Muhammad Hassan
Daniel Große
Rolf Drechsler

Erweiterte virtuelle Prototypen für heterogene Systeme

Springer Vieweg

Erweiterte virtuelle Prototypen für heterogene Systeme

Muhammad Hassan · Daniel Große ·
Rolf Drechsler

Erweiterte virtuelle Prototypen für heterogene Systeme

Springer Vieweg

Muhammad Hassan
DFKI GmbH
Bremen, Deutschland

Daniel Große
Johannes Kepler University of Linz
Linz, Österreich

Rolf Drechsler
University of Bremen and DFKI GmbH
Bremen, Deutschland

ISBN 978-3-031-53151-4 ISBN 978-3-031-53152-1 (eBook)
https://doi.org/10.1007/978-3-031-53152-1

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

Dieses Buch ist eine Übersetzung des Originals in Englisch „Enhanced Virtual Prototyping for Heterogeneous Systems“ von Muhammad Hassan, publiziert durch Springer Nature Switzerland AG im Jahr 2023. Die Übersetzung erfolgte mit Hilfe von künstlicher Intelligenz (maschinelle Übersetzung). Eine anschließende Überarbeitung im Satzbetrieb erfolgte vor allem in inhaltlicher Hinsicht, so dass sich das Buch stilistisch anders lesen wird als eine herkömmliche Übersetzung. Springer Nature arbeitet kontinuierlich an der Weiterentwicklung von Werkzeugen für die Produktion von Büchern und an den damit verbundenen Technologien zur Unterstützung der Autoren.

Planung/Lektorat: Charles Glaser
Springer Vieweg ist ein Imprint der eingetragenen Gesellschaft Springer Nature Switzerland AG und ist ein Teil von Springer Nature.
Die Anschrift der Gesellschaft ist: Gewerbestrasse 11, 6330 Cham, Switzerland

Das Papier dieses Produkts ist recycelbar.

An Khushboo und Maryam,
Marie,
und
Anna.

Vorwort

Die erfolgreiche Co-Design und Verifizierung von sicheren multidisziplinären heterogenen *Systemen-auf-Chips* (SOCs) mit engen Interaktionen zwischen *Hardware/Software* (HW/SW) Systemen und ihrer analogen physischen Umgebung ist eine zunehmend entmutigende Aufgabe. In dieser Hinsicht hat das Aufkommen von *virtuellen Prototypen* (VPs) auf der Abstraktionsebene des *elektronischen Systemlevels* (ESL) das Design und die Verifizierung von heterogenen SOCs modernisiert. Ein VP ist im Wesentlichen ein ausführbares abstraktes Modell der gesamten HW-Plattform und wird vorwiegend in der C++-basierten Systemmodellierungssprache SystemC zusammen mit *Transaktionslevel-Modellierung* (TLM) Techniken und seiner Mixed-Signal-Erweiterung SystemC AMS erstellt. Die deutlich frühere Verfügbarkeit sowie die signifikant schnellere Simulation im Vergleich zu den *Register Transfer Level* (RTL) Modellen und SPICE-Level-Modellen gehören zu den Hauptvorteilen von VPs. Daher ermöglicht das virtuelle Prototyping das HW/SW Co-Design und die Verifizierung sehr früh im Designprozess. Als Referenz für die (frühe) eingebettete SW-Entwicklung und HW-Verifizierung ist die funktionale Korrektheit und Sicherheitsvalidierung von VPs sehr wichtig. Daher wird ein VP einer rigorosen funktionalen Verifizierung unterzogen. Allerdings hat der moderne VP-basierte Verifizierungsfluss immer noch Schwächen, insbesondere aufgrund des Fehlens von Methoden zur Erfassung der komplexen Interaktionen zwischen digitalen und analogen Designs sowie der Nichtverfügbarkeit von Sicherheitsvalidierungstechniken. Dieses Buch schlägt mehrere neuartige Ansätze vor, die verschiedene Verifizierungsaspekte abdecken, um den modernen VP-basierten Verifizierungsfluss stark zu verbessern. Die Kapitel des Buches sind im Wesentlichen in vier Teile gegliedert: Der erste Teil führt eine neue Verifizierungsperspektive für VPs ein, indem er *metamorphes Testing* (MT) verwendet, da keine Referenzmodelle/Werte für die Verifizierung benötigt werden, im Gegensatz zum modernen VP-basierten Verifizierungsfluss. Der zweite Teil verbessert die Code-Coverage-Closure-Methoden im modernen VP-basierten Verifizierungsfluss durch Berücksichtigung von *Mutationsanalyse* und stärkeren Coverage-Metriken wie *Datenfluss*-Coverage. Der dritte Teil

behandelt eine Reihe von neuartigen, systematischen und leichtgewichtigen funktionalen Coverage-getriebenen Verifizierungsmethoden zur Verbesserung der Coverage-Closure. Der vierte und letzte Teil des Buches präsentiert neuartige Ansätze zur frühzeitigen Sicherheitsvalidierung von VPs. Alle Ansätze werden detailliert vorgestellt und umfangreich mit mehreren Experimenten bewertet, die ihre Wirksamkeit bei der starken Verbesserung des modernen VP-basierten Verifizierungsflusses deutlich demonstrieren.

Bremen, Deutschland — Muhammad Hassan
Linz, Österreich — Daniel Große
Bremen, Germany — Rolf Drechsler
November 2021

Danksagungen

Zunächst möchten wir den Mitgliedern der Forschungsgruppe für *Computerarchitektur* (AGRA) an der Universität Bremen sowie den Mitgliedern der Forschungsabteilung für *Cyber-Physische Systeme* (CPS) am *Deutschen Forschungszentrum für Künstliche Intelligenz* (DFKI) in Bremen danken. Wir schätzen die großartige Atmosphäre und anregende Umgebung. Darüber hinaus möchten wir allen Mitautoren der Arbeiten danken, die den Ausgangspunkt für dieses Buch bildeten: Hoang M. Le, Vladimir Herdt, Mingsong Chen und Mehran Goli. Wir danken insbesondere Karsten Einwich und Thilo Vörtler von COSEDA Technologies GmbH für viele interessante Diskussionen und erfolgreiche Zusammenarbeiten.

Inhaltsverzeichnis

Liste der Algorithmen

Abbildungsverzeichnis

Tabellenverzeichnis

Kapitel 1
Einleitung

Internet der Dinge (IOT) und *5G* (fünfte Generation der Technologiestandards für Breitband-Mobilfunknetze) haben eine Fülle von Möglichkeiten ermöglicht, die einst undenkbar waren. Während *5G* die Hochgeschwindigkeitsverbindung und die allgegenwärtige Abdeckung bietet, sind es die intelligenten IOT-Geräte, die die Daten sammeln und transportieren, die das Versprechen und das Potenzial von IOT antreiben. Diese intelligenten Geräte sind ein hervorragendes Beispiel 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 den am schnellsten wachsenden Marktsegmenten in der Elektronik- und Halbleiterindustrie. Getrieben durch Wachstumschancen in verschiedenen Anwendungsbereichen, passen viele Halbleiterhersteller ihre Strategie an und verlagern ihren Fokus von separaten *Integrierten Schaltkreisen* (ICs), die eine Funktion ausführen, hin zu einer stärker integrierten Lösung von *Radiofrequenz* (RF) und leistungsstarken *Analog/Mixed-Signal* (AMS) Designs. Aufgrund dieser Branchenverschiebung enthalten die meisten SOCs heute heterogene Elemente wie analoge Sensoren, Mixed-Signal-Wandler, digitale Prozessoren, die SW ausführen, und RF-Transceiver, die eng auf einem einzigen Die integriert sind. Während diese Verschiebung zu leistungsstarken, effizienten und platzsparenden Geräten geführt hat, z. B. Apple M1 SOC [6], hat sie den Aufwand für die Entwicklung und Verifizierung dieser hochkomplexen Geräte erheblich erhöht und gleichzeitig die erforderliche *Time-To-Market* (TTM) erreicht.

Die erste Herausforderung in diesem Zusammenhang ist die Abhängigkeit von HW und SW. Traditionell wurden HW und SW isoliert entwickelt und trafen erst in den späten Integrations- und Testphasen aufeinander. Infolgedessen bestand immer eine sequenzielle Abhängigkeit zwischen den Entwicklungsphasen von HW und SW, wie in Abb. 1.1a dargestellt. Daher konnte die SW erst ordnungsgemäß getestet werden, wenn die ersten Siliziumprototypen des SOC verfügbar waren. Insbesondere HW-abhängige SW wie Gerätetreiber und Low-Level-Kernel-Code

M. Hassan et al., *Erweiterte virtuelle Prototypen für heterogene Systeme*,
https://doi.org/10.1007/978-3-031-53152-1_1

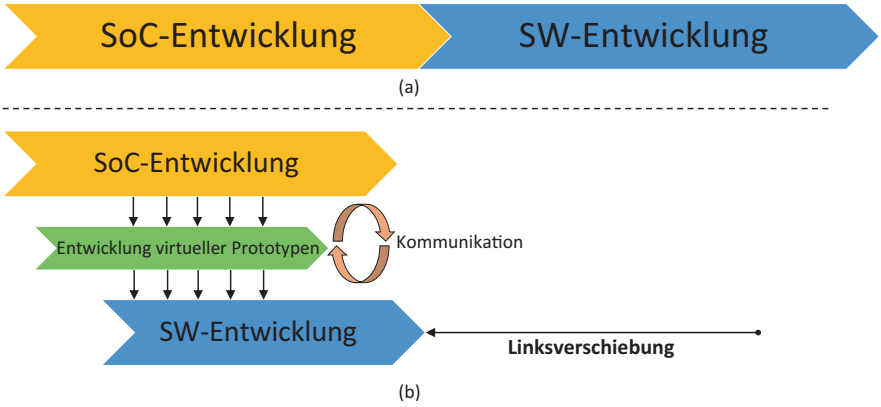

Abb. 1.1 Frühe SW-Entwicklung unter Nutzung des Shift-Left-Konzepts

konnten erst geschrieben werden, nachdem das Siliziumdesign abgeschlossen war. Eine Lösung zur Verringerung der TTM, die von der Industrie weitgehend übernommen wurde, besteht darin, von der vollständigen internen HW-Entwicklung abzurücken und stattdessen größere Mengen an vorverifiziertem Drittanbieter-*Geistigem Eigentum* (IP) zu verwenden. Dies ermöglicht es ihnen, sich stärker auf das *Alleinstellungsmerkmal* (USP) ihrer HW und SW zu konzentrieren. Mit der zunehmenden SW-Funktionalität und den komplexen Interaktionen zwischen verschiedenen HW-Komponenten hat die Designkomplexität um ein Vielfaches zugenommen, was die Designverifizierung von heterogenen SOCs zu einer zunehmend entmutigenden Aufgabe macht.

Die zweite Herausforderung bei der Verifizierung von heterogenen SOCs ist die langsame gemeinsame Simulation von *Register Transfer Level* (RTL) und SPICE (Simulation Program with Integrated Circuit Emphasis) Modellen für den digitalen und analogen/RF-Teil des SOC [9]. Traditionell war die Verifizierungsmethodik für analoge/RF-IPs ad hoc und diese IPs wurden immer von separaten Teams verifiziert. Sie wurde durch gerichtete Tests über Sweeps, Ecken und Monte-Carlo-Analysen gesteuert. Leider hat sich dies bis heute nicht viel geändert und schafft einen Engpass im Design- und Verifizierungsprozess. Auf der anderen Seite hatten digitale IPs formalisierte Verifizierungsmethoden, die von separaten Teams verwendet wurden. Dazu gehörten ausführbare Verifizierungspläne, erzeugung von beschränkt-zufälligen Stimuli [119], Testbench-Automatisierung, Assertions und Abdeckungsmetriken. Diese vorverifizierten analogen, RF- und digitalen IPs wurden später in einem größtenteils digitalen SOC-Design integriert und SW wurde darauf ausgeführt, um zu testen, ob alles wie erwartet funktioniert. Aufgrund der multifunktionalen Natur der heterogenen SOCs sind jedoch insbesondere die analogen und RF-IPs sehr komplex geworden und enthalten erhebliche digitale Steuerlogik. Darüber hinaus hat die Interaktion von analogen/RF- und digitalen IPs, insbesondere wenn man die darauf laufende SW berücksichtigt,

erheblich zugenommen [77]. Daher sind die traditionellen Verifizierungsansätze nicht mehr ausreichend. Die gemeinsame Simulation, obwohl langsam, gilt immer noch als Goldstandard aufgrund ihrer hohen Genauigkeit und kann nicht ignoriert werden. Sie ist jedoch zu langsam für Chip-Level-Simulationen, es sei denn, sie wird äußerst selektiv eingesetzt.

Drittens ist die Designraum- und Architekturerkundung eingeschränkt. Angesichts der Systemanforderungen ist die Suche nach der optimalen Systemkonfiguration eine mühsame Aufgabe. Jede Parameteränderung, egal wie gering, kann den Designer ein paar Tage in der Designphase kosten. Daher ist die Erkundung sehr selektiv.

Schließlich hat die weit verbreitete Praxis der Integration von Drittanbieter-IPs die modernen SOCs berüchtigt unsicher gemacht, da sie als Fahrzeug für Boshaftigkeit genutzt werden können. Zum Beispiel der jüngste Sicherheitskompromiss von SOCs, die Intels Mikroprozessor-IPs und Actel ProASIC3-IPs verwenden. Die ersteren wurden durch die *„Meltdown und Spectre“* Schwachstellen [79, 89] ausgenutzt und die letzteren durch die JTAG-Schwachstelle [108]. Dies unterstreicht die Tatsache, dass legitime kommerzielle Off-the-Shelf-IPs Benutzerinformationen auf eine Weise manipulieren oder bei der Manipulation helfen können, die ihre Benutzer weder erwarten noch schätzen. Darüber hinaus kann ein SOC nach der Fertigung nicht gepatcht werden und erfordert daher ein neues Design.

Nach einer Schätzung kann die traditionelle funktionale Verifizierung von heterogenen SOCs bis zu 70 % der Projektzeit in Anspruch nehmen. Dennoch resultiert sie in vielen Neudrehungen, die hauptsächlich aus Mixed-Signal-Verifizierungsproblemen resultieren [77]. Dies geschieht hauptsächlich aufgrund schwächerer Verifizierungsmethoden, Tools oder Bibliotheken, die nicht in der Lage sind, *vermeidbare* HW- und SW-Fehler frühzeitig in der Designphase zu erkennen. Daher sind Tools, Bibliotheken und komplexe AMS-Verifizierungsmethoden erforderlich, die (1) die *HW/SW-serielle Abhängigkeit* im Design und der Verifizierung von heterogenen SOCs entfernen und stattdessen HW/SW-Co-Design ermöglichen (2) die *Simulationgeschwindigkeit erhöhen* und gleichzeitig eine gute Genauigkeit bieten (3) eine *schnelle Designraum- und Architekturerkundung* ermöglichen (4) eine *frühe Sicherheitsvalidierung* bieten

Zusammenfassend lässt sich sagen, dass das erfolgreiche Co-Design von sicheren multidisziplinären heterogenen SOCs, die enge Interaktionen zwischen HW/SW-Systemen und ihrer analogen physischen Umgebung aufweisen, eine Herausforderung darstellt. Da die TTM kürzer wird, wird die Fähigkeit, komplexe heterogene SOCs zu modellieren und zu simulieren, bei denen digitale HW/SW funktional mit AMS-IPs verflochten ist, d. h. RF-Schnittstellen, Leistungselektronik, Sensoren und Aktuatoren, immer wichtiger. Wenn solche Gesamtsystem- und Architekturebenenmodelle so früh wie möglich im Designzyklus verfügbar sind, werden die Architekturerkundung und Designprobleme sowie Sicherheitslücken drastisch reduziert.