



Firmware Development

A Guide to Specialized Systemic
Knowledge

—

Subrata Banik
Vincent Zimmer

Apress®

Firmware Development

**A Guide to Specialized
Systemic Knowledge**

**Subrata Banik
Vincent Zimmer**

Apress®

Firmware Development: A Guide to Specialized Systemic Knowledge

Subrata Banik
Bangalore, Karnataka, India

Vincent Zimmer
Issaquah, WA, USA

ISBN-13 (pbk): 978-1-4842-7973-1
<https://doi.org/10.1007/978-1-4842-7974-8>

ISBN-13 (electronic): 978-1-4842-7974-8

Copyright © 2022 by Subrata Banik and Vincent Zimmer

This work is subject to copyright. All rights are reserved by the Publisher, whether the whole or part of the material is concerned, specifically the rights of translation, reprinting, reuse of illustrations, recitation, broadcasting, reproduction on microfilms or in any other physical way, and transmission or information storage and retrieval, electronic adaptation, computer software, or by similar or dissimilar methodology now known or hereafter developed.

Trademarked names, logos, and images may appear in this book. Rather than use a trademark symbol with every occurrence of a trademarked name, logo, or image we use the names, logos, and images only in an editorial fashion and to the benefit of the trademark owner, with no intention of infringement of the trademark.

The use in this publication of trade names, trademarks, service marks, and similar terms, even if they are not identified as such, is not to be taken as an expression of opinion as to whether or not they are subject to proprietary rights.

While the advice and information in this book are believed to be true and accurate at the date of publication, neither the authors nor the editors nor the publisher can accept any legal responsibility for any errors or omissions that may be made. The publisher makes no warranty, express or implied, with respect to the material contained herein.

Managing Director, Apress Media LLC: Welmoed Spahr
Acquisitions Editor: Susan McDermott
Development Editor: Laura Berendson
Coordinating Editor: Jessica Vakili
Copyeditor: Kim Wimpsett

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 <http://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/Firmware-Development>. For more detailed information, please visit <http://www.apress.com/source-code>.

Printed on acid-free paper

Table of Contents

About the Authors	vii
About the Technical Reviewer	ix
About the Foreword Author	xi
Foreword by Christian Walter	xiii
Preface	xv
Acknowledgments	xix
Introduction	xxi
Chapter 1: Spotlight on Future Firmware	1
Migrating to Open Source Firmware	3
Ring -1: System Firmware	5
Ring -2: System Management Mode	5
Ring -3: Manageability Firmware	6
Open Source System Firmware Development	10
Hybrid System Firmware Model	12
Open Source System Firmware Model	47
Open Source Device Firmware Development.....	69
Legacy Device Firmware/Option ROM	71
UEFI OpROM	77
Why Is Open Source Device Firmware Needed?	82

TABLE OF CONTENTS

Open Source Manageability Firmware Development.....	84
Baseboard Management Controller	88
Zephyr OS: An Open Source Embedded Controller Firmware Development	102
Summary.....	126
Chapter 2: Tools	129
Build Tools.....	132
EDKII Build Tools and Process	134
coreboot Build Tools and Process.....	149
Configuration Tools	162
Human Interface Infrastructure	163
YAML-Based Configuration.....	166
Firmware Configuration Interface.....	168
Binary Configuration Tool (BCT)/Config Editor	170
Flashing Tools	171
Hardware-Based Tools.....	172
Summary.....	174
Chapter 3: Infrastructure for Building Your Own Firmware.....	177
Overview of Source Control Management	178
Version Control System	179
Version Control Repository Hosting Service	200
Code Review Application	203
Best Known Mechanism of Source Code Management.....	208
Code of Conduct.....	210
Coding Standard	212
Indentation	214
Maximum Columns per Line.....	215

Using Braces	216
Need for Spaces	217
Naming Conventions.....	218
Typedefs	219
Commenting	220
Write a Good Commit Message	221
Summary.....	225
Chapter 4: System Firmware Debugging	227
Hardware-Assisted Debugging	233
Generic Debugging	234
SoC-Specific Debugging.....	238
OxM-Secific Debugging.....	256
Software-Assisted Debugging	261
Traditional Breakpoint	261
I/O-Based Checkpoint.....	262
Serial Message or Serial Buffer.....	265
Preboot Environment.....	266
ACPI Debug.....	267
Windows Debugger	268
GNU Debugger	270
Summary.....	272
Chapter 5: Security at Its Core	273
Revisiting the Definition of Firmware with a Security Mindset.....	276
Why Is Firmware Security Required?	277
Platform Configuration for Firmware	286
Firmware with Security Mindset in a Computing System	287
Summary.....	303

TABLE OF CONTENTS

Chapter 6: Looking at the Future of System Firmware	305
Designing LITE Firmware	309
Design Principle.....	313
Conclusion.....	325
Designing a Feature Kernel.....	326
Design Principle.....	328
Conclusion.....	329
Design Multithreaded System Firmware.....	330
Design Principles.....	334
Conclusion.....	341
Innovation in Hardware Design	342
Design Principles.....	344
Conclusion.....	351
Summary.....	352
Appendix A: The Evolution of System Programming Languages	353
The History of System Programming Languages.....	354
System Programming Languages Today	356
The Future of System Programming Languages.....	358
Appendix B: initramfs: A Call for Type-Safe Languages	367
Glossary	373
Reference	379
Websites	379
Books, Conferences, Journals, and Papers.....	383
Index	385