, wurde ein neuer Raum für Weiterentwicklung kreiert. Die Rahmenlinien dieses Raumes sind lediglich durch internationale Normen und Standards festgelegt. Die International Electrotechnical Commission (IEC) 61508 als Grundnorm für die Implementierung der funktionalen Sicherheit von elektrischen, elektronischen und programmierbar-elektronischen Systemen definiert solche Rahmenlinien in Form verschiedener Anforderungen, die im gesamten Entwicklungsprozess zu erfüllen sind.

[1] [Bör07] Börcsök, J.; *Elektronische Sicherheitssysteme : Hardwarekonzepte, Modelle und Berechnung*. 2007.

[2] [WSJ17] Wollschlaeger, M., Sauter, T. und Jasperneite, J.; *The Future of Industrial Communication: Automation Networks in the Era of the Internet of Things and Industry 4.0*. 2017.

[3] [Mic17] Michahelles, F.; *Internet of Things Reality Check*. 2017.

In der ersten Ausgabe von 1998 war die IEC 61508 sehr limitiert, so dass eine redundante Systemarchitektur, die eine fundamentale Sicherheitsmaßnahme darstellt, mehr oder minder immer ähnlich gestaltet werden musste. Dies alles wegen der Anforderung einer echten physikalischen Trennung, die den Einsatz zweier getrennter Chip-Dies auf einer Platine implizierte. Aufgabe der Ingenieure war die Analyse der potentiellen Gefahren außer der Chip Dies und die Implementierung der zusätzlichen Schutzmechanismen in Form von externen Watchdogs, einer Takt- und Spannungsüberwachung etc. Sowohl Application Specific Integrated Circuits (ASICs) als auch Field Programmable Gate Arrays (FPGAs) haben ihren Einsatz gefunden, abhängig von dem Einsatzbereich des anvisierten Systems sowie von der gewünschten Leistungsfähigkeit und der Stückanzahl[4]. Dementsprechend bestand eine Diskrepanz in Bezug auf den Stand der Technik, weil sich das System-On-Chip (SOC) Konzept inzwischen als Mainstream etabliert hatte. Auf der anderen Seite führte die Größe sicherheitsgerichteter Systeme zur inakzeptablen Unwirtschaftlichkeit.

Die zweite Ausgabe der IEC61508 von 2010 strebte danach, die erwähnten Nachteile zu beseitigen und den SOC-Aspekten näher zu kommen, indem das On-Chip-Redundanz (OCR) Konzept eingeführt worden ist. Folglich konnte die redundante Systemarchitektur auf einem Chip Die implementiert werden. Nun wurde eine weitere Herausforderung generiert - die Analyse von potentiellen Gefahren auf dem Chip. Außerdem fordert die Norm neben der Analyse von Fehlern infolge gemeinsamer Ursache auf dem gesamten System auch eine detaillierte Analyse solcher Fehler auf dem Chip und die Implementierung von Milderungsmechanismen.

Die weltweiten FPGA-Leader, Xilinx und Altera, behaupten, dass ihre FPGAs als Plattform für die OCR verwendet werden können. Trotz der Zertifizierung der Tools für sicherheitsgerichtete Anwendungen beim TÜV Rheinland 2013[5] und 2014 wurde bis jetzt kein FPGA-basiertes System entwickelt, welches die Anforderungen der funktionalen Sicherheit erfüllt. Die eingeführten Konzepte der Isolierung mit den Xilinx Tools bzw. der Komponentenseparation mit den Altera Tools beruhen nur auf der logischen Trennung sicherheitsgerichteter Komponenten auf dem Chip und einer geprüften Methodologie zur Zuweisung von I/O-Blöcken bzw. zur Kommunikation zwischen getrennten Komponenten. Andere entscheidende Aspekte, wie die Vermeidung oder Milderung der Fehler infolge gemeinsamer Ursache (Common Cause Failures, CCF) wurden entweder überhaupt nicht (Altera[6]) oder nur sehr oberflächlich (Xilinx[7]) betrachtet.

[4] [Hay10] Hayek, A.; *Modellierung, Implementierung und Bewertung einer sicherheitsgerichteten 1oo2-Architektur mit VHDL auf FPGA-Ebene*. 2010.

[5] [McN13] McNeil, S.; *Developing Secure Designs with the Spartan-6 Family Using the Isolation Design Flow*. 2013.

[6] [15a]; *FPGA-based Safety Separation Design Flow for Rapid Functional Safety Certification*. 2015.

[7] [CGB12] Corradi, G., Girardey, R. und Becker, J.; *Xilinx tools facilitate development of FPGA applications for IEC61508*. 2012
[HCM15] Hallett, E., Corradi, G. und McNeil, S.; *Xilinx Reduces Risk and Increases Efficiency for IEC61508 and ISO26262 Certified Safety Applications*. 2015.

1.2 Zielsetzung

Der Einsatz von FPGA-basierten Mikrocontrollern für sicherheitskritische Anwendungen ist sehr stark mit dem traditionellen Konzept der Trennung und der Rückwirkungsfreiheit verbunden[8]. Solch eine Architektur basiert meistens auf drei FPGAs, auf denen drei Mikrocontroller parallel in Betrieb sind. Zwei von diesen repräsentieren eine typische redundante Sicherheitsarchitektur. Der dritte ist ein sogenannter Kommunikationsprozessor.

Das erste Ziel dieser Arbeit ist es, sich von der Tradition zu distanzieren und eine neue Architektur vorzustellen, die zwei wichtige Aspekte verknüpft:

- Implementierung eines kompletten Rechners auf Basis eines 32-Bit Mikrocontrollers auf dem FPGA, um zu einer vollständigen Kommunikationsarchitektur beizutragen.
- Implementierung eines „warm redundanten“ Konzeptes, um die Verwendung des Kommunikationssystems für die Sicherheitsanwendungen zu ermöglichen. Bisher fanden solche Systeme Einsatz nur als BlackBox-Kanäle[8]. Durch eine sicherheitsbezogene Struktur und Architektur wird dem anvisierten System ein universelles Einsatzpotenzial verliehen.

Ein weiteres Ziel ist die Analyse aller möglichen Fehler infolge gemeinsamer Ursache und die Implementierung von Vermeidungs- oder Milderungsmechanismen. Dadurch werden konkrete Anforderungen aus der zweiten Edition der IEC 61508 erfüllt. In der Kombination mit den Aspekten der Vermeidung von systematischen Fehlern kann das Zielsystem bezüglich der Anforderungen des Sicherheitsintegritätslevels 2 (SIL) verifiziert werden.

Als Quellen von Fehlern infolge gemeinsamer Ursache auf einem FPGA kommen in Betracht:

- I/O Blöcke
- Taktmanagement
- Spannungsversorgung
- Überwachung des Konfigurationsspeichers

Um das Konzept der warmen Redundanz zu implementieren, sind gewisse sicherheitstechnische Maßnahmen für die Ausgangsumschaltung zwischen den redundanten Systemen zu berücksichtigen. Diese gehören zur architekturspezifischen Quelle von Fehlern infolge gemeinsamer Ursache. Ein sicherheitsrelevanter Multiplexer soll die Umschaltung vom Haupt- auf das redundante Mikrocontrollersystem in einer sicheren und testbaren Art und Weise realisieren und somit als Milderungsmaßnahme eingesetzt werden.

[8] [13]; *A Validated Methodology for Designing Safe Industrial Systems on a Chip.* 2013 [10a]; *Developing Functional Safety Systems with TÜV-Qualified FPGAs.* 2010.

Neben der neuartigen redundanten Architektur und dem Ausgangsmultiplexer wird des Weiteren die Verteilung der Eingangssignale besonders behandelt. Dies ist die Folge der spezifischen Einschränkungen von verwendeten Entwicklungstools. Der Verteilungsprozess ist auch sicher und testbar zu implementieren. Somit ergeben sich vier sicherheitsrelevante Module - zwei Mikrocontrollersysteme, ein Ausgangsmultiplexer und ein Modul für die Verteilung der Eingangssignale. Sie werden auf zwei diversen Wege verifiziert:

- bezüglich der Anforderungen zur On-Chip-Trennung bzw. -Isolierung,
- bezüglich der Anforderungen an den Sicherheitsintegritätslevel 2.

Diese Verifikationsaspekte werden die Limitierungen und Lücken bisheriger Forschungsarbeiten zum Einsatz von FPGAs in sicherheitsgerichteten Applikationen überwinden.

Obwohl die IEC 61508 der thermischen Betrachtung des Chips sehr große Bedeutung beimisst, wurde sie bis jetzt in FPGA-bezogenen Entwicklungen kaum berücksichtigt. Eine intensive thermodynamische Analyse soll durchgeführt werden, um nachzuweisen, dass die Temperatur als CCF-Faktor ein tolerierbares Risiko darstellt.

Die vielseitige Diskussion über den Einsatz von rezenten FPGA-Strukturen in sicherheitsgerichteten Systemen strebt an, einen Überblick zu schaffen, was in der Zukunft anders zu gestalten ist, um die FPGA-Plattform als einen starken Konkurrenten zu den ASICs zu profilieren.

1.3 Aufbau

Das nächste Kapitel befasst sich mit dem Stand der Technik und legt Grundbegriffe der Sicherheitstechnik, die Grundlagen der allgemeinen FPGA-Struktur und einen Ausschnitt aus der Norm IEC 61508 dar. Somit wird eine Basis für den Einstieg in den Bereich der funktionalen Sicherheit für FPGA-basierte Systeme aufgebaut.

In Kapitel 3 werden die anvisierte Systemarchitektur und das Konzept zur Implementierung des sicherheitsgerichteten Systems auf Basis eines 32-Bit ColdFire Mikrocontrollers vorgestellt. Hierzu gehört auch die Analyse des traditionellen FPGA-Designflusses und des neuen, auf der Isolierung sicherheitsbezogener Komponenten basierenden Konzeptes.

Um das zu entwickelnde System konform zur Norm IEC 61508 zu gestalten, werden diverse Sicherheitsmaßnahmen implementiert. Warme Redundanz ist erforderlich, um das Hindernis einer intensiven On-Chip-Diagnostik zu überwinden. Der sichere Multiplexer ist zu entwerfen, um das Umschalten von Ausgängen in einer sicheren und testbaren Art und Weise zu erreichen. Um den Wert des Diagnosedeckung-Parameters gemäß den SIL

2 Anforderungen zu erhöhen, werden alle Quellen der Fehler infolge gemeinsamer Ursache ausgiebig untersucht und Vermeidungs- oder Milderungsmaßnahmen entwickelt. Alle diese Aspekte behandelt das Kapitel 4.

Im fünften Kapitel werden konkrete Ergebnisse evaluiert und die erwähnten Verifikationen durchgeführt, um sicherzustellen, ob die Anforderungen an den gewünschten SIL 2 erfüllt worden sind. Diesem Kapitel gehört auch eine detaillierte thermodynamische Analyse des Gesamtsystems an, die sicherheitstechnische Vorteile eines FPGAs im Vergleich zum ASIC hervorhebt.

Die vorliegende Arbeit wird auf Basis einer komparativen Auseinandersetzung mit den aktuellen Entwicklungen und Forschungsarbeiten in Kapitel 6 bewertet. Zum anderen werden verschiedene FPGA-Typen betrachtet, um in der Zukunft einen neuen Diskurs zur Entwicklung von FPGAs für Sicherheitsanwendungen anzustoßen.

Das letzte Kapitel fasst diese Dissertation zusammen und schließt mit Ausblicken ab, die sich aus den erreichten Ergebnissen und Analysen ergeben.

2 Stand der Technik

In diesem Kapitel werden erforderliche Grundlagen dargestellt, damit der Zusammenhang zwischen der funktionalen Sicherheit, FPGAs und dem normbasierten Systementwurf verdeutlicht wird. Die IEC 61508 ist eine weltweit etablierte Norm für die Entwicklung sicherheitsgerichteter Systeme. Da unsere Forschung primär auf FPGAs basiert, werden nur die relevanten Aspekte dieser Norm angesprochen.

2.1 Sicherheitstechnische Grundlagenbetrachtungen für integrierte Schaltungen

Das zentrale Thema bei der Betrachtung der funktionalen Sicherheit eines Systems ist die Bestimmung und Bewertung des Risikos[9]. Aus diesem Kernbegriff leiten sich alle anderen Begriffe der Sicherheitstechnik wie Zuverlässigkeit, Verfügbarkeit, Sicherheit, AusfallwahrscheinlicProbability of Failure on Demandhkeit etc. ab.

Ein absolut sicheres und fehlerfreies System existiert nicht[10]. Aufgrund dessen ist es notwendig eine grundlegende Analyse durchzuführen, inwieweit bestehende Gefahren ein sicherheitsrelevantes System beeinträchtigen können. Daher fließen die folgenden zwei Aspekte in die Risikodefinition ein:

- Schwere eines Unfalls, der von einer bestimmten Gefahr verursacht wurde (S)
- Auftrittswahrscheinlichkeit eines Unfalls (H)

In der Literatur[11] wird das Risiko R als folgende Relation definiert:

$$R = H * S \tag{2.1}$$

Diese Definition ist qualitativer Natur und wird gegenüber quantitativen Maßnahmen bevorzugt, weil diese auf komplexere Systeme sehr schwierig angewandt werden können.

[9] [Bör15] Börcsök, J.; *Funktionale Sicherheit : Grundzüge sicherheitstechnischer Systeme*. 2015.

[10] [Mon99] Montenegro, S.; *Sichere und fehlertolerante Steuerungen : Entwicklung sicherheitsrelevanter Systeme*. 1999.

[11] [Bör07] Börcsök, J.; *Elektronische Sicherheitssysteme : Hardwarekonzepte, Modelle und Berechnung*. 2007

[IEC10b] IEC61508; *Anforderungen an sicherheitsbezogene elektrische/elektronische/programmierbare elektronische Systeme*. 2010.

Als Hauptgrund wird der Rechenaufwand genannt[12]. Nichtsdestotrotz, entsprechen die qualitativen Ansätze dem logischen Denken eines Menschen und sind somit adäquater anzuwenden.

Die Schwere eines Unfalls und dessen Auftrittswahrscheinlichkeit werden von diversen Normen und Standards unterschiedlich interpretiert. Da diese Studie auf der Implementierung eines zur IEC 61508 konformen Systems basiert, werden an dieser Stelle Definitionen aus dieser Norm erörtert[13].

Tabelle 2.1: Risikoklassifizierung nach IEC 61508 [IEC10b]

	Bedeutung			
Häufigkeit	**Katastrophal**	**Kritisch**	**Geringfügig**	**Unbedeutend**
Häufig	I	I	I	II
Wahrscheinlich	I	I	II	III
Gelegentlich	I	II	III	III
Zukünftig	II	III	III	IV
Unwahrschein.	III	III	IV	IV
Unglaublich	IV	IV	IV	IV

Tabelle 2.2: Bedeutung der Risikoklassen nach IEC 61508 [IEC10b]

Risikoklasse	**Definition**
I	Inakzeptables Risiko
II	Unerwünscht und nur bei nicht reduzierbarem Risiko oder unverhältnismäßig stark zunehmenden Kosten akzeptabel
III	Tolerierbares Risiko, wenn die Kosten der Risikoreduzierung überschritten werden
IV	Unbedeutendes Risiko

In Bezug auf die Formel 2.1 wird das Risiko auf folgende Art klassifiziert: Die römischen Zahlen I - IV verweisen auf eine Risikoklasse. Wie aus Tabelle 2.1 ersichtlich, wird jeder Kombination aus Häufigkeit des Ausfalls und seinem Schweregrad eine bestimmte Risikoklasse zugeordnet. Deren Bedeutung lässt sich aus Tabelle 2.2 entnehmen.
Je intensiver die Schwere eines Unfalls ist, umso unwahrscheinlicher muss die Auftrittswahrscheinlichkeit sein, damit ein akzeptables Risiko erreicht wird. Auf der anderen Seite, betrachtet aus der Perspektive des Parameters H, kann ein Risiko nur dann to-

[12] [Bör15] Börcsök, J.; *Funktionale Sicherheit : Grundzüge sicherheitstechnischer Systeme*. 2015
[Bör07] Börcsök, J.; *Elektronische Sicherheitssysteme : Hardwarekonzepte, Modelle und Berechnung*. 2007.

[13] [IEC10b] IEC61508; *Anforderungen an sicherheitsbezogene elektrische/elektronische/programmierbare elektronische Systeme*. 2010.

leriert werden, wenn H sehr wahrscheinlich ist, aber die Unfallschwere unbedeutend ist.

Eine andere Methode für die Bewertung des Risikos ist die Erstellung eines Risikographen. Hierbei spielt die Vertiefung der allgemeinen Parameter H und S eine Rolle, so dass neue Größen wie Eintrittswahrscheinlichkeit, Gefahrenabwendung etc. eingeführt werden. Eine ausführliche Beschreibung ist in[14] zu finden.

Bei der Betrachtung eines Equipment Under Control (EUC) wird das bestehende Risiko als inakzeptabel angenommen. In diesem Sinne sind unterschiedliche Maßnahmen einzusetzen, um eine tolerierbare Stufe zu erreichen. Da die Norm sehr konservativ ist, wird das erreichte Risiko - das so genannte Restrisiko - in bestimmtem Maße niedriger sein als das tolerierbare. Die Integration von sicherheitsgerichteten Systemen ist nur ein Teil dieser Maßnahmen, die zur notwendigen Risikoreduzierung beitragen und zusammen mit anderen Methoden die Sicherheitsintegrität bilden, wie dies in Abbildung 2.1 dargestellt wird (siehe Teil 5 der Norm[15]).

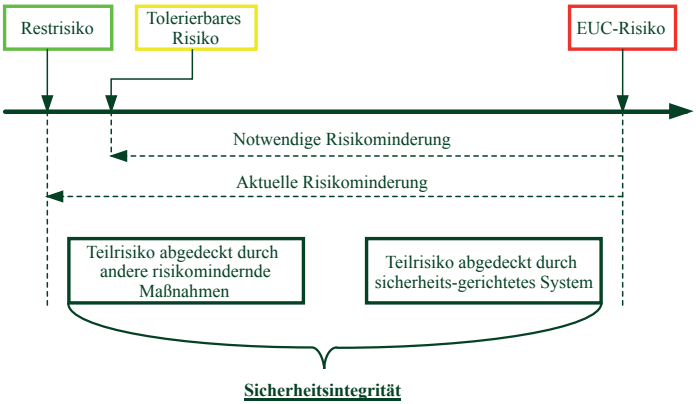


Abbildung 2.1: Konzept der Risikominderung, vgl. [IEC10f]

Im Teil 4 der Norm wird die **Sicherheitsintegrität** folgendermaßen definiert: „*Wahrscheinlichkeit eines sicherheitsrelevanten Systems, die geforderten Sicherheitsfunktionen unter allen festgelegten Bedingungen innerhalb eines festgelegten Zeitraumes zufriedenstellend auszuführen*“.

[14] [Bör07] Börcsök, J.; *Elektronische Sicherheitssysteme : Hardwarekonzepte, Modelle und Berechnung*. 2007
[IEC10b] IEC61508; *Anforderungen an sicherheitsbezogene elektrische/elektronische/programmierbare elektronische Systeme*. 2010.

[15] [IEC10f] IEC61508; *Beispiele von Methoden für die Bestimmung von Sicherheits-Integritätsleveln*. 2010.

Ein Synonym zum Begriff der Sicherheitsintegrität ist die Wahrscheinlichkeit, dass das System genau zu dem Zeitpunkt ausfällt, in dem es gefordert wird. Im Englischen wird die Abkürzung **PFD** verwendet, die für „Probability of Failure on Demand“ steht. Bei der Berechnung wird der mittlere Wert PDF_{avg}[16] berücksichtigt.

$$PDF_{avg} = \frac{1}{T} \int_0^T P(t)\,\mathrm{d}t \tag{2.2}$$

P(t) bezieht sich auf die **Fehlerwahrscheinlichkeit**, die dem Begriff Ausfallwahrscheinlichkeit F(t) äquivalent ist. Diese Größe ist eng mit der Zuverlässigkeit des Systems *R(t)* verbunden, da sie deren Komplement darstellt[17].

$$F(t) = 1 - R(t) \tag{2.3}$$

Die Zuverlässigkeit wird auf verschiedene Weisen definiert. Im dritten Teil der Norm ist folgende kompakte Definition gegeben „*Wahrscheinlichkeit der richtigen Funktion über einen gegebenen Zeitraum unter bestimmten Bedingungen*“.
Dieser Begriff ist untrennbar vom Begriff **Ausfallrate** λ, der in der Sicherheitstechnik eine fundamentale Bedeutung hat. Liegt eine zeitlich abfallende Ausfallrate vor, dann nimmt R(t) die Form aus der Abbildung 2.2 an.

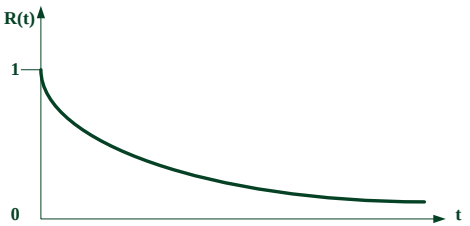


Abbildung 2.2: Zuverlässigkeitsfunktion im zeitlichen Verlauf, Quelle: [MP10]

Mathematisch wird R(t) ausgedrückt als[18]:

$$R(t) = e^{-\int_0^t \lambda(\tau)dt} \tag{2.4}$$

Falls angenommen werden kann, dass die Ausfallrate konstant ist und somit $\lambda(t) = \lambda$, dann gilt folgende Gleichung[18]:

[16] [Bör15] Börcsök, J.; *Funktionale Sicherheit : Grundzüge sicherheitstechnischer Systeme*. 2015.
[17] [MP10] Meyna, A. und Pauli, B.; *Taschenbuch der Zuverlässigkeitstechnik : Quantitative Bewertungsverfahren*. 2010.
[18] [Pec95] Pecht, M.; *Product reliability, maintainability, and supportability handbook*. 1995.

$$R(t) = e^{-\lambda t} \tag{2.5}$$

Die Ausfallrate einer Betrachtungseinheit kann als Wahrscheinlichkeit interpretiert werden, die sich auf ein Zeitintervall bezieht, in dem die Einheit nicht ausgefallen ist. So wird diese Größe durch die mittlere Lebensdauer ausgedrückt (Mean Time To Failure, MTTF)[19]. Diese Formulierung gilt nur in dem Falle, wenn λ konstant ist[19].

$$\lambda = \frac{1}{MTTF} \tag{2.6}$$

In der Realität kann diese Annahme nicht so trivial getroffen werden. Für die Betrachtung des variablen Verhaltens der Ausfallrate bietet sich die Weibull-Verteilung an[20], die so genannte „Badewannen-Kurve". Es wird zwischen drei Phasen unterschieden[19]:

- Frühe Phase, bei der die Ausfallrate den höchsten Wert aufweist. Als Hauptursachen werden Materialschwäche und Fertigungsfehler genannt.
- Nutzungsphase, bei der die Ausfallrate konstant ist.
- Verschleißphase, bei der zum Verschleiß, Alterung oder Ermüdung der betrachtenden Einheit kommt. Als Konsequenz steigt die Ausfallrate an.

Abbildung 2.3: Ausfallrate λ im zeitlichen Verlauf, Quelle: [MP10]

Die Bestimmung der **mittleren Lebensdauer** ist die meistangewandte Methode, um die Zuverlässigkeit eines Systems oder einer Komponente zu beurteilen[21]. Demzufolge wird diese Größe auf folgende Weise definiert:

$$MTTF = \int_0^\infty R(t)dt \tag{2.7}$$

[19] [MP10] Meyna, A. und Pauli, B.; *Taschenbuch der Zuverlässigkeitstechnik : Quantitative Bewertungsverfahren*. 2010.

[20] Nach dem schwedischen Forscher Ernst Hjalmar Waloddi Weibull, 1887-1979. Ursprünglich für Werkstoffermüdung verwendet ([MP10] Meyna, A. und Pauli, B.; *Taschenbuch der Zuverlässigkeitstechnik : Quantitative Bewertungsverfahren*. 2010)

[21] [Pec95] Pecht, M.; *Product reliability, maintainability, and supportability handbook*. 1995.

An dieser Stelle werden noch zwei weitere für die Bewertung der Sicherheit sehr relevante Aspekte betrachtet, nämlich die **mittlere Brauchbarkeitsdauer MTBF** (Mean Time Between Failures) und die **mittlere Instandsetzungszeit MTTR** (Mean Time To Repair). Letztere bezieht sich auf die Zeit, die benötigt wird, eine defekte Einheit zu reparieren. Die mittlere Brauchbarkeitsdauer wird in der Literatur[22] wie folgt formuliert:

$$MTBF = MTTF + MTTR \tag{2.8}$$

Eine der wichtigsten sicherheitstechnischen Größen aus dem Bereich der Luftfahrt ist die **Verfügbarkeit A**. Sie wird in der sicherheitstechnischen Literatur[22] als Wahrscheinlichkeit definiert, mit der eine betrachtete Einheit reparierbar und zu einem bestimmten Zeitpunkt funktionsfähig ist.

$$A = \frac{MTTF}{MTTF + MTTR} \tag{2.9}$$

Die IEC 61508 ist ein internationaler Standard, der den gesamten Sicherheitslebenszyklus eines Systems definiert und steuert. Sie verknüpft die nationalen Normen und Standards aus dem EU-Raum, um die funktionale Sicherheit elektrischer, elektronischer und programmierbar-elektronischer Systeme zu implementieren. Geprägt wird die IEC 61508 durch ihren allgemeinen Charakter, so dass sich die Normen für spezielle Anwendungsgebiete komfortabel ableiten lassen, wie z. B. International Organization for Standardization (ISO) 26262 für die Automobilindustrie oder IEC 61511 für die Prozessindustrie [Bör07]. Der Titel des Standards ist *„Funktionale Sicherheit sicherheitsbezogener, elektrischer/elektronischer/programmierbarer elektronischer Systeme“*. Bestehend aus sieben Teilen werden alle Entwicklungsphasen eines Systems abgedeckt, von der Spezifikation über die Implementierung bis zur Dokumentation. Die einzelnen Teile befassen sich mit:

- Allgemeine Anforderungen[23]
- Anforderungen an sicherheitsbezogene elektrische/elektronische/programmierbare elektronische Systeme[24]
- Anforderungen an Software[25]

[22] [Bör07] Börcsök, J.; *Elektronische Sicherheitssysteme : Hardwarekonzepte, Modelle und Berechnung*. 2007
[Pec95] Pecht, M.; *Product reliability, maintainability, and supportability handbook*. 1995
[MP10] Meyna, A. und Pauli, B.; *Taschenbuch der Zuverlässigkeitstechnik : Quantitative Bewertungsverfahren*. 2010.

[23] [IEC10a] IEC61508; *Allgemeine Anforderungen*. 2010.

[24] [IEC10b] IEC61508; *Anforderungen an sicherheitsbezogene elektrische/elektronische/programmierbare elektronische Systeme*. 2010.

[25] [IEC10c] IEC61508; *Anforderungen an Software*. 2010.

- Begriffe und Abkürzungen[26]
- Beispiele von Methoden für die Bestimmung von Sicherheits-Integritätsleveln[27]
- Anwendungsrichtlinie für Teile 2 und 3[28]
- Überblick über Verfahren und Maßnahmen[29]

In Anlehnung an die Norm und die sicherheitstechnische Literatur wurde in diesem Kapitel der Begriff der Sicherheitsintegrität erläutert. An dieser Stelle ist es von Bedeutung, ein tieferes Verständnis dieser Größe zu schaffen, weil aus ihr die tatsächliche Sicherheitsqualität eines zu betrachtenden Systems abgeleitet wird. Demzufolge werden andere Aspekte aus der Norm[30] näher betrachtet, nämlich

- die Hardware-Integrität und
- die systematische Integrität,

damit Parallelen zu den Grundprinzipien der Sicherheitsanalyse bzw. der Sicherheitsbewertung eines Systems gezogen werden.
Bei der systematischen Integrität wird die Erfüllung folgender Pfade als Zielsetzung definiert[30]:

- Pfad 1_S: Vermeidung von systematischen Fehlern
- Pfad 2_S: Nachweis über den Einsatz betriebsbewährter Komponenten
- Pfad 3_S: Anforderungen an die existierenden Softwarekomponenten

Bei der Beurteilung dieser Art der Integrität wird „die systematische Eignung“ eines Systems oder einer Systemkomponente untersucht. Diese ist im zweiten Teil der Norm als ein Potenzial definiert, welches ein systematischer Fehler mitbringt und welches zum Ausfall der Sicherheitsfunktion führen kann. In diesem Sinne fordert die IEC 61508 die Implementierung der Unabhängigkeit zwischen den Systemkomponenten. Als Maßnahmen eignen sich die funktionale oder die technologische Diversität etc.

Um die Hardware-Integrität zu bestimmen, bieten sich zwei Pfade an[30]:

- Pfad 1_H, der auf der Implementierung der Hardwarefehlertoleranz und dem Anteil sicherer Ausfälle basiert
- Pfad 2_H, der auf etablierten Zuverlässigkeitsdaten verschiedener Bauteile basiert

[26] [IEC10e] IEC61508; *Begriffe und Abkürzungen*. 2010.
[27] [IEC10f] IEC61508; *Beispiele von Methoden für die Bestimmung von Sicherheits-Integritätsleveln*. 2010.
[28] [IEC10d] IEC61508; *Anwendungsrichtlinie für Teile 2 und 3*. 2010.
[29] [IEC10g] IEC61508; *Überblick über Verfahren und Maßnahmen*. 2010.
[30] [IEC10b] IEC61508; *Anforderungen an sicherheitsbezogene elektrische/elektronische/programmierbare elektronische Systeme*. 2010.

Unabhängig davon, aus welcher Perspektive die Sicherheitsintegrität betrachtet wird, wird sie quantitativ als ein bestimmter Level ausgedrückt. Die IEC 61508 sieht für jedes System einen SIL von 1 bis 4 vor. Dabei steht der SIL 1 für den niedrigsten und der SIL 4 für den höchsten erreichbaren Level. Somit sind die zu erfüllenden Anforderungen bei dem vierten am anspruchsvollsten.
Um den SIL eines sicherheitsrelevanten Systems bestimmen zu können, gilt es zunächst festzulegen, von welchem Typ das System ist. In diesem Sinne wird zwischen Typ A und Typ B unterschieden. Beim Typ A sind folgende Bedingungen erfüllt[31]:

- Das Ausfallverhalten aller Systemkomponenten ist eindeutig definiert,
- das Verhalten der Systemkomponenten unter den Fehlerbedingungen ist vorhersehbar,
- es existieren ausreichende Ausfalldaten, mit denen die Ausfallrate konsistent bestimmt werden kann.

Falls mindestens eine dieser drei Bedingungen nicht erfüllt ist, wird das System als Typ B kategorisiert.
Im Kontext des Pfades 1_H wird der SIL wie in den Tabellen 2.3 und 2.4 angegeben klassifiziert.

Tabelle 2.3: SIL für die Sicherheitsfunktion eines Systems oder einer Systemkomponente vom Typ A [IEC10b]

Anteil sicherer Ausfälle einer Komponente	**Hardwaretoleranz**		
	0	1	2
<60 %	SIL1	SIL2	SIL3
60 % - <90 %	SIL2	SIL3	SIL4
90 % - <99 %	SIL3	SIL4	SIL4
≥99 %	SIL3	SIL4	SIL4

Tabelle 2.4: SIL für die Sicherheitsfunktion eines Systems oder einer Systemkomponente vom Typ B [IEC10b]

Anteil sicherer Ausfälle einer Komponente	**Hardwaretoleranz**		
	0	1	2
<60 %	nicht erlaubt	SIL1	SIL2
60 % - <90 %	SIL1	SIL2	SIL3
90 % - <99 %	SIL2	SIL3	SIL4
≥99 %	SIL3	SIL4	SIL4

Eine weitere Bezugnahme zur Definition des SIL basiert auf der Häufigkeit der Anforderung der Sicherheitsfunktion. Ist die Anforderungsrate niedrig, kann der SIL mittels

[31] [IEC10b] IEC61508; *Anforderungen an sicherheitsbezogene elektrische/elektronische/programmierbare elektronische Systeme.* 2010.

PFD_{avg} ausgedrückt werden. Diese Art der Klassifizierung ist in Tabelle 2.5 dargestellt[32]. Wird auf der anderen Seite die Sicherheitsfunktion öfter oder kontinuierlich angefordert, dann wird der Sicherheitsintegritätslevel mittels der mittleren Häufigkeit eines gefahrbringenden Ausfalls pro Stunde (PFH) kategorisiert, siehe Tabelle 2.6.

Tabelle 2.5: SIL einer Sicherheitsfunktion im Betrieb mit niedriger Anforderungsrate [MP10]

Sicherheits-Integritätslevel (SIL)	**Mittlere Wahrscheinlichkeit eines gefahrbringenden Ausfalls bei Anforderung der Sicherheitsfunktion (PFD_{avg})**
4	$\geq 10^{-5}$ bis $<10^{-4}$
3	$\geq 10^{-4}$ bis $<10^{-3}$
2	$\geq 10^{-3}$ bis $<10^{-2}$
1	$\geq 10^{-2}$ bis $<10^{-1}$

Tabelle 2.6: SIL einer Sicherheitsfunktion im Betrieb mit hoher oder kontinuierlicher Anforderungsrate [MP10]

Sicherheits-Integritätslevel (SIL)	**Mittlere Häufigkeit eines gefahrbringenden der Sicherheitsfunktion pro Stunde (PFH)**
4	$\geq 10^{-9}$ bis $<10^{-8}$
3	$\geq 10^{-8}$ bis $<10^{-7}$
2	$\geq 10^{-7}$ bis $<10^{-6}$
1	$\geq 10^{-6}$ bis $<10^{-5}$

Um die Sicherheitsintegrität eines betrachteten Systems beurteilen zu können, schreibt die Norm IEC 61508 eine detaillierte Fehlerart- und auswirkungsanalyse (FMEA) vor. Als erster Schritt bietet sich eine Blockdiagrammdarstellung des gesamten Systems an[33], in der die Ausfallrate jeder Systemkomponente und ihr Einfluss auf die Ausführung der Sicherheitsfunktion genau betrachtet wird. In diesem Sinne unterscheidet man zwischen zwei Ausfallarten:

- ungefährlichem und
- gefahrbringendem Ausfall

Wiederum können diese zwei Arten um zwei weitere erweitert werden, abhängig davon, ob ein Ausfall durch die Diagnosemechanismen aufgedeckt werden kann oder nicht.

[32] [MP10] Meyna, A. und Pauli, B.; *Taschenbuch der Zuverlässigkeitstechnik : Quantitative Bewertungsverfahren*. 2010.

[33] [IEC10d] IEC61508; *Anwendungsrichtlinie für Teile 2 und 3*. 2010
[IEC10g] IEC61508; *Überblick über Verfahren und Maßnahmen*. 2010.

Der Diagnosedeckungsgrad (DC) setzt sich aus der Gesamtrate aller durch Diagnosetests aufgedeckten gefahrbringenden Ausfälle und solcher, die nicht erkannt werden können, zusammen. Diese sicherheitstechnische Größe wird wie folgt definiert[34]:

$$DC = \frac{\sum \lambda_{Dd}}{\sum \lambda_{Dd} + \sum \lambda_{Du}} \tag{2.10}$$

Bei der Betrachtung des Anteils der sicheren Ausfälle (SFF), werden neben den gefahrbringenden auch die ungefährlichen (entdeckbaren und nicht entdeckbaren) Ausfälle in die Relation einbezogen[34]:

$$SFF = \frac{\sum \lambda_S + \sum \lambda_{Dd}}{\sum \lambda_S + \sum \lambda_{Dd} + \sum \lambda_{Du}} \tag{2.11}$$

Wie schon erwähnt, basiert die Implementierung sicherheitsgerichteter Systeme auf einem redundanten Einsatz der Systeme oder Systemkomponenten, die für die Ausführung der Sicherheitsfunktion von grundlegender Bedeutung sind. Ursprünglich wurden solche Systeme mit mehreren separaten Chips realisiert. Seit der zweiten Edition der IEC 61508 ist es möglich, redundante Systemarchitekturen auf einem einzelnen Chip zu implementieren. Dieses Konzept wurde als On-Chip-Redundanz (OCR) bezeichnet und wird durch folgende Charakteristiken geprägt (siehe Anhang E des zweiten Teils der Norm[34]):

- Die redundanten Systeme sind auf dem Chip physikalisch zu trennen und als unabhängige Kanäle zu betrachten. Dies impliziert mehrere unabhängige Blöcke auf einem Chip-Die.
- Die Distanz zwischen den getrennten Systemen-, Systemkomponenten ist ausreichend, um Kurzschlüsse oder Übersprechen zu vermeiden. Diese Barriere darf keine Logik enthalten.
- Leitungen zwischen den separaten Blöcken sind erlaubt, jedoch muss eine adäquate Distanz implementiert werden, damit Kurzschlüsse und Übersprechen nicht auftreten.
- Jeder Kanal muss eigene I/O-Pins besitzen. Das Teilen der I/O-Pins mit anderen Kanälen ist nicht erlaubt.
- Der Diagnosedeckungsgrad DC jedes Kanals darf minimal 60 % betragen.

Bei der Entwicklung von OCR-Systemen ist eine tiefe Analyse der Ausfälle infolge gemeinsamer Ursachen (Common Cause Faiulre CCF) unvermeidbar. Demzufolge definiert die Norm einen β_{ic}-Faktor[34], der Bezug zu allen Entwicklungsaspekten nimmt:

- Entwurf

[34] [IEC10b] IEC61508; *Anforderungen an sicherheitsbezogene elektrische/elektronische/programmierbare elektronische Systeme.* 2010.

- Konstruktion
- Umgebungsbedingungen etc.

Der β_{ic}-Faktor ist auch quantitativ berechenbar. Die Norm definiert einen Startwert von 33 % und fordet, dass eine Minderung auf mindestens 25 % zu erreichen ist. Somit ist während des Entwicklungsprozesses auf die vorgegebenen Maßnahmen zu achten, die diesen Faktor erhöhen bzw. verringern (siehe Tabellen E1 und E2 in Anhang E des zweiten Normteils[35]).

2.2 FPGAs und ihr Einsatz in sicherheitsgerichteten Systemen

FPGAs gehören zur Familie programmierbarer Logikbausteine. Obwohl die primären Einsatzbereiche die Entwicklung von Prototypen und verschiedene Testansätze waren, hat sich diese Plattform mit der Zeit in einem breiteren Spektrum von Anwendungen durchgesetzt. In medizinischen Elektroniksystemen, in der Weltraumforschung und allen anderen Gebieten, wo eine geringe Anzahl von Chips gefordert wird, gelten FPGAs als eine attraktive Lösung. Als Hauptursache hierfür können Eigenschaften wie Rekonfigurierbarkeit, robuste I/Os und geringe Entwicklungskosten genannt werden. Auf dem Markt gibt es aktuell zwei konkurrierende Firmen, Xilinx und Intel Altera, die den größten Anteil am Weltmarkt abdecken. Xilinx ist jedoch Marktführer.

2.2.1 Aufbau eines FPGA

Herstellerunabhängig weisen alle FPGA-Typen eine ähnliche Struktur auf. Diese ist in Abbildung 2.4[36]auf der nächsten Seite dargestellt.

- Logikblock ist ein FPGA-Element, das aus den Grundelementen - Look-Up-Tabellen (LUT), Multiplexer und D-FlipFlops zusammengesetzt wird. Dieses Element kann beliebige logische Funktion implementieren und wird deswegen als konfigurierbar bezeichnet. Daher stammt die Bezeichnung CLB - konfigurierbarer logischer Block[37].
- Verdrahtung bezeichnet die physikalische Verbindung zwischen den FPGA-Elementen. Man unterscheidet zwischen lokalen und globalen Verdrahtungselementen. Die lokalen verbinden mehrere benachbarte Logikblöcke miteinander, während sich die globalen über das gesamte FPGA spannen[36].

[35] [IEC10b] IEC61508; *Anforderungen an sicherheitsbezogene elektrische/elektronische/programmierbare elektronische Systeme*. 2010.

[36] [Sau10] Sauer, P.; *Hardware-Design mit FPGA : Eine Einführung in den Schaltungsentwurf mit FPGA-Bausteinen*. 2010, S. 13.

[37] [Jan01] Jansen, D.; *Handbuch der Electronic Design Automation : mit 176 Tabellen*. 2001.

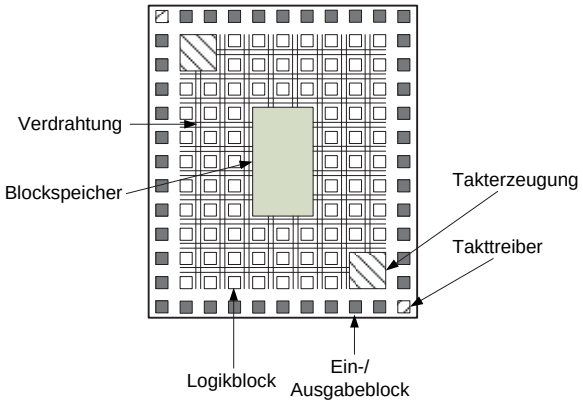


Abbildung 2.4: Aufbau eines FPGA-Bausteins, Quelle [Sau10, S. 13]

- Speicherblock besteht aus einer Vielzahl von Block-RAMs. Mit dem RAM ist in diesem Kontext ein Speicher gemeint, auf dessen einzelne Speicherworte mit jedem Zugriff wahlfrei zugegriffen werden kann.
- Look-Up-Tabelle ist eine Wahrheitstabelle, mit deren Hilfe neben den Grundfunktionen (logisches AND, OR, XOR, NOT, NOR und XNOR) beliebige andere Funktionen realisiert werden können[38].
- Multiplexer ist auch ein Grundelement, welches erlaubt, aus einer Reihe von Eingangssignalen ein bestimmtes Signal auszuwählen und weiterzuschalten. Die Multiplexer existieren innerhalb eines Logikblockes, aber auch im freien Raum zwischen den einzelnen Logikblöcken. Die Funktion der Letzteren ist die Verdrahtung[39].
- D-FlipFlop ist ein Logikbaustein, der als Register zum Speichern von einzelnen Bits dient.
- Ein- bzw. Ausgabeblöcke (IOB) sind direkt mit Anschlüssen (Pins) von FPGA verbunden. Diese Anschlüsse können so konfiguriert werden, dass sie als Eingang, Ausgang oder als Ein- und Ausgang verwendet werden[38].
- Die Anzahl der Blöcke zur Takterzeugung ist abhängig von der FPGA-Größe. Ein FPGA beinhaltet mehrere Anschlüsse für die Ein- und Ausgabe von Taktsignalen. Dies ist notwendig zur Optimierung von Laufzeit und somit zur Minimierung

[38] [Jan01] Jansen, D.; *Handbuch der Electronic Design Automation : mit 176 Tabellen*. 2001.
[39] [FMM12] Farooq, U., Marrakchi, Z. und Mehrez, H.; *Tree-based heterogeneous FPGA architectures : application specific exploration and optimization*. 2012.

der zeitlichen Verschiebung des Taktsignals. Die erste Phase des erzeugten Taktsignals ist die Vervielfachung in einem Taktaufbereitungsblock oder die Synchronisierung mit anderen Signalen. Für diese Zwecke wird meistens ein Frequenzvervielfacher, ein sogenannter Phased-Locked-Loop-Block (PLL) verwendet. Die abgeleiteten Taktsignale stehen in einem festen Taktverhältnis zum ursprünglichen Takt[40].

2.2.2 FPGA-Designmethodik

Beim Entwurf von Schaltungen auf einem FPGA handelt es sich um eine Emulation der gezielten Schaltungsfunktionalität. Diese wird in einer Hardware-Beschreibungssprache (HDL), wie z. B. Verilog oder VHDL, umgesetzt[41]. Der nächste Schritt ist die Synthese des HDL-Codes, um daraus ein für FPGA realistisches und adäquates Modell zu generieren. Als Ergebnis ergibt sich eine Netzliste, die aus den FPGA-Elementen (einzelnen Gattern) besteht. Die synthetisierte Netzliste soll auf konkreten FPGA-Ressourcen abgebildet werden, was in der Implementierungsphase durch das Mapping und Routing erfolgt. Wie die verwendeten CLBs, IOBs und Verdrahtungselemente konfiguriert bzw. verbunden werden, wird in einem Konfigurationsspeicher bestimmt[42]. Deswegen ist der letzte Prozess bei einem FPGA-Design die Generierung des Bitstroms, der im Konfigurationsspeicher geladen wird. Eine detaillierte Darstellung des Entwurfsflusses wird in Abbildung 2.5[43] auf der nächsten Seite gegeben.

2.2.3 FPGA für sicherheitsgerichtete Anwendungen

Die Entwicklung von sicherheitsgerichteten Systemen ist mit einem großen Aufwand verbunden, weil verschiedenste Aspekte wie Architektur, Überwachungsmechanismen, Dokumentierung des Entwicklungsprozesses, Tools etc. betrachtet werden müssen. Chronologisch betrachtet war Intel Altera erster Repräsentant von solchen Systemen auf FPGA-Basis[44]. Das Unternehmen hat sehr eng mit dem Überwachungsinstitut TÜV Rheinland zusammengearbeitet und die aktuellen Trends aus der ASIC-Welt auf die FPGA-Plattform überführt[45].
Für konkrete Anwendungen wurden mehrere FPGAs eingesetzt, um das Konzept der Redundanz zu implementieren. Um den Einsatz seiner Tools und Hardware im Bereich

[40] [Sau10] Sauer, P.; *Hardware-Design mit FPGA : Eine Einführung in den Schaltungsentwurf mit FPGA-Bausteinen*. 2010, vergl. S. 29.
[41] [Chu08a] Chu, P. P.; *FPGA prototyping by Verilog examples : Xilinx Spartan-3 version*. 2008
[Chu08b] Chu, P. P.; *FPGA prototyping by VHDL examples : Xilinx Spartan-3 version*. 2008.
[42] [Hay10] Hayek, A.; *Modellierung, Implementierung und Bewertung einer sicherheitsgerichteten 1oo2-Architektur mit VHDL auf FPGA-Ebene*. 2010.
[43] [SSB14] Sklyarov, V., Skliarova, I. und Barkalov, A.; *Synthesis and Optimization of FPGA-Based Systems*. 2014.
[44] [10a]; *Developing Functional Safety Systems with TÜV-Qualified FPGAs*. 2010.
[45] [13]; *A Validated Methodology for Designing Safe Industrial Systems on a Chip*. 2013.

der funktionalen Sicherheit effizienter zu ermöglichen, hat Altera damals[46] einen Zertifizierungsprozess beim TÜV Rheinland durchgeführt. Auf diese Art und Weise konnten traditionelle sicherheitsbezogene Systeme implementiert werden.

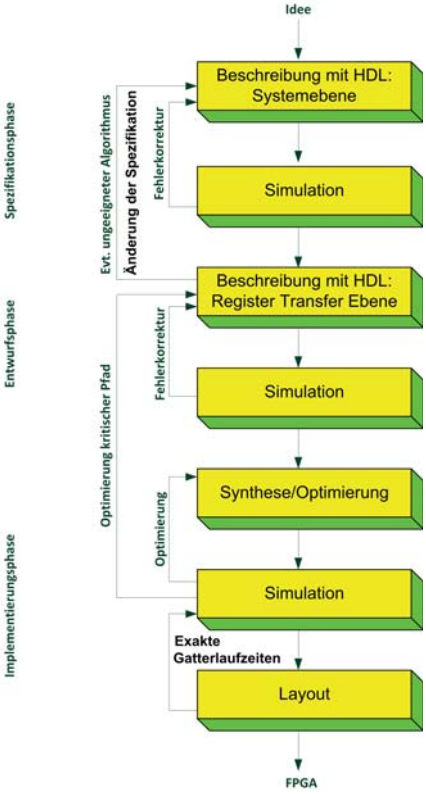


Abbildung 2.5: Schaltungsentwurf mit FPGA, vgl. [SSB14]

Mit der zweiten Ausgabe der IEC 61508 von 2010 wurde ein Raum für Innovationen geschaffen. Als Hauptgrund dafür lässt sich die Einführung des Konzeptes „On-Chip-Redundanz“ nennen. In[47] wurden konkrete Maßnahmen basierend auf einer Schutzregion zur Implementierung der OCR präsentiert. Weiterhin hat derselbe Autor eine

[46] [10a]; *Developing Functional Safety Systems with TÜV-Qualified FPGAs*. 2010.

[47] [Hay10] Hayek, A.; *Modellierung, Implementierung und Bewertung einer sicherheitsgerichteten 1oo2-Architektur mit VHDL auf FPGA-Ebene*. 2010.

Studie[48] über allgemeine Ansätze für die OCR durchgeführt und konkrete Lösungen vorgeschlagen, die lediglich noch verifiziert und zertifiziert werden sollten. Die Verifizierung solcher Lösungen wurde in einer weiteren Arbeit[49] vorgenommen, so dass Xilinx 2013 ein Konzept namens „Isolation Design Flow“[50] veröffentlicht hat. Somit war zu behaupten, dass die Xilinx-FPGAs und die Tools für die Entwicklung der Systeme mit den Anforderungen der IEC 61508 konform geworden sind[51]. Abbildung 2.6 zeigt den traditionellen Designfluss sowie die Erweiterungen im IDF.

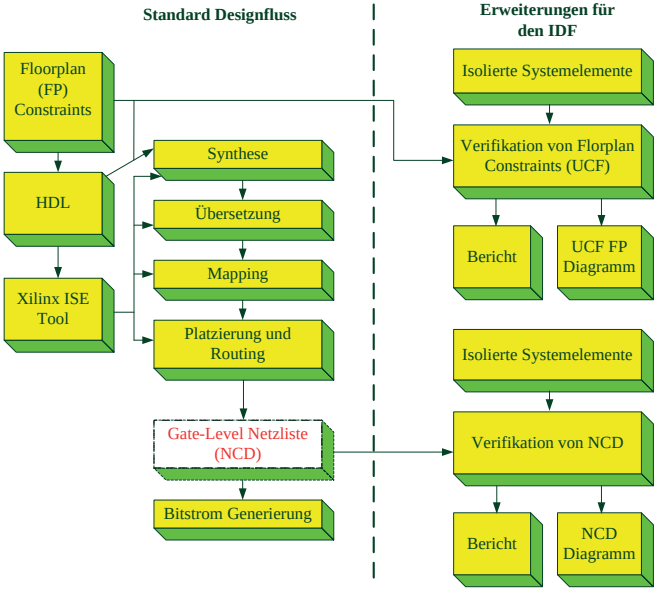


Abbildung 2.6: Isolations-Designfluss im Vergleich zum traditionellen Designfluss, vgl. [HCM15]

Der IDF unterscheidet sich signifikant vom traditionellen Designfluss, weil im gesamten Entwicklungsprozess viel mehr zu beachten ist - beginnend beim Floorplaning bis hin

[48] [BHU08] Borcsok, J., Hayek, A. und Umar, M.; *Implementation of a 1oo2-RISC-architecture on FPGA for safety systems.* 2008.

[49] [CGB12] Corradi, G., Girardey, R. und Becker, J.; *Xilinx tools facilitate development of FPGA applications for IEC61508.* 2012
[GHB10] Girardey, R., Hübner, M. und Becker, J.; *Safety Aware Place and Route for On-Chip Redundancy in Safety Critical Applications.* 2010.

[50] [Cor13c] Corbett, J. D.; *The Xilinx Isolation Design Flow for Fault-Tolerant Systems.* 2013.

[51] [HCM15] Hallett, E., Corradi, G. und McNeil, S.; *Xilinx Reduces Risk and Increases Efficiency for IEC61508 and ISO26262 Certified Safety Applications.* 2015.

zur Verifikation der Gatter-Netzliste. Andererseits sind Flexibilität und Selbstständigkeit während der Implementierung zu den Hauptmerkmalen geworden, da der Entwickler nicht nur die Geometrie des Designs definiert, sondern auch direkten Einfluss auf die Zuweisung der FPGA-Ressourcen hat.

Folgende Charakteristiken des IDFs sind unbedingt zu berücksichtigen[52]:

- Vor der Synthese sollen die sicherheitsgerichteten Systemkomponenten definiert werden, welche in späteren Phasen zu isolieren sind.
- Das User Constraint File (UCF) bestimmt die physikalischen Eigenschaften des zu implementierenden Systems und ist vor der Generierung der Gatter-Netzliste zu verifizieren.
- Einzelne, isolierte Komponenten werden getrennt synthetisiert und anschließend alloziert, platziert und verdrahtet.
- Am Ende wird die Isolierung auf der Gatter-Ebene verifiziert. Ein generierter Bericht gibt ausführliche Informationen darüber, ob alle Isolierungsregeln eingehalten wurden. Die visuelle Darstellung des implementierten Systems mit Isolierungsbereichen wird in einem Diagramm gegeben.

Neben den Standardentwicklungstools von Xilinx ISE erfolgt an dieser Stelle der Einsatz eines neuen Tools zur Verifikation der On-Chip-Redundanz namens „Isolation Verification Tool“. Das IVT stellt zwei Modi zur Verfügung - einmal zur Verifikation des UCF und einmal zur Verifikation der Netzliste[53].

Der Isolierungsdesignflow wird konkret umgesetzt, indem zwischen den sicherheitsbezogenen Systemkomponenten bestimmte Trennungsbereiche aufgebaut sowie die Zwischenverbindungen nach einem spezifischen Konzept definiert werden. Die Trennungsbereiche können vertikal und horizontal implementiert werden. Tabelle 2.7 auf der nächsten Seite zeigt in Anlehnung an[54], wie viele Hauptelemente eines Spartan 6 FPGAs erforderlich sind, um eine vertikale bzw. eine horizontale On-Chip-Trennung zu realisieren. Dieses Konzept ist nur für die Spartan 6 Familie relevant und kann nicht auf andere FPGA-Typen überführt werden, weil bei ihnen andere Regeln für die Trennungskonstruktion anzuwenden sind. Die konkrete Umsetzung dieser Trennungsaspekte wird detailliert im Abschnitt 3.3 behandelt.
Betrachtet aus der Sicht der Norm IEC 61508 wird festgestellt, dass der IDF nur die hardwarespezifische Seite des Entwicklungsprozesses abdeckt und sich somit ausschließlich auf Teil 2 der Norm bezieht. Da aber die HDL-Programme auch als Software interpretiert werden, ist es wiederum erforderlich die Aspekte aus Teil 3 zu berücksichtigen.

[52] [Cor13c] Corbett, J. D.; *The Xilinx Isolation Design Flow for Fault-Tolerant Systems*. 2013.
[53] [Cor13b] Corbett, J. D.; *IVT 7.41 Release Notes and Installation Guide*. 2013
[Cor13a] Corbett, J. D.; *Isolation Verification Tool (IVT) Software User Manual*. 2013.
[54] [McN13] McNeil, S.; *Developing Secure Designs with the Spartan-6 Family Using the Isolation Design Flow*. 2013.

Tabelle 2.7: Anzahl der erforderlichen FPGA-Elemente für den Aufbau einer On-Chip-Trennung

FPGA-Element	Beschreibung	Minimale Anzahl für die vertikale Trennung	Minimale Anzahl für die horizontale Trennung
CLB	Konfigurierbarer Logikblock	1	1
BRAM	Block-RAM	1	1
IOB	Input-Output Block	1	1
DCM	Digitaler Clock-Manager	nicht erlaubt	1
DSP	Digitaler Signal-Prozessor	1	2
PLL	Phase Locked Loop	nicht erlaubt	1
MCB	Hardened Memory Controller	1	1
GTP	High Speed Transceiver	nicht erlaubt	nicht erlaubt
PCIE	PCI Express EndPoint	nicht erlaubt	nicht erlaubt

Analog zum IDF von Xilinx hat Intel Altera auch einen eigenen Designfluss entwickelt und zertifiziert. Der trägt den Namen „Safety Separation Design Flow“(SSDF)[55].
Identisch zum IDF werden im ersten Entwicklungsschritt die nicht sicheren und die sicherheitsrelevanten Systemkomponenten definiert. Danach werden die separaten Partitionen für alle Systemmodule erstellt. Die etablierten Designschritte wie Synthese, Platzierung und Verdrahtung werden im Anschluss ausgeführt. Am Ende des Sicherheits-Separierungs-Designflusses wird die On-Chip-Trennung der sicherheitsrelevanten Systemkomponenten verifiziert (siehe Abbildung 2.7 auf der nächsten Seite).
Die konzeptuellen Unterschiede zwischen dem IDF und dem SDF sind minimal. In beiden Flows werden separate Partitionen für sicherheitsgerichtete Module erstellt. Dies ist die Kernerweiterung in Bezug auf die traditionelle Designkonzepten. Sowohl der Aufbau von solchen Partitionen als auch die abschließende Verifikation der Trennungsbereichen erfolgt integriert und Tool-spezifisch. Wird der gesamte Entwicklungsprozess betrachtet, dann ist festzustellen, dass die Intel Altera Tools automatisierter sind. Dies bedeutet nicht, dass sie vorteilhafter gegenüber den Xilinx Tools sind. Durch die manuelle Erstellung von Trennungsbarrieren hat der Entwickler bei den Xilinx Tools deutlich besseren Einblick in das OCR-Design aber auch eine gewisse Kontrolle über den gesamten Entwicklungsprozess.

[55] [15a]; *FPGA-based Safety Separation Design Flow for Rapid Functional Safety Certification*. 2015.

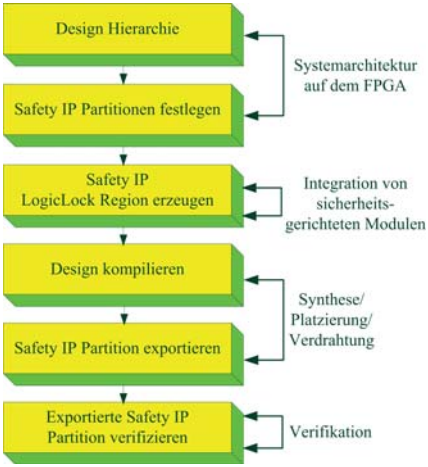


Abbildung 2.7: Sicherheits-Separierungs-Designfluss von Altera, vgl. [15a]

Wird eine Parallele zur Norm gezogen, dann ist festzustellen, dass alle Entwicklungsphasen nach dem V-Modell auch beim IDF ihre Relevanz besitzen. Vor der konkreten Implementierung ist eine Anforderungsspezifikation zu erstellen, damit zwischen den nicht sicheren und sicherheitsrelevanten Funktionen bzw. Systemkomponenten differenziert werden kann. Somit wird die erste Phase im IDF und SSDF beeinflusst, nämlich die Definition der zu isolierenden Komponenten. Wird der Bezug zur FPGA-spezifischen Seite des Entwicklungsprozesses hergestellt, wird die Verifikation des initialen User Constraint Files betrachtet, wodurch auch die Systemarchitektur zum Teil überprüft wird. In[56] wurde ein modifiziertes V-Modell für den FPGA-basierten Systementwurf präsentiert. Dieses Modell kann um die IDF-spezifischen Merkmale erweitert werden, damit in der Zukunft ein Standardentwicklungsprozess für die Implementierung der sicherheitsrelevanten Systeme auf FPGA-Basis definiert werden wird.

2.3 Thermodynamische Grundlagen für integrierte Schaltungen

Die Entwicklung sicherheitsgerichteter Systeme auf einem FPGA impliziert eine grundlegende thermodynamische Analyse sowie die Integration bestimmter Maßnahmen, um

[56] [Hay10] Hayek, A.; *Modellierung, Implementierung und Bewertung einer sicherheitsgerichteten 1oo2-Architektur mit VHDL auf FPGA-Ebene.* 2010.

die aktuelle Temperatur auf dem Chip zu messen und in einer kritischen Situation adäquat reagieren zu können.

Mit der zunehmenden Anzahl der Transistoren und der sinkenden Größe der FPGAs gewinnen die thermalen Effekte immer mehr an Bedeutung, weil sie direkt die Schaltzeit der Transistoren beeinflussen. Diese Beziehung beruht auf der Tatsache, dass die steigende Temperatur eine langsamere Umschaltzeit verursacht, was wiederum nicht nur zu Timing-Problemen im Design führt, sondern auch zu physikalischen Defekten[57].

Die Temperatur hat einen signifikanten Einfluss auf die Zuverlässigkeit und die Ausfallrate. In[58] wird berichtet, dass die Halbierung der Betriebstemperatur eines elektronischen Systems, angegeben in °C, dessen Ausfallrate um eine halbe bis ganze Zehnerpotenz reduzieren kann. Aus diesen Gründen verleiht auch die Norm IEC 61508 der Betrachtung und Überwachung der Temperatur eine große Bedeutung, die sich konkret in der Reduzierung des β_{ic}-Faktors um 9 % manifestiert.

Bei der Zuführung der elektrischen Energieleistung für bestimmte Informationsverarbeitungsprozesse in einem elektronischen Bauteil oder Gerät entfällt nur ein geringer Teil auf die tatsächliche Verarbeitung, während der größte Teil die Verlustleistung produziert. Die Verlustleistung P_V ist äquivalent zur Wärme[58] und soll in Form eines Wärmestromes $\dot{Q}$ auf diverse Arten abgeführt werden. In der Literatur[59] werden grundlegend drei Arten der Wärmeübertragung aufgeführt:

- Wärmeleitung - bei diesem Typ entsteht zwischen den benachbarten Atomen oder Molekülen eines Stoffes eine Übertragung der kinetischen Energie in Form von interatomaren oder -molekularen Impulsen.
- Wärmekonvektion - diese Art bezieht sich auf die Wärmeübertragung von einem festen Körper auf ein Fluid oder umgekehrt.
- Wärmestrahlung - wird in Form des Energietransports auf Basis von elektromagnetischen Wellen im Infrarotbereich realisiert.

Die angesprochene P_V wird nicht nur von elektronischen Bauteilen freigesetzt, sondern auch von Leitungsverbindungen. Dazu wird unterschieden zwischen

- widerstandsabhängigen Leitungsverlusten und
- frequenzabhängigen Schaltverlusten[58].

Wenn eine elektrische Spannung U am Widerstand R anliegt, dann wird die Verlustleistung wie folgt berechnet [LB14]:

$$P_V = \frac{U^2}{R} = I^2 \times R \tag{2.12}$$

[57] [Kle05] Klein, M.; *Static Power and the Importance of Realistic Junction Temperature Analysis*. 2005.

[58] [LB14] Lienig, J. und Brümmer, H.; *Elektronische Gerätetechnik : Grundlagen für das Entwickeln elektronischer Baugruppen und Geräte*. 2014.

[59] [Sei17] Seidel, M.; *Thermodynamik - Verstehen durch Üben : Band 2 Wärmeübertragung*. 2017.

Daraus entsteht eine Temperaturerhöhung ΔT des Widerstandes R in Bezug auf die umgebende Luft. Die entstandene Temperaturdifferenz führt zum Wärmestrom $\dot{Q}$, der zwischen Widerstandsoberfläche und der Umgebung entsteht.

Wird die thermodynamische Analyse auf eine integrierte Schaltung, wie z. B. ein FPGA, angewandt, dann sind folgende Szenarien der Wärmeübertragung möglich:

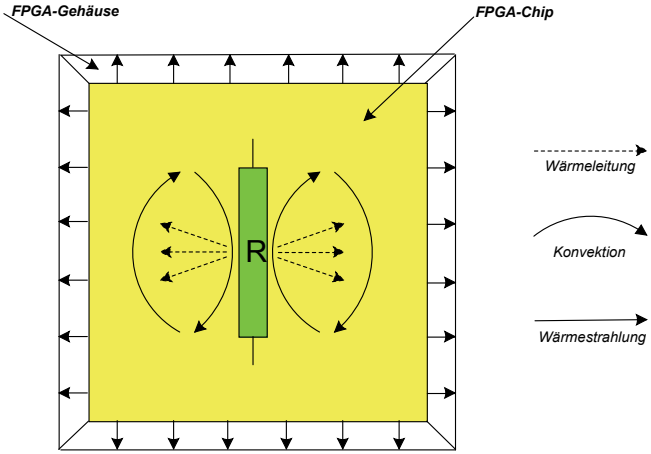


Abbildung 2.8: Wärmeübertragung auf einem FPGA, vgl. [LB14]

Bei einer thermodynamischen Analyse wird auf die Betrachtung von instationären Zuständen wie Aufwärmung oder Abkühlung verzichtet. Stattdessen wird die Annahme eines stationären Zustandes getroffen, wo $P_V = \dot{Q}$ gilt. Als Schwerpunkt dieser Analyse dient entweder die Temperatur der Oberfläche eines Widerstandes oder im Falle einer integrierten Schaltung die Temperatur der Sperrschicht eines Halbleiters. Um die Prozesse der Wärmeübertagung auch quantitativ beschreiben zu können, hat sich in der Praxis ein Netzwerkmodell in Bezug auf das elektrische Netzwerk etabliert[60]. Das Model ist in Abbildung 2.9 auf der nächsten Seite dargestellt.

An dieser Stelle kommt das 2. Kirchhoffsche Gesetz (Maschenregel) zur Anwendung[61].

[60] [Sta+03] Stan, M. R. u. a.; *HotSpot: a dynamic compact thermal model at the processor-architecture level*. 2003
[LB14] Lienig, J. und Brümmer, H.; *Elektronische Gerätetechnik : Grundlagen für das Entwickeln elektronischer Baugruppen und Geräte*. 2014.

[61] [Zas18] Zastrow, D.; *Elektrotechnik : ein Grundlagenlehrbuch : mit 547 Abbildungen, 141 Beispielen und 224 Übungsaufgaben mit Lösungen sowie 27 Übersichten als Wissensspeicher*. 2018.

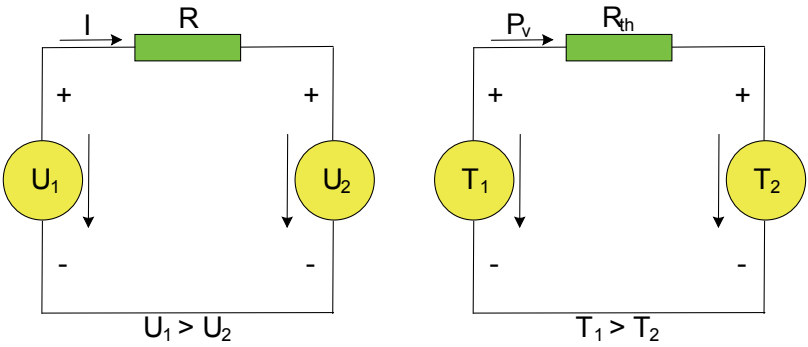


Abbildung 2.9: Analogie zwischen elektrischem und thermischem Netzwerk, vgl. [Sta+03]

Aus dem 2. Kirchhoffschen Gesetz folgt, dass die Differenz aller Spannungen in einem Stromkreis gleich null ist:

$$U_1 - U_2 - I \times R = 0, U_1 - U_2 = I \times R \tag{2.13}$$

Analog gilt beim thermischen Netzwerk:

$$T_1 - T_2 - P_v \times R_{th} = 0, T_1 - T_2 = P_v \times R_{th} \tag{2.14}$$

Somit folgt, dass die Temperaturdifferenz dem Produkt der Verlustleistung (Wärmestrom) und des thermischen Widerstandes entspricht. Die Anwendung dieses Modells wird im Abschnitt 5.2 detaillierter vorgestellt.

3 Konzept

In den vorherigen Kapiteln wurde das traditionelle Konzept eines sicherheitsgerichteten SoC basierend auf einer 1oo2-Sicherheitsarchitektur und einem nicht sicheren Kommunikationssystem näher erläutert. Das Kommunikationssystem wird dabei als ein Blackbox-Kanal interpretiert, d. h. sein interner Aufbau ist für die sicherheitstechnische Betrachtung irrelevant[62]. Das sicherheitsbezogene 1oo2-System ist kommunikationstechnisch gesehen signifikant eingeschränkter als das nicht sichere System[63]. Es kann aber auf die Schnittstellen des Blackbox-Kanals zugreifen, um bestimmte Applikationen zu realisieren. Dadurch werden die Kapazitäten eines Mikrocontrollers innerhalb der sicherheitsrelevanten Architektur bedeutend degradiert, weil sein volles Potenzial nur über das Kommunikationssystem genutzt werden kann.
Die erste Intention dieser Forschungsarbeit war die Eliminierung dieser Diskrepanz, indem die zwei genannten Aspekte - sicherheitsgerichtete Architektur und vollkommene Kommunikationskapazitäten - miteinander verknüpft werden.

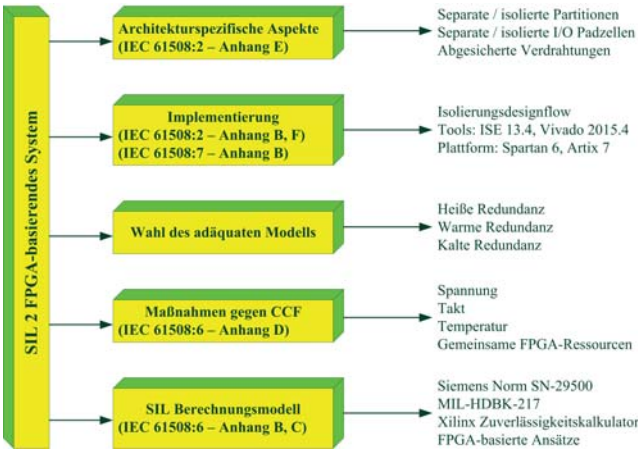


Abbildung 3.1: Konzept zur Implementierung des SIL 2, FPGA-basierten Systems

[62] [Bör15] Börcsök, J.; *Funktionale Sicherheit : Grundzüge sicherheitstechnischer Systeme*. 2015.
[63] [13]; *A Validated Methodology for Designing Safe Industrial Systems on a Chip*. 2013.

Um die Konformität mit den SIL 2-Anforderungen zu gewährleisten, sind dem anvisierten FPGA-System Charakteristiken aus dem Diagramm 3.1 inhärent. Die architekturspezifischen und implementierungsbezogenen Aspekte werden in den Abschnitten 3.1 bis 3.3 präsentiert und aus der Konzeptperspektive argumentiert. Die Wahl des passenden Redundanzmodells erfolgt in Abschnitt 3.4. Maßnahmen zur Vermeidung der Fehler infolge gemeinsamer Ursache und das Konzept zur Wahl eines passenden SIL-Berechnungsmodells werden am Ende dieses Kapitels dargestellt.

3.1 Konzeptuelles Modell für ein komplettes auf CFv2SPP basierendes Rechnersystem

Als Basissystem der anvisierten Sicherheitsarchitektur wird der ColdFire-Mikrocontroller verwendet, der eine Vielfalt von Peripherieschnittstellen zur Verfügung stellt, die zum Paket SPP (Standard Product Platform) gehören[64]. Die wichtigsten Komponenten des CFv2SPP sind:

- 32-Bit V2 ColdFire Kern, der zum Mikrocontrollertyp „Motorola MCF5208“ kompatibel ist
- AMBA-AHB Crossbar Umschalter, der zwischen verschiedenen internen und externen Masters und Slaves umschaltet
- 32 KB interner SRAM und 32 KB interner Cache-Speicher
- Diverse Bussysteme - IPS, AHB und FlexBus
- Diverse Peripherieschnittstellen

Abbildung 3.2 auf der folgenden Seite soll die interne Struktur verdeutlichen. Weitere Details sind in[65] zu finden. Um zu einer kompletten Rechnerarchitektur auf CFv2SPP-Basis beizutragen, werden folgende Änderungen bzw. Erweiterungen vorgenommen:

- Am AHB-Bus werden der SDRAM und die PROFIBUS-Schnittstelle angeschlossen,
- Am FlexBus wird der Flash-Speicher angeschlossen,
- Über den IPS-Bus werden LCD-, CAN-, USB- und parallele Schnittstelle integriert,
- Im SPP-Paket sind diverse Schnittstellen schon enthalten (UART, Ethernet-Controller, I2C, SPI und DMA-Timer). Sie sollen nur noch mit den FPGA-Pins verbunden werden.

[64] [07a]; *CFV2SPP5208 Integration Guide*. 2007.
[65] [07a]; *CFV2SPP5208 Integration Guide*. 2007
[07b]; *CFV2SPP5208 User Guide*. 2007.

Auf die Integration einer SATA-Schnittstelle wird aus Gründen der Komplexität des Zielsystems und der daraus resultierenden technischen Einschränkungen verzichtet. Die Einschränkungen beziehen sich auf die Systemfrequenz von 40 MHz, während für die SATA-Integration eine Taktfrequenz von 150-200 MHz gefordert wird[66].

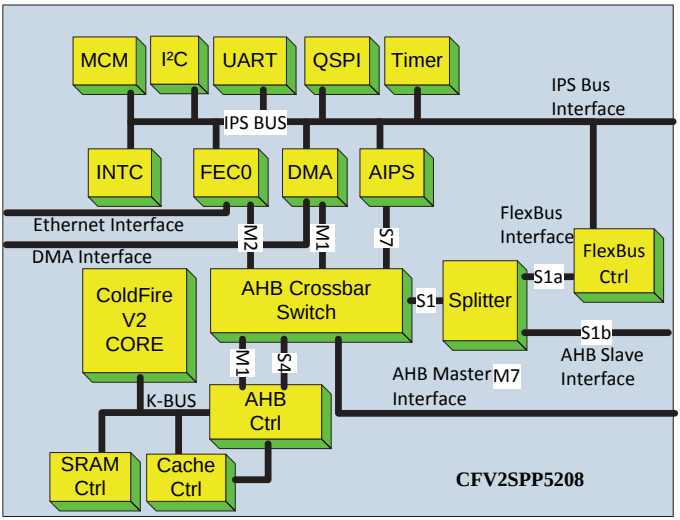


Abbildung 3.2: Interner Aufbau des CFv2SPP-Mikrocontrollers, vgl. [07a]

3.2 Systemarchitektur

Um das anvisierte Rechnersystem sicherheitstechnisch zu entwerfen, ist es erforderlich, folgende Aspekte zu konkretisieren:

- eine redundante Architektur,
- eine parallele Verteilung der Inputs und
- eine sichere Umschaltung der Outputs.

Dabei werden folgende Maßnahmen aus dem siebten Teil der IEC 61508[67] gemäß den Tabellen B.2 und B.6 aus der IEC 61508:2 umgesetzt:

[66] [GST13] Gorman, C., Siqueira, P. und Tessier, R.; *An open-source SATA core for Virtex-4 FPGAs*. 2013.

[67] [IEC10g] IEC61508; *Überblick über Verfahren und Maßnahmen*. 2010.

- Anhang B, Abschnitt B.3.2 Strukturierter Entwurf
- Anhang B, Abschnitt B.3.4 Modularisierung
- Anhang B, Abschnitt B.3.5 Rechnerunterstützte Entwurfswerkzeuge

3.2.1 Redundantes CFv2SPP-System

Den Kern der anvisierten Systemarchitektur stellen die zwei identischen CFv2SPP-Mikrocontrollersysteme dar, welche die On-Chip-Redundanz bilden. Dieser Aspekt ist notwendig, um die Sicherheit und die Verfügbarkeit des Gesamtsystems zu erhöhen. Bei jedem CFv2SPP-System handelt es sich um die im vorherigen Abschnitt beschriebene Struktur.
Die globalen Systeminputs werden an beide CF2vSPP-Instanzen verteilt, während die Outputs nur von einer Instanz global ausgeführt werden dürfen. In diesem Kontext kann das Gesamtsystem aus zwei Perspektiven betrachtet werden:

- extern als ein singuläres System und
- intern als ein redundantes System.

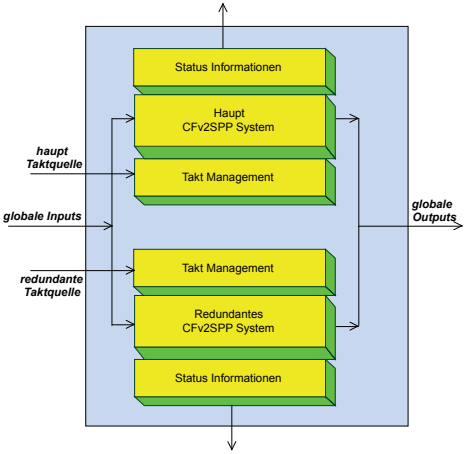


Abbildung 3.3: Aufbau der redundanten Architektur

Der interne, architektur-spezifische Aufbau des redundanten Systems ist in Abbildung 3.3 gegeben und basiert auf folgenden Prinzipien:

- jedes CFv2SPP-System hat eine separate Taktquelle und separate Taktmanagement-Komponenten,

- jedes CFv2SPP-System stellt die separaten Statusinformationen extern zur Verfügung,
- die beiden CFv2SPP-Systeme teilen sich die globalen Inputs und
- die beiden Systeme führen ihre Outputs an einen Multiplexer aus, um die globalen Outputs treiben zu können.

An dieser Stelle sind noch zwei weitere Module zu kontextualisieren, die sich auf das I/O-Arrangement fokussieren.

3.2.2 DistributedInputs

Um die redundante Funktionalität des Gesamtsystems zu gewährleisten, müssen die beiden CFv2SPP-Instanzen mit denselben Inputs parallel verbunden werden. Dieser Aspekt ist grundlegend umstritten, weil die Norm für redundante Systeme die Verwendung separater Inputs und Outputs fordert. Um diese Einschränkung zu beseitigen, implementiert das Modul „DistributedInputs„ die Verteilung der Input-Pins an die beiden CFv2SPP-Instanzen in Form von modulbasierten Zwischenverbindungen. Abbildung 3.4 soll diese Umsetzung in Anlehnung an das „Trusted Routing“-Konzept des Xilinx IDFs[68] verdeutlichen.

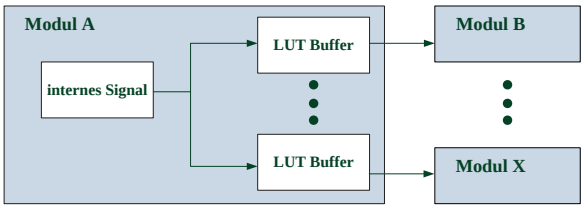


Abbildung 3.4: „Trusted Routing“-Konzept

Somit werden für jedes globale Inputsignal zwei separate LUTs verwendet, wodurch die Verteilung der Inputs redundant ausgelegt wird. Dies gilt analog für alle anderen Zwischenverbindungen im Gesamtsystem, z. B. für die Signalverläufe zwischen den CF2SPP-Instanzen. Dieser Aspekt stellt zusammen mit dem Aufbau der Trennungsbereiche die subtilste sicherheitstechnische Anforderung dar, wenn die Implementierung der OCR auf einem FPGA im Fokus steht. Beim „Trusted Routing„-Konzept wird zwischen folgenden Verbindungsmodellen unterschieden [McN15]:

[68] [McN15] McNeil, S.; *Developing Secure Designs with the Spartan-6 Family Using the Isolation Design Flow.* 2015
[Hal15] Hallett, E.; *Isolation Design Flow for Xilinx 7 Series FPGAs or Zynq-7000 AP SoCs (ISE Tools).* 2015.

- 1-zu-1-Signalverläufe (Modul zum Modul)
- 1-zu-N-Signalverläufe (ein Modul zu mehreren Modulen)
- Eingang-zum-Ausgang-Signalverlauf

Zusätzlich werden gemäß den Anforderungen aus der IEC 61508:2[69], Anhang A, Tabelle A.7 folgende Maßnahmen aus dem siebten Normteil[70] umgesetzt:

- Anhang A, Abschnitt A.6.4 Überwachte Ausgaben
- Anhang A, Abschnitt A.6.5 Eingabevergleich/-entscheidung

3.2.3 SafeMultiplexer

Es wurde schon erwähnt, dass ein redundantes System aus zwei Perspektiven interpretiert werden kann - extern als ein singuläres und intern als ein komplexes, aus mehreren Instanzen bestehendes System. Demzufolge sind die globalen Outputs nur von einer Instanz zu treiben. Um diese traditionelle Einschränkung zu eliminieren, wird ein Mechanismus im Modul „SafeMultiplexer„ implementiert, welches ermöglicht, dass die beiden CFv2SPP-Systeme auf die globalen Outputs zugreifen. Der Zugriff erfolgt nicht parallel, sondern separat und wird nur von der Systeminstanz ausgeführt, die aktuell in Betrieb ist. Die Hauptmerkmale des sicheren Multiplexers sind:

- Redundante Architektur
- Built-In-Self-Test (BIST)
- Externe Testbarkeit

Da dieses Modul zu den sicherheitstechnischen Maßnahmen gehört, wird es im nächsten Kapitel näher beschrieben. Die zu integrierenden Maßnahmen aus [IEC10g] beziehen sich auf:

- Anhang A, Abschnitt A.7.3 Vollständige Hardwareredundanz
- Anhang A, Abschnitt A.7.4 Inspektion durch Verwendung von Testmustern
- Anhang A, Abschnitt A.7.6 Informationsredundanz

[69] [IEC10b] IEC61508; *Anforderungen an sicherheitsbezogene elektrische/elektronische/programmierbare elektronische Systeme.* 2010.
[70] [IEC10g] IEC61508; *Überblick über Verfahren und Maßnahmen.* 2010.

3.3 Isolierung einzelner OCR-Komponenten

In Abschnitt 2.3.3 wurde der Isolierungs-Designfluss von Xilinx erwähnt. Für jede sicherheitsrelevante Komponente des Systems wird eine eigene Partition auf dem FPGA benötigt. In diesem Kontext besteht die On-Chip-Redundanz nicht nur aus den CFv2-SPP-Instanzen, sondern auch aus den Modulen „DistributedInputs„ und „SafeMultiplexer„. Diese vier Komponenten werden durch die Bildung der Barrieren separiert und isoliert. Die Barrieren bestehen aus den nicht verwendeten FPGA-Komponenten und können horizontal oder vertikal implementiert werden. In Abschnitt 2.2.3 sind die Regeln für den Trennungsaufbau auf einem Spartan6 FPGA aufgelistet. Zu den in dieser Studie verwendeten Spartan6 XC6SLX150 und Artix7 XC7A200T FPGAs sind weitere Informationen in[71] zu finden. Um Fehlerarten wie Kurzschlüsse und Übersprechen zwischen den ausgetauschten Signalen zu vermeiden, wurde das Konzept „Trusted Routing“ eingeführt. Durch die Instanziierung einzelner LUT-Buffer wird jedes verteilte Signal unabhängig getrieben. Von den Xilinx-Entwicklungstools wird nur die “Modul zum Modul“-Verdrahtung automatisch umgesetzt. Bei den anderen zwei Verdrahtungsarten sind die LUT-Buffer manuell zu instanziieren. Abbildung 3.5 soll die anvisierte OCR-Architektur verdeutlichen. Die gelb-grünen Kästen repräsentieren die isolierten, sicherheitsrelevanten Komponenten, während die weißen Balken die Trennungsbarrieren darstellen.

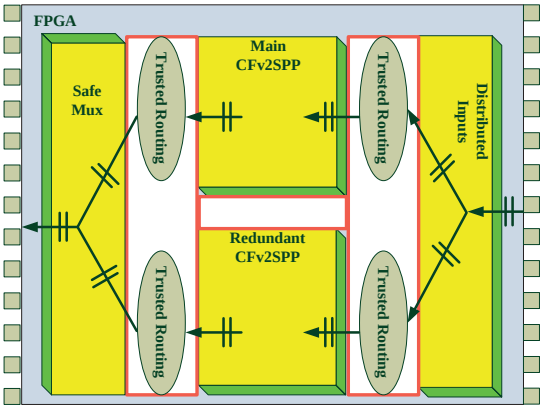


Abbildung 3.5: Anvisierte OCR-Architektur

[71] [McN15] McNeil, S.; *Developing Secure Designs with the Spartan-6 Family Using the Isolation Design Flow*. 2015
[Hal15] Hallett, E.; *Isolation Design Flow for Xilinx 7 Series FPGAs or Zynq-7000 AP SoCs (ISE Tools)*. 2015
[Hal16] Hallett, E.; *Isolation Design Flow for Xilinx 7 Series FPGAs or Zynq-7000 AP SoCs (Vivado Tools)*. 2016.

3.4 Warme Redundanz

Bei der Auslegung einer redundanten Systemarchitektur kommen drei Prinzipien zum Einsatz[72]:

- Heiße Redundanz, bei der die redundanten Komponenten parallel in Betrieb sind und denselben Prozess ausführen
- Kalte Redundanz, bei der nur eine Komponente aktuell in Betrieb ist. Die redundante Komponente wird erst dann aktiviert, wenn die aktuelle ausgefallen ist
- Warme Redundanz, bei der alle Komponenten gleichzeitig aktiviert werden, wobei sich nur eine Komponente tatsächlich in Betrieb befindet. Die andere Komponente ist in einer Art Stand-by-Modus und wartet auf das Aktivierungssignal, um in den echten Betrieb zu wechseln.

Im Bereich der funktionalen Sicherheit hat sich die heiße Redundanz als das meist verbreitete Modell etabliert[73]. Wenn die Erhöhung der Hardware-Fehlertoleranz (HFT) im Fokus steht, dann soll erwähnt werden, dass die Norm IEC 61508 die heiße Redundanz als einziges Konzept akzeptiert, welches die HFT erhöht[74]. Handelt es sich dabei um eine duale Architektur und den HFT-Wert 1, dann werden überwiegend Konzepte wie Hardware- oder Software-Vergleicher integriert. In diesem Kontext besteht ein 1oo2-System aus zwei Systemen, von denen das eine System zur kontinuierlichen Überprüfung des anderen mittels des erwähnten Vergleichers verwendet wird. Im Falle einer registrierten Ungleichheit soll das Gesamtsystem in den sicheren Zustand überführt werden.
Durch die kontinuierliche Komparation zweier Systeminstanzen kann nicht erkannt werden, welche Instanz fehlerhaft war. Konsequenterweise ergibt sich ein schwerwiegender Nachteil dieser Systemarchitekturen - die ausgefallene Systemkomponente kann nicht maskiert werden[75].
Auf der anderen Seite könnte mit einer kalten Redundanz das fehlerhafte Verhalten der Systemkomponente über eine intensive interne und externe Diagnostik registriert werden. Die kritische Situation entsteht bei der Aktivierung der redundanten Komponenten. Denn die Zeit, die für die Aktivierung der redundanten Systeminstanz erforderlich ist, impliziert eine große Gefahr, weil sich das Gesamtsystem in einem vollkommen

[72] [MP10] Meyna, A. und Pauli, B.; *Taschenbuch der Zuverlässigkeitstechnik : Quantitative Bewertungsverfahren*. 2010.
[73] [MP10] Meyna, A. und Pauli, B.; *Taschenbuch der Zuverlässigkeitstechnik : Quantitative Bewertungsverfahren*. 2010
[Bör15] Börcsök, J.; *Funktionale Sicherheit : Grundzüge sicherheitstechnischer Systeme*. 2015.
[74] [IEC10b] IEC61508; *Anforderungen an sicherheitsbezogene elektrische/elektronische/programmierbare elektronische Systeme*. 2010.
[75] [APM14] Anwer, J., Platzner, M. und Meisner, S.; *FPGA Redundancy Configurations: An Automated Design Space Exploration*. 2014
[Ich+10] Ichinomiya, Y. u. a.; *Improving the Robustness of a Softcore Processor against SEUs by Using TMR and Partial Reconfiguration*. 2010.

undefinierten Zustand befindet.
Ein verbreitetes Konzept zur Maskierung ausgefallener Systemkomponenten ist die Komponenten-Verdreifachung (Triple Module Redundancy, TMR) und der Einsatz eines Voters, der nach dem Prinzip der Mehrheitsentscheidung funktioniert[76]. Wegen ihrer Einfachheit gilt die TMR als führend, um FPGA-basierte Systeme sicherheitstechnisch zu implementieren. Als Ergebnis entstanden im Laufe der Zeit zahlreiche Publikationen, wie z. B.[77]. Mit komparativen Analysen über die Vor- und Nachteile des TMR-Konzeptes auf einem FPGA haben sich mehrere Studien beschäftigt[78]. Als Fazit könnte zusammengefasst werden, dass die TMR-Architekturen zu komplex sind und extrem viele Ressourcen benötigen, während die Komponenten-Verdopplung (Dual Module Redundancy DMR) auf der anderen Seite nicht imstande ist, die ausgefallene Systemkomponente zu maskieren.
Ein gravierender Nachteil der TMR wurde in allen erwähnten Studien nicht hervorgehoben, nämlich die Problematik der Mehrheitsentscheidung. Beim Voting zwischen drei Ergebnissen kann nicht ausgeschlossen werden, dass zwei Ergebnisse fehlerhaft sind und nur eins korrekt. In dieser Situation würde das Gesamtsystem als funktionierend angesehen werden, obwohl zwei Systemkomponenten ausgefallen sind. Dies kann zu katastrophalen Konsequenzen führen. Die Verwendung eines Mehrheitsentscheiders auf den FPGA-basierten TMR-Systemen ist somit sehr fragwürdig, obwohl Xilinx in dieses Konzept sehr stark investiert hat und ein TMR Konzept entwickelte, bei dem alle I/Os, Logikbausteine und Voters verdreifacht werden[79]. Jede einzelne Verdreifachung

[76] [MUM10] Matsumoto, K., Uehara, M. und Mori, H.; *Evaluating the Fault Tolerance of Stateful TMR.* 2010.

[77] [Hon+12] Hong, C. u. a.; *Design and implementation of fault-tolerant soft processors on FPGAs.* 2012
[Ich+10] Ichinomiya, Y. u. a.; *Improving the Robustness of a Softcore Processor against SEUs by Using TMR and Partial Reconfiguration.* 2010
[KP09] Kyriakoulakos, K. und Pnevmatikatos, D.; *A novel SRAM-based FPGA architecture for efficient TMR fault tolerance support.* 2009
[Hal+15] Halawa, H. H. u. a.; *FPGA-based reliable TMR controller design for S2A architectures.* 2015
[Cet+13] Cetin, E. u. a.; *Towards bounded error recovery time in FPGA-based TMR circuits using dynamic partial reconfiguration.* 2013.

[78] [LCR03] Lima, F., Carro, L. und Reis, R.; *Designing fault tolerant systems into SRAM-based FPGAs.* 2003
[SKK10] Straka, M., Kastil, J. und Kotasek, Z.; *Modern fault tolerant architectures based on partial dynamic reconfiguration in FPGAs.* 2010
[Ama13] Amari, S. V.; *Optimal design configurations of fault-tolerant systems.* 2013
[MUM10] Matsumoto, K., Uehara, M. und Mori, H.; *Evaluating the Fault Tolerance of Stateful TMR.* 2010
[JCG12] Jacobs, A., Cieslewski, G. und George, A. D.; *Overhead and reliability analysis of algorithm-based fault tolerance in FPGA systems.* 2012
[Kre+12] Kretzschmar, U. u. a.; *Robustness of different TMR granularities in shared wishbone architectures on SRAM FPGA.* 2012
[Cet+13] Cetin, E. u. a.; *Towards bounded error recovery time in FPGA-based TMR circuits using dynamic partial reconfiguration.* 2013.

[79] [10b]; *Xilinx Power Tools Tutorial: Spartan-6 and Virtex-6 FPGAs.* 2010
[Car06] Carmichael, C.; *Triple Module Redundancy Design Techniques for Virtex FPGAs.*

funktioniert nach dem Prinzip der Mehrheitsentscheidung. Dies ist auch ein kritischer Aspekt, weil jeder Voter die Quelle von Fehlern infolge gemeinsamer Ursache darstellt. Reflektierend über den Anhang A der IEC 61508:2 kann festgestellt werden, dass die Qualität der Mehrheitsentscheidung immer im Fokus steht (siehe Tabelle A.4 in[80]). Um die aufgezeigten Nachteile der DMR- und TMR-Architekturen zu beseitigen, fokussiert sich diese Studie auf die Implementierung einer DMR, die nach dem Modell warmer Redundanz funktioniert.
Die beiden CFv2SPP-Instanzen werden parallel hochgefahren, während sich nur eine tatsächlich in Betrieb befindet. Das redundante CFv2SPP-System befindet sich in einem Modus, in dem die Systemtests periodisch ausgeführt werden. Eine intensive interne und externe Diagnostik ist imstande, den Ausfall des Hauptsystems zu registrieren. Dabei wird das Statussignal generiert und an das redundante System gesendet, um aus dem Still- in den Betriebsmodus überführt zu werden. Auf die konkrete Implementierung dieses Konzeptes wird im nächsten Kapitel näher gegangen.

3.5 CCF-Vermeidungskonzept und SIL-Berechnungsmodell

In Abschnitt 1.2 wurden die Quellen der Fehler infolge gemeinsamer Ursache erwähnt. Konzeptuell betrachtet, handelt es sich in dieser Dissertation um:

- neuartige Implementierungen beim Taktmanagement und der Spannungstrennung auf dem FPGA,
- die Übernahme des Standes der Technik im Kontext der Überwachung des Konfigurationsspeichers,
- eine eigene Implementierung von diversen Maßnahmen gemäß den Anforderungen aus [IEC10b] (siehe Anhang A, Tabelle A.1, A.4 und A.8), um den Grad der Diagnosedeckung (DC) auf durch den SIL 2 geforderten 90 % zu erhöhen,
- eine Erweiterung des Standes der Technik bezüglich der Alternativen für eine thermodynamische Analyse.

Die ersten drei Aspekte werden im nächsten Kapitel grundlegend behandelt. Obwohl die konzeptuellen Maßnahmen rigoros sind und von manchen Studien kritisiert werden (siehe[81]), basieren sie einerseits auf den Richtlinien der Norm und stellen andererseits

2006.

[80] [IEC10b] IEC61508; *Anforderungen an sicherheitsbezogene elektrische/elektronische/programmierbare elektronische Systeme*. 2010.

[81] [SEN04b] Shamshiri, S., Esmaeilzadeh, H. und Navabi, Z.; *Test instruction set (TIS) for high level self-testing of CPU cores*. 2004
[LC01] Lai, W.-C. und Cheng, K.-T.; *Instruction-level DfT for testing processor and IP cores in system-on-a-chip*. 2001
[ST10] Sosnowski, J. und Tupaj, L.; *CPU Testability in Embedded Systems*. 2010.

einen Mittelweg zwischen Komplexität und Pragmatik dar. Die Diskussion und Argumentation diesbezüglich erfolgt in Kapitel 6.

Die thermodynamische Betrachtung involviert die eingeführte Systemarchitektur und gewisse analytische Maßnahmen in der Simulation mittels des Tools HotSpot, um nachzuweisen, dass die Propagierung der Wärme auf dem FPGA ein tolerierbares Risiko darstellt. Die Umsetzung dieses Konzeptes wird in Abschnitt 5.2 präsentiert. Die Studien aus diesem Feld fokussieren sich meistens auf die Maßnahmen zur Temperaturüberwachung bzw. zur Temperaturreduzierung (siehe Kapitel 6). Als Sicherheitsmaßnahmen werden folgende Aspekte aus dem siebten Teil der Norm[82] implementiert:

- Anhang B, Abschnitt B.6.1 Funktionstest unter Umgebungsbedingungen
- Anhang B, Abschnitt B.6.7 Worst-Case-Analyse
- Anhang B, Abschnitt B.6.9 Test unter Grenzbedingungen

Durch Ermittlung des PFD_{avg}-Wertes wird die Konformität zum SIL 2 begründet. Werden die Berechnungsmodelle auf einem FPGA in Betracht gezogen, dann können entweder zu rigorose Konzepte verwendet werden (z. B. bei Einsatz des militärischen Standards MIL-HDBK-217 oder der Siemensnorm SN 29500) oder solche, welche die Struktur des FPGAs in den Mittelpunkt rücken und sehr optimistische Ergebnisse aufweisen (wie z. B. die Vorgehensweise aus[83] oder die Verwendung des Xilinx-Zuverlässigkeitskalkulators).
Das Konzept dieser Studie basiert auf der Synthese zwischen der SN 29500 und dem Xilinx-Zuverlässigkeitskalkulator, um den Kompromiss zwischen Praxis und Pragmatik zu finden.

Die Validierung des Gesamtsystems wird anhand folgender Maßnahmen aus der [IEC10g] durchgeführt:

- Anhang B, Abschnitt B.3.6 Simulation
- Anhang B, Abschnitt B.5.1 Funktionstest gegen Anforderungen
- Anhang B, Abschnitt B.5.2 Black-Box-Test
- Anhang C, Abschnitt C.5.3 Schnittstellenprüfung
- Anhang C, Abschnitt C.5.22 Reaktionszeiten und Speicherbeschränkungen

[82] [IEC10g] IEC61508; *Überblick über Verfahren und Maßnahmen*. 2010.
[83] [HD12] Hock, O. und Drgona, P.; *PWM modulator with increased reliability in FPGA circuit*. 2012.

4 Strukturelle Maßnahmen und Modelle zur Betrachtung von Fehlervermeidungs- und Fehlerbeherrschungsaspekten

Im Kapitel über die sicherheitstechnischen Grundlagen wurde erläutert, dass sich die Sicherheitsintegrität in zwei Schwerpunkte gliedert: Hardware- und systematische Integrität. Die Implementierung der OCR auf einem FPGA deckt die hardwarespezifischen Anforderungen der Integrität ab. Dieses Kapitel befasst sich mit den Modellen zur Vermeidung der Ausfälle infolge gemeinsamer Ursache und zur Beherrschung der kritischen Fehler, die zu einem gefährlichen Ausfall des Gesamtsystems führen können. Somit wird der Fokus auf die systematische Eignung gelegt.

Wie schon erwähnt, tendieren die zertifizierten Tools und die Designmethodologie von Xilinx und Altera nur zu einer sicherheitsgerichteten Trennung der kritischen Systemteile auf dem FPGA. In[84] hat Xilinx versucht, die Quellen der Ausfälle infolge gemeinsamer Ursache zu identifizieren und dementsprechend passende Konzepte zur Vermeidung oder Fehlerbeherrschung zu entwickeln. Als CCF-Quellen werden folgende Kategorien bezeichnet:

- I/Os
- Taktmanagement
- Spannung
- Konfigurationsspeicher

Lediglich ein sehr wichtiger Faktor wird ausgelassen - die Temperatur.

Nach einer detaillierten Analyse kann festgestellt werden, dass die von Xilinx vorgeschlagenen Ansätze einen hypothetischen Charakter haben. Beispielsweise wird für die Vermeidung der CCF bezogen auf das Taktmanagement eine Duplizierung des Taktes als Maßnahme genannt. Es wird nicht argumentiert, welche sicherheitstechnischen Vorteile dadurch erzielt werden. Auf andere kritische Aspekte in der Literatur[84] wird im Kapitel 6 näher eingegangen.

In den folgenden Abschnitten werden in dieser Studie ausgearbeitete Modelle zur CCF-Vermeidung und Beherrschung dargestellt. Manche von ihnen werden in Anlehnung an

[84] [HCM15] Hallett, E., Corradi, G. und McNeil, S.; *Xilinx Reduces Risk and Increases Efficiency for IEC61508 and ISO26262 Certified Safety Applications.* 2015.

die standardisierten Techniken von Xilinx und Intel Altera implementiert - wie die I/O-Trennung und die Überwachung des Konfigurationsspeichers, während zur Trennung des Taktes und der Spannung eigene, neuartige Modelle entwickelt worden sind. Die Beschreibung neuartiger Konzepte zur Erhöhung der Diagnosedeckung erfolgt im Abschnitt 4.2. Die Analyse der Temperatur als eines bedeutenden Faktors der Ausfälle infolge gemeinsamer Ursache wird im nächsten Kapitel präsentiert.

4.1 I/Os-Trennung

Die Input- und Outputpins eines FPGAs sind in einer Bank gruppiert. Je nach Typ und Größe des FPGAs variiert auch die Anzahl der Banken. Als Zielplattform wird ein Xilinx Spartan 6 LX150 FPGA mit dem Paket FGG900 verwendet. Es besteht aus 6 Banken, welche eine unterschiedliche Anzahl von Pins beinhalten[85], wie in Tabelle 4.1 dargestellt.

Tabelle 4.1: I/O-Banken des Spartan6 FPGAs

Spartan6 SLX FGG900		
Bank	Anzahl der Pins	Insgesamt
0	132	**576**
1	94	
2	130	
3	114	
4	52	
5	54	

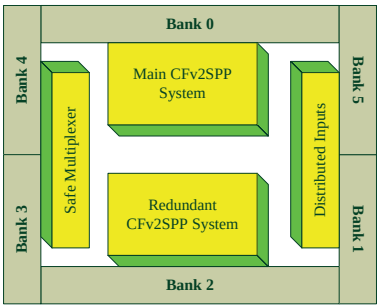


Abbildung 4.1: Trennung der I/Os

[85] [14b]; *Spartan-6 FPGA Packaging and Pinouts*. 2014.

Als Maßnahme zur Vermeidung der CCF definiert Xilinx im IDF , dass jede isolierte, für die Sicherheit relevante Komponente eine separate I/O-Bank besitzen soll. Eine Kollision in dem Sinne, dass sich zwei isolierte Komponenten eine Bank teilen, ist nicht erlaubt. Dieses Konzept wird also architekturspezifisch umgesetzt und entspricht den Anforderungen einer Zuweisung getrennter I/O-Pins zu jeder sicherheitsrelevanten Komponente aus dem zweiten Teil der IEC 61508[86].

Das Gesamtsystem besteht aus vier isolierten Komponenten, welche die OCR bilden. Die Trennung der I/Os wird durch die in Abbildung 4.1 illustrierte Bankzuweisung implementiert.

4.2 Trennung des Taktmanagements

Wenn der gemeinsame Takt für die CFv2SPP-Instanzen verwendet wird, tritt der CCF-Effekt eindeutig auf. Folgende Fehlerszenarien sind möglich und sollen betrachtet werden:

- der globale Takteingang wird mit einem fehlerhaften Taktsignal getrieben,
- die von FPGA-Bauteilen vorgenommene Taktgenerierung ist fehlerhaft,
- die Partition des CFv2SPP-Systems, in der der Takt generiert wird, fällt aus.

Da die anvisierte Systemarchitektur auf dem Prinzip der warmen Redundanz basiert, bringt der synchrone Betrieb beider CFv2SPP-Systeme keinen Vorteil. Auch die maximale Frequenz bleibt identisch, unabhängig davon, ob nur ein oder zwei globale Takte existieren.
Das Spartan 6 LX150 FPGA stellt insgesamt 32 globale Takte zur Verfügung, die an die 16 globalen Taktmultiplexer angeschlossen werden können[87].

Das folgende Konzept wurde entwickelt, um die auf dem gemeinsamen Takt basierenden CCFs zu eliminieren:

- Jede Partition der CFv2SPP-Instanz verfügt über einen separaten globalen Takteingang. Dieser Eingang befindet sich physikalisch auf dem Rand des FPGAs, wo die Instanz platziert ist (somit ist die Anforderung sowohl der IEC 61508 als auch des Xilinx IDFs erfüllt).
- Jede Partition verfügt über einen separaten Baustein für das Taktmanagement (DCM oder PLL).

[86] [IEC10b] IEC61508; *Anforderungen an sicherheitsbezogene elektrische/elektronische/programmierbare elektronische Systeme*. 2010.
[87] [15c]; *Spartan-6 FPGA Clocking Resources*. 2015.

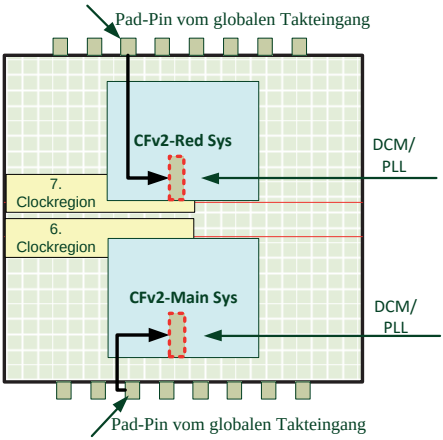


Abbildung 4.2: Trennung des Taktmanagements

Die Betrachtung des Taktnetzwerkes eines CFv2SPP Systems ist genauso essentiell für die Trennung und die Vermeidung der CCFs. Es ist zu berücksichtigen, dass ein CFv2SPP-System aus folgenden Takten besteht[88]:

- Fast Clock für den Core
- Slow Clock (Fast Clock / 2) für die Busse und Peripherie
- Ethernet Clocks
- SPI Clocks

Sie werden alle an die globalen Taktmultiplexer angeschlossen. In unserer Systemarchitektur führt diese Konstellation zu gewissen Isolierungsverletzungen, weil sich bestimmte Takt-Pfade zweier CFv2SPP-Instanzen überkreuzen. Um diese Anomalien unter Kontrolle zu bringen, ist ein Verständnis des Taktmanagements auf dem Spartan6 FPGA erforderlich.

Ein Spartan 6 besteht aus 24 Clock-Regionen. Das gesamte Taktnetzwerk wird mit Hilfe von 16 globalen Taktmultiplexern (BUFGMUX) aufgebaut. Acht von ihnen gehören der sechsten Clock-Region und die restlichen acht der siebten an[89]. Die siebte Clock-Region ist ganz nahe der Partition des redundanten Systems, während die sechste ganz nahe am Haupt-System liegt. Aus diesem Grund sollen im Tool PlanAhead während

[88] [07a]; *CFV2SPP5208 Integration Guide*. 2007.
[89] [15c]; *Spartan-6 FPGA Clocking Resources*. 2015.

des Floorplaning-Prozesses folgende Verbindungen bzw. Zuweisungen manuell erstellt werden:

- die Clocks des Hauptsystems werden an den globalen Multiplexer der sechsten Region angeschlossen,
- die Clocks des redundanten CFv2SPP-Systems werden an den globalen Multiplexer der siebten Region angeschlossen.

4.3 Trennung der Spannungsversorgung

Um durch die gemeinsame Spannung verursachte Systemausfälle zu vermeiden, ist es erforderlich, für die beiden CFv2SPP-Systeme eine separate, unabhängige Spannungsversorgungsebene zu integrieren. Aktuell existiert auf dem Markt nur ein FPGA-basiertes SoC mit dualen, getrennten Spannungsebenen - Zynq7000 von Xilinx. Dieses SoC besteht aus einem Hardcore-Chip und einem FPGA. Da aber für die programmierbare Logik eine gemeinsame Spannungsebene verwendet wird[90], bringt dieses FPGA keine besonderen Vorteile im Vergleich zu anderen Typen mit singulärer Ebene.

Nichtsdestotrotz ist eine gewisse Spannungstrennung auf dem Spartan 6 FPGA doch möglich. Um passende Modelle zu entwickeln, müssen die Arten der Spannungsversorgung auf dem Spartan6 FPGA verstanden werden. In Anlehnung an[91] wird zwischen folgenden Spannungsversorgungspins unterschieden:

- V_{CCINT}, welche für die Versorgung der programmierbaren Logik des FPGAs zuständig sind (1.2 V)
- V_{CCAUX}, welche die Bereiche des Taktmanagements versorgen (optional zwischen 2.5 und 3.3 V)
- V_{CCO} für die Versorgung von I/O-Elementen
- V_{REF}, auch für die Versorgung von I/O-Pins, wenn HSTL-/SSTL-Standards zum Einsatz kommen [92]

Da die Spannungsversorgungspins der I/O-Banken getrennte Versorgungsschienen besitzen[93], wird die konkrete Trennung realisiert, indem für das Hauptsystem nur die Pins der zweiten Bank und für das redundante CFv2SPP nur die Pins der Bank null verwendet werden. Damit CCF im Modul „SafeMux“ vermieden werden, wird dieses Modul

[90] [18a]; *Zynq-7000 All Programmable SoC Overview*. 2018
[18b]; *Zynq-7000 All Programmable SoC, Technical Reference Manual*. 2018.

[91] [16c]; *Spartan-6 FPGA Power Management*. 2016.

[92] Es existieren auch weitere Typen von Spannungsversorgungspins auf dem Spartan6 FPGA. Da sie keine Relevanz für unser Design haben, werden sie außer Betracht gelassen. Für Details kann auf [16c] zugegriffen werden.

[93] [15d]; *Spartan-6 FPGA Data Sheet: DC and Switching Characteristics*. 2015.

mit den Pins der Bank drei versorgt. Analog zu diesem Verfahren wird die Partition des Moduls „DistributedInputs“ an die Pins der ersten Bank angeschlossen.

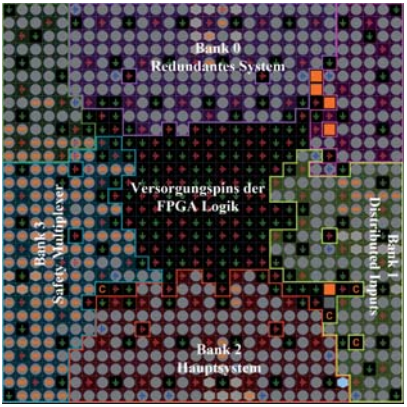


Abbildung 4.3: Trennung der Spannungsversorgung

Um die Trennung der Ressourcen für das Taktmanagement zu implementieren, werden für das Hauptsystem ausschließlich die V_{CCAUX}-Pins der Bank drei verwendet. Dementsprechend werden für das redundante System nur die Pins der Bank null reserviert. Auf die V_{CCAUX}-Pins aus dem mittleren Bereich soll verzichtet werden, weil sie zusammen mit allen V_{CCINT}-Pins an einer gemeinsamen Versorgungsschiene angeschlossen sind und somit keine Möglichkeit zur Vermeidung der CCFs bereitstellen.

4.4 Überwachung des Konfigurationsspeichers

Auf einem FPGA sind drei Speicherarten zu finden:

- verteilter Speicher,
- Blockspeicher und
- Konfigurationsspeicher.

Der verteilte Speicher setzt sich aus einzelnen FlipFlops (FFs) der konfigurierbaren Logikblöcke zusammen. Der Aufbau eines Blockspeichers wurde im Kapitel 2 erläutert. Beim Konfigurationsspeicher handelt es sich um einen arraybasierten Speicher, der aus einzelnen Frames besteht[94]. Diese Art ist über die Gesamtfläche des FPGAs platziert und stellt zahlenmäßig größte Menge von FPGA-Elementen dar. Wie schon

[94] [17c]; *Spartan-6 FPGA Configuration*. 2017.

beschrieben, bestimmt der Inhalt des Konfigurationsspeichers die gewünschte Systemfunktionalität. Dafür ist allerdings nur ein geringer Teil erforderlich, so dass der Rest für die Überwachung irrelevant ist[95]. Bei der Fehlerbetrachtung wird zwischen permanenten und transienten Fehlern unterschieden. Während sich die ersteren entweder auf Herstellungsfehler oder Beschädigung der Hardware beziehen, sind die anderen viel gefährlicher, weil sie während des Betriebs entstehen und somit signifikante Konsequenzen für die Systemfunktion haben können.[96] Dies geschieht, weil die FPGAs sehr empfindlich gegenüber radioaktiver Strahlung sind, die durch bestimmte chemische Prozesse zur Manipulation einzelner Speicherzellen führt[97]. Eine derartige Änderung des Inhalts von Speicherzellen wird in der Literatur als „Single Event Upset“ bezeichnet. Die Klassifizierung, Analyse und Bewertung solcher Effekte ist detailliert in[98] gegeben.

In der Studie[99] befasst sich der Autor mit einer zuverlässigen Generierung des Bitstromes für den Konfigurationsspeicher. Zusammengefasst beruht das Prinzip auf der unabhängigen Erstellung mehrerer Bitströme auf diversen Rechnern, die danach über einen CRC[100]-basierten Algorithmus auf Unterschiede geprüft und anschließend im Konfigurationsspeicher geladen werden. Dadurch wird sichergestellt, dass kein fehlerhafter Bitstrom geladen wird. Dieses Konzept kann auch verwendet werden, um die Fehler im Konfigurationsspeicher zu erkennen, während das System in Betrieb ist. Über den ICAP wird die aktuelle Konfiguration zurückgelesen und mit der ursprünglichen verglichen. Im Falle einer Inkonsistenz kann der Speicher dynamisch rekonfiguriert[101] werden.

Um den Konfigurationsspeicher kontinuierlich zu überwachen, bietet sich die Integration eines Soft-Error-Mitigation (SEM) Controllers von Xilinx[102] an. Dieser Controller ist als IP-Core[103] verfügbar und beinhaltet im Wesentlichen die folgenden Segmente [15b]:

- Internal Configuration Access Port ICAP-Schnittstelle. Dies ist der Zugriffsport

[95] [17b]; *Device Reliability Report*. 2017.

[96] Die permanenten Fehler können auch während des Systembetriebes entstehen. In diesem Kontext sind sie aber deutlich effektiver aufzudecken als die transienten, weil sie ein definiertes Verhalten aufweisen.

[97] [HS15] Hussein, J. und Swift, G.; *Mitigating Single-Event Upsets*. 2015.

[98] [Van+16] Vanat, T. u. a.; *Comparing proton and neutron induced SEU cross section in FPGA*. 2016
[Jin+11] Jing, N. u. a.; *Quantitative SEU Fault Evaluation for SRAM-Based FPGA Architectures and Synthesis Algorithms*. 2011
[Ber+04] Bernardi, P. u. a.; *On the evaluation of SEU sensitiveness in SRAM-based FPGAs*. 2004.

[99] [Hay10] Hayek, A.; *Modellierung, Implementierung und Bewertung einer sicherheitsgerichteten 1oo2-Architektur mit VHDL auf FPGA-Ebene*. 2010.

[100] Cyclic Redundancy Check CRC ist ein etabliertes Verfahren für die Fehleraufdeckung während der Speichervorgänge und der Datenübertragung. Es basiert auf dem Einsatz eines Prüfcodes und der zyklischen Überprüfung gespeicherter bzw. übertragener Daten[SKP12].

[101] [12a]; *Partial Reconfiguration User Guide*. 2012.

[102] [15b]; *LogiCORE IP Soft Error Mitigation Controller v3.4.1*. 2015.

[103] Der Begriff Intellectual Property (IP) bezieht sich auf wiederverwendbare Software- und Hardwarekomponenten, z. B. eine in VHDL implementierte Funktion [Hal+14]

für den internen Konfigurationsspeicher. Über ihn kann der Inhalt des Speichers gelesen und neu beschrieben werden. Der ICAP ist auf einem Xilinx-FPGA als fest verdrahtete Hardwarekomponente vorhanden

- FRAME ECC-Schnittstelle, die den Zugriff auf Informationen und Ergebnisse der Fehlerentdeckungsfunktion ermöglicht
- Status-Schnittstelle, die dem User Einblick in die aktuelle Aufgabe des Controllers verschafft, sei es die Analyse, Überprüfung oder Korrektur des Konfigurationsspeichers
- Error Injection-Schnittstelle, um eine Möglichkeit bereitzustellen, die Fehler in den Konfigurationsspeicher einzupflanzen. Demzufolge kann der Controller während des Betriebs selbst getestet werden
- Monitor-Schnittstelle, welche die Kommunikation zwischen dem Benutzer und dem Controller ermöglicht. Der Controller ist so implementiert, dass er einerseits die Benutzerbefehle über diese Schnittstelle liest und die passende Aufgabe ausführt und andererseits die Statusinformationen als ASCII-Zeichen ausgibt. Weitere Details bezüglich der Struktur und der Funktionsweise sind in[104] zu finden.

Die Funktionalitäten des SEM-Controllers umfassen [15b]:

- Initialisierung des Controllers, nachdem das FPGA-System hochgefahren ist
- Einpflanzung der Fehler, wenn der Ruhezustand erreicht wird. Auf diese Weise kann ein Selbst-Test durchgeführt werden
- Fehlerentdeckung basierend auf dem Error Correcting Code (ECC)[105] und CRC-Algorithmen
- Fehlerkorrektur basierend auf dem Prinzip der partiellen Rekonfiguration
- Fehlerklassifizierung. Dieses Feature ist sehr nützlich, weil es die erkannten Fehler in zwei Gruppen unterteilt: essentielle und nicht essentielle Fehler. Die nicht essentiellen beziehen sich auf die Speicherzellen, die für die Systemfunktionalität irrelevant sind und somit ignoriert werden können.

Wie ein SEM-Controller zu integrieren ist, kann aus[104] und[106] entnommen werden.

[104] [15b]; *LogiCORE IP Soft Error Mitigation Controller v3.4.1.* 2015
[SKP12] Schönfeld, D., Klimant, H. und Piotraschke, R.; *Informations- und Kodierungstheorie.* 2012.

[105] ECC ist ein etabliertes Verfahren für die Fehlerkorrektur während der Speichervorgänge und der Datenübertragung. Es basiert auf dem Einsatz eines so genannten Blockcodes, der zum Prüfen und Korrigieren gespeicherter bzw. übertragener Daten verwendet wird [SKP12].

[106] [Wel15] Welter, M.; *Demonstration of Soft Error Mitigation IP and Partial Reconfiguration Capability on Monolithic Devices.* 2015.

4.5 Erhöhung des DC

Neben der Betrachtung der Ausfälle infolge gemeinsamer Ursache und der Entwicklung von Maßnahmen, die zur Vermeidung oder Milderung führen, ist es fundamental wichtig, auch solche Modelle zu implementieren, die zur Erhöhung des DC-Faktors beitragen. Somit wird der SFF erhöht und der gewünschte SIL 2 erreicht. In Bezug auf Anhang A des zweiten Teils der IEC 61508 sind Teststrukturen für folgende Systemkomponenten und Szenarien zu entwerfen: CPU, Bussystem, den internen Speicher, die Behandlung von Interrupts und Resets (siehe Tabelle A.1 aus[107]). Weiterhin wird ein neuwertiges Konzept des sicheren Multiplexers entwickelt, welches redundant und testbar ist, damit die Systemoutputs auf eine sichere Art und Weise verwendet werden können. Um die DC des Gesamtsystems zu erhöhen, wird im Modul „DistributedInputs“ das Konzept der Informationsredundanz in Anlehnung an die Tabelle A.8 aus[107] umgesetzt. Da für das anvisierte System keine ausreichenden Ausfalldaten existieren, wird es als Typ B klassifiziert. Somit ist für den SIL 2 gemäß der Tabelle 2.4 ein DC von 90 % - $<$ 99 % zu erreichen.

4.5.1 Selbst-Tests

Einige Studien[108] befassen sich mit CPU-Tests, die im Groben den Anforderungen der Norm entsprechen. Ein Nachteil ist die Beschränkung auf die Register- und ALU-Ebene. In[109] sind dieselben Defizite zu finden, wobei die Teststrukturen zusätzlich durch bestimmte Fehlereinpflanzungsmechanismen verifiziert werden.
Um alle Anforderungen aus dem Anhang A, Tabelle A.1 der IEC 61508[107]zu erfüllen, werden im Rahmen dieser Dissertation folgende Tests implementiert:

- Test aller Adressierungsarten
- Test aller CPU-Register (Walking-Bit-Test)
- Test aller MOVE-Befehle
- Test aller arithmetischen Befehle
- Test aller logischen Befehle
- Test aller Schiebebefehle

[107] [IEC10b] IEC61508; *Anforderungen an sicherheitsbezogene elektrische/elektronische/programmierbare elektronische Systeme*. 2010.

[108] [Wil11] Wilamowski, B. M.; *The industrial electronics handbook : Industrial communication systems*. 2011
[TP07] Tamandl, T. und Preininger, P.; *Online Self Tests for Microcontrollers in Safety Related Systems*. 2007.

[109] [Pre+13] Preschern, C. u. a.; *Verifying generic IEC 61508 CPU self-tests with fault injection*. 2013.

- Test aller Bitmanipulationsbefehle
- Test der Programmsteuerungsbefehle
- Test der Systemsteuerungsbefehle
- Test aller Befehle der EMA-Einheit
- Test aller Register des MCMs
- Test aller Register des DMA-Timers
- Galpat-Test für den internen SRAM.

Bei allen Tests wird der erwartete Wert mit dem aktuellen verglichen. Die Überprüfung des Condition Codes wird an allen Stellen durchgeführt, wo das realisierbar ist. Die konkrete Implementierung wird mit Hilfe von[110] umgesetzt. In Bezug auf Teil 7 der Norm[111] werden folgende Sicherheitsmaßnahmen implementiert:

- Anhang C, Abschnitt C.3.3 Assertion-Programmierung
- Anhang C, Abschnitt C.5.5 Durchführung von Testfällen aus der Fehlererwartung
- Anhang C, Abschnitt C.5.6 Durchführung von Testfällen nach Fehlereinpflanzung

Die Tabelle A.1 aus IEC 61508:2[112] reflektierend wird ein DC-Wert von 90 % erreicht.

4.5.2 Implementierung der warmen Redundanz

Im Abschnitt 3.4 wurde argumentiert, warum das Konzept der warmen Redundanz eingesetzt wird. Da der DC des sicheren Multiplexers durch komplette Redundanz der Bussysteme signifikant erhöht wird (siehe nächsten Abschnitt), erleichtert seine Implementierung die Erreichung des SIL 2 und macht das Gesamtsystem „fail-operational“[113]. Nichtsdestotrotz kann das System ohne großen Aufwand in ein „fail-safe“[114] konvertiert werden, falls dies gefordert wird.
Die beschriebenen Selbst-Tests sind nur ein Teil der detaillierten und grundlegenden Diagnostik des Gesamtsystems. Eine solche Diagnostik garantiert das Ausmaskieren des ausgefallenen CFv2SPP-Systems und stellt den ersten Schritt zur Aktivierung des redundanten Systems dar. In diesem Kontext wurden folgende Features entwickelt:

[110] [05]; *ColdFire Family Programmers Reference Manual*. 2005
[07b]; *CFV2SPP5208 User Guide*. 2007.

[111] [IEC10g] IEC61508; *Überblick über Verfahren und Maßnahmen*. 2010.

[112] [IEC10b] IEC61508; *Anforderungen an sicherheitsbezogene elektrische/elektronische/programmierbare elektronische Systeme*. 2010.

[113] Ein System ist fail-operational, wenn es nach einem registrierten Ausfall mit dem Betrieb fortsetzen kann, wie z. B. ein Flugzeug. Zugleich gibt es Anwendungen, wo ein sicherer Zustand zu erreichen ist, wenn es zum Ausfall kommt. Solche Systeme werden als fail-safe bezeichnet [Per+14].

[114] [Per+14] Perez, J. u. a.; *A Safety Certification Strategy for IEC-61508 Compliant Industrial Mixed-Criticality Systems Based on Multicore Partitioning*. 2014.

- die Statusüberprüfung des CFv2SPP-Systems durch die Verwendung interner Statussignale *pst_data* und *mfrz_b*, die vermitteln, ob die CPU korrekt funktioniert. Kombiniert mit den Selbst-Tests kann sehr schnell erkannt werden, dass ein nicht tolerierbarer Fehler aufgetreten ist. Die Statussignale werden forciert, indem jeder nicht bestandene Test einen STOP-Befehl auslöst.
- Das interne Watchdog-Modul ist über das Signal *ipg_swt_reset_b* geeignet einen Fehlzustand der CPU zu signalisieren.
- Der SEM-Controller verfügt auch über ein Statussignal, welches aktiviert wird, wenn ein Fehler im Konfigurationsspeicher aufgedeckt worden ist.
- Über den internen DMA-Timer wird ein Heartbeat-Signal erzeugt.

Ein externer Watchdog kann in VHDL implementiert werden. Seine sicherheitsgerichteten Funktionalitäten umfassen:

- die Überwachung des Heartbeat-Signals. Es ist zu erwähnen, dass das Heartbeat-Signal periodisch auf zwei diverse Werte konfiguriert wird. In der ersten Periode läuft es mit einem Takt, der fünf Mal langsamer als der Systemtakt des CFv2SPP Systems ist, und zwar für eine Zeitspanne von 5 ms. Danach wird der DMA-Timer so umkonfiguriert, dass das Heartbeat-Signal acht Mal langsamer als der Systemtakt ist. Die relevante Zeitspanne beträgt wiederum 5 ms. Diese Dynamik soll gewährleisten, dass der Watchdog ständig zwei unterschiedliche Prüfsequenzen erwartet und auswertet, wodurch die Gefahr eines falschen Triggerns vermieden wird.
- die Überprüfung der oben genannten Statussignale. Im Falle eines Fehlers wird das Hauptsystem deaktiviert und das redundante aktiviert.

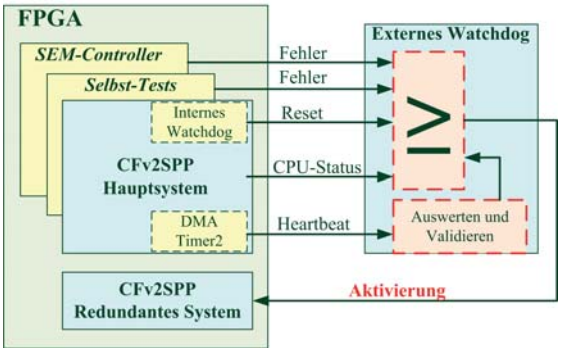


Abbildung 4.4: Das Gesamtsystem, basierend auf dem redundanten Aufbau und einem externen Watchdog

Wie die Abbildung 4.4 zeigt, ermöglicht die intensive Diagnostik zusammen mit dem externen Watchdog die Implementierung des Konzeptes der warmen Redundanz. Die konkrete Realisierung wird in dem folgenden Diagramm dargestellt:

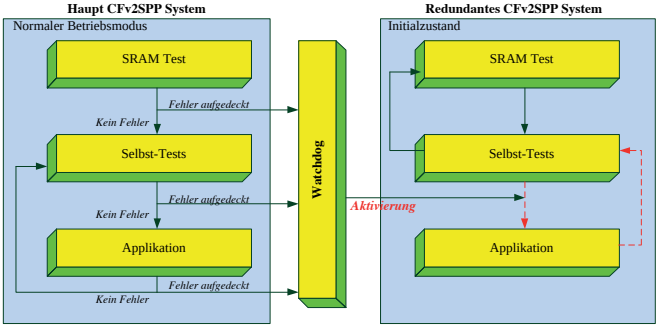


Abbildung 4.5: Konzept der warmen Redundanz

Die beiden CFv2SPP-Instanzen werden parallel hochgefahren und initialisiert. Nach der Initialisierung führen sie den SRAM- und die Selbst-Tests aus. Das Hauptsystem beginnt danach mit dem eigentlichen Task. Das redundante System bleibt hingegen in einem Initialzustand, in dem die Selbst-Tests periodisch ausgeführt werden. Wenn ein Task erfolgreich bearbeitet wurde, können die Selbst-Tests neu ausgeführt werden, bevor ein neuer Task gestartet wird. Wenn durch die Diagnostik ein Fehler aufgedeckt wird, deaktiviert der Watchdog das Hauptsystem und aktiviert das redundante, indem es den Initialzustand verlässt und mit der Taskausführung beginnt. An dieser Stelle sind verschiedene Szenarien möglich, z. B.:

- dass das redundante System mit dem Betrieb von Anfang an beginnt oder
- dass das redundante System mit dem vom Hauptsystem zuletzt ausgeführten Task das Betrieb fortsetzt.

Dies ist die Aufgabe eines sicherheitsgerichteten Betriebssystems und ist somit außerhalb der Betrachtung dieser Forschungsarbeit.

4.5.3 Sicherer Multiplexer

Der externe Watchdog aktiviert das redundante System. An dieser Stelle tritt ein kritischer Vorgang auf, weil Systemausgänge, die vom Hauptsystem betrieben wurden, nun sicher an das redundante System übergeben werden sollen. Aus der Perspektive des

Hauptsystems sollen als Erstes die Stuck-at-Fehler[115] betrachtet werden[116]. Um diese Fehler zu erkennen, wird jedes Outputsignal redundant über zwei verschiedene LUTs ausgeführt. Somit wird das „Trusted Routing“-Prinzip umgesetzt. Die redundante Information ist nicht nur dupliziert, sondern auch invertiert. Analog zu diesem Verfahren werden auch die Outputs des redundanten Systems behandelt.

Der sichere Multiplexer besteht aus drei Komponenten:

- dem Hauptmultiplexer,
- dem redundanten Multiplexer und
- einem Parity Checker

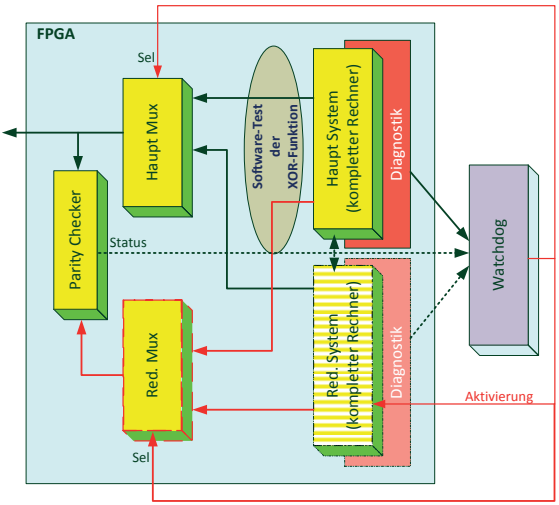


Abbildung 4.6: Das Gesamtsystem mit warm redundanter CFv2SPP-Architektur, externem Watchdog und sicherem Multiplexer

Der Hauptmultiplexer bekommt die tatsächlichen Signale beider CFv2SPP-Systeme und entscheidet anhand eines Selectsignals, welche davon sowohl an die Systemoutputs

[115] Stuck-at-Fehler sind solche Signaldefekte, bei denen der Signalwert permanent auf 0 oder 1 gesetzt ist. Als Hauptursachen solcher Fehler gelten Kurzschlüsse oder Hardwaredefekte.

[116] [KK03] Kubalik, P. und Kubatova, H.; *Design of self checking circuits based on FPGA*. 2003
[Bor+11] Borecky, J. u. a.; *Fault Models Usability Study for On-line Tested FPGA*. 2011
[FH03] Fernandes, D. A. und Harris, I. G.; *Application of built in self-test for interconnect testing of FPGAs*. 2003
[LB03] Lala, P. K. und Burress, A. L.; *Self-checking logic design for FPGA implementation*. 2003.

als auch an den Parity Checker übergeben werden sollen. Das Selectsignal kommt von dem externen Watchdog als Resultat der intensiven Diagnostik. Fällt das Hauptsystem aus, dann wird das redundante selektiert und umgekehrt.

Der redundante Multiplexer bekommt die invertierten Signale beider CFv2SPP-Systeme und entscheidet über das beschriebene Selectsignal, welche Signale dem Parity Checker zu übergeben sind. Ein weiterer kritischer Fall kann auftreten, wenn eine oder beiden LUTs, die für die Übertragung normaler und invertierter Signale verantwortlich sind, defekt sind. In diesem Falle wird der falsche Wert am Systemoutput ausgegeben. Dieser Effekt wird verhindert, indem die beiden CFv2SPP-Instanzen mit einem Testmodus versorgt werden, in dem die Outputsignale in vier möglichen Kombinationen überprüft werden. Vom Parity Checker wird ein passendes Ergebnis erwartet - eine 1, wenn die getriggerten Signalwerte unterschiedlich sind, und eine 0, wenn sie gleich sind.

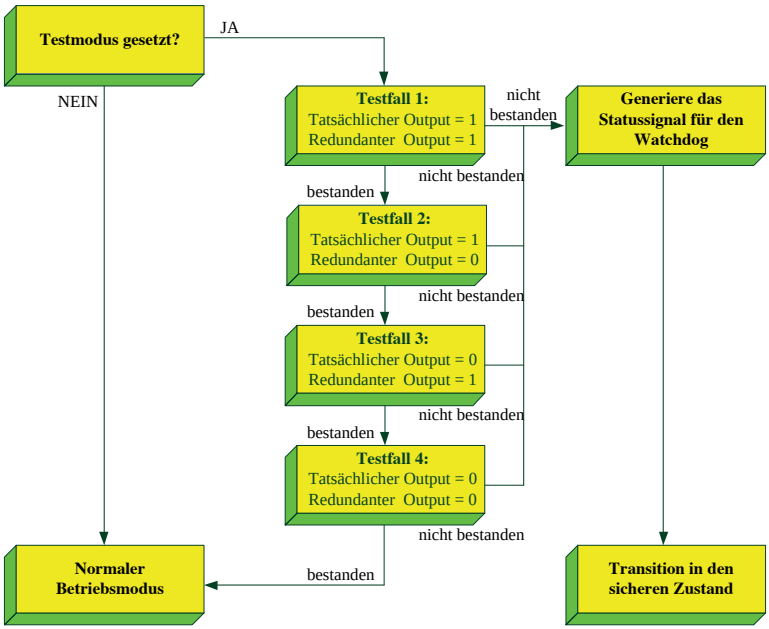


Abbildung 4.7: Erweiterter Testmodus für den sicheren Multiplexer

Dieses Konzept wird durch Implementierung folgender Register in jedem CFv2SPP-System umgesetzt:

- Ein 1-Bit-Register für das Umschalten zwischen dem normalen Betriebsmodus und dem Testmodus

- Fünf 32-Bit-Register für die Simulation bzw. Überprüfung der tatsächlichen Outputs
- Fünf 32-Bit-Register für die Simulation bzw. Überprüfung der redundanten (negierten) Outputs

Um eine höhere Testabdeckung zu erreichen, wird softwaretechnisch den erwähnten Selbst-Tests der Algorithmus aus Abbildung 4.7 hinzugefügt. Der Parity Checker bekommt laufend die tatsächlichen und die invertierten Outputsignale des aktiven Systems und vergleicht sie. Die zu vergleichenden Signale müssen immer unterschiedlich sein, damit das Ergebnis positiv ist. Im anderen Fall, wenn das Ergebnis negativ ist, signalisiert der ParityChecker, dass ein kritischer Fehler aufgetreten ist und dass das Gesamtsystem in einen sicheren Zustand gebracht werden soll. Wegen des redundanten Aufbaus, der internen und externen Testbarkeit wurde für den DC des sicheren Multiplexers ein Wert von 99 % erreicht (siehe Tabelle A.1, Anhang A der [IEC10b]).

4.5.4 Überwachung der Inputs

Um die Bewertung der Sicherheit für das Gesamtsystem durchzuführen, sind noch die Überwachungsmaßnahmen bei der Verteilung der Inputsignale zu integrieren. Im Abschnitt 3.2.2 wurde die elementare Implementierung basierend auf dem „Trusted Routing“-Konzept des IDFs vorgestellt, wo ein Inputsignal über zwei separate LUTs an die beiden CFv2SPP-Instanzen verteilt wird. Um dieses Konzept sicherheitstechnisch zu modellieren, wird in Anlehnung an den Anhang A des zweiten Teils der IEC 61508[117] zunächst die Informationsredundanz gebildet und anschließend getestet. Somit werden die in Abschnitt 3.2.2 präsentierten Maßnahmen implementiert und ein DC von 90 % erreicht.

Die folgenden Extensionen des Moduls „DistributedInputs“ wurden umgesetzt:

- Das Inputsignal wird an eine zusätzliche LUT angeschlossen.
- Das Outputsignal der ursprünglichen LUT wird nicht nur an eine CFv2SPP-Instanz weitergeleitet, sondern auch an die zusätzliche LUT zurückgeführt.
- In der eingefügten LUT wird das Outputsignal mit dem Inputsignal verglichen. Das Ergebnis wird über ein Pad extern ausgegeben und zur kontinuierlichen Überwachung bereitgestellt.

[117] [IEC10b] IEC61508; *Anforderungen an sicherheitsbezogene elektrische/elektronische/programmierbare elektronische Systeme*. 2010.

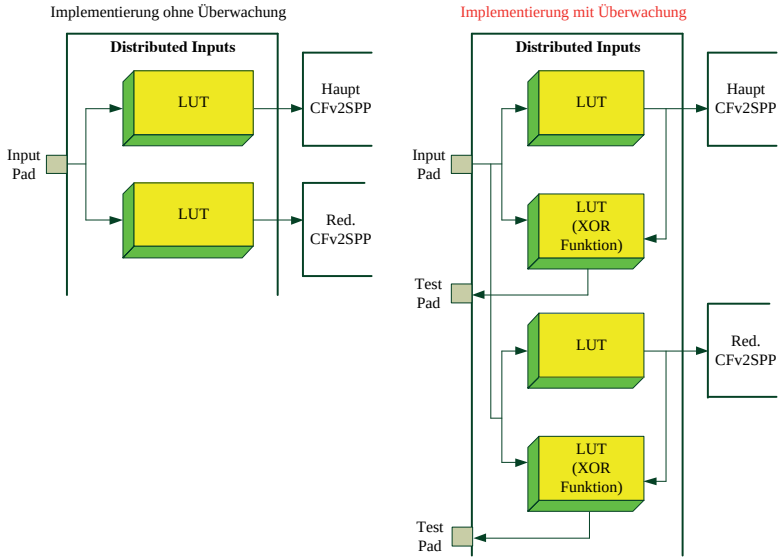


Abbildung 4.8: Sicherheitsmaßnahmen für die Verteilung der Inputsignale

5 Ergebnisse und Evaluierung

Die Implementierung des Zielsystems bestand aus drei Phasen:

- Integration diverser Schnittstellen in einem CFv2SPP-System auf dem Spartan 6 XC6SLX150 FPGA, womit zur kompletten Rechnerarchitektur beigetragen wird
- Implementierung der Sicherheitsmaßnahmen, welche die Entwicklung der warm redundanten sicherheitsbezogenen Architektur ermöglicht haben
- Verifikation des Entwurfs anhand der Software-Tests auf dem FPGA bzw. durch die Simulation der Netzliste des Gesamtsystems mit funktionalen und Selbst-Tests
- Verifikation der On-Chip-Trennung anhand der Überprüfung von isolierten sicherheitsgerichteten Modulen mittels des Xilinx „Isolation Verification Tools“

Dieses Kapitel beginnt mit der Präsentation der Implementierungsergebnisse. Danach wird das System über die Sicherheitsgrößen β_{ic}, DC und SIL evaluiert. Abschließend wird eine thermodynamische Analyse durchgeführt, um die thermische Eignung des FPGA-basierten Systems in sicherheitstechnischen Anwendungen zu bewerten.

5.1 Modellwertung

Folgende Schnittstellen wurden in das CFv2SPP-System integriert:

- 32 KByte interner SRAM,
- 32 KByte interner Cache-Speicher,
- SDRAM mit einem SDRAM-Controller über den AHB-Bus,
- Flash-Speicher über den FlexBus,
- CAN über den IPS-Bus,
- USB über den IPS-Bus,
- LCD über den AHB-Bus.

Im SPP waren die folgenden Schnittstellen schon vorhanden: DMA-Timer, Ethernet, I2C, SPI und UART. Um die Korrektheit der Integration zu validieren, wurden grundlegende, funktionale Software-Tests implementiert und durchgeführt.

Um die sicherheitstechnischen Aspekte zu implementieren, war es erforderlich, die Inputs und Outputs adäquat anzubinden. Die entworfene redundante Systemarchitektur wirkt nach außen als ein singuläres System, während intern zwei getrennte Systeme existieren.
Wie im Abschnitt 3.2 über die Systemarchitektur beschrieben, ist die Verteilung von Inputs nicht kritisch. Basierend auf dem erwähnten Konzept der zuverlässigen Verdrahtung wurden alle Inputs über das Modul „DistributedInputs“ an die zwei CFv2SPP-Instanzen angebunden und über die integrierten Built-In-Self-Test-Maßnahmen verifiziert.
Das Anschließen der Outputs war sehr sensibel, weil sie nur von einem System getrieben werden können. Dies hat zur Entwicklung des sicheren Multiplexers geführt, wie im Abschnitt 4.5.3 beschrieben. Da die Outputs beider CFv2SPP-Instanzen an den sicheren Multiplexer weitergeleitet werden mussten, kam an dieser Stelle wieder das Konzept der zuverlässigen Verdrahtung zum Einsatz.
Obwohl dieses Verdrahtungskonzept laut Xilinx vollautomatisch in den Tools integriert ist[118], haben sich bei der Entwicklung folgende Schwierigkeiten ergeben:

- die begrenzte Anzahl der Verbindungen zwischen den isolierten Komponenten,
- die fehlerhafte Verifikation mit dem IVT nach dem automatisierten Kompilierungsprozess,
- das Sinken der Leistung.

Die folgende Tabelle verleiht einen Überblick über die maximalen Anzahl an Verbindungen, die eine isolierte Komponente mit den anderen Komponenten realisieren konnte.

Tabelle 5.1: Anzahl der Verbindungen zwischen den isolierten Komponenten

Spartan 6 XC6SLX150	
Systemkomponente	**Anzahl der zuverlässigen Verbindungen mit anderen Komponenten**
DistributedInputs	18
CFv2SPP-Main	283
CFv2SPP-Redundant	283
SafeMux	548

Im Abschnitt 3.3 wurde die Isolierung der einzelnen Systemkomponenten beschrieben. An dieser Stelle ist es wichtig zu erwähnen, dass durch die Partitionierung und die

[118] [McN13] McNeil, S.; *Developing Secure Designs with the Spartan-6 Family Using the Isolation Design Flow.* 2013
[McN15] McNeil, S.; *Developing Secure Designs with the Spartan-6 Family Using the Isolation Design Flow.* 2015.

zuverlässige Verdrahtung die Gesamtsystemleistung auf 40 MHz begrenzt worden ist. Des Weiteren mussten über 40 % der FPGA-Ressourcen auf den CFv2SPP-Partitionen ungenutzt bleiben, damit das Design überhaupt kompiliert werden konnte. Als Konsequenz ergab sich die Limitierung für die Integration der oben erwähnten Schnittstellen. Tabelle 5.2 zeigt die Statistik über die verwendeten und nicht verwendeten Ressourcen pro Partition bzw. pro Systemkomponente sowie eine Liste der integrierten Schnittstellen. Die maximale Taktfrequenz beträgt dabei 40 MHz.

Tabelle 5.2: Statistik über die verwendeten Spartan 6 Ressourcen und die integrierten Schnittstellen

Spartan 6 XC6SLX150		
Die integrierten Schnittstellen	**Ressourcenverbrauch**	
	Komponente	**% vom gesamten FPGA**
Flash-Speicher, SDRAM-Speicher, CAN, UART, I2C, DMA-Timer 0, DMA-Timer 1, Profibus	DistributedInputs	1,6
	CFv2SPP-Main	33,27 (davon 1/3 nicht verwendet)
	CFv2SPP-Redundant	40,37 (davon 1/2 nicht verwendet)
	SafeMux	1,6

Nach dem automatischen Designprozess wurde durch das IVT berichtet, dass bestimmte Isolierungsverletzungen vorhanden sind, obwohl alle Designregeln aus der Literatur[119] eingehalten worden sind.

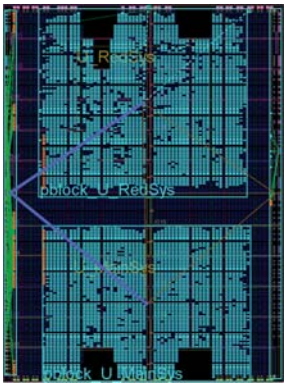


Abbildung 5.1: Implementierungsergebnis des sicherheitsgerichteten CFv2SPP-Systems auf dem Spartan 6 XC6SLX150

[119] [Cor13c] Corbett, J. D.; *The Xilinx Isolation Design Flow for Fault-Tolerant Systems.* 2013.

Nach der detaillierten Analyse wurde festgestellt, dass die Startknoten der zuverlässigen Verdrahtungen problematisch platziert sind. Dieses Problem wurde behoben, indem die FPGA-Elemente, mit denen die Startknoten realisiert worden sind, manuell im PlanAhead-Tool platziert wurden. Das Ergebnis einer erfolgreichen Kompilierung und Verifikation wird in Abbildung 5.1 dargestellt.
Wie bereits erwähnt, war es aufgrund der Ressourcenverschwendung nicht möglich, alle geplanten Schnittstellen zu integrieren. Da das XC6SLX150 das größte FPGA aus der Spartan 6 Familie ist, war es an dieser Stelle notwendig, ein größeres FPGA aus einer anderen Familie zu nehmen, damit diese Limitierung beseitigt wird. Das Artix 7 wurde ausgewählt, weil es eine sehr ähnliche Struktur wie das Spartan 6 aufweist, womit die im Kapitel 4 dargestellten Maßnahmen zur Fehlervermeidung und Fehlerbeherrschung ohne großen Aufwand übernommen werden konnten. Tabelle 5.3 gibt einen Überblick über die integrierten Schnittstellen sowie über den Ressourcenverbrauch auf dem Artix 7 FPGA vom Typ XC7A200TFFG1156.

Tabelle 5.3: Statistik über die verwendeten Artix 7 Ressourcen und die integrierten Schnittstellen

Artix 7 XC7A200TFFG1156		
Die integrierten Schnittstellen	**Ressourcenverbrauch**	
	Komponente	**% vom gesamten FPGA**
Flash-Speicher, SDRAM-Speicher, CAN, UART, I2C, DMA-Timer 0, DMA-Timer 1, Profibus, LCD, SEM_Cntrl	DistributedInputs	0,6
	CFv2SPP-Main	38,42 (davon über 1/2 nicht verwendet)
	CFv2SPP-Redundant	32,26 (davon 1/2 nicht verwendet)
	SafeMux	4,46

Aufgrund der enormen Ressourcenverschwendung konnte nur noch das LCD-Modul integriert werden. Wegen der Größe und der Komplexität wurde auf die Integration der Ethernet- und USB-Controller verzichtet. Die maximale Anzahl der zuverlässigen Verdrahtungen wird in der folgenden Tabelle aufgelistet.

Tabelle 5.4: Anzahl der Verbindungen zwischen den isolierten Komponenten auf dem Artix 7

Artix 7 XC7A200TFFG1156	
Systemkomponente	**Anzahl der zuverlässigen Verbindungen mit anderen Komponenten**
DistributedInputs	18
CFv2SPP-Main	345
CFv2SPP-Redundant	345
SafeMux	672

Als maximale Taktfrequenz wurden wiederum 40 MHz erreicht. Damit das Design frei von den Isolierungsfehlern umgesetzt werden konnte, waren die manuellen Ressourcenzuordnungen wieder erforderlich. Das auf dem Artix 7 entworfene sicherheitsgerichtete System wird in Abbildung 5.2 dargestellt.

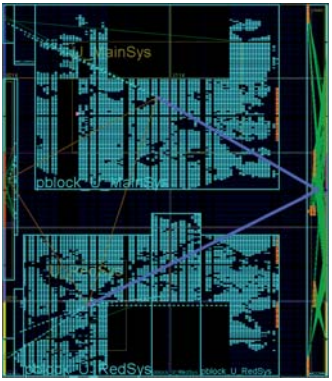


Abbildung 5.2: Implementierungsergebnis des sicherheitsgerichteten CFv2SPP-Systems auf dem Artix 7 XC7A200TFFG1156

Auf dem Artix 7 ergaben sich dieselben Probleme wie auf dem Spartan 6:

- die begrenzte Anzahl der Verbindungen zwischen isolierten Komponenten,
- die fehlerhafte Verifikation mit dem IVT nach dem automatisierten Kompilierungsprozess,
- das Sinken der Leistung.

Dieses Phänomen wurde dann auf den verschiedenen Spartan 6, Artix 7 und Virtex 6 FPGAs näher betrachtet. Dabei wurde festgestellt, dass diese Nachteile nach der Isolierung als ein systematisches Problem auftreten. Als kritischster Nachteil kann die begrenzte Anzahl der Verbindungen zwischen den isolierten Komponenten hervorgehoben werden. Dies ist der Grund, warum die restlichen Schnittstellen im System nicht integriert werden konnten. Im Kapitel 6 werden die Konsequenzen dieser Eingrenzung tiefer analysiert und die sicherheitstechnischen Aspekte des FPGA-Designs reflektiert.

Um die Qualität der implementierten On-Chip-Redundanz, bestehend aus zwei CFv2-SPP-Systemen und zwei zusätzlichen Modulen - „DistributedInputs“ und „SafeMux“ - zu evaluieren, ist es erforderlich gewesen, den β_{ic}-Faktor zu bewerten.

In Anlehnung an den Anhang E des zweiten Teils der IEC 61508[120] wird zwischen den

[120] [IEC10b] IEC61508; *Anforderungen an sicherheitsbezogene elektrische/elektronische/programmierbare elektronische Systeme*. 2010.

Maßnahmen unterschieden, die den β_{ic}-Faktor erhöhen bzw. verringern (siehe Tabellen E1 und E2). Als Basiswert definiert die Norm einen Wert von 33 % und fordert die Senkung auf höchstens 25 %. Die Tabellen A.1 und A.3 aus dem Anhang sind ein Ausschnitt des erwähnten Anhangs E und legen alle Maßnahmen dar.

In Bezug auf die im Kapitel 4 präsentierten Sicherheitsmaßnahmen und Tabellen A.1-4 wird β_{ic} durch folgende Faktoren beeinflusst:

- Verringerung um 4 % durch die Implementierung der Isolierungsbereiche[121]
- Verringerung um 2 % durch die separaten I/O Pins
- Verringerung um 9 % durch eine ausführliche thermodynamische Analyse
- Erhöhung um 2 % wegen den kreuzungsfreien Verbindungsleitungen zwischen den isolierten Komponenten

$$\beta_{ic} = 33\% - 4\% - 2\% - 9\% + 2\% = 20\% \tag{5.1}$$

In den folgenden Abbildungen wird das Verifikationsergebnis der implementierten OCR-Architektur auf dem Spartan 6 bzw. auf dem Artix 7 dargestellt:

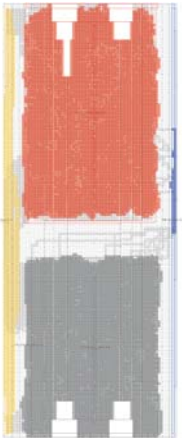


Abbildung 5.3: Verifikationsergebnis auf dem Spartan 6

Mit der Bewertung des β_{ic}-Faktors wurden die Normanforderungen zur Vermeidung der Ausfälle infolge gemeinsamer Ursache erfüllt.

[121] Dies gilt nur im Falle, dass für das System zusätzlich die Maßnahmen aus der Studie [GHB10] implementiert werden. Im Kapitel über die Wertung der Arbeit wird dieser Punkt ausführlich diskutiert.

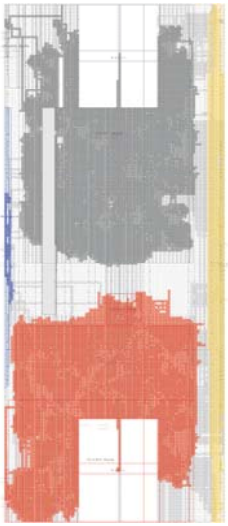


Abbildung 5.4: Verifikationsergebnis auf dem Artix 7

Der nächste Schritt ist die Betrachtung der Sicherheitsintegrität. Dies erfolgt durch die Berechnung der Ausfallrate des Gesamtsystems und des PFD_{avg}-Wertes sowie durch die Bestimmung des Anteils der sicheren Ausfälle. Als Ergebnis wird am Ende der SIL-Wert ermittelt, womit die Sicherheit des implementierten Systems beurteilt wird.

Da ein FPGA-System im Fokus dieser Studie steht, bietet sich für Berechnung der Ausfallraten die Anwendung des Xilinx Zuverlässigkeitskalkulators an. Diese Methode ist im Bereich der funktionalen Sicherheit noch nicht etabliert, weil keine ausreichenden Rückdaten aus dem praktischen Einsatz zur Verfügung stehen. Deswegen wird an dieser Stelle zusätzlich die Gatter-Äquivalenz-Methode angewendet. Daraus werden die Mittelwerte gebildet und dann als Referenzdaten eingesetzt. Somit werden zwei Maßnahmen verknüpft, die sehr unterschiedlichen Charakter haben. Die Gatter-Äquivalenz[122] wird von der Norm anerkannt und empfohlen, ist aber sehr konservativ und liefert pessimistischere Ergebnisse. Auf der anderen Seite ist der Xilinx-Kalkulator

[122] Der $Pfad_{2H}$ sieht den Einsatz der bewährten Zuverlässigkeitsdaten vor. Die Siemensnorm 29500 ist für die Berechnung von Ausfallraten über die Anzahl der Gatter oder der Transistoren weit etabliert. Dabei handelt es sich sehr oft um die pessimistischeren Ergebnisse [AG05a]. Bei der Gatter-Äquivalenz wird eine betrachtete Systemkomponente in die Anzahl der logischen NAND-Gatter umgewandelt (weil mit einer Kombination der NAND-Gatter alle anderen logischen Funktionen implementiert werden können). Über die Referenzdaten von verschiedenen Bauelementen stellt diese Norm die Möglichkeit bereit, die Ausfallrate aus der Anzahl der Gatter oder der Transistoren zu bestimmen.

adäquater, liefert aber optimistischere Ergebnisse.

Obwohl in[123] betont wird, dass die FPGA-Ressourcen im NAND-Gatter sehr einfach konvertiert werden können, ist so eine Umwandlung kein trivialer Process. In[124] wird berichtet, dass Xilinx ab der Virtex 5 Serie keine Angaben mehr über die durchschnittliche Anzahl der Gatter macht. Als Grund wird die funktionale Diskrepanz zwischen den Logikelementen eines FPGAs und den Standardgattern eines ASICs genannt; das Artix 7 FPGA besteht nähmlich aus 6-eingängigen LUTs. Mit so einer LUT kann ein Inverter implementiert werden, wofür nur ein einziges Gatter verwendet wird, aber auch eine komplexe logische Funktion, für welche sechs Gatter verwendet werden müssen [125]. Weiterhin fließen auch andere FPGA-Elemente in die Betrachtung mit ein, wie die FlipFlops, BlockRAMs etc.

Tabelle 5.5: Bestimmung der Anzahl von NAND-Gattern im Modul CFv2SPP (Main und Redundant)

FPGA Ressource		**Äquivalente Anzahl der NAND-Gatter**
Typ	Anzahl	
INV	247	x 1 = 247
LUT1	414	x 1 = 414
LUT2	901	x 2 = 1802
LUT3	2520	x 3 = 7560
LUT4	2489	x 4 = 9956
LUT5	5659	x 5 = 28295
LUT6	10652	x 6 = 63912
MUX	2752	x 2 = 5504
FlipFlop	11999	x 6 = 71994
Schieberegister	33	x 64 = 2112
Insgesamt:		**191 796 NAND Gatter**

Um die Ausfallrate des vorliegenden, sicherheitsgerichteten Systems über die Gatter-Äquivalenz zu bestimmen, werden für jede sicherheitsbezogene Komponente (CFv2SPP Main, CFv2SPP Redundant, DistributedInputs, SafeMux und SEM-Controller) die folgenden Basiselemente ermittelt (siehe Tabelle 5.5 für die CFv2SPP-Instanzen):

- die verwendeten Inverter und LUTs mit der ganz exakten Anzahl der Eingänge (z. B. LUT1 steht für eine LUT mit einem Eingang),
- die verwendeten Multiplexer-Komponenten,
- die verwendeten FlipFlops und

[123] [Pos15] Posner, S. M.; *How many ASIC Gates does it take to fill an FPGA?* 2015.
[124] [Ins12] Instruments, N.; *Vorteile der Virtex-5-FPGAs von Xilinx.* 2012.
[125] Für eine LUT, die aus n Eingängen besteht, werden n * NAND-Gatter gebraucht [Alf08]
Ein FlipFlop besteht durchschnittlich aus 6 NAND-Gattern [ARV07]
Die Annahme für die Schieberegisterkonversion beruht auf den Xilinx-Daten aus [Alf08]

- die verwendeten Schieberegister.

Danach wird für jede dieser Kategorien in Anlehnung an die Siemensnorm 29500-2[126] die Gatter-Äquivalenz erzeugt und daraus anschließend die Ausfallrate berechnet. Für die Bewertung der Sicherheit werden noch die Speicher (SRAM, Cache, SDRAM und Flash) betrachtet.

Über den zweiten Teil der SN 29500 und die Daten[126], die sich auf die Ausfallraten von Mikrocontrollern beziehen, ergibt sich für den betrachteten CFv2SPP-Mikrocontroller der folgende Failure-In-Time (FIT)-Wert[127]:

$$Integrationsgrad > 10^4 - 10^5\, Gatter => \lambda_{\mathbf{CFv2SPP-Core}} = 80\ FIT \tag{5.2}$$

Um die Gesamtausfallrate einer CFv2SPP-Instanz zu bestimmen, müssen noch die Daten des SRAMs und des Cache-Speichers aufaddiert werden. Da der Cache auch mit den BlockRAM-Komponenten implementiert wird, kann er bei dieser Betrachtung auch als ein SRAM betrachtet werden. Referenziert über die SN 29500 und die Daten bezüglich der Speicherkomponenten, beträgt die Ausfallrate:

$$SRAM\ 32\ KB => \lambda_{\mathbf{SRAM}} = 10\ FIT \tag{5.3}$$

$$Cache\ 32\ KB => \lambda_{\mathbf{Cache}} = 10\ FIT \tag{5.4}$$

$$\begin{aligned} \lambda_{\mathbf{CFv2SPP-Gesamt}} &= \lambda_{CFv2SPP-Core} + \lambda_{SRAM} + \lambda_{Cache} \\ &= 80\ FIT + 10\ FIT + 10\ FIT = 100\ FIT \end{aligned} \tag{5.5}$$

Tabelle 5.6: Bestimmung der Anzahl von NAND-Gattern im Modul „DistributedInputs“

FPGA Ressource		**Äquivalente Anzahl der NAND-Gatter**
Typ	Anzahl	
LUT1	18	x 1 = 18
PLL	2	x 1500 = 3000
Insgesamt:		**3018 NAND Gatter**

Referenziert über die Daten für die Bus-Interface- und analogen Schaltkreise aus der SN 29500, ergibt sich für das Modul „DisitributedInputs“ die folgende Ausfallrate:

$$Integrationsgrad > 500\, Gatter => \lambda_{\mathbf{DistributedInputsLogik}} = 5\ FIT \tag{5.6}$$

$$\begin{aligned} \lambda_{\mathbf{DistributedInputsGesamt}} &= \lambda_{DistributedInputsLogik} + 2 \times \lambda_{PLL} \\ &= 5\ FIT + (2 \times 20\ FIT) = 45\ FIT \end{aligned} \tag{5.7}$$

[126] [AG05b] AG, S.; *SN 29500-2: Teil-2 Erwartungswerte von integrierten Schaltkreisen*. 2005.

[127] Die Ausfallrate wird meistens in Failure In Time (FIT) ausgedrückt. Dabei handelt es sich um die Anzahl der Ausfälle pro 10^9 Stunden [Bör15].

[127] In Anlehnung an ([Ant+03] Antreich, K. u. a.; *Modeling, Simulation, and Optimization of Integrated Circuits*. 2003) besteht eine PLL aus ungefähr 1500 Transistoren. Bezüglich der Norm [AG05b] ergibt sich daraus eine Ausfallrate von 20 FIT.

Tabelle 5.7: Bestimmung der Anzahl von NAND-Gattern im Modul SEM-Controller

FPGA Ressource		**Äquivalente Anzahl der NAND-Gatter**
Typ	Anzahl	
LUT5	34	x 5 = 170
LUT6	658	x 6 = 3948
FlipFlops	531	x 6 = 3186
Insgesamt:		**7304 NAND Gatter**

Der SEM Controller wird über die Daten bezüglich der Peripherie aus der SN 29500 wie folgt ausgewertet:

$$Integrationsgrad > 10^3 - 10^4\, Gatter => \lambda_{\mathbf{SEMCntrl}} = 30\, FIT \tag{5.8}$$

Tabelle 5.8: Bestimmung der Anzahl von NAND-Gattern im Modul „SafeMux“

FPGA Ressource		**Äquivalente Anzahl der NAND-Gatter**
Typ	Anzahl	
LUT1	100	x 1 = 100
LUT2	3	x 2 = 6
LUT3	287	x 3 = 861
LUT4	23	x 4 = 92
LUT5	4	x 5 = 20
LUT6	47	x 6 = 282
MUX	2	x 2 = 4
Insgesamt:		**1365 NAND Gatter**

Das Modul „SafeMux“ kann auch über die Daten für die Bus-Interface-Schaltkreise bewertet werden:

$$Integrationsgrad > 500\, Gatter => \lambda_{\mathbf{SafeMux}} = 8\, FIT \tag{5.9}$$

Nun werden die Ausfallraten über den Xilinx-Zuverlässigkeitskalkulator ermittelt. Dabei werden die folgenden Eigenschaften des Artix 7 FPGAs berücksichtigt:

- Die Ausfallrate des Konfigurationsspeichers beträgt 73 FIT/Mbit[128].
- Die Ausfallrate des BlockRAMs beträgt 66 FIT/Mbit[130].
- Ein FPGA-Slice besteht aus 4 LUTs[129].

[128] [17b]; *Device Reliability Report*. 2017.
[129] [16a]; *7 Series FPGAs Configurable Logic Block*. 2016.

Nach der Literatur[130] setzt sich die Gesamtausfallrate einer betrachteten Einheit aus der Ausfallrate des Konfigurationsspeichers λ_{KS} und der Ausfallrate des BRAM-Speichers λ_{BR} zusammen. Der Zuverlässigkeitskalkulator berechnet diese einzelnen Ausfallraten über die Anzahl der Konfigurationsbits für Slices, BlockRAMs unnd I/O Blöcke bzw. über die Anzahl der Speicherbits für die verwendeten BlockRAMs. Beispiele sind in[130] gegeben. Aus diesem Dokument wurden folgende Daten entnommen:

Tabelle 5.9: Relation zwischen den FPGA-Elementen und der Anzahl zugehöriger Konfigurationsbits

Artix 7 XC7A200TFFG1156	
FPGA-Element	**Anzahl der Konfigurationsbits**
Slice	1166
BlockRAM (36 KB)	9396
BlockRAM (18 KB)	4698
I/O-Block	2850

Es ist noch zu erwähnen, dass nicht die Gesamtgröße des Konfigurationsspeichers betrachtet wird, sondern nur die 10 %, weil der Rest keine Auswirkung auf das Systemdesign hat[130]. Um den gesamten Konfigurationsspeicher relevant für die Betrachtung zu machen, wären alle Grundelemente des FPGAs für das anvisierte Systemdesign zu verwenden. Dies ist aber aus diversen technischen, entwicklungsbezogenen und physikalischen Gründen nicht realisierbar, z. B. wegen Timingvorgaben, Systemgröße etc.
Die Ausfallrate werden bezüglich [17b] und [16a] nach den Formeln 5.10 und 5.11 berechnet:

$$\lambda_{KS} = 10\% \times (Anzahl\,der\,FPGA - Elemente) \times (Konfigurationsbits) \times 73\,FIT/Mbit \tag{5.10}$$

$$\lambda_{BR} = (Anzahl\,der\,BlockRAM - Blöcke) \times (Speicherbits) \times 66\,FIT/Mbit \tag{5.11}$$

Der CFv2SPP-Mikrocontroller beinhaltet die folgenden relevanten FPGA-Elemente (siehe Tabelle 5.5):

- 22635 LUTs. Daraus ergeben sich ca. 5659 Slices
- 17 BlockRAM (36 KB)
- 9 BlockRAM (18 KB)

[130] [17b]; *Device Reliability Report*. 2017.

- 4 I/O-Blöcke

Für den Konfigurationsspeicher ergeben sich die folgenden Ausfallraten:

- $\lambda_{KonfigSlice}$ = 0,1 * 5659 * 1166 bit * 73 FIT/Mbit = 48,17 FIT
- $\lambda_{KonfigBRAM36}$ = 0,1 * 17 * 9396 bit * 73 FIT/Mbit = 1,17 FIT
- $\lambda_{KonfigBRAM18}$ = 0,1 * 9 * 4698 bit * 73 FIT/Mbit = 0,31 FIT
- $\lambda_{KonfigIO}$ = 0,1 * 4 * 2850 bit * 73 FIT/Mbit = 0,083 FIT

Die Gesamtausfallrate des Konfigurationsspeichers beträgt:

$$\begin{aligned}\lambda_{KS_{CFv2SPP}} &= \lambda_{KonfigSlice} + \lambda_{KonfigBRAM36} + \lambda_{KonfigBRAM18} + \lambda_{KonfigIO} \\ &= 49,73\,FIT\end{aligned} \tag{5.12}$$

Bei der Betrachtung des BlockRAM-Speichers folgt:

- λ_{BRAM36} = 17 * 36000 bit * 66 FIT/Mbit = 40,39 FIT
- λ_{BRAM18} = 9 * 18000 bit * 66 FIT/Mbit = 10,69 FIT

$$\lambda_{BR_{CFv2SPP}} = \lambda_{BRAM36} + \lambda_{BRAM18} = 51,08\,FIT \tag{5.13}$$

Für die Gesamtausfallrate des CFv2SPP-Mikrocontrollers gilt dann:

$$\lambda_{CFv2SPP-Gesamt} = \lambda_{KS_{CFv2SPP}} + \lambda_{BR_{CFv2SPP}} = 100,81\,FIT \tag{5.14}$$

Um die Ausfallrate des Moduls „DistributedInputs“ zu berechnen, werden die folgenden Ressourcen betrachtet:

- 18 LUTs. Daraus ergeben sich 4,5 Slices
- 22 I/O Blöcke

Für den Konfigurationsspeicher ergeben sich folgende Ausfallraten:

- $\lambda_{KonfigSlice}$ = 0,1 * 4,5 * 1166 bit * 73 FIT/Mbit = 0,038 FIT
- $\lambda_{KonfigIO}$ = 0,1 * 22 * 2850 bit * 73 FIT/Mbit = 0,46 FIT

Die Gesamtausfallrate des Konfigurationsspeichers beträgt:

$$\lambda_{KS_{DistributedInputs}} = \lambda_{KonfigSlice} + \lambda_{KonfigIO} = 0,5\,FIT \tag{5.15}$$

Dieses Modul beinhaltet keinen BlockRAM-Speicher. Es besteht aber aus 2 PLLs. Da Xilinx keine Daten über das Ausfallverhalten der eingesetzten PLLs zur Verfügung stellt, werden an dieser Stelle die Daten aus[131] übernommen. Die Gesamtausfallrate setzt sich somit aus der λ der PLLs und der $\lambda_{KS_{DistributedInputs}}$ zusammen.

$$\lambda_{DistributedInputs} = \lambda_{KS_{DistributedInputs}} + 2 \times 2,4\,FIT = 5,3\,FIT \tag{5.16}$$

Bezüglich des SEM-Controllers werden die folgenden Ressourcen betrachtet:

- 4118 LUTs. Daraus ergeben sich ca. 1029 Slices
- 7 BlockRAM (36 KB)
- 3 BlockRAM (18 KB)

Somit ergeben sich die folgenden einzelnen Ausfallraten:

- $\lambda_{KonfigSlice}$ = 0,1 * 1029 * 1166 bit * 73 FIT/Mbit = 8,76 FIT
- $\lambda_{KonfigBRAM36}$ = 0,1 * 7 * 9396 bit * 73 FIT/Mbit = 0,48 FIT
- $\lambda_{KonfigBRAM18}$ = 0,1 * 3 * 4698 bit * 73 FIT/Mbit = 0,10 FIT

Daraus folgt:

$$\lambda_{KS_{SEMCntrl}} = \lambda_{KonfigSlice} + \lambda_{KonfigBRAM36} + \lambda_{KonfigBRAM18} = 9,34\,FIT \tag{5.17}$$

Für die Berechnung der Ausfallrate der BlockRAMs werden laut Xilinx-Angabe[132] nur 36208 Bits gefordert:

$$\lambda_{BR_{SEMCntrl}} = 36208\,bit \times 66FIT/Mbit = 2,39\,FIT \tag{5.18}$$

Die Gesamtausfallrate beträgt:

$$\lambda_{SEMCntrl} = \lambda_{KS_{SEMCntrl}} + \lambda_{BR_{SEMCntrl}} = 11,73\,FIT \tag{5.19}$$

Das Modul „SafeMux“ besteht aus den folgenden Ressourcen:

- 464 LUTs. Daraus ergeben sich 116 Slices

[131] [14a]; *Quarterly Reliability Report*. 2014.
[132] [17b]; *Device Reliability Report*. 2017.

- 147 I/O-Blöcke

Die Ausfallrate des Konfigurationsspeichers ergibt sich aus:

- $\lambda_{KonfigSlice}$ = 0,1 * 116 * 1166 bit * 73 FIT/Mbit = 0,99 FIT
- $\lambda_{KonfigIO}$ = 0,1 * 147 * 2850 bit * 73 FIT/Mbit = 3,06 FIT

Da dieses Modul keinen BlockRAM-Speicher enthält, ist die Ausfallrate des Konfigurationsspeichers zugleich die Gesamtausfallrate.

$$\lambda_{SafeMux} = \lambda_{KS_{SafeMux}} = \lambda_{KonfigSlice} + \lambda_{KonfigIO} = 4,05\,FIT \tag{5.20}$$

Somit wurde die Bewertung mittels des Xilinx-Zuverlässigkeitskalkulators abgeschlossen. Im Folgenden werden die λ-Mittelwerte in Bezug auf die Gatter-Äquivalenz gebildet und im Anschluss die Zuverlässigkeitsfunktion des gesamten sicherheitsgerichteten Systems bestimmt. Dafür ist es erforderlich, ein Zuverlässigkeitsblockdiagramm zu erstellen (siehe Abbildung 5.5), um aus der internen Systemstruktur abzuleiten, wie die einzelnen Systemkomponenten miteinander agieren und wie sich eine solche Interaktion auf die Berechnung der Gesamtzuverlässigkeit bzw. des PFD_{avg}-Wertes auswirkt[133]. Bei den Komponenten ohne Redundanz handelt es sich um eine Serienschaltung, bei der die Zuverlässigkeitsfunktionen einzelner Systemkomponenten einfach multipliziert werden[133],[134]:

$$R_{ser} = R_1(t) \times R_2(t) \times ... \times R_n(t) \tag{5.21}$$

Die redundanten Komponenten werden wie eine Parallelschaltung interpretiert [Bör15], [IEC10d]. Bei einem redundanten System aus zwei Komponenten ergibt sich:

$$R_{par} = R_1(t) + R_2(t) - R_1(t) \times R_2(t) \tag{5.22}$$

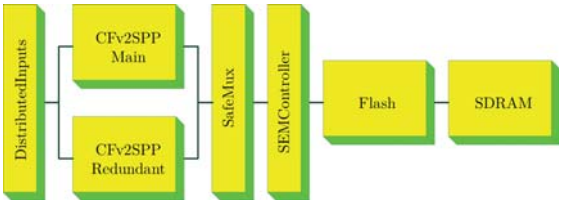


Abbildung 5.5: Zuverlässigkeitsblockdiagramm des Gesamtsystems

[133] [Bör15] Börcsök, J.; *Funktionale Sicherheit : Grundzüge sicherheitstechnischer Systeme*. 2015.
[134] [IEC10d] IEC61508; *Anwendungsrichtlinie für Teile 2 und 3*. 2010.

An dieser Stelle ist erwähnenswert, dass diese Gleichungen nur unter der Annahme einer konstanten Ausfallrate $\lambda(t) = \lambda$ gelten.

Das zu betrachtende System besteht aus der seriellen Verschaltung folgender Komponenten:

- DistributedInputs
- Zwei CFv2SPP Systeme
- SafeMux
- SEM-Controller
- Flash-Speicher
- SDRAM

Die zwei CFv2SPP-Systeme sind redundant ausgelegt und somit parallel verschaltet.

Tabelle 5.10: Berechnung der mittleren Ausfallraten

SystemKomponente	**Ausfallrate in FIT**		
	Gatter Äquivalenz	**Xilinx Kalkulator**	**Mittelwert**
CFv2SPP-Main	100	100,81	100,405
CFvSPP-Redundant	100	100,81	100,405
DistributedInputs	45	5,3	25,15
SEMController	30	11,73	20,87
SafeMux	8	4,05	6,03

In Bezug auf Tabelle 5.10 lassen sich die einzelnen Zuverlässigkeitsfunktionen für die Zeit $t = 8760\,Stunden$ wie folgt berechnen:

$$R_{DistributedInputs} = e^{-\lambda_{DistributedInputs} \times t} = e^{\frac{-25,15}{10^9 h} \times 8760h} = 0,9997 \tag{5.23}$$

$$R_{CFv2SPP-Main} = e^{-\lambda_{CFv2SPP-Main} \times t} = e^{\frac{-100,405}{10^9 h} \times 8760h} = 0,9991 \tag{5.24}$$

$$R_{CFv2SPP-Redundant} = e^{-\lambda_{CFv2SPP-Redundant} \times t} = e^{\frac{-100,405}{10^9 h} \times 8760h} = 0,9991 \tag{5.25}$$

$$R_{SafeMux} = e^{-\lambda_{SafeMux} \times t} = e^{\frac{-6,03}{10^9 h} \times 8760h} = 0,9999 \tag{5.26}$$

$$R_{SEMController} = e^{-\lambda_{SEMController} \times t} = e^{\frac{-20,87}{10^9 h} \times 8760h} = 0,9998 \tag{5.27}$$

Für die Ausfallrate eines 64-MB SDRAMs bieten sich folgende Quellen an:

- die Siemensnorm 29500 mit der Angabe von 70 FIT,
- der Speicherhersteller Micron[135] mit der Angabe von 4 FIT und
- das Ergebnis der Studie[136] mit dem Wert von 66,1 FIT.

Da die Werte von Micron zu optimistisch sind, wird an dieser Stelle die Studie [SL12] als Referenzquelle verwendet.

$$R_{SDRAM} = e^{-\lambda_{SDRAM} \times t} = e^{\frac{-66,1}{10^9 h} \times 8760h} = 0,9994 \tag{5.28}$$

Beim Referenzieren der Ausfallrate des 16-MB Flash Speichers stehen zwei Quellen zur Verfügung - die Siemensnorm 29500 und das Datenblatt von Samsung[137]. Die SN 29500 legt eine Ausfallrate von 50 FIT dar, während Samsung einen Wert von 7,21 FIT vorsieht. Da der Unterschied nicht so extrem ist wie im Falle des SDRAMs, lässt sich der Mittelwert bilden und einsetzen.

$$R_{Flash} = e^{-\lambda_{Flash} \times t} = e^{\frac{-29}{10^9 h} \times 8760h} = 0,9997 \tag{5.29}$$

Bezüglich der Formel 5.22 ergibt sich für das redundante 1oo2-CFv2SPP-System folgendes Ergebnis:

$$\begin{aligned} R_{1oo2-System}(t) = R_{CFv2SPP-Main}(t) + R_{CFv2SPP-Redundant}(t) - \\ R_{CFv2SPP-Main}(t) \times R_{CFv2SPP-Redundant}(t) \\ R_{1oo2-System} = 0,9991 + 0,9991 - (0,9991 \times 0,9991) = 0,9982 \end{aligned} \tag{5.30}$$

In Anlehnung an die Formel 5.21 kann die gesamte Zuverlässigkeitsfunktion wie folgt berechnet werden:

$$\begin{aligned} R_{Gesamt} = R_{DistributedInputs} \times R_{1oo2-System} \times R_{SafeMux} \times R_{SEMController} \\ \times R_{SDRAM} \times R_{Flash} \\ R_{Gesamt} = 0,9997 \times 0,9999 \times 0,9982 \times 0,9998 \times 0,9994 \times 0,9997 = 0.9970 \end{aligned} \tag{5.31}$$

Um den PFD_{avg}-Wert zu berechnen und somit den Sicherheitsintegritätslevel des Gesamtsystems zu bestimmen, soll noch der Diagnosedeckungsgrad DC von einzelnen

[135] [06]; *Internal Qualification and Reliability Report*. 2006.
[136] [SL12] Sridharan, V. und Liberty, D.; *A study of DRAM failures in the field*. 2012.
[137] [03]; *Samsung 128Mb NAND Flash Qualification and Reliability Report*. 2003.

isolierten Komponenten kategorisiert werden. Dies ist in Tabelle 5.11 gegeben. In Anlehnung an[138] und[139] wird angenommen, dass die Ausfallrate λ der Ausfallrate gefährlicher Ausfälle λ_D entspricht. Daraus folgt:

$$\lambda_D = \lambda_{DD} + \lambda_{DU} \tag{5.32}$$

$$\lambda_{DU} = \lambda_D \times (1 - DC);\ \lambda_{DD} = \lambda_D \times DC \tag{5.33}$$

Für eine Reihenarchitektur wird gemäß [Bör07] folgende Formel für die PFD_{avg}-Berechnung eingesetzt:

$$PFD_{avg} = \lambda_{Du} \times \frac{T}{2} \tag{5.34}$$

Tabelle 5.11: Kategorisierung des Diagnosedeckungsgrades

Systemkomponente	**DC Wert**	**Maßnahmen**	**Referenz zur IEC 61508**
CFv2SPP Instanz	90 %	Test aller ALU Befehle, Test des Registersatzes, Test der Adressierung, SRAM-Test	Teil 2: Anhang A, Tabelle A.1
DistributedInputs	90 %	Redundanter Aufbau, interne Testbarkeit (DC Fehlermodell)	Teil 2: Anhang A, Tabelle A.7
SafeMux	99 %	Redundanter Aufbau, interne Testbarkeit, externe Testbarkeit (DC Fehlermodell)	Teil 2: Anhang A, Tabelle A.1

Für die einzelnen Komponenten des Blockdiagramms aus Abbildung 5.5 beträgt die Rate aller gefahrbringenden, unerkannten Ausfälle:

$$\begin{aligned}
\lambda_{DU-CFv2SPP} &= 100,405 \times (1 - 0,90) = 10,041\ FIT \\
\lambda_{DU-DistributedInputs} &= 25,15 \times (1 - 0,90) = 2,515\ FIT \\
\lambda_{DU-SafeMux} &= 6,03 \times (1 - 0,99) = 0,063\ FIT \\
\lambda_{DU-SEMController} &= 20,87 \times (1 - 0) = 20,87\ FIT \\
\lambda_{DU-Flash} &= 29 \times (1 - 0) = 29\ FIT \\
\lambda_{DU-SDRAM} &= 66,1 \times (1 - 0) = 66,1\ FIT
\end{aligned} \tag{5.35}$$

[138] [Bör07] Börcsök, J.; *Elektronische Sicherheitssysteme : Hardwarekonzepte, Modelle und Berechnung*. 2007.

[139] [IEC10b] IEC61508; *Anforderungen an sicherheitsbezogene elektrische/elektronische/programmierbare elektronische Systeme*. 2010.

Daraus ergeben sich die separaten PFD_{avg} Werte:

$$\begin{aligned}
PFD_{avg-DistributedInputs} &= 2,515 \times 10^{-9}\frac{1}{h} \times (\frac{8760}{2}h) = 11,01 \times 10^{-6} \\
PFD_{avg-SafeMux} &= 0,063 \times 10^{-9}\frac{1}{h} \times (\frac{8760}{2}h) = 0,276 \times 10^{-6} \\
PFD_{avg-SEMController} &= 20,87 \times 10^{-9}\frac{1}{h} \times (\frac{8760}{2}h) = 91,41 \times 10^{-6} \\
PFD_{avg-Flash} &= 29 \times 10^{-9}\frac{1}{h} \times (\frac{8760}{2}h) = 127,02 \times 10^{-6} \\
PFD_{avg-SDRAM} &= 66,1 \times 10^{-9}\frac{1}{h} \times (\frac{8760}{2}h) = 289,52 \times 10^{-6}
\end{aligned} \tag{5.36}$$

Für die PFD_{avg}-Berechnung des 1oo2-CFv2SPP-Systems wird in Anlehnung an [Bör07] folgende Formel verwendet:

$$\begin{gathered}
PFD_{avg} = [((\lambda_{DU-CFv2SPP})^2 \times \frac{T^2}{3}] + [\beta \times \lambda_{DU-CFv2SPP} \times \frac{T}{2}] \\
mit\ \beta = \beta_{ic} = 20\%
\end{gathered} \tag{5.37}$$

Somit folgt:

$$\begin{gathered}
PFD_{avg-1oo2} = [10,041^2 \times 10^{-18}\frac{1}{h} \times \frac{8760^2}{3}h] + [0,20 \times 10,041 \times 10^{-9}\frac{1}{h} \times \frac{8760}{2}h] \\
PFD_{avg-1oo2} = 2578937942,6352 \times 10^{-18} + 8795,916 \times 10^{-9} \\
PFD_{avg-1oo2} = 8,798 \times 10^{-6}
\end{gathered} \tag{5.38}$$

Die Gesamt-PFD_{avg} ergibt sich aus der Summe der einzelnen PFD_{avg}-Werte:

$$\begin{gathered}
PFD_{avg-gesamt} = PFD_{avg-1oo2} + PFD_{avg-DistributedInputs} + PFD_{avg-SafeMux} \\
+PFD_{avg-SEMController} + PFD_{avg-Flash} + PFD_{avg-SDRAM} \\
PFD_{avg-gesamt} = (8,798 + 11,01 + 0,276 + 91,41 + 127,02 + 289,52) \times 10^{-6} \\
PFD_{avg-gesamt} = 0,528 \times 10^{-3}
\end{gathered} \tag{5.39}$$

Reflektierend über Tabelle 2.5 mit den SIL-Werten einer Sicherheitsfunktion im Betrieb mit niedrigerer Anforderungsrate wird festgestellt, dass das Gesamtsystem SIL 3 konform ist, wenn als Prüfintervall ein Jahr definiert ist.

Wird für das Prüfintervall T der Wert von zwei Jahren gesetzt (17520 h), was gemäß

der Norm praxisrelevanter ist[140], dann folgt:

$$\begin{aligned} PFD_{avg-1oo2} &= 17,596 \times 10^{-6} \\ PFD_{avg-DistributedInputs} &= 22,03 \times 10^{-6} \\ PFD_{avg-SafeMux} &= 0,552 \times 10^{-6} \\ PFD_{avg-SEMController} &= 182,82 \times 10^{-6} \\ PFD_{avg-Flash} &= 254,04 \times 10^{-6} \\ PFD_{avg-SDRAM} &= 579,04 \times 10^{-6} \\ PFD_{avg-gesamt} &= 0,106 \times 10^{-2} \end{aligned} \tag{5.40}$$

Somit wurde das Ziel eines SIL 2-konformen Systems erreicht.

5.2 Thermodynamische Analyse

Der Trend in Richtung kleinerer Halbleiterstrukturen bringt neben vielen Vorteilen wie geringeren Kosten, höherer Leistung etc. auch gewisse Nachteile. Ein gravierender Nachteil ist die große Verlustleistung und die Existenz einer statischen Leistung[141], die in enger Beziehung mit der Temperatur steht, so dass die Erhöhung der Umgebungstemperatur eine drastische Änderung der Chipeigenschaften verursachen kann[142]. Als Konsequenz ergeben sich meistens Timing-Probleme, welche die Funktionalität eines Systems stark beeinträchtigen. Demzufolge ist eine thermodynamische Analyse bei der Entwicklung von sicherheitsgerichteten Systemen von großer Relevanz. In Bezug auf die IEC 61508-2 wird der Einsatz von Temperatursensoren suggeriert. Diese sind in der Trennungsbarriere zu platzieren[143], was bei den aktuellen FPGA-Typen aus technologischen Gründen nicht realisierbar ist. Die einzige Lösung wäre die Implementierung von Ring-Oszillatoren, die laut vielen Studien[144] eine passende Alternative zu den Temperatursensoren darstellen.[145]

[140] [IEC10d] IEC61508; *Anwendungsrichtlinie für Teile 2 und 3*. 2010.

[141] [And05] Anderson, J.; *Power Optimization and Prediction Techniques for FPGA*. 2005.

[142] [CWH11] Cordes, K., Waag, A. und Heuck, N.; *Integrierte Schaltungen : Grundlagen, Prozesse, Design, Layout*. 2011
[Kle05] Klein, M.; *Static Power and the Importance of Realistic Junction Temperature Analysis*. 2005.

[143] [IEC10b] IEC61508; *Anforderungen an sicherheitsbezogene elektrische/elektronische/programmierbare elektronische Systeme*. 2010.

[144] [Woj+14] Wojciechowski, B. u. a.; *Hardware microprocessor thermal emulation using synthetic heat sources and temperature sensors in FPGA*. 2014
[HAP11] Happe, M., Agne, A. und Plessl, C.; *Measuring and Predicting Temperature Distributions on FPGAs at Run-Time*. 2011.

[145] Ein Ring-Oszillator ist eine Schaltung, die aus einer ungeraden Anzahl Invertierern besteht. Die Invertierer sind in Reihe verschaltet und arbeiten mit einer bestimmten Frequenz, so dass der

Es ist zu argumentieren, dass die Temperaturerhöhung in den separaten Systemkomponenten ein tolerierbares Risiko darstellt. Solch eine Analyse könnte durchgeführt werden, indem beim Systembetrieb die Umgebungstemperatur erhöht wird, während mit einer Infrarotkamera die entstandenen Hotspots und die Wärmeausbreitung aufgezeichnet werden[146]. Eine andere Messungsmethode wäre der Einsatz eines Simulationstools. HotSpot ist das Tool, mit dem sehr präzise Ergebnisse erreicht werden können, weil es viele Charakteristiken wie Chipeigenschaften, Floorplan des Systems, horizontale und vertikale Wärmeausbreitung etc. betrachtet. Ein weiteres wichtiges Merkmal dieses Tools ist die Umsetzung des thermischen Netzwerkmodells (siehe Abschnitt 2.3). Die Studie[147] hat eine komparative Analyse von Daten, die mit den Temperatursensoren gewonnen wurden, und denen, die von der Simulation mit HotSpot erfasst wurden, durchgeführt. Dabei wurde festgestellt, dass die beiden Ergebnisse sehr stark miteinander korrelieren. In[148] erwähnen die HotSpot-Autoren eine erfolgreiche Zusammenarbeit mit IBM, um genauere Daten zum Leistungsverbrauch des IBM Prozessors POWER7+[149] zu gewinnen und daraus ein präziseres Temperaturverhalten dieses Prozessors abzubilden. Nach der Validierung der erfassten Daten wurde ein durchschnittlicher Fehler von 0,43 °C registriert.

Da das implementierte System aktuell nur in Form einer Gatter-Netzliste verfügbar ist, wird die thermodynamische Analyse auf Basis dieses Tools durchgeführt. Für die Vorbereitung der Simulation werden

- die physikalischen Eigenschaften des Artix 7 FPGA übermittelt,
- der Floorplan des CFv2SPP-basierten Systems mit OCR erstellt,
- die Matrix mit den Leistungsverbrauchsdaten einzelner OCR-Komponenten generiert. Dies erfolgt mit Hilfe des Tools Xilinx Power Analyzer (XPA)[150] (Alternativen sind die Tools SPICE[151] oder Wattch[152]). Dabei werden die Leistungsdaten in

Ausgang jedes Invertierers ständig zwischen 0 und 1 oszilliert. Mit Hilfe eines Zählers kann die Frequenz des Ring-Oszillators bestimmt werden. Wenn sich die Umgebungstemperatur ändert, dann ändert sich auch die Umschaltgeschwindigkeit der Transistoren und somit die Frequenz des Ringoszillators.[LGB00]

[146] [NR11] Nowroz, A. N. und Reda, S.; *Thermal and Power Characterization of Field-programmable Gate Arrays*. 2011
[PSB09] Pedre, S., Stoliar, A. und Borensztejn, P.; *Real Time Hot Spot Detection Using FPGA*. 2009
[JC12] Jevtic, R. und Carreras, C.; *A complete dynamic power estimation model for datapaths in {FPGA} {DSP} designs*. 2012.

[147] [Vel+05] Velusamy, S. u. a.; *Monitoring temperature in FPGA based SoCs*. 2005.

[148] [ZSS15] Zhang, R., Stan, M. R. und Skadron, K.; *HotSpot 6.0: Validation, Acceleration and Extension*. 2015.

[149] [12b]; *POWER7 and POWER7+ Optimization and Tuning Guide*. 2012.

[150] [10b]; *Xilinx Power Tools Tutorial: Spartan-6 and Virtex-6 FPGAs*. 2010.

[151] [TGM15] Tang, X., Gaillardon, P. E. und Micheli, G. D.; *FPGA-SPICE: A simulation-based power estimation framework for FPGAs*. 2015.

[152] [BTM00] Brooks, D., Tiwari, V. und Martonosi, M.; *Wattch: a framework for architectural-level power analysis and optimizations*. 2000.

regelmäßigen Zeitabständen erfasst. Die Matrix dient als Eingangsfile für die Berechnung der Matrix mit den Temperaturwerten mittels HotSpot. Im Anschluss wird in Form eines Diagramms dargestellt, wie sich die Wärme über die separaten Systemkomponenten verteilt.

Die konkrete Temperatursimulation basiert auf den folgenden drei Betrachtungen und deren Vergleich:

- Temperaturanalyse im Falle, dass die beiden CFv2SPP-Systeme nur die Selbst-Tests ausführen
- Temperaturanalyse im Falle, dass ein CFv2SPP-System einen anspruchsvollen Task ausführt, während das andere System nur die Selbst-Tests ausführt
- Analyse mit sporadischen extremen Temperaturwerten, mit denen beobachtet werden soll, ob die Temperaturerhöhung im Hauptsystem das redundante System beeinträchtigen kann

Die Erstellung der Matrix mit Leistungsverbrauchsdaten ist nicht trivial, weil das Tool Xilinx Power Analyser nur einen durchschnittlichen Wert bereitstellt. Die Tools SPICE und Wattch vereinfachen diesen Prozess signifikant. Leider sind sie nur für bestimmte, ASIC-basierte Mikroprozessoren vorgesehen, so dass ihr Einsatz beim ColdFire V2 Mikroprozessor auf einem FPGA zu inakzeptablen Ungenauigkeiten führen würde. Um die zeitliche Abtastung des Leistungsverbrauchs für das Zielsystem durchführen zu können, wurde das folgende Konzept entwickelt:

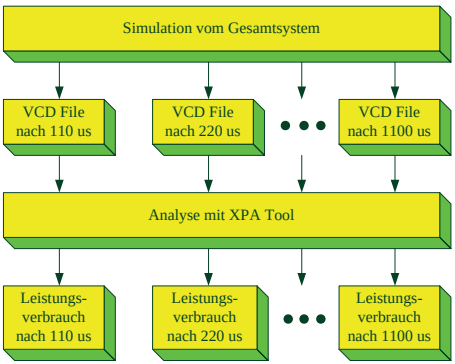


Abbildung 5.6: Zeitliche Abtastung des Leistungsverbrauchs

Das Konzept beinhaltet:

- Simulation der Gatter-Netzliste mit den Cadence-Tools

- Aufteilung der Simulationslaufzeit in zehn Abschnitte, die jeweils 110 μs dauern (da die Simulationsdauer der Selbst-Tests ca. 1100 μs beträgt)
- Erstellung eines Value Change Dump (VCD) Files für jeden Simulationsabschnitt, um die Verhaltensänderungen verschiedener Signale des beobachteten Systems aufzuzeichnen[153]. Dieses File dient als Input für das XPA Tool, damit genauere Ergebnisse des Leistungsverbrauchs erzielt werden[154]
- Iterative Generierung des Leistungsverbrauch-Berichtes mit dem XPA-Tool, damit die Daten für zehn verschiedene Zeitintervalle gewonnen werden.

Bevor die konkreten Ergebnisse präsentiert werden, wird in Tabelle 5.12 die Struktur einer Default-Analyse und einer auf dem VCD File basierenden Analyse vorgestellt. Dabei ist zu beachten, dass bei der Default-Analyse das XPA-Tool die durchschnittlichen Werte bezogen auf eine vektorlose Abschätzung kalkuliert[155]. Auf der anderen Seite wird bei der Betrachtung mit dem VCD File die Häufigkeit der Signalumschaltung präzise aufgezeichnet und mit den realistischen Umschaltraten verknüpft.

Tabelle 5.12: XPA-Analyse mit den Default- und den VCD-basierten Werten

	Leistungsverbrauch in Watt bei 40 MHz Systemfrequenz	
Systemkomponente	Ohne VCD File	Mit dem VCD basierend auf den Selbst-Tests
CFv2SPP Main System	0,03200	0,07150
CFv2SPP Redundantes System	0,03300	0,07350
Safe Multiplexer	0,00067	0,00046
Distributed Inputs	0,18500	0,18500
Statische Verlustleistung	0,11600	0,116
BRAM	0,00240	0,01800
Insgesamt:	**0,36907**	**0,46446**

Um die thermische Simulation durchzuführen, sind zunächst die physikalischen Eigenschaften des zu beobachtenden FPGAs im HotSpot-Tool zu konfigurieren. Dies erfolgt in Tabelle 5.13 auf der nächsten Seite und basiert auf den Ergebnissen, die der XPA zur Verfügung gestellt hat, sowie auf den Daten aus[156]. Weiterhin wurden die folgenden Annahmen getroffen:

- Die statische Verlustleistung wird jeder Systemkomponente proportional zu ihrer Partitions-Größe zugeordnet (dies entspricht der belegten FPGA-Fläche).

[153] [Wil08] Williams, J.; *Digital VLSI Design with Verilog : A Textbook from Silicon Valley Technical Institute*. 2008.

[154] [10b]; *Xilinx Power Tools Tutorial: Spartan-6 and Virtex-6 FPGAs*. 2010
[JC12] Jevtic, R. und Carreras, C.; *A complete dynamic power estimation model for datapaths in {FPGA} {DSP} designs*. 2012.

[155] [10b]; *Xilinx Power Tools Tutorial: Spartan-6 and Virtex-6 FPGAs*. 2010.

[156] [17a]; *7 Series FPGAs Packaging and Pinout*. 2017.

- Jedem Trennungsbereich wird auch ein Teil der statischen Verlustleistung proportional zu der belegten FPGA-Fläche zugeordnet.

- Die Trennungsbereiche werden während der Temperaturanalyse als Systemkomponenten betrachtet. Es gibt insgesamt drei solche Bereiche: Fence1, Fence2 und Fence3.

Tabelle 5.13: Physikalische Eigenschaften des Artix7 FPGAs

Eigenschaften	Artix 7 FPGA xc7a200tffg1156
Größe	35x35 mm
Höhe	2,5 mm
Solder-Ball Höhe	0,7 mm
Anzahl der Pads	600
Raumtemperatur	298,15 K

In Anlehnung an den Xilinx-PlanAhead-Floorplan wurde der folgende Floorplan für die Simulation mit HotSpot erstellt:

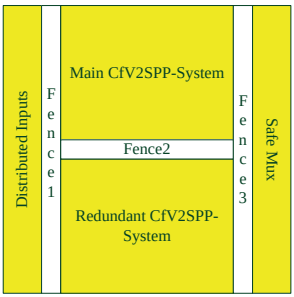


Abbildung 5.7: Floorplan des zu analysierenden Systems

Aus den Abbildungen 5.8, 5.9 und 5.10 auf der nächsten Seite ist es zu erkennen, dass die Temperatur über die gesamte FPGA-Fläche propagiert. Obwohl das Modul „DistributedInputs“ den größten Leistungsverbrauch aufweist und der erste Trennungsbereich (Fence1) einen der niedrigsten, ist die entstandene Temperatur in Fence1 trotzdem nur um 0,02 °C geringer als die vom „DistributedInputs“.

Weiterhin weisen die beiden CFv2SPP-Systeme ein identisches thermisches Verhalten auf. Da Fence3 und „SafeMux“ am weitesten von „DistributedInputs“ entfernt platziert sind, ist die ausgelöste Temperatur dementsprechend am niedrigsten. Sicherheitstechnisch betrachtet ist dieses Szenario unkritisch, weil die abgetastete Temperatur im Rahmen der Umgebungstemperatur bleibt.

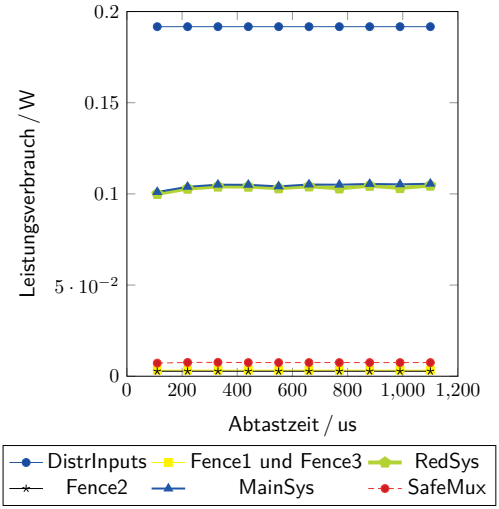


Abbildung 5.8: Leistungsverbrauch einzelner Systemkomponenten während der Selbst-Tests

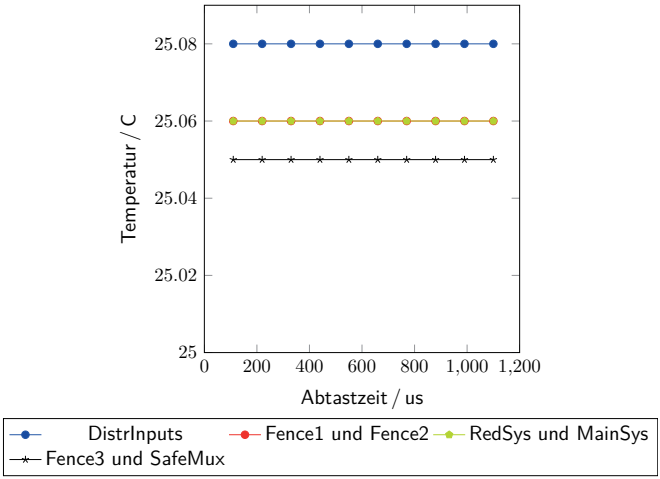


Abbildung 5.9: Temperaturverhalten im System während der Selbst-Tests

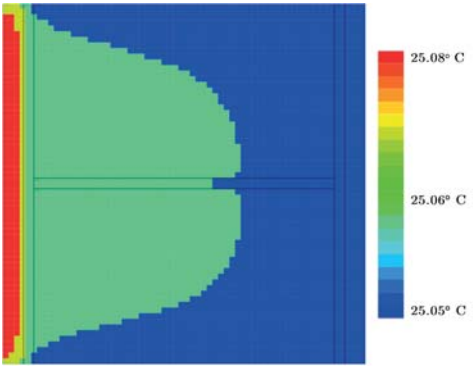


Abbildung 5.10: Thermische Ausbreitung nach der Analyse mit HotSpot bei der Ausführung der Selbst-Tests

Um das thermodynamische Verhalten des Systems näher zu betrachten, wird im Folgenden der Fall analysiert, bei dem das redundante System die Selbst-Tests ausführt, während sich das Hauptsystem in einem intensiven Task befindet, damit ein höherer Leistungsverbrauch provoziert wird. Dafür werden zunächst die folgenden Annahmen getroffen:

- Alle Logikzellen des CFv2-Cores des Hauptsystems werden aufgesucht und gespeichert. Das sind etwa 10000 FPGA-Elemente, vor allem die LUTs.
- Der Simulationsablauf entspricht dem obigen Fall mit 10 Abschnitten, die jeweils 110 μs dauern. Bei jedem Abschnitt wird das VCD File erstellt.
- In jedem Abschnitt werden die genannten Logikzellen mit 0 und 1 getriggert, und zwar mit einer Frequenz, die der folgenden Gleichung entspricht:

$$F = \frac{250}{11 - n} MHz \tag{5.41}$$

  Dabei bezieht sich n auf den aktuellen Simulationsabschnitt.

Die Ergebnisse der Leistungs- und Temperaturanalyse werden in Abbildungen 5.11 und 5.12 auf der nächsten Seite dargestellt. In dieser Konstellation werden nur „DistributedInputs“, CFv2SPP Main und CFv2SPP Redundant betrachtet. Die anderen Systemkomponenten können vernachlässigt werden, weil sie alle dieselbe Temperatur von 25 °C aufweisen. Die mit HotSpot gewonnenen Ergebnisse während der Ausführung von Selbst-Tests und der intensiven Signalumschaltung im Hauptsystem sind fast identisch.
Obwohl Änderungen im Leistungsverbrauch des Hauptsystems vorhanden sind, sind sie nicht ausreichend, um das redundante System zu beeinträchtigen. Dafür sprechen drei Gründe:

- Die Logikzellen verrichten eine durchschnittliche Leistung von 20 μW.
- Die wärmste Partition ist noch immer die vom „DistributedInputs“, weil das Hauptsystem erst nach der sechsten Iteration den Wert von 0,1917 Watt übersteigt, während das Modul „DistributedInputs“ in allen Iterationen den konstanten Wert von 0,1917 Watt hat.
- Leitung und Konvektion der Wärme.

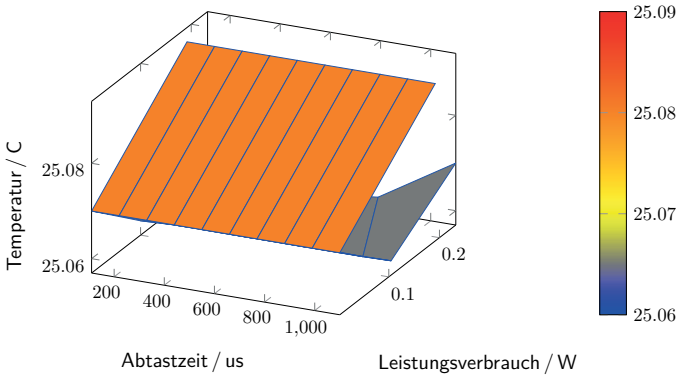


Abbildung 5.11: Korrelation zwischen Temperatur und Leistungsverbrauch während der intensiven Signalumschaltung

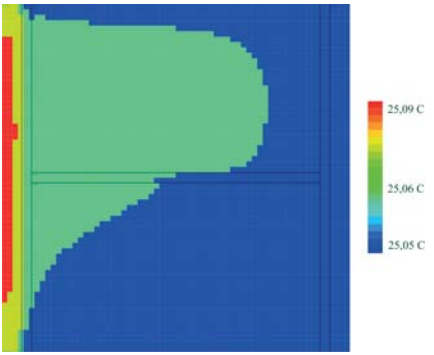


Abbildung 5.12: Thermische Ausbreitung nach der Analyse mit HotSpot während der intensiven Signalumschaltung im Hauptsystem

Eine Alternative zur Erhöhung des Leistungsverbrauchs ist die Änderung der Umgebungstemperatur. Die bisherigen Betrachtungen basierten auf 25 °C. Nun wird die

Umgebungstemperatur auf 70 °C erhöht. Dies bewirkt einerseits den Temperaturanstieg auf dem FPGA und andererseits den Anstieg der Verlustleistung. Die Letztere wird verdreifacht.

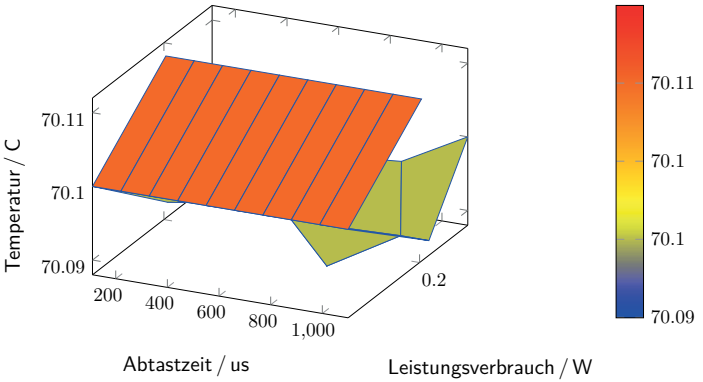


Abbildung 5.13: Korrelation zwischen Temperatur und Leistungsverbrauch während der intensiven Signalumschaltung bei erhöhter Umgebungstemperatur

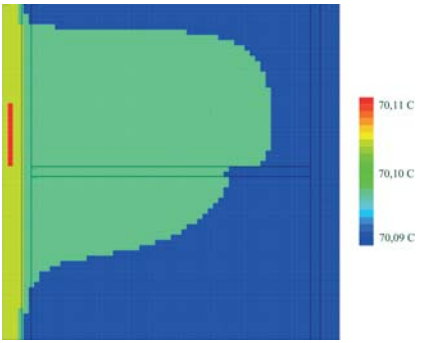


Abbildung 5.14: Thermische Ausbreitung nach der Analyse mit HotSpot während der intensiven Signalumschaltung im Hauptsystem bei erhöhter Umgebungstemperatur

Bei Betrachtung der Ergebnisse aus den Abbildungen 5.13 und 5.14 ist zu erkennen, dass der thermische Unterschied zwischen den Partitionen „DistributedInputs“ und CFv2SPP Main noch kleiner geworden ist und dass die Wärmeleitung in Richtung des CFv2SPP Redundant intensiviert wurde. Wie bei den ersten zwei Szenarien kann auch aus diesem Ansatz geschlossen werden, dass das thermische Verhalten des Gesamtsys-

tems sicherheitstechnisch unkritisch ist, weil die Temperaturoszillation im Rahmen von 1 °C bleibt.
Im Folgenden wird ein Worstcase untersucht, bei dem die Leistung des CFv2SPP Main schrittweise von 50 auf 100 Watt erhöht wird. Für alle anderen Systemkomponenten bzw. Partitionen werden die Daten aus dem vorherigen Beispiel übernommen. Danach wird die Messung noch einmal wiederholt, und zwar unter der Annahme, dass sich die Leistung des CFv2SPP Main von 100 auf 150 Watt erhöht. Die Zeitspanne für diese zwei Beobachtungen beträgt 10 ms.

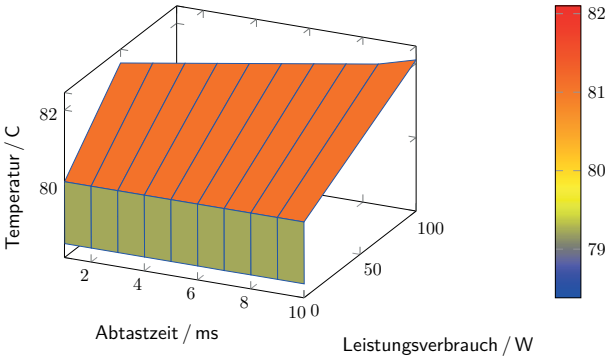


Abbildung 5.15: Korrelation zwischen Temperatur und Leistungsverbrauch beim Leistungsverbrauch von 50 - 100 Watt im CFv2SPP Main

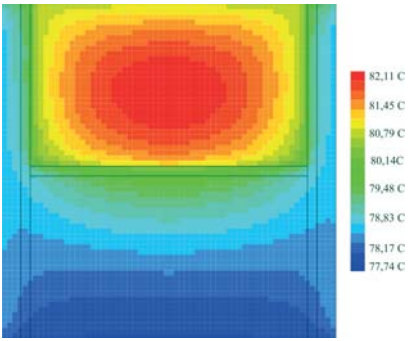


Abbildung 5.16: Thermische Ausbreitung nach der Analyse mit HotSpot beim Leistungsverbrauch von 50 - 100 Watt im CFv2SPP Main

In Abbildung 5.15 werden nur die Komponenten CFv2SPP Main, Fence2 und CFv2SPP Redundant betrachtet, weil die Propagierung der Temperatur des CFv2SPP Main in

Richtung des CFv2SPP Redundant von großer Bedeutung ist. Aus Abbildung 5.16 ist zu erkennen, dass der Unterschied zwischen den Heißpunkten des CFv2SPP Main und der Fence2 nur 2 °C ist, wobei der Unterschied zwischen den Heißpunkten des CFv2SPP Main und des CFv2SPP Redundant 4 °C beträgt. Damit wird nachgewiesen, dass die physikalische Trennung der redundanten Systeme auf dem FPGA im thermischen Sinne vorteilhaft ist. Wird die Leistung in der Partition des CFv2SPP Main schrittweise von 100 auf 150 Watt erhöht, dann wird folgendes Verhalten registriert.

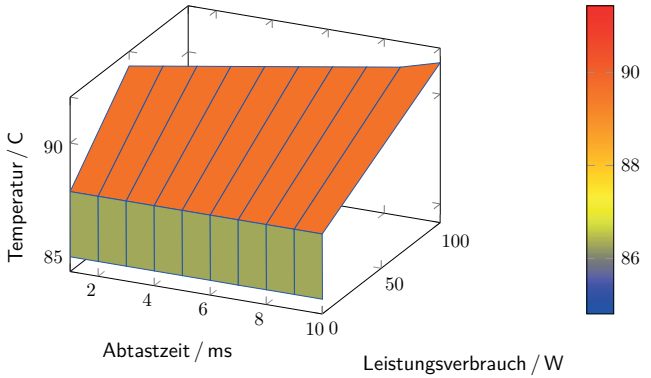


Abbildung 5.17: Korrelation zwischen Temperatur und Leistungsverbrauch beim Leistungsverbrauch von 100 - 150 Watt im CFv2SPP Main

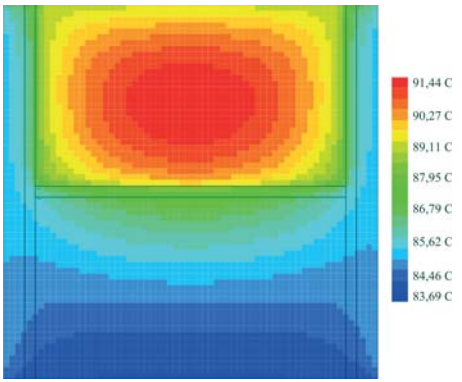


Abbildung 5.18: Thermische Ausbreitung nach der Analyse mit HotSpot beim Leistungsverbrauch von 100 - 150 Watt im CFv2SPP Main

Beim Vergleich dieser zwei extremen Fälle kann festgestellt werden, dass sich die Tem-

peratur in der Partition des redundanten Systems beim Anstieg im Hauptsystem mit der Zeit immer langsamer erhöht. Dieser Schluss wird in Diagramm 5.19 anhand einer größeren Betrachtungsspanne validiert.

Um die Validierung zu bekräftigen, wurden alle präsentierten Beobachtungen unter der Annahme einer logikfreien Trennung durchgeführt. Dies bedeutet, dass alle drei Trennungsbarrieren (Fence1, Fence2 und Fence3) keine statischen Verlustleistungen aufweisen. Dabei wurde bei allen erzielten Ergebnissen eine Abweichung von 0,01 °C festgestellt, was aus Sicht der funktionalen Sicherheit vernachlässigt werden darf.

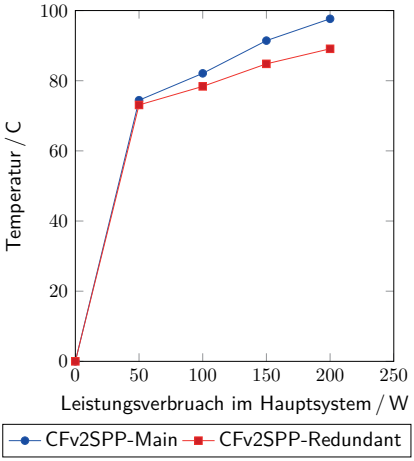


Abbildung 5.19: Entwicklung der Temperatur im redundanten System während des Anstiegs im Hauptsystem

6 Wertung, Abgrenzung und Ausblick

Der Fokus dieser Forschungsarbeit lag auf der Entwicklung eines neuen Sicherheitskonzeptes, welches sich in der sicheren und zuverlässigen Umschaltung der Systemoutputs manifestiert, wodurch die Implementierung einer neuen redundanten Architektur ermöglicht wurde. Als Basis wurde das in Abschnitt 3.1 präsentierte CFv2SPP-Mikrocontrollersystem verwendet, das aufgrund seiner Peripherie- und Speicherschnittstellen die Charakteristiken eines kompletten Rechnersystems aufweist. Das Hauptziel dieser Studie bezieht sich somit auf den Nachweis der Konformität zu dem Sicherheitsintegritätslevel 2 (SIL 2) und komprimiert in sich drei Betrachtungsebenen, die als Nebenziele bezeichnet werden können:

- Sicherheitsmaßnahmen zur Vermeidung von Ausfällen infolge gemeinsamer Ursache (CCF) auf dem FPGA
- Erhöhung der diagnostischen Abdeckung (DC-Faktor)
- Bewertung der Sicherheit anhand eines realistischen und praxis-relevanten Modells

Die neuartige Architektur basiert auf der Umsetzung des Prinzips der warmen Redundanz, welches die Integration von Sicherheitsmaßnahmen wie Takt- und Spannungstrennung (im gewissen Maße), Input- und Outputüberwachung effektiv ermöglicht sowie die Behandlung der sicherheitskritischen Zeit für die Aktivierung des redundanten Systems unter Kontrolle bringt. Wie in Abschnitt 3.4 präsentiert, besteht das System aus zwei CFv2SPP-Instanzen, die parallel hochfahren. Die beiden Systeme führen zunächst die Selbst-Tests aus, um die Startverifikation durchzuführen. Danach wechselt das Hauptsystem in den Betriebsmodus, während das redundante System die Selbst-Tests weiter periodisch ausführt. Wird durch die Diagnostikmaßnahmen ein kritischer Fehler aufgedeckt, wird im Hauptsystem der Betriebsmodus gestoppt und das redundante eingeschaltet. Auf diese Weise wird das ausgefallene System markiert und ausgeschaltet, womit das traditionelle Hindernis einer 1oo2-Architektur überwunden worden ist.

Dieses Kapitel beginnt mit der Darstellung der drei genannten Ebenen. Da als Startpunkt der Systemimplementierung die Annahmen von Xilinx und Intel Altera über die zertifizierten Designmethodologien für einen OCR-Entwurf definiert wurden, erfolgt danach eine qualitative Analyse und Evaluierung dieser Methodologien und eingesetzten Entwicklungstools aus der Sicherheitsperspektive. Mit einer Betrachtung der Aspekte für den Einsatz der vorliegenden Dissertation und der aktuellen FPGA-Strukturen in der Domäne der funktionalen Sicherheit wird das Kapitel abgeschlossen.

Im Kapitel 4 wurde die Implementierung von Mechanismen für die Behandlung der Ausfälle infolge gemeinsamer Ursache dargestellt, mit denen der β_{IC}-Faktor auf 20 % reduziert worden ist. Problematisch an dieser Stelle sind die vom Xilinx IDF definierten Maßnahmen zur Isolierung einzelner Systemkomponenten, aber auch die fehlenden Angaben zum Abstand zwischen den Leitungen, die auf dem Prinzip zuverlässiger Verdrahtung (Trusted Routing) beruhen. Es ist nicht vollkommen nachvollziehbar, ob solche Leitungen kreuzungsfrei sind, weil dieses Prinzip nur die Verwendung unterschiedlicher LUTs impliziert, die als Startpunkt für die Bildung einzelner Verdrahtungen dienen. Dank der intensiven thermodynamischen Analyse kann dieser Aspekt auch ignoriert werden, weil es den β_{IC} um die akzeptablen 2 % erhöht. Nichtsdestotrotz dient die vorgenommene Isolierung zu einer modularen und systematischen Designvorgehensweise sowie zur Trennung der I/O-Padzellen, die von der IEC 61508 gefordert werden (siehe Tabelle F.1 im Anhang F der[157]).
Die FPGA-Studien[158] aus dem Feld der CCF-Betrachtung adressieren nur die funktionale Sicht eines Systems und setzen den Akzent auf die Implementierung und Evaluierung des Diversitätsprinzips, sei es in der Anforderungsspezifikation, der Systemumsetzung oder im Verifikationsverfahren. Dabei konzentrieren sie sich hochfrequent auf den Einsatz verdreifachter Redundanz (Triple Module Redundancy), ohne dabei die kritischen Aspekte bezogen auf die Qualität des Mehrheitsentscheiders zu betrachten (siehe Anforderungen an einen Mehrheitsentscheider in Tabelle A.4, Anhang A der[159]). Nur eine einzige Studie setzt sich mit essentiellen Aspekten der CCFs auf dem FPGA auseinander und implementiert ein konkretes Konzept für die Reduzierung des β_{IC}-Faktors[160]. Als Reduzierungsmaßnahmen werden eine diversitäre Architektur, die Isolierung durch den Xilinx IDF und die Überwachung des Konfigurationsspeichers genannt. Die Maßnahmen aus der vorliegenden Dissertation reflektierend, kann konstatiert werden, dass:

[157] [IEC10b] IEC61508; *Anforderungen an sicherheitsbezogene elektrische/elektronische/programmierbare elektronische Systeme*. 2010.

[158] [ZY18] Zhu, L. und Yu, L.; *A design of decentralized dual mode redundant hot standby arbitration switch-over logic and architecture*. 2018
[Bor+16] Borecky, J. u. a.; *Enhanced Duplication Method with TMR-Like Masking Abilities*. 2016
[Kha16] Kharchenko, V.; *Diversity for safety and security of embedded and cyber physical systems: Fundamentals review and industrial cases*. 2016
[Mac+14] Macii, D. u. a.; *Design of a Redundant FPGA-Based Safety System for Railroad Vehicles*. 2014
[NSB11] Niknahad, M., Sander, O. und Becker, J.; *FGTMR - Fine grain redundancy method for reconfigurable architectures under high failure rates*. 2011
[KSS11] Kharchenko, V., Siora, O. und Sklyar, V.; *Multi-Version FPGA-Based Nuclear Power Plant IC Systems: Evolution of Safety Ensuring*. 2011
[TS09] Tummeltshammer, P. und Steininger, A.; *Power supply induced common cause faults-experimental assessment of potential countermeasures*. 2009.

[159] [IEC10b] IEC61508; *Anforderungen an sicherheitsbezogene elektrische/elektronische/programmierbare elektronische Systeme*. 2010.

[160] [CGB12] Corradi, G., Girardey, R. und Becker, J.; *Xilinx tools facilitate development of FPGA applications for IEC61508*. 2012.

- die anderen CCF-Quellen wie Taktmanagement, Spannungsversorgung und Temperatur außer Betracht geblieben sind,

- der implementierte Voter auf dem diskutablen Konzept der Mehrheitsentscheidung basiert, weil keine qualitativen Maßnahmen implementiert worden sind, die von der Norm in Anhang A der[161] gefordert werden,

- die Konzepte des Isolierungs-Designflusses ohne Überprüfung der Rückwirkungsfreiheit übernommen und für die Berechnung des β_{ic} verwendet worden sind.

Obwohl unser Ansatz für die Vermeidung der CCFs bezogen auf die Spannungsversorgung keiner galvanischen Trennung entspricht, ermöglicht er die Trennung von einzelnen Spannungsschienen, wodurch die Ausfälle von I/O-Padzellen, Taktmanagement-Komponenten und Versorgungspins zwischen den zwei CFv2SPP-Systemen keine Rückwirkung aufweisen. Da ein FPGA ein fertiges und nicht modifizierbares Hardwareprodukt ist, ist zu behaupten, dass diese Maßnahme ein Maximum an Spannungstrennung darstellt.
Die Studien zur thermodynamischen Analyse des FPGAs können in zwei Hauptkategorien unterteilt werden:

- praktische Ansätze, die auf dem Einsatz von Ring-Oszillatoren[162] und Infrarotkameras[163] basieren, sowie die Ansätze, die in FPGAs integrierte Temperatursensoren verwenden[164],

- simulationsbasierte Ansätze[165].

[161] [IEC10b] IEC61508; *Anforderungen an sicherheitsbezogene elektrische/elektronische/programmierbare elektronische Systeme*. 2010.

[162] [He+15] He, W. u. a.; *A self-tuned thermal compensation system for reducing Process Variation influence in side-channel attack resistant dual-rail logic*. 2015
[Web+13] Weber, P. u. a.; *Toolset for measuring thermal behavior of FPGA devices*. 2013
[Naf+12] Nafkha, A. u. a.; *Leakage power consumption in FPGAs: Thermal analysis*. 2012.

[163] [Li+16] Li, J. u. a.; *Thermal distribution measurement on FPGA using optimized ring oscillator (RO)-based thermal sensor network*. 2016
[Amr+13] Amrouch, H. u. a.; *Analyzing the thermal hotspots in FPGA-based embedded systems*. 2013.

[164] [Cha+15] Chafi, P. R. u. a.; *A platform for dynamic thermal management of FPGA-based soft-core processors via Dynamic Frequency Scaling*. 2015
[HN15] Hashamdar, T. und Noori, H.; *Thermal management of FPGA-based embedded systems at operating system level*. 2015.

[165] [Bar+10] Bartolini, A. u. a.; *A Virtual Platform Environment for Exploring Power, Thermal and Reliability Management Control Strategies in High performance Multicores*. 2010
[Man+08] Mangalagiri, P. u. a.; *Thermal-aware reliability analysis for Platform FPGAs*. 2008
[Hua+08] Huang, W. u. a.; *Accurate, Pre-RTL Temperature-Aware Design Using a Parameterized, Geometric Thermal Model*. 2008
[Sta+03] Stan, M. R. u. a.; *HotSpot: a dynamic compact thermal model at the processor-architecture level*. 2003.

Gemeinsam ist allen diesen Studien das Statement, dass der interne Temperatursensor eines FPGAs inadäquat ist, um die präzisen Messungen durchzuführen. Der Grund dafür liegt in der mittleren Platzierung des Sensors, so dass die von der Mitte des FPGAs weiter entfernten Hotspots nicht registriert werden können.
Die Studie[166] hat nachgewiesen, dass der Cache-Speicher als größter Wärmeauslöser von diversen Mikrocontrollersystemen auf dem FPGA zu charakterisieren ist. In[167] wird eine Maßnahme zur Temperaturregelung präsentiert, bei der bestimmte Tasks vom Betriebssystem abgeschaltet werden, wenn eine erhöhte Temperatur registriert wird.
Eine sicherheitstechnische Analyse des thermischen Verhaltens von FPGAs ist keiner der angegeben Studien explizit inhärent, weil sie sich überwiegend auf die Implementierung von verschiedenen Methoden zur Leistungsreduzierung fokussieren.

Bei der Evaluierung des vorgelegten thermischen Modells hat sich erwiesen, dass sich die Verschwendung der FPGA-Ressourcen während des Entwicklungsprozesses (wird später näher erläutert) auf das thermodynamische Verhalten des Systems sehr positiv auswirkt. Durch die Separierung und Isolierung der sicherheitsrelevanten Komponenten wird die resultierende Gatter-Netzliste über die gesamte FPGA-Fläche verteilt. Dieser Effekt führt zur Vermeidung von Hotspots auf dem FPGA und zu einer effizienten Wärmeabfuhr. Nähere Betrachtungen und präzisere Ergebnisse diesbezüglich sind in der Studie[168] dargelegt.
Mit der in Abschnitt 5.2 durchgeführten Analyse wurde nachgewiesen, dass auch bei einem unkontrollierten Temperaturanstieg von 100 °C im Haupt-CFv2SPP-System die Temperatur im redundanten System noch immer in einem tolerierbaren Bereich von etwa 85 °C liegt. Der Grund dafür ist nicht nur die Anzahl der belegten FPGA-Elemente, sondern auch das Spannen des Systems über die gesamte Chipfläche. Dadurch wird auch die Entstehung von Hotspots in bestimmten Systemkomponenten eliminiert. Es sollen noch die verbrauchten Ströme und Eigenschaften von I/O-Pads betrachtet werden. Auf einer Seite fließen auf den einzelnen Ressourcen sehr kleine Ströme (in diesem Design wurde für eine LUT die durchschnittliche Leistung von 20 μWatt abgeschätzt), so dass die Auslösung eines extremen Temperaturanstiegs durch die intensive Applikation praktisch unmöglich ist. Auf der anderen Seite sind die I/O-Pads eines FPGA-Chips so robust, dass sogar Kurzschlüsse keine Gefahr darstellen[169].

Um die Ergebnisse der thermodynamischen Analyse vollkommen zu evaluieren, wäre es erforderlich, noch eine praktische Untersuchung des Systems mittels einer Infrarotkamera durchzuführen. Da das implementierte System aktuell in Form einer Gatter-

[166] [Amr+13] Amrouch, H. u. a.; *Analyzing the thermal hotspots in FPGA-based embedded systems*. 2013.
[167] [HN15] Hashamdar, T. und Noori, H.; *Thermal management of FPGA-based embedded systems at operating system level*. 2015.
[168] [Vel+05] Velusamy, S. u. a.; *Monitoring temperature in FPGA based SoCs*. 2005.
[169] [Pen18] Penney, K.; *Hot Swapping with FPGAs*. 2018
[Cra10] Crabill, E.; *Eliminating I/O Coupling Effects when Interfacing Large-Swing Single-Ended Signals to User I/O Pins on Spartan-3 Families*. 2010.

Netzliste verfügbar ist, kann so eine Analyse erst in einer zukünftigen Studie erfolgen. Nichtsdestotrotz basieren die gewonnenen Ergebnisse auf dem Simulationstool HotSpot, welches auf diversen FPGAs und ASIC intensiv validiert worden ist[170]. In[171] wurde die Validierung auf FPGA-Basis präsentiert. Es wurde nachgewiesen, dass die Simulationsergebnisse sehr stark mit denen einer Infrarotkamera korrelieren. Weiterhin hat die Studie[172] gezeigt, dass das HotSpot-Tool im Vergleich zu Ring-Oszillatoren eine durchschnittliche Abweichung von nur 0,64 °C aufweist. Somit kann argumentiert werden, dass die vorliegende Analyse auch zuverlässige Resultate aufweist.

Um das Ausfallverhalten des Systems mit einer hohen Abdeckung zu diagnostizieren, wurden die Überwachungsmaßnahmen in allen Systemkomponenten integriert - bei der Verteilung von Inputsignalen, dem CPU-Betrieb und der Behandlung von Outputumschaltung. Durch die Implementierung eines sicheren Multiplexers wurde nicht nur eine sichere Outputumschaltung ermöglicht. Dadurch wurden auch die internen Busse des CFv2SPP-Systems mit vollständiger Redundanz ausgelegt, weil der Flash und der SDRAM an den FlexBus bzw. an den AHB-Bus angeschlossen wurden. Dieser Aspekt erhöht signifikant die Fehlerlaufdeckungsrate bei den Bussen (siehe Tabelle 5.11 im Abschnitt 5.1).
Das funktionale Verhalten des Systems wurde durch eine intensive Simulation der Gatter-Netzliste auf Basis der Ausführung der Selbst-Tests, diverser Testapplikationen und der externen Trigger der Outputumschaltung verifiziert. Da die Gatter-Netzliste ein valider Repräsentant des physikalischen FPGA-Verhaltens ist, können die durchgeführten Tests als zuverlässig und aussagekräftig angenommen werden.

Die Implementierung der Selbst-Tests der ColdFire V2 CPU wurde in Abschnitt 4.5.1 präsentiert. Der komplette Befehlssatz, alle Adressierungsarten, die internen Register und der SRAM wurden mittels assemblerbasierter Software-Tests abgedeckt. Jeder Testfall wurde separat simuliert und beobachtet, ob ein gezielt generiertes Fehlverhalten zur Ausführung des STOP-Befehls und somit zum Triggern des Statussignals *mfrz_b* geführt hat.
Die Studien[173] kritisieren diesen Ansatz aus der Komplexitäts- und Laufzeitperspektive. Stattdessen fokussieren sie sich auf die Generierung von Zufallstestvektoren, die zusätzliche Hardware implizieren. Die CPU-Tests sind in Assembler implementiert und

[170] [Ska18] Skadron, K.; *Has HotSpot been validated?* 2018
[ZSS15] Zhang, R., Stan, M. R. und Skadron, K.; *HotSpot 6.0: Validation, Acceleration and Extension.* 2015.

[171] [Vel+05] Velusamy, S. u. a.; *Monitoring temperature in FPGA based SoCs.* 2005.

[172] [Man+08] Mangalagiri, P. u. a.; *Thermal-aware reliability analysis for Platform FPGAs.* 2008.

[173] [ST10] Sosnowski, J. und Tupaj, L.; *CPU Testability in Embedded Systems.* 2010
[SEN04b] Shamshiri, S., Esmaeilzadeh, H. und Navabi, Z.; *Test instruction set (TIS) for high level self-testing of CPU cores.* 2004
[LC01] Lai, W.-C. und Cheng, K.-T.; *Instruction-level DfT for testing processor and IP cores in system-on-a-chip.* 2001.

werden manuell in der Applikation an der Stelle von NOP-Befehlen eingefügt[174], wodurch die Programmlaufzeit nicht beeinträchtigt wird. Dieses Konzept ist timingspezifisch betrachtet effizienter als unseres. Eine weitere spezifische Charakteristik aus der Literatur[175] ist das Prinzip des Fehlerinjizierens.
Die anderen relevanten Studien[176] basieren ihre Konzepte auch auf dem Fehlerinjizieren, lediglich ohne die Anforderung einer zusätzlichen Hardware. Es wird über eine Fehlerabdeckung von > 90 % berichtet, während in[177] eine Fehlerabdeckung von durchschnittlich 85 % aufgeführt wird.
Ein sicherheitstechnischer Nachteil ist allen diesen Studien inhärent, nämlich die Evaluierung der Fehlerabdeckung. Beim Fehlerinjizieren liegt der Fokus vielmehr auf der Quantität der eingepflanzten Fehler und weniger auf der Qualität der Testfälle. Somit wird bewertet, wie viele Fehlerfälle durch bestehende Testmechanismen aufgedeckt werden können. An dieser Stelle fehlt der Bezug zur Diagnosedeckung (DC-Faktor), die sich auf die Rate aller nicht aufgedeckten gefährlichen Fehler bezieht. Keine dieser Studien berichtet, ob der komplette Befehlssatz der eingesetzten CPU getestet worden ist. Die Studie[178] macht einen Kompromiss zwischen der Fehler- und der Diagnosedeckung durch die Implementierung generischer Selbst-Tests für diverse CPUs konform zur IEC 61508. Da die Tests in der Programmiersprache C implementiert worden sind, wird der Grad der Diagnosedeckung nach der Kompilierung sinken.
Obwohl unser Testkonzept komplex ist (ca. 2500 Codezeilen) und eine Laufzeit von 1200 μs bei der Taktfrequenz von 40 MHz impliziert, liegt der erreichte Diagnosedeckungsgrad bei 90 %. Die Vorteile, die das Verfahren des Fehlerinjizierens bietet, wurden

[174] [SEN04b] Shamshiri, S., Esmaeilzadeh, H. und Navabi, Z.; *Test instruction set (TIS) for high level self-testing of CPU cores*. 2004.

[175] [SEN04b] Shamshiri, S., Esmaeilzadeh, H. und Navabi, Z.; *Test instruction set (TIS) for high level self-testing of CPU cores*. 2004
[LC01] Lai, W.-C. und Cheng, K.-T.; *Instruction-level DfT for testing processor and IP cores in system-on-a-chip*. 2001.

[176] [LC17] Lin, C. und Chen, C.; *A Processor and Cache Online Self-Testing Methodology for OS-Managed Platform*. 2017
[Ber+14] Bernardi, P. u. a.; *MIHST: A Hardware Technique for Embedded Microprocessor Functional On-Line Self-Test*. 2014
[The+14] Theodorou, G. u. a.; *Software-Based Self-Test for Small Caches in Microprocessors*. 2014
[Con+09] Constantinides, K. u. a.; *A Flexible Software-Based Framework for Online Detection of Hardware Defects*. 2009
[PG05] Paschalis, A. und Gizopoulos, D.; *Effective software-based self-test strategies for on-line periodic testing of embedded processors*. 2005.

[177] [SNM16] Skitsas, M. A., Nicopoulos, C. A. und Michael, M. K.; *DaemonGuard: Enabling O/S-Orchestrated Fine-Grained Software-Based Selective-Testing in Multi-/Many-Core Microprocessors*. 2016
[Ber+16] Bernardi, P. u. a.; *Development Flow for On-Line Core Self-Test of Automotive Microcontrollers*. 2016
[SEN04a] Shamshiri, S., Esmaeilzadeh, H. und Navabi, Z.; *Instruction level test methodology for CPU core software-based self-testing*. 2004.

[178] [Pre+13] Preschern, C. u. a.; *Verifying generic IEC 61508 CPU self-tests with fault injection*. 2013.

partiell durch die separate Simulation und Beobachtung jedes Testfalls mit abgedeckt. Somit können die zwei diskutablen Aspekte toleriert werden, weil die Intention bei der Implementierung eines sicherheitsrelevanten Systems nicht unbedingt die Effizienz ist, sondern vielmehr die Zuverlässigkeit der Konzepte.

Die Bewertung der Sicherheit anhand der Bestimmung der Ausfallrate einzelner Systemkomponenten wurde über zwei diverse Methoden durchgeführt. Die pessimistischen Ergebnisse, gewonnen über die Bildung der Gatter-Äquivalenz bezüglich der konservativen Siemensnorm 29500, wurden über die Ergebnisse des Zuverlässigkeitskalkulators von Xilinx validiert.

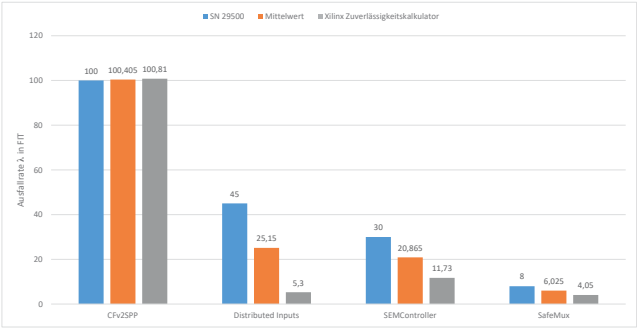


Abbildung 6.1: Ausfallratenvergleich zwischen den SN-29500-basierten Ergebnissen und den mit dem Xilinx-Zuverlässigkeitskalkulator gewonnenen Werten

Da die von der SN 29500 gelieferten Werte durchschnittlich um den Faktor 4 größer sind (die einzige Ausnahme ist das CFv2SPP-System wegen der zu hohen Anzahl von BlockRAMs, die sich sehr negativ auf die Ermittlung der Ausfallrate auswirken), wurden die Resultate beider Methoden kombiniert und ein Mittelwert gebildet, damit für die Berechnung des PFD_{avg}-Wertes ein realistisches Verhalten eingesetzt werden konnte. Validiert über das Prüfintervall von zwei Jahren wurde nachgewiesen, dass das Gesamtsystem dem SIL 2 konform ist.

Wissenschaftliche Publikationen, die sich mit der Berechnung der Ausfallrate von FPGA basierten Systemen beschäftigen, verwenden den MIL-HDBK-217 Standard als Referenz[179]. Der Graph aus Abbildung 6.2 auf der nächsten Seite stellt den Vergleich zwischen unseren Ergebnissen und den auf dem MIL-HDBK-217 basierenden Werten dar (wie die einzelnen Ausfallraten zu ermitteln sind, ist in Anhang A.3 zu finden). Die mit

[179] [WCB16] Wang, Q., Chen, D. und Bai, H.; *A method of space radiation environment reliability prediction*. 2016
[Rad14] Radu, M.; *Reliability and fault tolerance analysis of FPGA platforms*. 2014
[Shr+10] Shrikhande, S. V. u. a.; *Hardware Reliability prediction of Computer Based safety Systems of Indian Nuclear Plants*. 2010.

dem MIL-HDBK-217 gewonnenen Ergebnisse sind deutlich strenger als die Ergebnisse dieser Studie, aber auch strenger als die auf der SN 29500 basierenden Werte. Der Grund liegt einerseits in der Rigorosität des militärischen Standards und andererseits in dessen fehlender Aktualisierung. Die letzte Aktualisierung hat im Jahr 1995 stattgefunden. Diese Aspekte werden in den Studien[180] stark kritisiert, in denen anhand einer komparativen Analyse der Standards MIL-HDBK-217, Telcordia SR-332 und GJB-Z 299C argumentiert wird, dass der militärische Standard sehr ungeeignet für den praktischen Einsatz ist.
Ein sehr interessanter Aspekt beim Vergleich mit dem MIL-HDBK-217 ist die enorm große Diskrepanz beim „SafeMux“-Modul. Dies ist die Implikation eines Berechnungsparameters, der sich auf die Anzahl der Pins bezieht (siehe Anhang A.3). Da das „SafeMux“ die höchste Anzahl an Systempins besitzt, ist dieser Parameter dementsprechend bei ihm auch am höchsten.

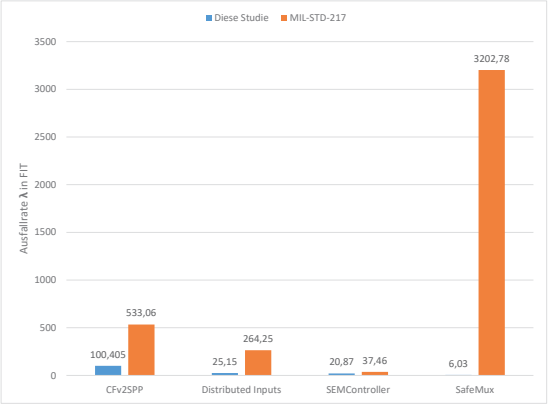


Abbildung 6.2: Ausfallratenvergleich mit den MIL-HDBK-217-basierten Ergebnissen

Eine weitere Studie, die sich mit der Ermittlung der Ausfallrate eines FPGA-Systems befasst, ist die[181]. Hier wurde ein eigenes Konzept entwickelt, das auf der Ausfallratenberechnung eines einzelnen Transistors basiert. Dabei wird als Referenz der jährliche Zuverlässigkeitsbericht von Xilinx verwendet, aus dem die Ausfallrate des gesamten FPGAs extrahiert wird. Daraus wird zunächst die Transistor-Ausfallrate ermittelt und anschließend die von einem Slice. Wie die Ergebnisse dieser Studie in Bezug zu unseren

[180] [Mou+13] Mou, H. u. a.; *A comparison and case studies of electronic product reliability prediction methods based on handbooks.* 2013
[Zho+12] Zhou, L. u. a.; *Reliability prediction for smart meter based on Bellcore standards.* 2012.

[181] [HD12] Hock, O. und Drgona, P.; *PWM modulator with increased reliability in FPGA circuit.* 2012.

Ergebnissen stehen, wird im Graphen auf der nächsten Seite dargestellt. Die Ermittlung einzelner Ausfallraten gemäß diesem Ansatz ist in Anhang A.4 gegeben.

Die Diskrepanz in diesem Vergleich ist auch sehr stark. Wird sich vollkommen auf die Ergebnisse des Xilinx-Zuverlässigkeitskalkulators bezogen, sind die gewonnenen Ergebnisse noch immer zu optimistisch. Somit ist zu behaupten, dass die Strategie aus unserer Studie ein praxisrelevantes Modell darstellt, welches in der Mitte zwischen dem zu rigorosen MIL-HDBK-217 und den zu optimierenden FPGA-spezifischen Ansätzen steht.

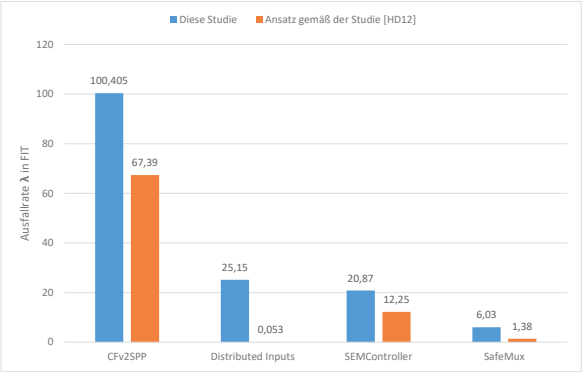


Abbildung 6.3: Ausfallratenvergleich mit den [HD12]-basierten Ergebnissen

Nun können die verwendeten Entwicklungstools und die Designmethodologie evaluiert werden. Dieser Aspekt ist enorm wichtig, weil die IEC 61508 bei der Implementierung von sicherheitsgerichteten Systemen die Qualifizierung der eingesetzten Tools fordert[182].

Xilinx und Intel Altera publizieren und präsentieren permanent[183], dass der Isolations-Designfluss sowie der Separations-Designfluss zur Erfüllung der Sicherheitsanforderungen geeignet sind. Über die getrennten logischen Partitionen kann ein OCR-System als konform bis zum Sicherheitsintegritätslevel 3 (SIL 3) implementiert werden. Solche Aussagen sind sehr kontrovers, weil die praktischen Umsetzungen sowohl von Xilinx als auch von Intel Altera dieser Stellungnahme widersprechen.

Intel Altera stellte ein Sicherheitskonzept basierend auf der redundanten NIOS II Architektur und verschiedenen sicherheitsgerichteten Funktionen in Form eines vom TÜV SÜD zertifizierten HDL-Codes vor[184]. Dies ist nur ein Initialzustand, weil der HDL-Code gemäß dem Separations-Designfluss auf einem FPGA kompiliert, synthetisiert

[182] [IEC10c] IEC61508; *Anforderungen an Software*. 2010.
[183] [Xil13] Xilinx; *Functional Safety Certificate*. 2013
[Alt16] Altera; *Functional Safety Certificate*. 2016.
[184] [Alt16] Altera; *Functional Safety Certificate*. 2016.

und umgesetzt werden muss. Zu erwarten wäre, dass die konkrete physikalische Umsetzung auf einem gemeinsamen FPGA-Chip realisiert wird. Die Umsetzungsergebnisse werden in[185] präsentiert. Sie basieren auf dem Einsatz von zwei getrennten FPGAs, mit denen die redundante Architektur implementiert wird. Dies ist aber keine OCR-Lösung, sondern eine klassische, traditionelle Trennung basierend auf zwei separaten Chips.

Werden die Xilinx-Lösungen betrachtet, dann sind nur die Sicherheitskonzepte auf dem Zynq 7 FPGA von Relevanz[186]. Für die anderen FPGA-Familien wie Virtex, Spartan oder Artix existieren aktuell keine Veröffentlichungen. Das Zynq 7 FPGA kann als ein SoC interpretiert werden, weil es aus zwei separaten Chips besteht. Diese sind jedoch im gemeinsamen Gehäuse verbaut und beziehen sich zum einen auf den ARM-Prozessor und zum anderen auf die programmierbare Logik[187]. Ein SIL 3 konformes System ist mit der Kombination der beiden Chips zu implementieren. Dieses Konzept ist das meistpräsente und -publizierte Sicherheitskonzept von Xilinx[188]. Solche Lösungen können nicht als On-Chip-Redundanz klassifiziert werden, sondern als eine Form der On-Package-Redundanz.

Aus diesen Schlüssen ergibt sich die Frage nach der Intention und der Brauchbarkeit der eingeführten Designflüsse für die Trennung sicherheitsbezogener Komponenten auf einem gemeinsamen FPGA. Obwohl die Tools schon vor vier Jahren zertifiziert worden sind, wurde bis jetzt kein zertifiziertes OCR-System entworfen, sondern nur die Ad-hoc-Lösungen präsentiert[189].

Was sind aber die Gründe für das Scheitern des OCR-Konzeptes auf dem FPGA? Im Anhang E des zweiten Teils der IEC 61508-2 wurden Anforderungen an die OCR-Implementierung auf einem ASIC präzise definiert und aufgelistet. In Anmerkung 13 äußert sich die Norm skeptisch über die anderen Technologien, unter anderem auch über die FPGAs[190]. Sowohl beim Entwicklungsprozess, der auf der HDL-Codierung der gewünschten Systemfunktionalität basiert, als auch beim Herstellungsprozess eines FPGAs fordert die Norm ein klares, systematisches Vorgehen nach dem etablier-

[185] [New16] NewTec; *Safe Flex*. 2016.

[186] [Xil18] Xilinx; *IEC 61508 specification certificate issued by Exida for high performance Zynq UltraScale+ family*. 2018
[HCM15] Hallett, E., Corradi, G. und McNeil, S.; *Xilinx Reduces Risk and Increases Efficiency for IEC61508 and ISO26262 Certified Safety Applications*. 2015.

[187] [18a]; *Zynq-7000 All Programmable SoC Overview*. 2018
[18b]; *Zynq-7000 All Programmable SoC, Technical Reference Manual*. 2018.

[188] [Mae18] Maeda, S.; *Xilinx Announces Availability of Automotive Qualified Zynq UltraScale+ MPSoC Family*. 2018
[HCM15] Hallett, E., Corradi, G. und McNeil, S.; *Xilinx Reduces Risk and Increases Efficiency for IEC61508 and ISO26262 Certified Safety Applications*. 2015.

[189] [McN15] McNeil, S.; *Developing Secure Designs with the Spartan-6 Family Using the Isolation Design Flow*. 2015
[CGB12] Corradi, G., Girardey, R. und Becker, J.; *Xilinx tools facilitate development of FPGA applications for IEC61508*. 2012.

[190] [IEC10b] IEC61508; *Anforderungen an sicherheitsbezogene elektrische/elektronische/programmierbare elektronische Systeme*. 2010.

ten V-Modell. Als Ergebnis eines solchen Entwicklungsprozesses entstehen diverse Anforderung- und Umsetzungsspezifikationen unterschiedlichen Detaillierungsgrades, aber auch die relevanten Testspezifikationen und Testberichte, welche Verifikations- und Validierungszwecke erfüllen. Um ihre Herstellungs- und Entwicklungsprozesse transparent zu machen, wird von den FPGA-Herstellern einerseits der Einblick in den technologischen Prozess gefordert, damit sichergestellt werden kann, dass die Anforderungen an einen ausreichende Abstand der Verdrahtungen zwischen den redundant ausgelegten Komponenten erfüllt sind und dass durch die physikalische Trennung die Rückwirkungsfreiheit der getrennten Komponenten garantiert wird. Andererseits soll jede Änderung in den Tools dokumentiert und ihre Auswirkung auf den gesamten Designfluss untersucht werden, damit sichergestellt wird, dass keine gefährlichen Implikationen entstehen. Als letztes Beurteilungskriterium, wiederum über die IEC 61508-2 reflektiert, kann das Fehlen einer aussagekräftigen thermodynamischen Analyse genannt werden. Deswegen zertifizieren die FPGA-Hersteller nur ihre Konzepte und nicht die konkreten Umsetzungen (siehe die Publikationen[191]).
Mit dem IDF bzw. SDF kann eine logische und physikalische Trennung realisiert werden. Die elektrischen Aspekte werden vernachlässigt. Dies ist der Hauptgrund, warum die beiden Hersteller bei konkreten Umsetzungen 2-Die-Lösungen verwenden. Durch die Bildung von Trennungsbarrieren kann nicht sichergestellt werden, dass keine elektrischen Nebeneffekte zwischen den isolierten Systemkomponenten entstehen. Solch eine Barriere besteht aus einer Vielzahl von lokalen und globalen Routingelementen, Multiplexern, nicht verwendeten Logik-, Speicher-, Clockingelementen etc. Besonders gefährlich und sicherheitskritisch sind die globalen Verdrahtungen, weil sie sich über die gesamte FPGA-Fläche spannen. Es muss nachgewiesen werden, dass der Trennungsbereich keine Auswirkung auf die sicherheitsbezogenen Systemkomponenten hat. Ein solcher Versuch wurde in der Studie[192] präsentiert und bezieht sich auf das Spartan 3 FPGA von Xilinx. Das Konzept basiert auf der Verbindung aller FPGA-Elemente aus der Trennungsbarriere zum Ground. Die Autoren berichten, dass der komplexeste Teil des Nachweises die Behandlung von globalen Verdrahtungen war. Diese Lösung gilt nur für die Spartan-Familie. Für die anderen FPGA-Typen müsste die Lösung angepasst oder sogar komplett neu erdacht werden.
Es ist nicht nur der Nachweis der elektrischen Rückwirkungsfreiheit diskutabel und problematisch. Im Laufe dieser Forschungsarbeit wurden mehrere kritische Aspekte des FPGA-Designs für Sicherheitsanwendungen aufgedeckt. An dieser Stelle werden sie aufgelistet und näher erläutert. Anschließend werden die Ansätze für die Eliminierung solcher Nachteile beschrieben.

Inkonsistenz beim Update von Tools. Der Xilinx IDF mit der Toolversion 13.4 erlaubt die Verwendung globaler Clockbuffer in verschiedenen isolierten Systemkomponenten. In diesem Fall werden solche Buffer in zwei CFv2SPP-Systemen eingesetzt.

[191] [Xil13] Xilinx; *Functional Safety Certificate*. 2013
[Alt16] Altera; *Functional Safety Certificate*. 2016.
[192] [GHB10] Girardey, R., Hübner, M. und Becker, J.; *Safety Aware Place and Route for On-Chip Redundancy in Safety Critical Applications*. 2010.

Mit der Version 14.7 ist dies nicht möglich, weil das Tool so eine Konstellation als Fehler markiert und fordert, dass für jede isolierte Systemkomponente nur die globalen Clockbuffer verwendet werden, die zu ihrer Partition gehören. Demzufolge verlieren sie ihren globalen Charakter. Eine mögliche Lösung für diesen Nachteil wäre, die Strategie aus der Toolversion 13.4 beizubehalten. Noch adäquater ist eine Methodologie, mit der die essentiellen Konzepte des IDFs konstant und konsistent bleiben, weil Änderungen dieser Natur einen neuen Qualifizierung- bzw. Zertifizierungsvorgang benötigen.

Verschwendung von Ressourcen. Durch die Bildung der OCR auf den Spartan 6 und Artix FPGAs wurde festgestellt, dass für jede Partition des Systems (in diesem Fall vier, siehe Abschnitt 3.3) mindestens 40 % mehr Ressourcen verwendet werden müssen, als es nötig ist, um das Design überhaupt kompilieren zu können. Dies war der Fall mit den Xilinx ISE Tools Version 13.4 und 14.7 sowie mit den verschiedenen Versionen des Vivado-Tools bis zur Version 2015.4. Auf diese Weise entsteht eine große Menge an verschwendeten Ressourcen, weil jedes CFv2SPP-System ca. 25 % des gesamten Spartan 6 XC6SLX150 FPGAs fordert. Pro CFv2SPP entstehen somit 10 % nicht verwendete Ressourcen. Wird das Artix 7 als Plattform betrachtet, dann sieht die Statistik noch pessimistischer aus, weil pro Partition des CFv2SPP-Systems fast 50 % aller zugeordneten FPGA-Elemente nicht verwendet werden. Um diesen Nachteil zu beseitigen, sollen in Zukunft Algorithmen für die Platzierung und Verdrahtung signifikant optimiert werden oder Untersuchungen über passende Geometrien der isolierten Systemkomponenten durchgeführt werden.

Anzahl der Verdrahtungen zwischen den redundanten Komponenten. Es ist nicht eindeutig, wo das Limit der Verdrahtungen zwischen zwei isolierten Blöcken liegt. In dieser Studie wurden beim erwähnten Spartan 6 FPGA 584 Verdrahtungen erreicht, was zum Übergang auf das Artix 7 geführt hat, damit weitere 124 Verbindungen zwischen den CFv2SPP-Systemen und dem „SafeMultiplexer“ implementiert werden konnten. Beide FPGA-Hersteller, Xilinx und Altera, sollten die konkreten Informationen über das Verdrahtungspotenzial für Verbindungen zwischen den isolierten Komponenten bereitstellen.

Manuelle Zuordnung von FPGA-Ressourcen. Verlässt man sich auf den automatisierten Design-Kompilierungsprozess, dann ist zu erwarten, dass das Design schon am Anfang scheitert. Obwohl alle Anforderungen des IDFs erfüllt sind, entstehen zahlreiche Fehler bei der Verifikation der Isolierung. Dies ist der Fall bei den größeren und komplexeren Designs wie in dieser Studie. Als Konsequenz soll der Entwickler auf eine intuitive Art und Weise versuchen, unterschiedliche Elemente aus der Gatter-Netzliste manuell im PlanAhead Tool zuzuordnen. Abbildung 6.4 auf der nächsten Seite verdeutlicht diesen Schluss, indem die Isolierungsfehler im blauen Kreis markiert sind.

Xilinx und Altera bieten Lösungen für verschiedene Bereiche, wo die eingebetteten Systeme zum Einsatz kommen. Obwohl funktionale Sicherheit und Chipdesign in den letzten Jahren sehr attraktiv geworden sind und ihr Einsatzbereich ständig erweitert und intensiviert wird, kann nicht behauptet werden, dass gewisse Ad-hoc-Strategien zum Erfolg führen, auch wenn sie von den renommierten FPGA-Herstellern kommen

(siehe Xilinx-Studie[193] zur Einführung des IDFs und Darstellung eines Ad-hoc-Systems mit der OCR). Es darf nicht vergessen werden, dass ein norm-basiertes Design enorm aufwendig und rigoros ist, weil verschiedene Prozesse durchzuführen sind: Spezifikation von Anforderungen, Validierungs- und Verifikationsprozesse, Dokumentation aller Entwicklungs- und Testprozesse etc.

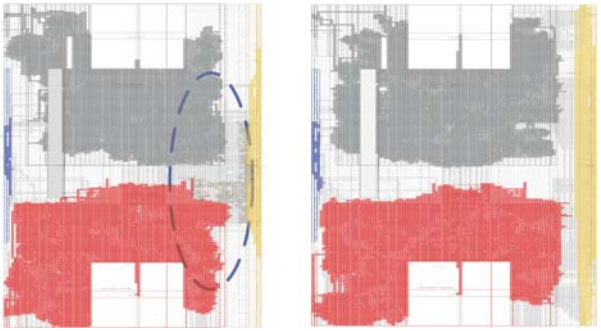


Abbildung 6.4: Ergebnis der Kompilierung: automatisch vs. manuell zugeordnete FPGA-Ressourcen

Aus den vorgelegten Betrachtungen und Ergebnissen kann geschlossen werden, dass die aktuellen FPGA-Typen die SIL 3 Anforderungen an OCR-Konzepte nicht erfüllen. Der Versuch der Entwicklung eines allgemeinen Trennungskonzeptes auf einem gemeinsamen FPGA der führenden FPGA-Hersteller ist aufgrund der fehlenden elektrischen Entkopplung gescheitert. Wird so ein Design mit einem ASIC-basierten verglichen, dann kann festgestellt werden, dass das ASIC-Design deutlich einfacher, konsistenter und effektiver ist, weil alle Aspekte der Trennung gemäß der IEC 61508 erfüllt werden können.
Dies bedeutet aber nicht, dass die FPGAs für SIL 2 Anwendungen nicht geeignet sind. Die Anforderungen an den Grad der Diagnosedeckung betragen 90 %, (siehe Tabelle 2.4), wodurch die elektrische Rückwirkung toleriert werden kann. Die unterschiedlichen Betriebsarten zweier CFv2SPP-Instanzen erhöhen auch das Konfidenzniveau der Rückwirkungsfreiheit, indem die propagierten Fehler zumindest indirekt durch implementierte Test- und Sicherheitsmaßnahmen erkannt werden. Der Anhang F des zweiten Normteils[194] definiert die Maßnahmen für die Vermeidung von systematischen Ausfällen während der Entwicklung von FPGA-basierten Systemen. Während diese Maßnahmen für SIL3 Systeme meistens obligatorisch sind (siehe Tabelle F.2 aus dem erwähnten Anhang), können sie bei SIL 2 Systemen auf Basis einer adäquaten Argumentation

[193] [CGB12] Corradi, G., Girardey, R. und Becker, J.; *Xilinx tools facilitate development of FPGA applications for IEC61508.* 2012.
[194] [IEC10b] IEC61508; *Anforderungen an sicherheitsbezogene elektrische/elektronische/programmierbare elektronische Systeme.* 2010.

ausgelassen werden.
Durch die intensive thermodynamische Analyse wurde nachgewiesen, dass die thermische Entkopplung über die Trennungsbereiche vorhanden ist, da diese zu einem zu vernachlässigenden Temperaturanstieg von nur 0,01 °C führt, was wiederum ein tolerierbares Risiko darstellt. Wie schon erwähnt, ist das thermische Verhalten eines FPGAs gegenüber dem eines ASICs deutlich stabiler, weil die FPGA-Bestandselemente sehr kleine Ströme verbrauchen und signifikant resistent für I/O-Kurzschlüsse sind. Der letztere Aspekt löst beim ASIC-Chip meistens einen kompletten Ausfall aus[195].
Die dritte Perspektive der Trennung und Entkopplung ist physikalischer Natur. Der IDF und der SDF implementieren dies durch die Bildung von Partitionen mit eigener Logik für jede sicherheitsrelevante Systemkomponente.

Demzufolge sollen in der Zukunft für SIL 3 Anwendungen nur noch Mechanismen für eine elektrische Entkopplung entwickelt werden. Ein möglicher Ansatz wäre die Auswirkungsanalyse globaler Verdrahtungen, die im Trennungsbereich existieren und sich über die gesamte FPGA-Fläche spannen. Angenommen, aus der Analyse würde folgen, dass solche Verdrahtungen ein tolerierbares Risiko für die Systemfunktionalität sind, wie z. B. im Falle des zu vernachlässigenden Temperaturanstiegs, dann wäre es behaupten, dass die FPGAs auch für SIL 3 Applikationen geeignet sind. Auf der anderen Seite bringt dies einen gewissen architekturspezifischen Nachteil mit sich . Die existierenden FPGA-Architekturen von Xilinx sind nicht alle optimal für ein sicherheitsrelevantes Design. Die Abbildung 6.5 zeigt die Platzierung von I/O-Banken auf den verschiedenen FPGA-Typen, die für den IDF vorgesehen sind. Es ist zu sehen, dass nur Spartan 6 und Artix 7 eine optimale I/O-Platzierung aufweisen, während es bei den anderen Typen nicht optimal ist, die Komponenten für OCR effizient zu platzieren.

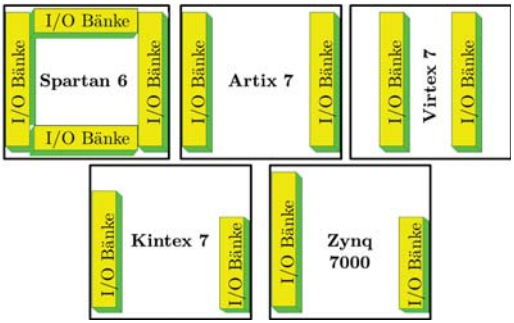


Abbildung 6.5: Platzierung von I/O-Bänken auf Xilinx-FPGAs

Ein anderer Ansatz für die Implementierung der elektrischen Entkopplung wäre die Einführung eines neuen FPGA-Typs mit den folgenden Eigenschaften:

[195] [16b]; *EMC design guide for ST microcontrollers*. 2016
[Gab14] Gabay, J.; *Protecting MCU I/O Lines from ESD and Other Transients*. 2014.

- Zwei oder mehr programmierbare Blöcke oder Partitionen auf einem FPGA, die voneinander mit einer echten Barriere getrennt sind. Die Barriere soll aus logikfreiem Silizium bestehen.
- Zwei oder mehr ICAP-Bauteile, damit bei der Überwachung des Konfigurationsspeichers Single Point of Failure vermieden werden kann.
- Temperatursensoren in den Trennungsbarrieren, damit die Sicherheitsanforderungen bezogen auf die Temperaturkontrolle erfüllt werden.

Bezüglich des Erweiterungspotenzials der dargelegten Studie sind folgende Aspekte relevant:

- Praktische Evaluierung des Gesamtsystems auf einem neuen FPGA aus der Familie Spartan 7, das seit September 2017 verfügbar ist. Dieser FPGA-Typ stellt viel mehr Ressourcen als sein Vorgänger Spartan 6 bereit, so dass die fehlenden Kommunikationsschnittstellen integriert werden können.
- In Bezug auf den obigen Aspekt könnte die praktische thermodynamische Analyse auf Basis einer Infrarotkamera durchgeführt werden.
- Erhöhung des Diagnosedeckungsgrades von Flash und SDRAM durch die Implementierung von Fehleraufdeckungs- und Fehlerkorrekturmaßnahmen, weil deren Ausfallraten den höchsten Wert bei der Sicherheitsbetrachtung aufgewiesen haben.

Bei der Betrachtung des sicherheitsgerichteten Multiplexers kann geschlossen werden, dass er eine neuartige Maßnahme ist und zwischen den etablierten Fehleraufdeckungsmechanismen wie Hardware- und Softwarevergleicher[196] steht. Er ist nicht so komplex wie ein Hardwarevergleicher, der verschiedene Inputs und Outputs vergleicht, weil beim Multiplexer nur die Outputs verglichen werden. Bei einem Softwarevergleicher hingegen werden die Ergebnisse über eine bestimmte Schnittstelle ausgetauscht und zum Vergleich herangezogen. Aufgrund dieser Flexibilität und des hohen Fehleraufdeckungsgrades kann das „SafeMux“ in Zukunft als eine Plattform für den Einsatz diverser Mikrocontroller auf einem gemeinsamen Chip verwendet werden.

[196] [IEC10b] IEC61508; *Anforderungen an sicherheitsbezogene elektrische/elektronische/programmierbare elektronische Systeme*. 2010.

7 Zusammenfassung

In der vorliegenden Studie wurde ein Beitrag zur Implementierung einer kompletten Rechnerarchitektur auf Basis eines 32-Bit ColdFire-Mikrocontrollers geleistet. Die primären Ergebnisse spalten sich in die Integration von spezifischen Sicherheitsmaßnahmen auf dem FPGA und eine intensive Sicherheitsevaluierung anhand der komparativen Analyse des Standes der Technik, wodurch der Sicherheitsintegritätslevel 2 des Gesamtsystems nachgewiesen wurde.

Der Integrationsaspekt basierte einerseits auf einer grundlegenden Betrachtung der Fehler infolge gemeinsamer Ursache und einer abschließenden Implementierung konkreter Vermeidungsmechanismen, mit denen der β_{ic}-Faktor auf einen akzeptablen Wert von 20 % reduziert worden ist. Andererseits wurde der Diagnosedeckungsgrad aller sicherheitsrelevanten Systemkomponenten auf einen für den SIL 2 geforderten Wert zwischen 90 und 99 % erhöht, indem diverse interne und externe Teststrukturen integriert wurden.

Die Sicherheitsevaluierung fokussierte sich auf die Suche nach einem Kompromiss zwischen der Pragmatik und der Rigorosität etablierter Sicherheitsnormen. Das Ziel wurde erreicht, indem die Ergebnisse von der SN 29500 mit den Ergebnissen des Xilinx-Zuverlässigkeitskalkulators zu einer Synthese gebracht wurden.

Die sekundäre Intention dieser Dissertation bestand in der Bewertung der aktuellen Entwicklungstools und der neuartigen Designmethodologien für die Entwicklung der On-Chip-Redundanz auf dem FPGA, um daraus ein zuverlässiges Argument abzuleiten, ob die aktuellen FPGA-Strukturen für die Domäne der funktionalen Sicherheit adäquat sind.

A Anhang

A.1 Designverifikation

A.1.1 Verifikation der Isolierung auf dem Spartan 6

Isolation Verification Report

Date: Wed Dec 06 15:36:42 2017 IVT Version: 7.41 ISE Build: O.87 ISE Development Version: ISE 13.4.0 Part: xc6slx150-2fgg900

Design: SafeDesign_routed.ncd

Section 1 - Isolated Modules

Group CFv2SPP_MainSys module: U_MainSys Group CFv2SPP_RedSys module: U_RedSys Group DistributedInputs module: U_DistributedInputs Group SafeMux module: U_SafeMux

Section 2 - Uncategorized User Global Nets

Total uncategorized user global nets: 573

Section 3 - Categorized Nets

Total categorized nets: 310

Section 4 - Trusted Bus Macros

No trusted bus macros were found.

...

...

Section 13 - I/O Buffer Isolation Violations

No I/O buffer isolation violations were found.

Section 14 - Package Pin Isolation Violations

No package pin isolation violations were found.

Section 15 - I/O Bank Isolation Violations

No I/O bank violations were found.

Section 16 - Isolation Verification Summary

Tile Adjacency

Net Adjacency Violations: 0 Logic Adjacency Violations: 0

Tile Content

Net Content Violations: 0 Logic Content Violations: 0

Inter-region Signals

Inter-region Net PIP Violations: 0 Inter-region Load Violations: 0

Special Fence Rules

Config Center Violations: 0 DSP Violations: 0 Implied Site Violations: 0 Top-level CMT Violations: 0 Supersite Violations: 0 GTX Violations: 0 Clock Buffer Column Violations: 0 Config Center Column Violations: 0

I/O Isolation

I/O Buffer Isolation Violations: 0 Package Pin Isolation Violations: 0 Bank Isolation Violations: 0

NCD Isolation Verification Summary

Total isolation violations: 0 Unrouted nets: 0

Isolation analysis completed.

Elapsed time: 0:03:03

A.1.2 Verifikation der Isolierung auf dem Artix 7

Isolation Verification Report

IVT Version: 7.41 ISE Build: O.87 ISE Development Version: ISE 13.4.0 ISE Installed Version: 14.7

Part: xc7a200t-1ffg1156

Design: SafeDesign_routed.ncd

Section 1 - Isolated Modules

Group CFv2SPP_MainSys module: U_MainSys Group CFv2SPP_RedSys module: U_RedSys Group DistributedInputs module: U_DistributedInputs Group SafeMux module: U_SafeMux

Section 2 - Uncategorized User Global Nets

Total uncategorized user global nets: 693

Section 3 - Categorized Nets

Total categorized nets: 414

Section 4 - Trusted Bus Macros

No trusted bus macros were found.

...

...

Section 13 - I/O Buffer Isolation Violations

No I/O buffer isolation violations were found.

Section 14 - Package Pin Isolation Violations

No package pin isolation violations were found.

Section 15 - I/O Bank Isolation Violations

No I/O bank violations were found.

Section 16 - Isolation Verification Summary

Tile Adjacency

Net Adjacency Violations: 0 Logic Adjacency Violations: 0

Tile Content

Net Content Violations: 0 Logic Content Violations: 0

Inter-region Signals

Inter-region Net PIP Violations: 0 Inter-region Load Violations: 0

Special Fence Rules

Config Center Violations: 0 DSP Violations: 0 Implied Site Violations: 0 Top-level CMT Violations: 0 Supersite Violations: 0 GTX Violations: 0 Clock Buffer Column Violations: 0 Config Center Column Violations: 0

I/O Isolation

I/O Buffer Isolation Violations: 0 Package Pin Isolation Violations: 0 Bank Isolation Violations: 0

NCD Isolation Verification Summary

Total isolation violations: 0 Unrouted nets: 0

Isolation analysis completed.

A.2 β_{IC}-Faktor

Dieser Abschnitt stützt sich auf die Tabellen aus dem Anhang E des zweiten Teils der IEC 61508.

Tabelle A.1: Verfahren und Maßnahmen, die den β_{IC} erhöhen [IEC10b]

Verfahren/Maßnahme	Delta β-Faktor [%]	Anmerkung
Watchdog on-chip als Überwachungselement verwendet	5	Überwachungselemente, die für eine Watchdogfunktion verwendet werden und notwendig sind, den erforderlichen DC oder den SFF zugewährleisten, sollten unter dem Aspekt von Ausfällen infolgegemeinsamer Ursache vorzugsweise außerhalb des IC realisiert werden. Die Verwendung eines (von) Watchdogs auf dem Chip kann im Vergleich mit einer externen Realisierung zu einem höheren DC oder höheren SFF führen.
Andere Überwachungselemente zum Beispiel Taktüberwachung	5	Siehe vorherige Anmerkung
Interne Verbindungen zwischen Blöcken durchkreuzungsfreie Leitungen zwischen Eingangs und Ausgangszellen separater, physikalischer Blöcke in verschiedenen Layern	2	Der Vergleich von Zuständen und Ergebnissen zwischen verschiedenen Blöcken sollte vorzugsweise außerhalb des IC realisiert werden. Es ist eine Analyse möglicher Ausfälle infolge gemeinsamer Ursache einschließlich FMEA von Stuck-at-Fehlern von internenVerbindungen erforderlich.

Tabelle A.2: Verfahren und Maßnahmen, die den β_{IC} erhöhen [IEC10b], Fortsetzung

Verfahren/Maßnahme	Delta β-Faktor [%]	Anmerkung
Interne Verbindungen zwischen Blöcken durchkreuzungsfreie Leitungen zwischen Eingangs und Ausgangszellen separater, physikalischer Blöcke in verschiedenen Layern	2	Insbesondere müssen die Auswirkungen eines Temperaturanstiegs durch Fehler berücksichtigt werden. Die Verifikation des Layouts sollte durch Analyse des endgültigen Layouts zum Beispiel unter Zuhilfenahme eines Werkzeugs erfolgen.
Interne Verbindungen zwischen Blöcken durch sich kreuzende Leitungen zwischen Eingangs und Ausgangszellen separater, physikalischer Blöcke	4	Der Vergleich von Zuständen und Ergebnissen zwischen separaten physikalischen Blöcken sollte vorzugsweise außerhalb des IC realisiert werden. Es ist eine Analyse möglicher Ausfälle infolge gemeinsamer Ursache einschließlich FMEA von Stuck-at-Fehlern und Kurzschlüssen von internen Verbindungen erforderlich. Insbesondere müssen die Auswirkungen eines Temperaturanstiegs durch Fehler berücksichtigt werden.

Tabelle A.3: Verfahren und Maßnahmen, die den β_{IC} verringern [IEC10b]

Verfahren/Maßnahme	Delta β-Faktor [%]
Diversitäre Maßnahmen zur Beherrschung von Ausfällen in verschiedenen Kanälen	4
Diversität in Funktion und Maßnahmen, um Ausfälle in verschiedenen Kanälen zu beherrschen	6
Test des E/E/PE-Systems in Bezug auf elektromagnetischeVerträglichkeit mit zusätzlicher Sicherheitsspanneohne Einfluss auf die Funktion des E/E/PE-Systems (zum Beispiel Bewertungskriterium A)	5
Für jeden Block eigener Pin zur Spannungsversorgung, so dass kein Block über die Spannungsversorgung eines anderen Blocks (zum Beispiel über interne Verbindungen) versorgt wird und keine Verbindung der Wannen separater physikalischer Blöcke innerhalb des IC	6
Strukturen, die physikalische Stellen voneinander isolieren und entkoppeln	2 - 4
Masse-Pin zwischen den Anschlusspins separater physikalischer Blöcke	2
Hoher Diagnosedeckungsgrad (DC > 99 %) jedes Kanals,Erkennung von Ausfällen durch den technischen Prozess und Erreichen des sicheren Zustands in angemessen kurzer Zeit	7
Temperatursensoren zwischen den Blöcken mit dauerhafter Abschaltung (intern oder extern) in den sicheren Zustand in angemessen kurzer Zeit, niedrige Wirksamkeit ohne Diagnose	2
Temperatursensoren zwischen den Blöcken mit dauerhafter Abschaltung (intern oder extern) in den sicheren Zustand in angemessen kurzer Zeit, hohe Wirksamkeit mit Diagnose	9
Analyse/Test der Auswirkungen von Fehlern (zum BeispielAnstieg der Temperatur). Abhängig von den Ergebnissender/des Analyse/Tests kann Vergleich zwischen Kanälen einschließlich Fehlererkennung und Erreichen des sicheren Zustands in angemessen kurzer Zeit erforderlich sein	9
Überwachungsschaltung, die für die erhöhte Temperatur entworfen ist	7

A.3 λ-Berechnung gemäß dem MIL-HDBK-217F

Analog zur SN 29500 wird bei der Ausfallratenberechnung gemäß dem militärischen Standard MIL-HDBK-217F auch die Gatteranzahl der betrachteten Systemkomponenten benötigt[197]. Für die λ-Berechnung von „DistributedInputs“, SEM-Controller und „SafeMux“ wird als Referenz der Abschnitt 5.1 verwendet, der sich auf FPGA-basierte Systeme mit einer Höchstzahl von 20 000 Gattern bezieht. Dementsprechend kommt die folgende Formel zum Einsatz:

$$\lambda = (C_1 \times \pi_T + C_2 \times \pi_E) \times \pi_Q \times \pi_L \frac{Failures}{10^6}\, h \tag{A.1}$$

C_1 - Komplexitätsausfallrate. Hängt von der Gatteranzahl ab.
C_2 - Package-Ausfallrate. Hängt von der Pinanzahl ab. Siehe Abschnitt 5.9.
π_T - Temperaturfaktor. Siehe Abschnitt 5.8.
π_E - Umgebungsfaktor. Siehe Abschnitt 5.10.
π_Q - Qualitätsfaktor. Siehe Abschnitt 5.10.
π_L - Erfahrungsfaktor. Siehe Abschnitt 5.10.

Die vier Faktoren sind identisch für alle drei Systemkomponenten und weisen die folgenden Werte auf:
$\pi_T = 0{,}19$ (für 40 °C)
$\pi_E = 6{,}0$ (Mittelwert)
$\pi_Q = 5{,}5$ (Mittelwert)
$\pi_L = 1$ (da das Artix 7 FPGA länger als zwei Jahre hergestellt wird)

Bezogen auf die Gatteranzahl einzelner Systemkomponenten ergeben sich die folgenden Werte:
$C_{\text{1-DistributedInputs}} = 0{,}0034$ (für 3018 Gatter)
$C_{\text{1-SEMController}} = 0{,}0068$ (für 7304 Gatter)
$C_{\text{1-SafeMux}} = 0{,}0017$ (für 1365 Gatter)

Bezogen auf die Pinanzahl einzelner Systemkomponenten folgt für die Package-Ausfallrate:
$C_{\text{2-DistributedInputs}} = 0{,}0079$ (für 22 Pins)
$C_{\text{2-SEMController}} = 0{,}00092$ (für 3 Pins)
$C_{\text{2-SafeMux}} = 0{,}097$ (für >224 Pins)

Eingesetzt in Formel (A.1) folgt:

$$\lambda_{DistributedInputs} = (0{,}0034 \times 0{,}19 + 0{,}0079 \times 6) \times 5{,}5 \times 1 \frac{Failures}{10^6} h = 264{,}25 FIT \tag{A.2}$$

[197] [MIL95] MIL-STD-217F; *Military Handbook: Reliability Prediction of Electronic Equipment.* 1995.

$$\lambda_{SEMController} = (0,0068 \times 0,19 + 0,00092 \times 6) \times 5,5 \times 1 \frac{Failures}{10^6} h = 37,46 FIT \quad \text{(A.3)}$$

$$\lambda_{SafeMux} = (0,0017 \times 0,19 \ + \ 0,097 \times 6) \times 5,5 \times 1 \frac{Failures}{10^6} \, h = 3202,78 \, FIT \quad \text{(A.4)}$$

Für die Berechnung der Ausfallrate des CFv2SPP-Systems wird die Gleichung aus Abschnitt 5.3 eingesetzt, die sich auf die integrierten Schaltungen mit mehr als 60 000 Gattern bezieht.

$$\lambda = (\lambda_{BD} \times \pi_{MFG} \times \pi_T \times \pi_{CD} \ + \ \lambda_{BP} \times \pi_E \times \pi_Q \times \pi_{PT} \ + \ \lambda_{EOS}) \times \frac{Failures}{10^6} \, h \quad \text{(A.5)}$$

λ_{BD} - Basisausfallrate. Für ein FPGA hat sie den Wert 0,24.
π_{MFG} - Korrekturfaktor des Herstellungsprozesses. Hat den Wert 0,55.
π_{CD} - Komplexitätsfaktor. Hat den Wert 16 für eine Chipfläche zwischen 1 und 2 cm^2.
λ_{BP} - Package-Basisausfallrate. Für 24 Pins des CFv2SPP-Systems ergibt sich der Wert 0,0026.
π_{PT} - Korrekturfaktor des Packages. Hat den Wert 1,0.
λ_{EOS} - Ausfallrate bei elektrischem Overstress. Für die elektrischen Eigenschaften des Artix 7 FPGAs ergibt sich der Wert 0,053.

Somit folgt für die Ausfallrate des CFv2SPP-Systems:

$$\lambda_{CFv2SPP} = (0,24 \times 0,55 \times 0,19 \times 16 + 0,0026 \times 6 \times 5,5 \times 1 + 0,053) \frac{Failures}{10^6} h = 533,06 FIT \quad \text{(A.6)}$$

A.4 λ-Berechnung gemäß dem Ansatz aus [HD12]

Die Studie[198] entwickelte einen eigenen Ansatz für die Ausfallratenberechnung auf dem Spartan 3 DSP FPGA. Der Ansatz basiert auf den folgenden Annahmen:

- Extrahieren der Gesamtausfallrate des Spartan 3 DSP FPGAs aus dem Xilinx-Zuverlässigkeitsbericht[199]
- Ermittlung der Ausfallrate eines Transistors [11]. $\lambda_{Transistor}$ = 3,6199 x 10^{-7} FIT / Mb
- Ermittlung der Ausfallrate von einem Slice [11]. λ_{Slice} = 6,2433 x 10^{-3} FIT / Mb

[198] [HD12] Hock, O. und Drgona, P.; *PWM modulator with increased reliability in FPGA circuit.* 2012.
[199] [11]; *Device Reliability Report.* 2011.

Nach der Kompilierung der einzelnen Systemkomponenten für das Spartan 3 DSP FPGA ergibt sich die folgende Anzahl an Slices:

CFv2SPP = 11318 Slices
DistributedInputs = 9 Slices
SEM-Controller = 2058 Slices
SafeMux = 232 Slices

Eingesetzt in λ_{Slice} folgt:

$$\lambda_{CFv2SPP} = 11318 \times 6,2433 \times 10^{-3} \frac{FIT}{1024 \times 1024} = 67,39\,FIT \tag{A.7}$$

$$\lambda_{DistributedInputs} = 9 \times 6,2433 \times 10^{-3} \frac{FIT}{1024 \times 1024} = 0,053\,FIT \tag{A.8}$$

$$\lambda_{SEMController} = 2058 \times 6,2433 \times 10^{-3} \frac{FIT}{1024 \times 1024} = 12,25\,FIT \tag{A.9}$$

$$\lambda_{SafeMux} = 232 \times 6,2433 \times 10^{-3} \frac{FIT}{1024 \times 1024} = 1,38\,FIT \tag{A.10}$$

B Literaturverzeichnis

[03] *Samsung 128Mb NAND Flash Qualification and Reliability Report*. JBK. Rev. 0.1. Samsung Electronics. 2003.

[05] *ColdFire Family Programmers Reference Manual*. CFPRM. Rev. 3.0. Freescale Semiconductor. März 2005.

[06] *Internal Qualification and Reliability Report*. Y27B MJP. Rev. A 8/06. Micron Technology, Inc. 2006.

[07a] *CFV2SPP5208 Integration Guide*. Rev. 1.0.0. IPextreme. Dez. 2007.

[07b] *CFV2SPP5208 User Guide*. Rev. 1.0.0. IPextreme. Dez. 2007.

[10a] *Developing Functional Safety Systems with TÜV-Qualified FPGAs*. WP-01123. Rev. 1.1. Altera. März 2010.

[10b] *Xilinx Power Tools Tutorial: Spartan-6 and Virtex-6 FPGAs*. UG733. Rev. 1.0. Xilinx. März 2010.

[11] *Device Reliability Report*. UG116. Rev. 8.0. Xilinx. Nov. 2011.

[12a] *Partial Reconfiguration User Guide*. UG702. Rev. 14.1. Xilinx. Apr. 2012.

[12b] *POWER7 and POWER7+ Optimization and Tuning Guide*. SG24-8079-00. 1.0. IBM. Nov. 2012.

[13] *A Validated Methodology for Designing Safe Industrial Systems on a Chip*. WP-01168. Rev. 1.3. Altera. März 2013.

[14a] *Quarterly Reliability Report*. DOC-62807. Rev. 1. Peregrine Semiconductor. 2014.

[14b] *Spartan-6 FPGA Packaging and Pinouts*. UG385. Rev. 2.3. Xilinx. Mai 2014.

[15a] *FPGA-based Safety Separation Design Flow for Rapid Functional Safety Certification*. an704. Rev. 1.2. Altera. Jan. 2015.

[15b] *LogiCORE IP Soft Error Mitigation Controller v3.4.1*. PG036. Rev. 3.4.1. Xilinx. 2015.

[15c] *Spartan-6 FPGA Clocking Resources*. UG382. Rev. 1.10. Xilinx. Juni 2015.

[15d] *Spartan-6 FPGA Data Sheet: DC and Switching Characteristics*. DS162. Rev. 3.1.1. Xilinx. Jan. 2015.

[16a] *7 Series FPGAs Configurable Logic Block*. UG474. Rev. 1.8. Xilinx. 2016.

[16b] *EMC design guide for ST microcontrollers*. AN1709. Rev. 2. ST. Feb. 2016.

[16c] *Spartan-6 FPGA Power Management*. UG394. Rev. 1.3. Xilinx. Jan. 2016.

[17a] *7 Series FPGAs Packaging and Pinout*. UG475. Rev. 1.15. Xilinx. 2017.

[17b] *Device Reliability Report*. UG116. Rev. 10.7.1. Xilinx. 2017.

[17c] *Spartan-6 FPGA Configuration*. UG380. Rev. 2.10. Xilinx. März 2017.

[18a] *Zynq-7000 All Programmable SoC Overview*. DS190. Rev. 1.11.1. Xilinx. Juli 2018.

[18b] *Zynq-7000 All Programmable SoC, Technical Reference Manual*. UG585. Rev. 1.12.2. Xilinx. Juli 2018.

[AG05a] AG, S. *SN 29500-1: Teil-1 Erwartungswerte Allgemeines Ausgabestand*. Ausgabe 2005-12. 2005.

[AG05b] AG, S. *SN 29500-2: Teil-2 Erwartungswerte von integrierten Schaltkreisen*. Ausgabe 2005-12. 2005.

[Alf08] Alfke, X. P. *Logic cell to Gate count*. 2008. URL: `https://forums.xilinx.com/t5/Virtex-Family-FPGAs/Logic-cell-to-Gate-count/td-p/5459`.

[Alt16] Altera. *Functional Safety Certificate*. 2016. URL: `https://nmi.org.uk/wp-content/uploads/2016/05/Altera_NMI-Func-Safety.pdf`.

[Ama13] Amari, S. V. *Optimal design configurations of fault-tolerant systems*. In: *2013 Proceedings Annual Reliability and Maintainability Symposium*. Jan. 2013, S. 1–6.

[Amr+13] Amrouch, H. u. a. *Analyzing the thermal hotspots in FPGA-based embedded systems*. In: *2013 23rd International Conference on Field programmable Logic and Applications*. Sep. 2013, S. 1–4.

[And05] Anderson, J. *Power Optimization and Prediction Techniques for FPGA*. Diss. University of Toronto, 2005.

[Ant+03] Antreich, K. u. a. *Modeling, Simulation, and Optimization of Integrated Circuits*. 2003.

[APM14] Anwer, J., Platzner, M. und Meisner, S. *FPGA Redundancy Configurations: An Automated Design Space Exploration*. In: *2014 IEEE International Parallel Distributed Processing Symposium Workshops*. Mai 2014, S. 275–280.

[ARV07] Agarwal, S., Ramanathan, P. und Vanathi, P. T. *Comparative analysis of low power high performance flip flops in the 0.13 micro meter technology*. In: *15th International Conference on Advanced Computing and Communications (ADCOM 2007)*. Dez. 2007, S. 209–213.

[Bar+10] Bartolini, A. u. a. *A Virtual Platform Environment for Exploring Power, Thermal and Reliability Management Control Strategies in High performance Multicores*. In: *Proceedings of the 20th Symposium on Great Lakes Symposium on VLSI*. Providence, Rhode Island, USA, 2010, S. 311–316.

[Ber+04] Bernardi, P. u. a. *On the evaluation of SEU sensitiveness in SRAM-based FPGAs*. In: *Proceedings. 10th IEEE International On-Line Testing Symposium*. Juli 2004, S. 115–120.

[Ber+14] Bernardi, P. u. a. *MIHST: A Hardware Technique for Embedded Microprocessor Functional On-Line Self-Test*. In: IEEE Transactions on Computers 63.11 (Nov. 2014), S. 2760–2771.

[Ber+16] Bernardi, P. u. a. *Development Flow for On-Line Core Self-Test of Automotive Microcontrollers*. In: IEEE Transactions on Computers 65.3 (März 2016), S. 744–754.

[BHU08] Borcsok, J., Hayek, A. und Umar, M. *Implementation of a 1oo2-RISC-architecture on FPGA for safety systems*. In: *2008 IEEE/ACS International Conference on Computer Systems and Applications*. März 2008, S. 1046–1051.

[Bor+11] Borecky, J. u. a. *Fault Models Usability Study for On-line Tested FPGA*. In: *2011 14th Euromicro Conference on Digital System Design*. Aug. 2011, S. 287–290.

[Bor+16] Borecky, J. u. a. *Enhanced Duplication Method with TMR-Like Masking Abilities*. In: *2016 Euromicro Conference on Digital System Design (DSD)*. Aug. 2016, S. 690–693.

[Bör07] Börcsök, J. *Elektronische Sicherheitssysteme : Hardwarekonzepte, Modelle und Berechnung*. 2., überarb. Aufl. Heidelberg: Hüthig, 2007.

[Bör15] Börcsök, J. *Funktionale Sicherheit : Grundzüge sicherheitstechnischer Systeme*. 4., aktualisierte Aufl. Berlin: VDE-Verlag, 2015.

[BTM00] Brooks, D., Tiwari, V. und Martonosi, M. *Wattch: a framework for architectural-level power analysis and optimizations*. In: *Proceedings of 27th International Symposium on Computer Architecture (IEEE Cat. No.RS00201)*. Juni 2000, S. 83–94.

[Car06] Carmichael, C. *Triple Module Redundancy Design Techniques for Virtex FPGAs*. XAPP197. Rev. 1.0.1. Xilinx. Juli 2006.

[Cet+13] Cetin, E. u. a. *Towards bounded error recovery time in FPGA-based TMR circuits using dynamic partial reconfiguration*. In: *2013 23rd International Conference on Field programmable Logic and Applications*. Sep. 2013, S. 1–4.

[CGB12] Corradi, G., Girardey, R. und Becker, J. *Xilinx tools facilitate development of FPGA applications for IEC61508*. In: *2012 NASA/ESA Conference on Adaptive Hardware and Systems (AHS)*. Juni 2012, S. 54–61.

[Cha+15] Chafi, P. R. u. a. *A platform for dynamic thermal management of FPGA-based soft-core processors via Dynamic Frequency Scaling*. In: *2015 23rd Iranian Conference on Electrical Engineering*. Mai 2015, S. 1093–1097.

[Chu08a] Chu, P. P. *FPGA prototyping by Verilog examples : Xilinx Spartan-3 version*. Wiley, 2008.

[Chu08b] Chu, P. P. *FPGA prototyping by VHDL examples : Xilinx Spartan-3 version*. [Nachdr.] Wiley, 2008.

[Con+09] Constantinides, K. u. a. *A Flexible Software-Based Framework for Online Detection of Hardware Defects*. In: IEEE Transactions on Computers 58.8 (Aug. 2009), S. 1063–1079.

[Cor13a] Corbett, J. D. *Isolation Verification Tool (IVT) Software User Manual*. Rev. 3.2. Xilinx. Dez. 2013.

[Cor13b] Corbett, J. D. *IVT 7.41 Release Notes and Installation Guide*. Rev. 7.41. Xilinx. Dez. 2013.

[Cor13c] Corbett, J. D. *The Xilinx Isolation Design Flow for Fault-Tolerant Systems*. WP412. Rev. 1.1. Xilinx. Okt. 2013.

[Cra10] Crabill, E. *Eliminating I/O Coupling Effects when Interfacing Large-Swing Single-Ended Signals to User I/O Pins on Spartan-3 Families*. Rev. 1.2. Xilinx. 2010.

[CWH11] Cordes, K., Waag, A. und Heuck, N. *Integrierte Schaltungen : Grundlagen, Prozesse, Design, Layout*. Pearson Studium - Elektrotechnik. Pearson Studium, 2011.

[FH03] Fernandes, D. A. und Harris, I. G. *Application of built in self-test for interconnect testing of FPGAs*. In: *International Test Conference, 2003. Proceedings. ITC 2003*. Bd. 1. Sep. 2003, S. 1248–1257.

[FMM12] Farooq, U., Marrakchi, Z. und Mehrez, H. *Tree-based heterogeneous FPGA architectures : application specific exploration and optimization*. New York, NY, 2012.

[Gab14] Gabay, J. *Protecting MCU I/O Lines from ESD and Other Transients*. 2014. URL: https://www.digikey.com/en/articles/techzone/2014/jun/protecting-mcu-io-lines-from-esd-and-other-transients.

[GHB10] Girardey, R., Hübner, M. und Becker, J. *Safety Aware Place and Route for On-Chip Redundancy in Safety Critical Applications*. In: *2010 IEEE Computer Society Annual Symposium on VLSI*. Juli 2010, S. 74–79.

[GST13] Gorman, C., Siqueira, P. und Tessier, R. *An open-source SATA core for Virtex-4 FPGAs*. In: *2013 International Conference on Field Programmable Technology (FPT)*. Dez. 2013, S. 454–457.

[Hal+14] Halt, G. B. u. a. *Intellectual Property in Consumer Electronics, Software and Technology Startups*. New York, NY: Springer New York, 2014, S. 61–66.

[Hal+15] Halawa, H. H. u. a. *FPGA-based reliable TMR controller design for S2A architectures*. In: *2015 IEEE 20th Conference on Emerging Technologies Factory Automation (ETFA)*. Sep. 2015, S. 1–8.

[Hal15] Hallett, E. *Isolation Design Flow for Xilinx 7 Series FPGAs or Zynq-7000 AP SoCs (ISE Tools)*. XAPP1086. Rev. 1.3.1. Xilinx. Feb. 2015.

[Hal16] Hallett, E. *Isolation Design Flow for Xilinx 7 Series FPGAs or Zynq-7000 AP SoCs (Vivado Tools)*. XAPP1222. Rev. 1.3. Xilinx. Sep. 2016.

[HAP11] Happe, M., Agne, A. und Plessl, C. *Measuring and Predicting Temperature Distributions on FPGAs at Run-Time*. In: *2011 International Conference on Reconfigurable Computing and FPGAs*. Nov. 2011, S. 55–60. DOI: 10.1109/ReConFig.2011.59.

[Hay10] Hayek, A. *Modellierung, Implementierung und Bewertung einer sicherheitsgerichteten 1oo2-Architektur mit VHDL auf FPGA-Ebene*. Zugl.: Kassel. Univ., Diss., 2010. Diss. Kassel, 2010.

[HCM15] Hallett, E., Corradi, G. und McNeil, S. *Xilinx Reduces Risk and Increases Efficiency for IEC61508 and ISO26262 Certified Safety Applications*. WP461. Rev. 1.0. Xilinx. Apr. 2015.

[HD12] Hock, O. und Drgona, P. *PWM modulator with increased reliability in FPGA circuit*. In: *2012 ELEKTRO*. Mai 2012, S. 121–124.

[He+15] He, W. u. a. *A self-tuned thermal compensation system for reducing Process Variation influence in side-channel attack resistant dual-rail logic*. In: *2015 Conference on Design of Circuits and Integrated Systems (DCIS)*. Nov. 2015, S. 1–6.

[HN15] Hashamdar, T. und Noori, H. *Thermal management of FPGA-based embedded systems at operating system level*. In: *2015 CSI Symposium on Real-Time and Embedded Systems and Technologies (RTEST)*. Okt. 2015, S. 1–6.

[Hon+12] Hong, C. u. a. *Design and implementation of fault-tolerant soft processors on FPGAs*. In: *22nd International Conference on Field Programmable Logic and Applications (FPL)*. Aug. 2012, S. 683–686.

[HS15] Hussein, J. und Swift, G. *Mitigating Single-Event Upsets*. WP395. Rev. 1.1. Xilinx. Mai 2015.

[Hua+08] Huang, W. u. a. *Accurate, Pre-RTL Temperature-Aware Design Using a Parameterized, Geometric Thermal Model*. In: IEEE Transactions on Computers 57.9 (Sep. 2008), S. 1277–1288.

[Ich+10] Ichinomiya, Y. u. a. *Improving the Robustness of a Softcore Processor against SEUs by Using TMR and Partial Reconfiguration*. In: *2010 18th IEEE Annual International Symposium on Field-Programmable Custom Computing Machines*. Mai 2010, S. 47–54.

[IEC10a] IEC61508. *Allgemeine Anforderungen*. 2. Ausgabe. 2010.

[IEC10b] IEC61508. *Anforderungen an sicherheitsbezogene elektrische/elektronische/-programmierbare elektronische Systeme*. 2. Ausgabe. 2010.

[IEC10c] IEC61508. *Anforderungen an Software*. 2. Ausgabe. 2010.

[IEC10d] IEC61508. *Anwendungsrichtlinie für Teile 2 und 3*. 2. Ausgabe. 2010.

[IEC10e] IEC61508. *Begriffe und Abkürzungen*. 2. Ausgabe. 2010.

[IEC10f] IEC61508. *Beispiele von Methoden für die Bestimmung von Sicherheits-Integritätsleveln*. 2. Ausgabe. 2010.

[IEC10g] IEC61508. *Überblick über Verfahren und Maßnahmen*. 2. Ausgabe. 2010.

[Ins12] Instruments, N. *Vorteile der Virtex-5-FPGAs von Xilinx*. 2012. URL: `http://www.ni.com/white-paper/7440/de/`.

[Jan01] Jansen, D. *Handbuch der Electronic Design Automation : mit 176 Tabellen*. München, 2001.

[JC12] Jevtic, R. und Carreras, C. *A complete dynamic power estimation model for data-paths in {FPGA} {DSP} designs*. In: Integration, the {VLSI} Journal 45.2 (2012), S. 172–185.

[JCG12] Jacobs, A., Cieslewski, G. und George, A. D. *Overhead and reliability analysis of algorithm-based fault tolerance in FPGA systems*. In: *22nd International Conference on Field Programmable Logic and Applications (FPL)*. Aug. 2012, S. 300–306.

[Jin+11] Jing, N. u. a. *Quantitative SEU Fault Evaluation for SRAM-Based FPGA Architectures and Synthesis Algorithms*. In: *2011 21st International Conference on Field Programmable Logic and Applications*. Sep. 2011, S. 282–285.

[Kha16] Kharchenko, V. *Diversity for safety and security of embedded and cyber physical systems: Fundamentals review and industrial cases*. In: *2016 15th Biennial Baltic Electronics Conference (BEC)*. Okt. 2016, S. 17–26.

[KK03] Kubalik, P. und Kubatova, H. *Design of self checking circuits based on FPGA*. In: *Proceedings of the 12th IEEE International Conference on Fuzzy Systems (Cat. No.03CH37442)*. Dez. 2003, S. 378–381.

[Kle05] Klein, M. *Static Power and the Importance of Realistic Junction Temperature Analysis*. WP221. Rev. 1.0. Xilinx. März 2005.

[KP09] Kyriakoulakos, K. und Pnevmatikatos, D. *A novel SRAM-based FPGA architecture for efficient TMR fault tolerance support*. In: *2009 International Conference on Field Programmable Logic and Applications*. Aug. 2009, S. 193–198.

[Kre+12] Kretzschmar, U. u. a. *Robustness of different TMR granularities in shared wishbone architectures on SRAM FPGA*. In: *2012 International Conference on Reconfigurable Computing and FPGAs*. Dez. 2012, S. 1–6.

[KSS11] Kharchenko, V., Siora, O. und Sklyar, V. *Multi-Version FPGA-Based Nuclear Power Plant IC Systems: Evolution of Safety Ensuring*. In: *Nuclear Power ? Control, Reliability and Human Factors*. Sep. 2011, S. 27–48.

[LB03] Lala, P. K. und Burress, A. L. *Self-checking logic design for FPGA implementation*. In: IEEE Transactions on Instrumentation and Measurement 52.5 (Okt. 2003), S. 1391–1398.

[LB14] Lienig, J. und Brümmer, H. *Elektronische Gerätetechnik : Grundlagen für das Entwickeln elektronischer Baugruppen und Geräte*. 2014.

[LC01] Lai, W.-C. und Cheng, K.-T. *Instruction-level DfT for testing processor and IP cores in system-on-a-chip*. In: *Proceedings of the 38th Design Automation Conference (IEEE Cat. No.01CH37232)*. Juni 2001, S. 59–64.

[LC17] Lin, C. und Chen, C. *A Processor and Cache Online Self-Testing Methodology for OS-Managed Platform*. In: IEEE Transactions on Very Large Scale Integration (VLSI) Systems 25.8 (Aug. 2017), S. 2346–2359.

[LCR03] Lima, F., Carro, L. und Reis, R. *Designing fault tolerant systems into SRAM-based FPGAs*. In: *Proceedings 2003. Design Automation Conference (IEEE Cat. No.03CH37451)*. Juni 2003, S. 650–655.

[LGB00] Lopez-Buedo, S., Garrido, J. und Boemo, E. *Thermal testing on reconfigurable computers*. In: IEEE Design Test of Computers 17.1 (Jan. 2000), S. 84–91.

[Li+16] Li, J. u. a. *Thermal distribution measurement on FPGA using optimized ring oscillator (RO)-based thermal sensor network*. In: *2016 13th IEEE International Conference on Solid-State and Integrated Circuit Technology (ICSICT)*. Okt. 2016, S. 1488–1490.

[Mac+14] Macii, D. u. a. *Design of a Redundant FPGA-Based Safety System for Railroad Vehicles*. In: *2014 17th Euromicro Conference on Digital System Design*. Aug. 2014, S. 683–686.

[Mae18] Maeda, S. *Xilinx Announces Availability of Automotive Qualified Zynq UltraScale+ MPSoC Family*. 2018. URL: https://www.xilinx.com/news/press/2018/xilinx-announces-availability-of-automotive-qualified-zynq-%5C%5C%20ultrascale-mpsoc-family.html.

[Man+08] Mangalagiri, P. u. a. *Thermal-aware reliability analysis for Platform FPGAs*. In: *2008 IEEE/ACM International Conference on Computer-Aided Design*. Nov. 2008, S. 722–727.

[McN13] McNeil, S. *Developing Secure Designs with the Spartan-6 Family Using the Isolation Design Flow*. XAPP1145. Rev. 1.1.1. Xilinx. Juni 2013.

[McN15] McNeil, S. *Developing Secure Designs with the Spartan-6 Family Using the Isolation Design Flow*. XAPP1145. Rev. 1.2. Xilinx. Sep. 2015.

[Mic17] Michahelles, F. *Internet of Things Reality Check*. In: IEEE Pervasive Computing 16.2 (2017), S. 90–91.

[MIL95] MIL-STD-217F. *Military Handbook: Reliability Prediction of Electronic Equipment*. MIL-STD-217F. Notice 2. Department of Defense„ USA. 1995.

[Mon99] Montenegro, S. *Sichere und fehlertolerante Steuerungen : Entwicklung sicherheitsrelevanter Systeme*. München [u.a.]: Hanser, 1999.

[Mou+13] Mou, H. u. a. *A comparison and case studies of electronic product reliability prediction methods based on handbooks*. In: *2013 International Conference on Quality, Reliability, Risk, Maintenance, and Safety Engineering (QR2MSE)*. Juli 2013, S. 112–115.

[MP10] Meyna, A. und Pauli, B. *Taschenbuch der Zuverlässigkeitstechnik : Quantitative Bewertungsverfahren*. 2., überarb. und erw. Aufl. Praxisreihe Qualitatswissen. München [u.a.]: Hanser: [s.n.], 2010.

[MUM10] Matsumoto, K., Uehara, M. und Mori, H. *Evaluating the Fault Tolerance of Stateful TMR*. In: *2010 13th International Conference on Network-Based Information Systems*. Sep. 2010, S. 332–336.

[Naf+12] Nafkha, A. u. a. *Leakage power consumption in FPGAs: Thermal analysis*. In: *2012 International Symposium on Wireless Communication Systems (ISWCS)*. Aug. 2012, S. 606–610.

[New16] NewTec. *Safe Flex*. 2016. URL: https://www.newtec.de/web/de/spektrum/FunktionaleSicherheit/SafeFlex/SafeFlex.php.

[NR11] Nowroz, A. N. und Reda, S. *Thermal and Power Characterization of Field-programmable Gate Arrays*. In: *Proceedings of the 19th ACM/SIGDA International Symposium on Field Programmable Gate Arrays*. FPGA '11. ACM, 2011, S. 111–114.

[NSB11] Niknahad, M., Sander, O. und Becker, J. *FGTMR - Fine grain redundancy method for reconfigurable architectures under high failure rates*. In: *The 16th North-East Asia Symposium on Nano, Information Technology and Reliability*. Okt. 2011, S. 186–191.

[Pec95] Pecht, M. *Product reliability, maintainability, and supportability handbook*. CRC Press, 1995.

[Pen18] Penney, K. *Hot Swapping with FPGAs*. XAPP1311. Rev. 1.1. Xilinx. 2018.

[Per+14] Perez, J. u. a. *A Safety Certification Strategy for IEC-61508 Compliant Industrial Mixed-Criticality Systems Based on Multicore Partitioning*. In: *2014 17th Euromicro Conference on Digital System Design*. Aug. 2014, S. 394–400.

[PG05] Paschalis, A. und Gizopoulos, D. *Effective software-based self-test strategies for on-line periodic testing of embedded processors*. In: IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems 24.1 (Jan. 2005), S. 88–99.

[Pos15] Posner, S. M. *How many ASIC Gates does it take to fill an FPGA?* 2015. url: `https://blogs.synopsys.com/breakingthethreelaws/2015/02/how-many-asic-gates-does-it-take-to-fill-an-fpga/`.

[Pre+13] Preschern, C. u. a. *Verifying generic IEC 61508 CPU self-tests with fault injection*. In: *2013 8th IEEE Design and Test Symposium*. Dez. 2013, S. 1–2.

[PSB09] Pedre, S., Stoliar, A. und Borensztejn, P. *Real Time Hot Spot Detection Using FPGA*. In: *Progress in Pattern Recognition, Image Analysis, Computer Vision, and Applications: 14th Iberoamerican Conference on Pattern Recognition, CIARP 2009, Guadalajara, Jalisco, Mexico, November 15-18, 2009. Proceedings*. Hrsg. von Bayro-Corrochano, E. und Eklundh, J.-O. Berlin, Heidelberg: Springer Berlin Heidelberg, 2009, S. 595–602.

[Rad14] Radu, M. *Reliability and fault tolerance analysis of FPGA platforms*. In: *IEEE Long Island Systems, Applications and Technology (LISAT) Conference 2014*. Mai 2014, S. 1–4.

[Sau10] Sauer, P. *Hardware-Design mit FPGA : Eine Einführung in den Schaltungsentwurf mit FPGA-Bausteinen*. Aachen, 2010.

[Sei17] Seidel, M. *Thermodynamik - Verstehen durch Üben : Band 2 Wärmeübertragung*. Berlin, 2017.

[SEN04a] Shamshiri, S., Esmaeilzadeh, H. und Navabi, Z. *Instruction level test methodology for CPU core software-based self-testing*. In: *Proceedings. Ninth IEEE International High-Level Design Validation and Test Workshop (IEEE Cat. No.04EX940)*. Nov. 2004, S. 25–29.

[SEN04b] Shamshiri, S., Esmaeilzadeh, H. und Navabi, Z. *Test instruction set (TIS) for high level self-testing of CPU cores*. In: *13th Asian Test Symposium*. Nov. 2004, S. 158–163.

[Shr+10] Shrikhande, S. V. u. a. *Hardware Reliability prediction of Computer Based safety Systems of Indian Nuclear Plants*. In: *2010 2nd International Conference on Reliability, Safety and Hazard - Risk-Based Technologies and Physics-of-Failure Methods (ICRESH)*. Dez. 2010, S. 127–132.

[Ska18] Skadron, K. *Has HotSpot been validated?* 2018. url: `http://lava.cs.virginia.edu/HotSpot/faq.htm`.

[SKK10] Straka, M., Kastil, J. und Kotasek, Z. *Modern fault tolerant architectures based on partial dynamic reconfiguration in FPGAs*. In: *13th IEEE*

Symposium on Design and Diagnostics of Electronic Circuits and Systems. Apr. 2010, S. 173–176.

[SKP12] Schönfeld, D., Klimant, H. und Piotraschke, R. *Informations- und Kodierungstheorie*. 2012.

[SL12] Sridharan, V. und Liberty, D. *A study of DRAM failures in the field*. In: *High Performance Computing, Networking, Storage and Analysis (SC), 2012 International Conference for*. Nov. 2012, S. 1–11.

[SNM16] Skitsas, M. A., Nicopoulos, C. A. und Michael, M. K. *DaemonGuard: Enabling O/S-Orchestrated Fine-Grained Software-Based Selective-Testing in Multi-/Many-Core Microprocessors*. In: IEEE Transactions on Computers 65.5 (Mai 2016), S. 1453–1466.

[SSB14] Sklyarov, V., Skliarova, I. und Barkalov, A. *Synthesis and Optimization of FPGA-Based Systems*. 2014.

[ST10] Sosnowski, J. und Tupaj, L. *CPU Testability in Embedded Systems*. In: *2010 Fifth IEEE International Symposium on Electronic Design, Test Applications*. Jan. 2010, S. 108–112.

[Sta+03] Stan, M. R. u. a. *HotSpot: a dynamic compact thermal model at the processor-architecture level*. In: Microelectronics Journal 34.12 (2003). Thermal Investigations of integrated circuits and systems at Therminic 2002, S. 1153–1165.

[TGM15] Tang, X., Gaillardon, P. E. und Micheli, G. D. *FPGA-SPICE: A simulation-based power estimation framework for FPGAs*. In: *2015 33rd IEEE International Conference on Computer Design (ICCD)*. Okt. 2015, S. 696–703.

[The+14] Theodorou, G. u. a. *Software-Based Self-Test for Small Caches in Microprocessors*. In: IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems 33.12 (Dez. 2014), S. 1991–2004.

[TP07] Tamandl, T. und Preininger, P. *Online Self Tests for Microcontrollers in Safety Related Systems*. In: *2007 5th IEEE International Conference on Industrial Informatics*. Bd. 1. Juni 2007, S. 137–142.

[TS09] Tummeltshammer, P. und Steininger, A. *Power supply induced common cause faults-experimental assessment of potential countermeasures*. In: *2009 IEEE/IFIP International Conference on Dependable Systems Networks*. Juni 2009, S. 449–457.

[Van+16] Vanat, T. u. a. *Comparing proton and neutron induced SEU cross section in FPGA*. In: *2016 IEEE 19th International Symposium on Design and Diagnostics of Electronic Circuits Systems (DDECS)*. Apr. 2016, S. 1–4.

[Vel+05] Velusamy, S. u. a. *Monitoring temperature in FPGA based SoCs*. In: *2005 International Conference on Computer Design*. Okt. 2005, S. 634–637.

[WCB16] Wang, Q., Chen, D. und Bai, H. *A method of space radiation environment reliability prediction*. In: *2016 Annual Reliability and Maintainability Symposium (RAMS)*. Jan. 2016, S. 1–6.

[Web+13] Weber, P. u. a. *Toolset for measuring thermal behavior of FPGA devices*. In: *19th International Workshop on Thermal Investigations of ICs and Systems (THERMINIC)*. Sep. 2013, S. 48–53.

[Wel15] Welter, M. *Demonstration of Soft Error Mitigation IP and Partial Reconfiguration Capability on Monolithic Devices*. XAPP1261. Rev. 1.0. Xilinx. Juni 2015.

[Wil08] Williams, J. *Digital VLSI Design with Verilog : A Textbook from Silicon Valley Technical Institute*. 2008.

[Wil11] Wilamowski, B. M. *The industrial electronics handbook : Industrial communication systems*. Boca Raton [u.a.]: CRC Press, 2011.

[Woj+14] Wojciechowski, B. u. a. *Hardware microprocessor thermal emulation using synthetic heat sources and temperature sensors in FPGA*. In: *20th International Workshop on Thermal Investigations of ICs and Systems*. Sep. 2014, S. 1–5.

[WSJ17] Wollschlaeger, M., Sauter, T. und Jasperneite, J. *The Future of Industrial Communication: Automation Networks in the Era of the Internet of Things and Industry 4.0*. In: IEEE Industrial Electronics Magazine 11.1 (März 2017), S. 17–27.

[Xil13] Xilinx. *Functional Safety Certificate*. 2013. URL: `https://www.xilinx.com/publications/prod_mktg/functional_safety_certificate.pdf`.

[Xil18] Xilinx. *IEC 61508 specification certificate issued by Exida for high performance Zynq UltraScale+ family*. 2018. URL: `https://www.xilinx.com/news/press/2018/xilinx-extends-functional-safety-into-ai-class-devices.html`.

[Zas18] Zastrow, D. *Elektrotechnik : ein Grundlagenlehrbuch : mit 547 Abbildungen, 141 Beispielen und 224 Übungsaufgaben mit Lösungen sowie 27 Übersichten als Wissensspeicher*. Wiesbaden, 2018.

[Zho+12] Zhou, L. u. a. *Reliability prediction for smart meter based on Bellcore standards*. In: *2012 International Conference on Quality, Reliability, Risk, Maintenance, and Safety Engineering*. Juni 2012, S. 631–634.

[ZSS15] Zhang, R., Stan, M. R. und Skadron, K. *HotSpot 6.0: Validation, Acceleration and Extension*. CS-2015-04. University of Virginia. Aug. 2015.

[ZY18] Zhu, L. und Yu, L. *A design of decentralized dual mode redundant hot standby arbitration switch-over logic and architecture*. In: *2018 International Conference on Electronics Technology (ICET)*. Mai 2018, S. 216–219.

Eigene Publikationen

[1] Gracic, E. ; Hayek, A. ; Boörcsök, J.: Approach to the development of an FPGA-based safety-related, complete communication computer system. In: *2014 X International Symposium on Telecommunications (BIHTEL)*, 2014, S. 1-6

[2] Gracic, E. ; Hayek, A. ; Börcsök, J.: Implementation of a fault- tolerant system using safety-related Xilinx tools conforming to the stan- dard IEC 61508. In: *2016 International Conference on System Reliability and Science (ICSRS)*, 2016, S. 78-83

[3] Gracic, E. ; Hayek, A. ; Börcsök, J.: Evaluation of FPGA design tools for safety systems with on-chip redundancy referring to the standard IEC 61508. In: *2017 2nd International Conference on System Reliability and Safety (ICSRS)*, 2017, S. 386-390

Obwohl die FPGAs als Designplattform sehr effektive und zeitlich betrachtet sehr pragmatische Entwicklungsmöglichkeiten anbieten, sind diese Aspekte nicht trivial in sicherheitsgerichtete Anwendungen zu überführen. In der vorliegenden Studie wurde ein Beitrag zur Implementierung einer kompletten Rechnerarchitektur auf Basis eines 32-Bit ColdFire-Mikrocontrollers geleistet. Die primären Ergebnisse spalten sich in die Integration von spezifischen Sicherheitsmaßnahmen auf dem FPGA und eine intensive Sicherheitsevaluierung anhand der komparativen Analyse des Standes der Technik, wodurch der Sicherheitsintegritätslevel 2 des Gesamtsystems nachgewiesen wurde.

Der Integrationsaspekt basierte einerseits auf einer grundlegenden Betrachtung der Fehler infolge gemeinsamer Ursache und einer abschließenden Implementierung konkreter Vermeidungsmechanismen, mit denen der $ß_{IC}$-Faktor auf einen akzeptablen Wert von 20% reduziert worden ist. Andererseits wurde der Diagnosedeckungsgrad aller sicherheitsrelevanten Systemkomponenten auf einen für den SIL 2 geforderten Wert zwischen 90 und 99% erhöht, indem diverse interne und externe Teststrukturen integriert wurden.

ISBN 978-3-7376-0873-2