Hochqualitativ Verifikationsablauf für Heterogene Systeme auf Basis Virtueller Prototypen[1]

Muhammad Hassan[2]

Abstract: In dieser Dissertation werden mehrere neuartige Ansätze entwickelt, die verschiedene Verifikationsaspekte abdecken, um den modernen, auf *Virtuellen Prototypen* (VP)-basierten, Verifikationsablauf stark zu verbessern. Die Beiträge sind im Wesentlichen in vier Bereiche unterteilt: Der erste Beitrag führt eine neue Verifikationsperspektive für VPs ein, indem er *Metamorphic Testing* (MT) verwendet, da im Gegensatz zu modernen VP-basierten Verifikationsabläufen keine Referenzmodelle/-werte für die Verifikation benötigt werden. Der zweite Beitrag schlägt hochqualitative Methoden zum Schließen der Code-Abdeckung in modernen VP-basierten Verifikationsabläufen vor, indem er Mutationsanalyse und stärkere Abdeckungsmetriken wie Datenfluss-Abdeckung berücksichtigt. Der dritte Beitrag besteht aus einer Reihe hochqualitativ, neuartiger, systematischer und leichtgewichtigen funktionalen Methoden zur Verbesserung der relevanten Abdeckungsmetriken. Der vierte und letzte Beitrag dieser Arbeit sind neuartige Ansätze, die eine frühzeitige Sicherheitsvalidierung von VPs ermöglichen. Alle Ansätze werden im Detail vorgestellt und ausführlich mit mehreren Experimenten evaluiert, die ihre Effektivität durch einen hochqualitativ VP-basierten Verifikationsfluss für heterogene Systeme deutlich machen.

1 Einführung

Internet Der Dinge (engl. *Internet-of-Things*, IOT) und intelligente Geräte sind ein Hauptbeispiel für heterogene *System-On-Chips* (SOCs), die aus zwei Teilen bestehen: (1) Mixed-Signal *Hardware* (HW), wo die analoge Welt auf die digitale Welt trifft, (2) und *Software* (SW), die unsichtbare Schicht, die uns mit der physischen Realität verbindet. Heterogene SOCs gehören zu dem am schnellsten wachsenden Marktsegmenten in der Elektronik- und Halbleiterindustrie. Angetrieben von den Wachstumschancen in verschiedenen Anwendungsbereichen passen sich viele Halbleiterhersteller an und verlagern ihren Schwerpunkt von separaten *Integrierten Schaltungen* (engl. *Integrated Circuits*, ICs), die nur eine Funktion erfüllen, hin zu einer stärker integrierten Lösung für *Hochfrequenz* (engl. *Radio Frequency*, RF) und leistungsstarke *Analog/Mixed-Signal* (AMS) Designs. Diese Verlagerung hat zwar zu einer hohen Leistungsfähigeit und sehr effizienten Geräte mit geringem Platzbedarf geführt, z.B. der Apple M1 SOC, aber es wurde dadurch den Aufwand für die Entwicklung und Verifikation dieser hochkomplexen Bauelemente erheblich gesteigert, um die notwendigen Anforderungen bezüglich *Time-To-Market* (TTM) zu erreichen.

Eine große Herausforderung in dieser Hinsicht ist die Abhängigkeit von HW und SW. Herkömmlicherweise wurden HW und SW isoliert entwickelt und trafen erst in den späten

[1] Englischer Titel der Dissertation: "Enhanced Modern Virtual Prototype based Verification Flow for Heterogeneous Systems"

[2] Deutsches Forschungszentrum für Künstliche Intelligenz (DFKI), muhammad.hassan@dfki.de

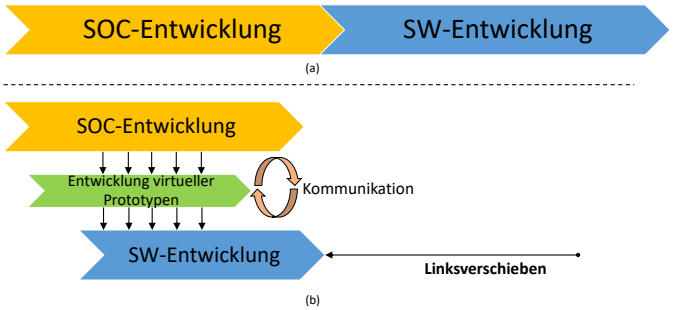

Abb. 1: Frühe SW-Entwicklung unter Nutzung des Linksverschiebungskonzepts

Integrations- und Testphasen aufeinander. Infolgedessen bestand immer eine sequentielle Abhängigkeit zwischen den HW- und SW-Entwicklungsphasen, wie in Abb. 1 (a) dargestellt ist. Daher konnte die SW erst dann richtig getestet werden, wenn die ersten Silizium-Prototypen des SOC verfügbar waren. Insbesondere HW-abhängige SW wie Gerätetreiber und Low-Level-Kernel-Code konnten erst geschrieben werden, nachdem das Siliziumdesign abgeschlossen war.

Eine weitere Herausforderung bei der Verifikation heterogener SOCs ist die langsame gemeinsame Simulationsgeschwindigkeit von *Register Transfer Level* (RTL) und SPICE-Modellen (Simulation Program with Integrated Circuit Emphasis) für den digitalen und den analogen/RF-Teil des SOCs [Ba10]. Traditionell war die Analog/RF-Verifikationsmethodik von Natur aus ad-hoc und diese IPs wurden immer von separaten Teams verifiziert. Sie wurde durch gezielte Tests über Sweeps, Ecken und Monte-Carlo-Analysen gesteuert. Diese vorverifizierten analogen, RF- und digitalen IPs wurden später in ein überwiegend digitales SOC-Design integriert und SW wurde darauf ausgeführt, um zu testen, ob alles wie erwartet funktioniert. Die gemeinsame Simulation ist zwar langsam, wird aber wegen ihrer hohen Genauigkeit immer noch als goldener Standard angesehen und kann nicht ignoriert werden. Für Simulationen auf Chipebene ist sie jedoch zu langsam, es sei denn, sie wird extrem selektiv eingesetzt.

Zusammenfassend lässt sich sagen, dass der erfolgreiche Co-Entwurf von sicheren multidisziplinären heterogenen SOCs, die enge Wechselwirkungen zwischen HW/SW-Systemen und ihrer analogen physikalischen Umgebung aufweisen, eine große Herausforderung darstellt. Je kürzer TTM wird, desto wichtiger wird die Fähigkeit, komplexe heterogene SOCs zu modellieren und zu simulieren, bei denen digitale HW/SW funktional mit AMS-IPs, d.h. HF-Schnittstellen, Leistungselektronik, Sensoren und Aktoren, verflochten sind. Wenn solche Modelle auf Gesamtsystem- und Architekturebene so früh wie möglich im Entwurfszyklus zur Verfügung stehen, werden die Probleme bei der Architekturexploration und beim Entwurf sowie den aufdeckung von Sicherheitslücken drastisch reduziert.

2 Entwurf und Verifizierung auf der Elektronischen Systemebene

In diesem Zusammenhang hat das Aufkommen *Virtueller Prototypen* (engl. *Virtual Prototypes*, VPs) auf der Abstraktionsebene der *Elektronischen Systemebene* (engl. *Electronic*

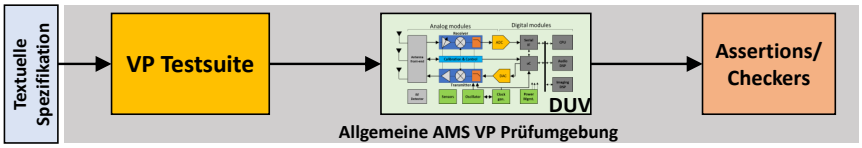

Abb. 2: Allgemeine AMS VP Prüfumgebung

System Level, ESL) den Entwurf und die Verifikation heterogener SOCs in vielerlei Hinsicht modernisiert [GD10, HGD20, Ha18, Ha17]. Der Grundgedanke besteht darin, ein abstraktes Referenzmodell des SOC auf Basis der schriftlichen Spezifikationen zu erstellen. Als Ergebnis wird eine ausführbare Beschreibung zur Verfügung gestellt, die als goldene Referenz für die HW- und SW-Entwicklung verwendet wird. Das *virtuelle Prototyping* bietet SW-Entwicklern und Systemarchitekten eine Umgebung für die SW-Entwicklung, die Betrachtung von Entwurfsalternativen bezüglich der Architektur oder das HW/SW-Co-Design. In einem vollständigen SOC-Entwurfsablauf liegt das virtuelle Prototyping zwischen der Funktions- und der Implementierungsebene. Auf dieser Abstraktionsebene nutzt das virtuelle Prototyping das *Linksverschiebungskonzepts* aufgrund seiner frühen Verfügbarkeit Abb. 1(b), d.h. der HW-Architekturentwurf und der SW-Entwicklungsfluss werden parallel und verschachtelt durchgeführt. Für den ESL-Entwurf ist die C++-basierte Systemmodellierungssprache SystemC zusammen mit *Transaction Level Modeling* (TLM)-Techniken (IEEE-Standard 1666) [In06] und deren Mixed-Signal-Erweiterung SystemC AMS [Ba13] mit überwiegend *Timed Data Flow* (TDF)-Modellentwicklung der Stand der Technik. Zu den Hauptvorteilen von VPs gehören die viel frühere Verfügbarkeit sowie die deutlich schnellere Simulationsgeschwindigkeit im Vergleich zu RTL-Modellen (für digitale) und SPICE-Level-Modellen (für AMS). Als Referenz für die (frühe) Entwicklung von eingebetteter SW und die HW-Verifikation ist die funktionale Korrektheit und Sicherheitsvalidierung von VPs sehr wichtig. Daher werden sowohl der gesamte VP als auch seine einzelnen Komponenten, d.h. Hochgeschwindigkeits-RF, AMS und digitale IPs, einer strengen Funktionsverifizierung unterzogen.

Trotz der jüngsten Fortschritte bei der formalen Verifikation von System-C/AMS-Modellen (siehe z.B. [GD10, Le16, He16]), ist die simulationsbasierte Verifikation dank ihrer Skalierbarkeit und einfachen Handhabung immer noch die Methode der Wahl für SystemC/AMS-basierte VP. Eine allgemeine simulationsbasierte AMS VP Verifikationsumgebung ist in Abb. 2 dargestellt. Sie folgt den Prinzipien des *gerichteten Testens* (engl. *Directed Testing*). Grundsätzlich werden die *textuellen Spezifikationen* verwendet, um manuell eine Reihe von Stimuli (*VP Testsuite*) zu erstellen, die auf das AMS DUV (das entweder ein ganzer VP, eine Reihe von Komponenten oder eine einzelne Komponente sein kann) angewendet werden, um bestimmte Szenarien zu testen. Für jeden Stimulus wird das tatsächliche Verhalten im Vergleich zum erwarteten Verhalten geprüft (z.B. spezifiziert durch Referenzausgaben in Form von *Assertions/Prüfern* oder zeitlichen Eigenschaften). Wenn die Assertions/Prüfer fehlschlagen, wird das DUV für fehlerhaft erklärt.

Dieser allgemeine simulationsbasierte Verifikationsablauf (gerichtetes Testen) ist zwar für die anfängliche Verifikation eines einfacheren DUV wichtig, aber für komplexe Entwürfe und eine gründliche Verifikation ist er nicht effektiv. Daher wird heutzutage ein moderner VP-Verifikationsablauf mit verschiedenen Methoden zur Ergänzung des allgemeinen

Verifikationsablaufs verwendet. Dies ist in Abb. 3 dargestellt. Die x-Achse zeigt vier farbige Balken, die die Methoden des modernen Verifikationsflusses vom Start bis zur Abnahme darstellen, und die y-Achse stellt die entsprechende Verifikationsqualität dar, die durch jeden Satz von Methoden erreicht wird. Der Grundgedanke ist, mit dem gerichteten Testen zu beginnen, wie zuvor beschrieben. Dies wird als grauer Farbbalken dargestellt. Die Verifikationsqualität ist in dieser Phase sehr schlecht, da die Teststimuli nur bestimmte Szenarien verifizieren. Anschließend wird die anfängliche Menge an Stimuli aus dem gerichteten Testen zusätzlich zu den Techniken des eingeschränkten Zufalls für Regressionstests verwendet. Regressionstests erfassen effektiv (1) Fehler, die während der DUV-Entwicklung eingeführt wurden, (2) und die Code-Abdeckung (ausgeübte Codezeilen) als Grundlinien und Trends. Dies wird durch einen orangefarbenen Balken dargestellt. Die durch Regressionstests erzielte überprüfungsqualität ist besser als bei gezielten Tests, aber immer noch schlecht, da der Schwerpunkt auf der Entwicklung von Stimuli liegt. Anschließend wird der Verifikationsfluss unter Nutzung der Code-Abdeckungs-Basislinien so umgestellt, dass eine geschlossene Code-Abdeckung erreicht wird und somit die Verifikationsqualität steigt. . Dies wird durch den blauen Farbbalken dargestellt. Am Ende wird die Abdeckungsmetrik auf funktionale Abdeckung umgestellt (ausgeübte Funktionen einer DUV) und die Stimuli werden verbessert, um einen Abschluss zu erreichen (gelber Farbbalken). An diesem Punkt wird die Qualität der Verifizierung als ausreichend angesehen und die Verifizierung wird abgeschlossen. Der moderne VP-Verifikationsablauf weist jedoch noch Schwächen auf, die zu qualitativ schlechten Teststimuli und VP führen. Die Schwächen werden im Folgenden kurz erörtert:

1. Bei Regressionstests ist die Verfügbarkeit von Referenzmodellen für den Vergleich der Ergebnisse immer noch eine große Herausforderung. Bei komplexen DUVs ist ein erheblicher Aufwand erforderlich, um das Referenzverhalten in einer ausführbaren Weise zu spezifizieren. Insbesondere die Interaktion von analogen Designs und digitaler Logik hat in modernen AMS SOCs erheblich zugenommen. Die Formalisierung solcher Interaktionen ist nicht trivial und sehr zeitaufwändig [HGD21a, HGD21b].
2. Die bestehenden Methoden zur Schließung der Code-Abdeckung sind zwar gut, aber in zweierlei Hinsicht unzureichend. Erstens verwenden sie nur schwache Abdeckungsmetriken, z.B. Anweisungsabdeckung und Verzweigungsabdeckung usw. Die schwachen Abdeckungsmetriken sind unempfindlich gegenüber varia-

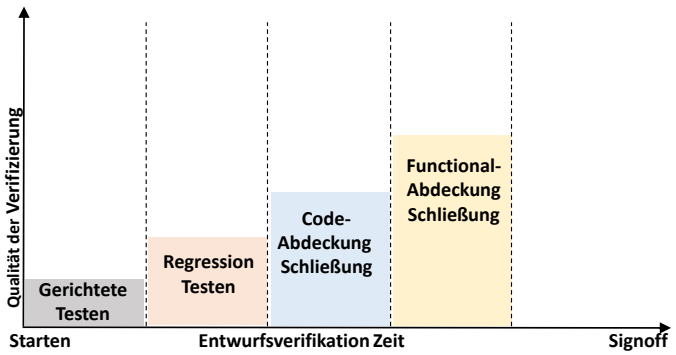

Abb. 3: Vier Stufen des modernen simulationsbasierten VP-Verifikationsablaufs

blen Interaktionen in dem VP, d.h. wie sich die in einem Teil des VP durchgeführten Berechnungen auf die anderen Teile auswirken. Zweitens berücksichtigen sie nicht die HW/SW-Interaktionen, die später zu einer großen Anzahl von IP-Integrationsproblemen führen.

3. Für eine gründliche Verifikation des DUV ist eine Verfolgung des Verifikationsfortschritts erforderlich. Bei der Verifikation digitaler Entwürfe ist insbesondere die funktionale Abdeckung die Metrik, die für diese Aufgabe verwendet wird, da sie es ermöglicht zu messen, ob alle Spezifikationen des Entwurfs verifiziert wurden. Während die funktionale Abdeckung in digitalen Design sehr gut verstanden wird, ist dies bei AMS nicht der Fall [Ha19], da kontinuierliche Signale und ihre Veränderung über die Zeit viel schwieriger zu erfassen sind.

4. Sicherheit ist heutzutage eines der wichtigsten Themen bei der Entwicklung eingebetteter Systeme. Die meisten Strategien zur Sicherung eingebetteter Systeme werden in SW implementiert. Eine potenzielle Hintertür in der HW, die nicht privilegierter SW den Zugriff auf vertrauliche Daten ermöglicht, macht jedoch selbst eine perfekt gesicherte SW unbrauchbar. Da der zugrundeliegende SOC nach der Implementierung nicht mehr gepatcht werden kann, ist es sehr wichtig, SOC-Hardware-Sicherheitsprobleme bereits in der Entwurfsphase zu erkennen und zu korrigieren.

Im nächsten Abschnitt werden die Beiträge dieser Arbeit erörtert, die die Qualität des modernen VP-Verifikationsablaufs stark verbessern. Diese Arbeit ist eine Zusammenfassung der Dissertation [Ha21].

3 Beitrag der Dissertation

In dieser Arbeit werden mehrere neue Ansätze und Methoden vorgeschlagen, um eine hochqualitativ VP Verifikation durchzuführen. Die Beiträge werden, wie in Abb. 4 gezeigt, nach den gezielten Tests in vier Hauptbereichen vorgeschlagen. Zunächst wird in dieser Arbeit eine neue Verifikationsperspektive für die VP-Verifikation vorgeschlagen: Metamorphes Testen zur effektiven Verifikation des VP ohne Referenzmodelle. Dies wird in Abb. 4 durch einen grünen Farbbalken dargestellt. Dann schlägt diese Arbeit Methoden, die eine starke Verbesserungen von bis zu 30% bei der Code-Abdeckung und Methoden zur Schließung der funktionalen Abdeckung vor (blaue bzw. gelbe Farbbalken). Schließlich wird eine Sicherheitsvalidierung des VPs eingeführt (pinkfarbener Balken), um Sicherheitsprobleme bereits in der Entwurfsphase zu erkennen. In diesem Zusammenhang konzentrieren wir uns auf digitale Systeme, die in den letzten Jahren kompromittiert wurden, z.B. Sicherheitslücken in SOCs, die Intels Mikroprozessor-IPs (Meltdown- und Spectre Schwachstellen) und Actel ProASIC3 IPs (JTAG-Schwachstelle) verwenden. Daher kann die frühzeitige Erkennung solcher Sicherheitslücken für das SOC entscheidend sein. Ein detaillierterer überblick über die Beiträge der Dissertation ist auf der linken Seite von Abb. 5 zu sehen. Die vier Bereiche der Beiträge verwenden allgemeine VP-Verifikationsumgebungen als Basis und bauen darauf deutlich erweiterte Verifikationsumgebungen auf:

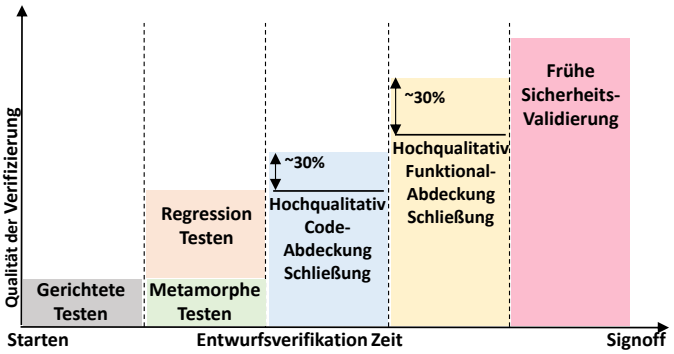

Abb. 4: Vorgeschlagener hochqualitativ VP-Verifikationsablauf

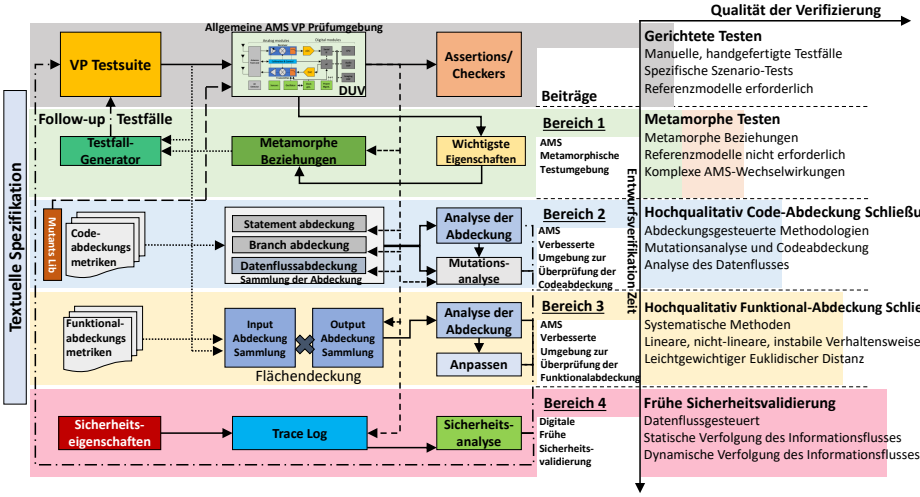

Abb. 5: Beiträge der Dissertation: Hochqualitativ VP-Verifikationsablauf

1. AMS metamorphische Testumgebung
2. AMS hochqualitativ Umgebung zur Überprüfung der Code-Abdeckung
3. AMS hochqualitativ Umgebung zur Überprüfung der Funktional-Abdeckung
4. Digitale frühe Sicherheitsvalidierung

Jeder Beitragsbereich erhöht die Verifikationsqualität des VP erheblich. Dies spiegelt sich auf der x-Achse in Abb. 5 (auf der rechten Seite) wider. Die y-Achse stellt die entsprechende Verifikationsumgebung und -methodik vom Start bis zur Abnahme im VP-Verifikationsablauf dar. Die Beiträge, die zu einer qualitativ hochwertigen Testbench und einem gründlich verifizierten VP führen, werden im Folgenden näher erläutert:

Beitragsbereich 1 - AMS Metamorphische Testumgebung Der erste Beitrag dieser Arbeit behebt die erste Schwäche - die Verfügbarkeit von Referenzmodellen. Der Beitrag führt eine neue Verifikationsperspektive für VPs ein, indem er *Metamorphisches Testen* (MT) verwendet. MT verifiziert ein DUV, indem es die bereits verfügbaren Testfälle

aus gerichteten oder Regressionstests (als Basisteststimuli bezeichnet) berücksichtigt, um neue Testfälle (als Folgeteststimuli bezeichnet) zu generieren, ohne dass ein Referenzmodell benötigt wird. MT tut dies, indem es einfach vorhandene Testfälle mit neu erstellten Testfällen in Beziehung setzt. Das zentrale Element von MT ist ein Satz von *Metamorphischen Relationen* (MR), die die Beziehung zwischen den Eingaben und Ausgaben aufeinanderfolgender DUV-Ausführungen anhand von Kerneigenschaften des DUV beschreiben. Da für MT keine Referenzmodelle erforderlich sind, ergänzt es wirksam die Regressionstests. Infolgedessen gewährleisten die identifizierten MRs die Korrektheit des DUV über mehrere DUV-Versionen hinweg während des Entwurfs und der Verifikation. Die vorgeschlagene AMS Metamorphische Testumgebung ist in Abb. 5 grün hinterlegt. Sie besteht aus (1) einem Testfallgenerator, (2) metamorphen Beziehungen und (3) Kerneigenschaften des DUV. Die Idee auf hoher Ebene ist die Erstellung von MRs unter Verwendung der Kerneigenschaften des DUV. Anschließend werden die MRs im Testfallgenerator Modul verwendet, um neue Testfälle zu erstellen, die Fehler aufdecken können.

Daher stellen wir in dieser Arbeit einen neuen MT-basierten Verifikationsansatz vor, um das lineare und nichtlineare Verhalten von HF-Verstärkern auf Systemebene zu verifizieren. Für die Klasse der HF-Verstärker identifizieren wir hochwertige MRs zur Verifizierung des linearen und nichtlinearen Verhaltens. Darüber hinaus gehen wir über reine Analog/RF-Systeme hinaus, d.h. wir erweitern MT, um AMS-Systeme zu verifizieren. Als anspruchsvolles AMS-System betrachten wir eine industrielle PLL und entwickeln eine Reihe von hochwertigen MRs. Diese MRs ermöglichen die Verifizierung des PLL Verhaltens auf Komponenten- und Systemebene zu überprüfen. Daher wird in dieser Arbeit ein MT-basierter Verifikationsansatz vorgeschlagen, der sowohl das Analog-Analog-, Analog-Digital-, Digital-Analog- als auch das Digital-Digital-Verhalten berücksichtigt.

Beitragsbereich 2 - AMS hochqualitativ Umgebung zur überprüfung der Code-Abdeckung Als zweiter Beitrag werden in dieser Arbeit Methoden zur Schließung der Code-Abdeckung mit hoher Qualität in modernen VP-basierten Verifikationsabläufen vorgeschlagen. Die Methoden erreichen eine signifikante Verbesserung der Verifikationsqualität um bis zu 30%. Die vorgeschlagene AMS hochqualitativ Umgebung zur Überprüfung der Code-Abdeckung ist in Abb. 5 in blauem Hintergrund dargestellt. Sie umfasst verschiedene Code-Abdeckungsmetriken und eine neuartige Abdeckungsanalyse. Darüber hinaus nutzt sie die Mutationsbibliothek und die Mutationsanalyse, um einen qualitativ hochwertigen VP zu erreichen. VP-basierte Designs ermöglichen das HW/SW-Co-Design und damit die softwaregetriebene Verifikation (engl: *Software Driven Verification*, SDV), die den Gesamtaufwand für die IP-Integration und -Verifikation erheblich zu reduzieren verspricht. Mit Hilfe von SystemC VPs können SW-Tests zur Verifikation der (neuen) integrierten IP-Blöcke und der HW/SW-Integration in einer frühen Entwurfsphase entwickelt und in den nachfolgenden Schritten wiederverwendet werden. Zu diesem Zweck schlagen wir in dieser Arbeit eine neuartige qualitätsgesteuerte Methodik vor, die auf einer Mutationsanalyse basiert. Durch die übertragung der wichtigsten Konzepte der mutationsbasierten Qualifizierung in den Kontext des SDV ist unsere Methodik in der Lage, ernsthafte Qualitätsprobleme in den SW-Tests zu erkennen. Das Herzstück ist eine neuartige Konsistenzanalyse, die die Abdeckung des IP in der HW/SW-Cosimulation auf leichtgewichtige Weise misst und diese Abdeckung mit den SW-Testergebnissen in Beziehung setzt, um ein

klares Feedback zu geben, wie die Qualität der Tests weiter verbessert werden kann. Obwohl dies ein notwendiger Schritt ist, haben Anweisungs- und Verzweigungsabdeckung im Zusammenhang mit SDV einige bekannte Einschränkungen hinsichtlich ihrer Fähigkeit, Fehler zu erkennen und die Gründlichkeit der Verifikation wiederzugeben. Sie sind unzureichend, wenn es darum geht, die Wechselwirkungen zwischen verschiedenen Elementen (Variablen) in einem VP zu berücksichtigen.

In dieser Hinsicht verbessert das Datenfluss-basierte Testen (engl: *Data Flow Testing*, DFT) die Qualität der Verifikation, indem es berücksichtigt, wie ein syntaktisches Element die Berechnung eines anderen beeinflussen kann. Daher schlagen wir in dieser Arbeit vor, DFT für SystemC/AMS VPs anzuwenden, da die modernen VPs nicht mehr nur digital sind, sondern multifunktionale AMS SOCs sind. Wir entwickeln zunächst eine Reihe von SystemC/AMS-spezifischen Abdeckungskriterien für DFT. Dies erfordert die Berücksichtigung (1) der SystemC-Semantik der Verwendung von nichtpräemptivem Thread-Scheduling mit Shared-Memory-Kommunikation und ereignisbasierter Synchronisation, (2) der SystemC-AMS-Semantik des Signalflusses im Allgemeinen und zeitgesteuerter Datenflussmodelle im Besonderen. Anschließend wird erläutert, wie die Datenfluss-Abdeckung für einen gegebenen VP mit einer Kombination aus statischen und dynamischen Analysetechniken automatisch berechnet werden kann. Die überdeckungsergebnisse liefern klare Vorschläge für den Verifikationsingenieur, neue Testfälle hinzuzufügen, um das Abdeckungsergebnis zu verbessern.

Beitragsbereich 3 - AMS hochqualitativ Umgebung zur Überprüfung der Funktional-Abdeckung Der dritte Beitrag dieser Arbeit ist eine Reihe von hochqualitativen Methoden zum Schließen der funktionalen Abdeckung in modernen VP-Verifikationsabläufen, die die Qualität der Verifikation um bis zu 30% erhöhen. Die AMS hochqualitativ Umgebung zur Überprüfung der Funktional-Abdeckung ist in Abb. 5 gelb unterlegt dargestellt. Sie umfasst Überdeckungssammelbehälter am Eingang und Ausgang des DUV sowie eine Überdeckungsanalyse. Darüber hinaus wird ein Anpassungsmodul eingeführt, um die Stimuliererzeugung automatisch zu steuern.

In dieser Arbeit wird ein Verifikationsansatz mit funktionaler Abdeckung als systematische Lösung für die Klasse der HF-Verstärker vorgeschlagen, um das lineare und nichtlineare Verhalten zu verifizieren. Sie überträgt die wichtigsten Konzepte der digitalen Funktions-Abdeckung auf den Kontext von SystemC AMS im Besonderen und Simulationen auf Systemebene im Allgemeinen. Um eine AMS-gesteuerte Verifikation der Funktions-Abdeckung zu ermöglichen, werden zwei Parameter zur Verfeinerung der Abdeckung auf der Eingangs- und Ausgangsseite eingeführt, um systematisch Eingangsstimuli zu erzeugen und Spezifikationen zu erfassen. Das Herzstück des Ansatzes ist die Abdeckungsanalyse, die die funktionale Abdeckung des DUV misst und dem Verifikationsingenieur ein klares Feedback gibt, um die Abdeckung abzuschließen. Die Parameter zur Verfeinerung der Abdeckung müssen jedoch manuell angepasst werden, was bei komplexen Systemen und instabilem Verhalten einen Engpass darstellt.

In diesem Zusammenhang wird ein *leichtgewichtiger Ansatz zur abdeckungsgesteuerten Stimulierung* (engl. *Lightweight Coverage-Directed Stimuli Generation*, LCDG) in Betracht gezogen. CDG ist eine Verifikationsmethodik, die darauf abzielt, die überdeckung

automatisch zu erreichen, indem überdeckungsdaten und mathematische Funktionen verwendet werden, um die nächsten Iterationen der Teststimuliererzeugung zu steuern. Das Herzstück des vorgeschlagenen LCDG-Ansatzes ist eine Überdeckungsanalyse, die funktionale überdeckungsdaten von Eingabe, Ausgabe und Prüfern in Kombination mit der *Euklidischen Distanz* nutzt, um eine Überdeckungsschließung zu erreichen. Die *Euklidische Distanz* ist im Gegensatz zu *Bayesschen Netzen* oder komplexen Wahrscheinlichkeitsverteilungsfunktionen wesentlich einfacher. Im Falle von Überdeckungslücken passt die Analyse automatisch die Parameter der Überdeckungsverfeinerung an, um die Überdeckung des DUV zu erhöhen. Infolgedessen gewährleisten diese leichtgewichtigen und systematischen Ansätze eine effiziente Konvergenz und eine gründliche Verifizierung der VP.

Beitragsbereich 4 - Digitale frühe Sicherheitsvalidierung Der letzte Beitrag dieser Arbeit ist die frühe Sicherheitsvalidierung des funktional verifizierten VPs. Die digitale Umgebung für die frühe Sicherheitsvalidierung ist in Abb. 5 rosa unterlegt dargestellt. Sie besteht aus drei Hauptkomponenten: (1) Sicherheitseigenschaften, (2) Trace-Logs und (3) Kombination aus statischer und dynamischer Sicherheitsanalyse. Unter Nutzung dieser Komponenten wird in dieser Arbeit ein neuartiger Ansatz zur SOC-Sicherheitsvalidierung auf Systemebene unter Verwendung von VPs vorgeschlagen. Das Herzstück des Ansatzes ist eine skalierbare statische Informationsflussanalyse, die potenzielle Sicherheitsverletzungen wie Datenlecks und nicht vertrauenswürdigen Zugriffe, d.h. *Vertraulichkeits-* bzw. *Integritätsprobleme*, erkennen kann.

Darüber hinaus ergänzt diese Arbeit den statischen Ansatz, indem sie eine dynamische Informationsflussanalyse für VPs vorstellt. Sie befasst sich insbesondere mit dem Sicherheitsmerkmal der IP-Isolierung, das heutzutage weit verbreitet ist, z.B. werden gesicherte Memory Mapped IOs (MMIOs) oder gesicherte Adressbereiche im Falle von Speichern als nicht zugänglich markiert. Eine Möglichkeit zur Gewährleistung der Sicherheit, ist die Definition von Isolation als Informationsflusspolitik in HW unter Verwendung des Begriffs der Nichteinmischung zu definieren. Der vorgeschlagene Ansatz ermöglicht die Validierung Laufzeitverhalten eines gegebenen SOC, der mit VPs implementiert wurde, gegen Sicherheitsbedrohungsmodelle, wie z.B. Informationslecks (*Vertraulichkeit*) und unbefugtem Zugriff auf Daten in einem Speicher (*Integrität*).

Fazit Zusammenfassend lässt sich sagen, dass diese Beiträge einen hochqualitativen VP-basierten Verifizierungsablauf vorschlagen, wie von den ausfuhrlichen Experimenten der Dissertation belegt wird [Ha21]. Einer der Hauptvorteile ist die drastisch verbesserte Verifikationsqualität in Kombination mit einem deutlich geringeren Verifikationsaufwand. Einerseits reduziert dies die Anzahl der unentdeckten Fehler und erhöht die Gesamtqualität des AMS SOC. Des Weiteren wird eine qualitativ hochwertige VP-Testsuite erstellt, die für die Verifikation der unteren Abstraktionsebenen verwendet werden kann.

Literaturverzeichnis

[Ba10] Barnasconi, Martin: SystemC AMS extensions: Solving the need for speed. 2010.

[Ba13] Barnasconi, Martin; Einwich, Karsten; Grimm, Christoph; Maehne, Torsten; Vachoux, Alain et al.: Standard SystemC AMS extensions 2.0 language reference manual. Accellera Systems Initiative, 2013.

[GD10] Große, Daniel; Drechsler, Rolf: Quality-Driven SystemC Design. Springer, 2010.

[Ha17] Hassan, Muhammad; Herdt, Vladimir; Le, Hoang M.; Große, Daniel; Drechsler, Rolf: Early SoC Security Validation by VP-based Static Information Flow Analysis. In: International Conference on Computer-Aided Design. S. 400–407, 2017.

[Ha18] Hassan, Muhammad; Große, Daniel; Le, Hoang M.; Vörtler, Thilo; Einwich, Karsten; Drechsler, Rolf: Testbench Qualification for SystemC-AMS Timed Data Flow Models. In: Design, Automation and Test in Europe. S. 857–860, 2018.

[Ha19] Hassan, Muhammad; Große, Daniel; Vörtler, Thilo; Einwich, Karsten; Drechsler, Rolf: Functional Coverage-Driven Characterization of RF Amplifiers. In: Forum on Specification and Design Languages. S. 1–8, 2019.

[Ha21] Hassan, Muhammad: Enhanced Modern Virtual Prototype based Verification Flow for Heterogeneous Systems. Dissertation, University of Bremen, 2021.

[He16] Herdt, Vladimir; Le, Hoang M.; Große, Daniel; Drechsler, Rolf: Compiled Symbolic Simulation for SystemC. In: International Conference on Computer-Aided Design. S. 52:1–52:8, 2016.

[HGD20] Herdt, Vladimir; Große, Daniel; Drechsler, Rolf: Enhanced Virtual Prototyping: Featuring RISC-V Case Studies. Springer, 2020.

[HGD21a] Hassan, Muhammad; Große, Daniel; Drechsler, Rolf: System-Level Verification of Linear and Non-Linear Behaviors of RF Amplifiers using Metamorphic Relations. In: ASP Design Automation Conf. 2021.

[HGD21b] Hassan, Muhammad; Große, Daniel; Drechsler, Rolf: System Level verification of Phase-Locked Loop using Metamorphic Relations. In: Design, Automation and Test in Europe. 2021.

[In06] Initiative, Open SystemC et al.: IEEE standard SystemC language reference manual. IEEE Computer Society, S. 1666–2005, 2006.

[Le16] Le, Hoang M.; Herdt, Vladimir; Große, Daniel; Drechsler, Rolf: Towards Formal Verification of Real-World SystemC TLM Peripheral Models – A Case Study. In: Design, Automation and Test in Europe. S. 1160–1163, 2016.

Muhammad Hassan erhielt 2015 den M.Sc. in Nachrichtentechnik von der RWTH Aachen, Deutschland. Danach begann er als Doktorand in der Arbeitsgruppe Rechnerarchitektur unter der Betreuung von Prof. Rolf Drechsler. Seit 2017 ist er als Wissenschaftlicher Mitarbeiter bei dem Deutschen Forschungszentrum fur Künstliche Intelligenz (DFKI) GmbH tätig. Im Jahr 2021 erhielt er den Dr.-Ing. Titel in Informatik von der Universität Bremen. Seine aktuellen Forschungsinteressen umfassen Virtual Prototyping sowie Verifikations- und Analysetechniken mit einem besonderen Fokus auf heterogene Systeme. In diesen Bereichen veröffentlichte er mehr als 10 peer-reviewed Journal- und Konferenzbeitrage mit zwei Best-Paper-Candidates und einem Best-Paper-Award bei der DVCON Europe.