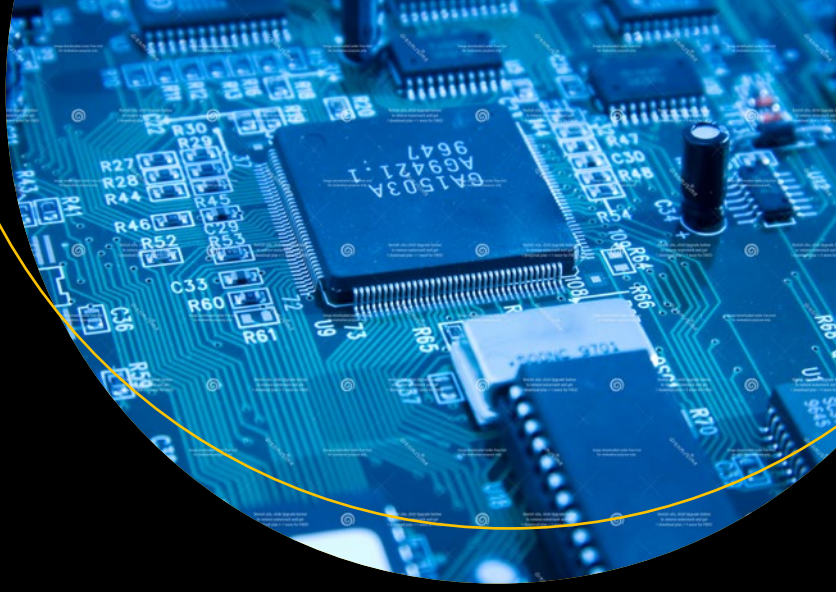

System Firmware

An Essential Guide to Open Source and Embedded Solutions

Subrata Banik
Vincent Zimmer

Apress®

System Firmware

An Essential Guide to Open Source and Embedded Solutions

Subrata Banik
Vincent Zimmer

Apress®

System Firmware: An Essential Guide to Open Source and Embedded Solutions

Subrata Banik
Bangalore, Karnataka, India

Vincent Zimmer
Tacoma, WA, USA

ISBN-13 (pbk): 978-1-4842-7938-0
ISBN-13 (electronic): 978-1-4842-7939-7
https://doi.org/10.1007/978-1-4842-7939-7

Managing Director, Apress Media LLC: Welmoed Spahr
Acquisitions Editor: Susan McDermott
Development Editor: Laura Berendson
Coordinating Editor: Jessica Vakili
Copy Editor: Mary Behr

Distributed to the book trade worldwide by Springer Science+Business Media New York, 1 NY Plaza, New York, NY 10004. Phone 1-800-SPRINGER, fax (201) 348-4505, e-mail orders-ny@springer-sbm.com, or visit www.springeronline.com. Apress Media, LLC is a California LLC and the sole member (owner) is Springer Science + Business Media Finance Inc (SSBM Finance Inc). SSBM Finance Inc is a **Delaware** corporation.

For information on translations, please e-mail booktranslations@springernature.com; for reprint, paperback, or audio rights, please e-mail bookpermissions@springernature.com.

Apress titles may be purchased in bulk for academic, corporate, or promotional use. eBook versions and licenses are also available for most titles. For more information, reference our Print and eBook Bulk Sales web page at www.apress.com/bulk-sales.

Any source code or other supplementary material referenced by the author in this book is available to readers on the GitHub repository: https://github.com/Apress/System-Firmware. For more detailed information, please visit www.apress.com/source-code.

Printed on acid-free paper

Table of Contents

About the Authors xi

About the Technical Reviewers xiii

Foreword by Jonathan Zhang xv

Preface xix

Acknowledgments xxi

Introduction xxiii

Chapter 1: Introduction 1

Lack of Open System Design 3

Misinterpretation of Firmware Definition 4

Attract the Talent 5

The Importance of Programming Knowledge 6

Specialized Education 8

The Origin of Firmware 10

Firmware Evolution 14

Distinction Between Firmware and Software 40

Introduction of Non-Host Firmware 41

Introduction to Device Firmware 42

Open Source vs. Closed Source 43

Summary 44

Chapter 2: Knowing Your Hardware 45

Computer Architecture 47

Instruction Set Architecture 50

Microarchitecture 55

System Architecture 62

CPU Internals 68

Internals of x86 Processors 68

System Memory Map 109

Legacy Address Range 109

Main Memory Address Range 112

PCI Memory Address Range 114

Main Memory Upper Address Range 116

Bus Architecture 118

Industry Standard Architecture (ISA) Bus 119

Extended Industry Standard Architecture (EISA) Bus 120

Peripheral Component Interconnect (PCI) Bus 121

Peripheral Component Interconnect Express (PCIe) Bus 129

Serial AT attachment (SATA) Bus 130

Universal Serial Bus (USB) 130

ARM Advanced Microcontroller Bus Architecture (AMBA) 132

Platform Runtime Power Management 133

ACPI Hardware/Registers 135

ACPI System Description Tables 137

ACPI Platform Firmware 139

System Power States 141

Summary 142

Chapter 3: Understanding the BIOS and Minimalistic Design.....145

What Is the BIOS? 146

Working Principle of BIOS.....147

Where Does the BIOS Reside?.....149

BIOS Work Model.....151

Types of BIOS.....154

Designing a Minimalistic Bootloader 159

Minimalistic Bootloader Design on x86 Platform 160

Minimalistic Bootloader Design on the ARM Platform.....197

Summary.....211

Chapter 4: System Firmware Architecture 213

UEFI Architecture 215

UEFI Specification.....217

Platform Initialization Specification.....244

coreboot Architecture.....260

Platform Initialization 262

Source Tree Structure.....280

Slim Bootloader Architecture 291

Boot Stages 293

Summary.....312

Chapter 5: Hybrid Firmware Architecture.....315

Understanding the System Firmware Development Model.....319

Generic 321

Platform Initialization (PI) 321

Understanding the System Firmware Supply Chain....324
Platform Initialization....324
Wrapper Layer....325
Boot Firmware....326
Spectrum of Open and Closed Source System Firmware....327
Current Industry Trends with Hybrid Firmware....330
Challenges Seen by Silicon Vendors with Open Sourcing....337
Datasheet Dependency....338
Third-Party IP Restrictions....339
Silicon Reference Code Development Without Compatibility....339
Early Platform Enabling with Non-PRQ'ed Silicon....340
Distinguished Product Features....340
Limited Customer Demand....340
Closed-Source Mindset....341
Documentation Is an Afterthought....342
Importance of a Specific System Firmware Architecture....342
Challenges Faced by the Open Community with Closed Sourcing....343
Security....343
Platform Enabling....344
Motivation Is Lagging....344
Hard to Debug....344
Ungoverned Growth for Closed Source Blobs....345
Hybrid Firmware Architecture....346
Ground Rules....346
Firmware Development Using Hybrid Firmware Architecture....348
Conventional Closed Source Firmware in the Hybrid Work Model....351
Application of Hybrid Firmware Architecture....369
Summary....382

Chapter 6: Payload.....385
Depthcharge.....390
Depthcharge Architecture.....391
Depthcharge Boot Flow.....407
Depthcharge Code Structure.....409
Value-Added Services.....411
UEFI Payload.....413
UEFI Payload Architecture.....415
UEFI Payload Boot Flow.....422
UEFI Payload Code Structure.....424
Value-Added Services.....426
LinuxBoot.....427
LinuxBoot Architecture.....429
LinuxBoot Boot Flow.....439
LinuxBoot Code Structure.....441
Value-Added Services.....443
Universal Payload Layer (UPL).....447
Universal Payload Image Format.....452
Universal Payload Interface.....455
Implementation of Universal Payload Layer.....458
Summary.....461
Chapter 7: Case Studies.....465
Reduce FW Booting Time Using Multi-Threaded Environment.....467
coreboot.....469
Bootstrap Processor.....470
Application Processor.....470
Multithreading.....470
ChromeOS.....471

Crosh 471
Depthcharge 471
Goal and Motivation 472
Implementation Schema 472
Setting Up the Board 476
Boot Time Measurement with existing System Firmware Design 478
Detailed Implementation 481
Firmware Boot Time Optimization for Capsule Update 490
Firmware Boot Time Optimization Conclusion 490
Supporting New CPU Architecture Migration with UEFI 491
Goal and Motivation 497
Implementation Schema 498
Setting Up the Code Base 502
Detailed Implementation 506
Porting a New CPU Architecture (Elixir) Conclusion 517
Reducing the System Firmware Boundary with LinuxBoot 517
Goal and Motivation 522
Implementation Schema 523
Setting Up the Board 527
Detailed Implementation 531
LinuxBoot Conclusion 539
Adopting a Hybrid Firmware Development Model 539
Goal and Motivation 543
Implementation Schema 543
Setting Up the Board 550
Detailed Implementation 554
Hybrid Firmware Development Model Conclusion 577
Summary 577

Appendix A: Postcodes **579**

Appendix B: Data Types **585**

Glossary **589**

Reference **595**

Websites 595

References for the Chapter 1 598

Books 598

Conferences, Journals, and Papers 598

Specifications and Guidelines 599

Websites 599

References for Chapter 5 601

Index **603**