

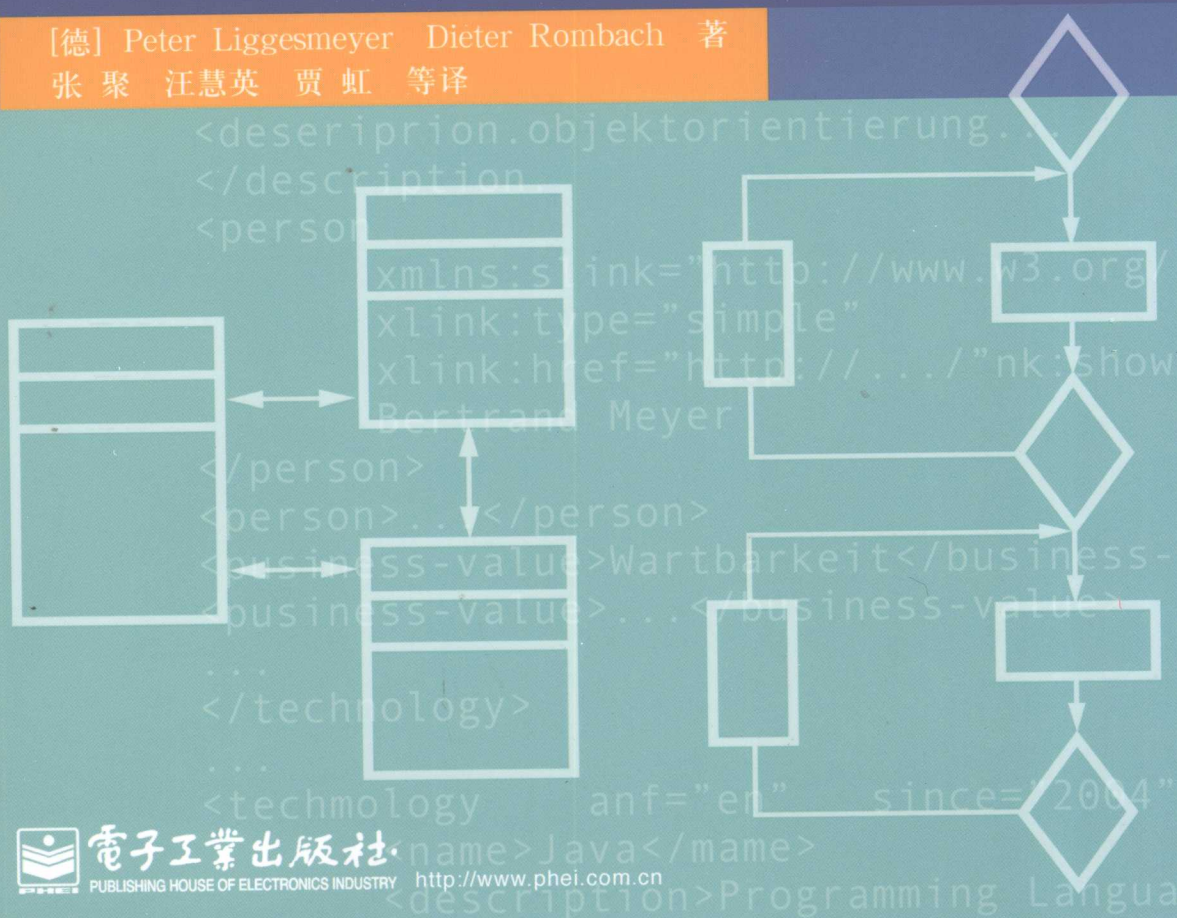
嵌入式系统软件工程 ——基础知识、方法和应用

Software Engineering eingebetteter Systeme

Grundlagen—Methodik—Anwendungen

[德] Peter Liggesmeyer Dieter Rombach 著

张聚 汪慧英 贾虹 等译



电子工业出版社

PUBLISHING HOUSE OF ELECTRONICS INDUSTRY

<http://www.phei.com.cn>

嵌入式系统软件工程

——基础知识、方法和应用

[德] Peter Liggesmeyer Dieter Rombach 著

张聚 汪慧英 贾虹 等译

电子工业出版社

Publishing House of Electronics Industry

北京·BEIJING

内 容 简 介

本书系统地阐述嵌入式系统软件工程所涉及的过程、方法、内容,以及在典型工业领域中的应用。全书内容分为两大部分:第一部分介绍嵌入式系统软件工程方法论,主要包括嵌入式软件的开发过程(需求工程、软件和系统体系结构、编程和测试等内容),开发和测试中所采用的标准,与安全性相关的软件系统的准入,以及嵌入式软件所涉及的法律问题;第二部分介绍嵌入式系统软件在汽车领域、轨道交通领域、航天领域、医疗器械、工业自动化、通信系统中的应用,在每个应用领域重点介绍具体应用领域的一些特定需求、技术和限制条件,以及它们对于嵌入式系统软件开发过程的影响。

本书有望为嵌入式系统软件工程领域的教学、科研和工程实践提供帮助,本书可供从事嵌入式系统软件开发和研究的工程技术人员使用和参考,也可作为高等院校相关专业的研究生和本科生的教材和参考书。

Software Engineering eingebetteter Systeme

Grundlagen – Methodik – Anwendungen

Peter Liggesmeyer Dieter Rombach

ISBN: 3827415330 ISBN-13: 978-3827415332

Copyright ©2005 by Elsevier. All rights reserved

Authorized Simplified Chinese translation edition published by the Proprietor.

ISBN: 981-259-785-9 ISBN-13: 978-981-259-785-4

Copyright © 2007 by Elsevier (Singapore) Pte Ltd. All rights reserved.

Printed in China by Publishing House of Electronics Industry under special arrangement with Elsevier (Singapore) Pte Ltd.

This edition is authorized for sale in China only, excluding Hong Kong SAR, Macau SAR and Taiwan. Unauthorized export of this edition is a violation of Copyright Act. Violation of this Law is subject to Civil and Criminal Penalties.

本书简体中文版由 Elsevier (Singapore) Pte Ltd. 授予电子工业出版社在中国大陆(不包括香港、澳门特别行政区以及台湾地区)发行与销售。未经许可之出口,视为违反著作权法,将受法律之制裁。

版权贸易合同登记号 图字: 01-2007-5188

图书在版编目(CIP)数据

嵌入式系统软件工程——基础知识、方法和应用 / (德) 利格斯迈尔 (Liggesmeyer, P.) 等著;
张聚等译. —北京: 电子工业出版社, 2009.1

书名原文: Software Engineering eingebetteter Systeme: Grundlage—Methodik—Anwendungen

ISBN 978-7-121-07492-9

I. 嵌… II. ①利… ②张… III. 微处理器—系统开发—软件工程 IV. TP332

中国版本图书馆 CIP 数据核字 (2008) 第 153817 号

策划编辑: 张 毅

责任编辑: 张燕虹

审 校: 于秀山 吴晓峰

印 刷: 北京机工印刷厂

装 订: 三河市鹏成印业有限公司

出版发行: 电子工业出版社

北京市海淀区万寿路 173 信箱 邮编: 100036

开 本: 720×1000 1/16 印张: 26.75 字数: 600 千字

印 次: 2009 年 1 月第 1 次印刷

印 数: 4000 册 定价: 45.00 元

凡所购买电子工业出版社图书有缺损问题, 请向购买书店调换。若书店售缺, 请与本社发行部联系, 联系及邮购电话: (010) 88254888。

质量投诉请发邮件至 zltz@phei.com.cn, 盗版侵权举报请发邮件至 dbqq@phei.com.cn。

服务热线: (010) 88258888。

译者序

嵌入式技术和系统在最近的一二十年内得到了快速的发展。目前,嵌入式系统广泛地应用于汽车、轨道交通、航天、医疗器械、工业自动化、通信系统、信息家电及消费类电子产品等众多的领域。嵌入式系统的许多功能是通过软件来实现的,软件对于嵌入式系统具有重要的技术和经济上的意义。嵌入式系统软件工程有别于通常的软件工程,嵌入式系统对软件提出了一些特殊的要求和限制,如在安全性、可靠性和实时性等方面,对于许多的技术应用领域提出了很高的要求,同时也会存在着一些限制的要求,如存储容量等方面的限制。

嵌入式系统的软件工程,目前在发达国家(特别是在德国)是研究的一个热点和重点。最近几年,国内对嵌入式系统软件方面的重要性及在工程实际中的广泛应用也有足够的认识。目前,国内也已经有不少的高校开设了嵌入式系统软件工程的本科专业和工程硕士点。但是,国内目前还没有系统地介绍嵌入式系统软件工程的图书。

本书及时反映了嵌入式系统软件方面的新技术和研究成果,内容新颖、全面和具体,由近 20 位在嵌入式系统的研究与应用领域的德国知名专家共同完成。该书由理论与应用两部分组成。第一部分介绍嵌入式系统软件工程方法,它们独立于具体应用领域。除了嵌入式系统的开发过程、开发和测试的标准、嵌入式系统的需求工程、软件体系结构、嵌入式软件编程和测试等内容外,还包括与安全性相关的嵌入式系统的市场准入、嵌入式软件所涉及的法律方面问题、嵌入式/实时 UML、嵌入式系统形式化开发方法和分析技术、安全性和可靠性分析、分布嵌入式技术、实时操作系统等与嵌入式系统的联系更为紧密的内容。第二部分内容介绍嵌入式软件在汽车、轨道交通、航天、医疗器械、工业自动化、通信系统等领域中的具体应用实例。

该书对嵌入式系统软件工程方面的教学、科研和工程应用工作会有很大的帮助,并可作为相关领域的高校教师、大学生,工程系统开发人员和技術人员的参考书。

参与本书翻译工作的有张聚博士(浙江工业大学)、汪慧英(同济大学)、贾虹(浙江工业大学)、罗如登(中南大学)、姚春燕(浙江工业大学)、孙小莉(同济大学)、马学童(同济大学)、张鹏(同济大学)。全书翻译工作由张聚统稿和组织完成。在翻译过程中,译者虽然力求准确和风格一致,但限于学识和水平,译文中必有不当之处,欢迎读者批评指正。

张聚

浙江工业大学

前言

许多人对于以“高技术”统称的产品感到很惊奇：能够很快、很安全地到达目的地的现代有轨列车和飞机，能够主动地修正行驶偏差的小汽车，以及能够无痛地给出人体内部详细图形的计算机断层扫描机器，仅仅是其中一些例子。

没有软件，现在这些系统将不能完成它们的功能。虽然有轨列车、飞机以及小汽车在几十年以前根本没有软件的情况下也能够工作，然而，它们是在不具有现在看来是很自然的一些特性为前提的；而计算机断层扫描机器在没有软件的情况下是根本不能工作的。计算机断层扫描机器是属于那些没有软件就不会存在的系统。

许多的现代技术产品，从手机到飞机，如果没有软件就根本无法工作。现在，技术系统的很大部分的产值是通过软件来实现的。根据西门子公司提供的数据，该公司高于 60% 的全球产值是通过软件来实现的。

因此，在满足软件质量、成本限制和时间要求的前提下，具备软件开发的能力是非常重要的。软件工程就是专门研究解决软件开发领域一系列的相关问题。现在已经有了一些关于软件工程方面的很好的书籍，它们既可以适合于学习，也适合于指导工程实践。

然而，我们在前面提到的一些应用领域，对软件工程提出了一些特殊的要求和限制。嵌入式系统的软件通常仅仅是整个系统的一个组成部分。因此，嵌入式软件的开发，就像魔方一样，必须能够适合整个系统的周围情况。此外，在许多的技术应用领域，存在着特别高的质量要求，如在安全性和可使用性方面，也会存在着一些限制的要求，如存储容量的限制。

因此，嵌入式系统的软件工程有别于通常的软件工程。相应地，嵌入式系统的软件工程必须能够适应嵌入式系统的一些特殊要求。

本书专门讨论嵌入式系统的软件工程。这是 Elsevier 学术出版社的信息主题项目策划人 Andreas Rüdinger 博士的创意。本书由两大部分组成：第一部分介绍嵌入式系统软件工程方法，它们独立于具体应用领域；第二部分介绍具体的应用实例。由于应用领域相关主题内容的丰富性，以及各个具体应用领域的相异性，使得对于每个应用领域必须由这方面的专家以合适的方式来撰写才能很好地完成这项工作。在本书各个章节的撰写中，我们得到了许多专家的支持，对于本书所有作者的友好合作，我们表示真诚的谢意。

本书中的每一章，都采用了相同的组织形式，以便阅读参考。由于大量作者参与了本书的写作，为了保证本书的完整性、系统性和一致性，出版社对于本书的章节都做了重新的编排，这项并不容易且费时的工作是由 Barbara Lühker 女士来协调完成的，因此非常感谢她！

用 LaTeX 来编排本书是由 Stefan Henze 先生完成的。Isabel Peuker 女士对于本书的章节进行了校正。在此，我们对于他们的合作，表示衷心的感谢。

Peter Liggesmeyer Dieter Rombach

2005 年 3 月于凯撒斯劳滕

目 录

第 1 章 绪论	1
1.1 软件对于嵌入式系统的意义	2
1.2 软件工程的环境分析	2
1.2.1 软件开发过程	3
1.2.2 软件结构	4
1.2.3 软件质量保证	5
1.3 用于嵌入式系统的软件工程	6
1.4 本书的主要内容	7
第 2 章 嵌入式软件的开发过程	10
2.1 动因	11
2.2 定义与概念	12
2.2.1 基本概念	12
2.2.2 过程种类	15
2.3 嵌入式软件开发过程的特点	19
2.3.1 多学科开发	19
2.3.2 跨企业的开发与同步工程	21
2.3.3 非功能性特征	21
2.3.4 经济性	21
2.3.5 长的产品生命周期	22
2.4 特定领域过程模型的建立	22
2.4.1 现有的用于嵌入式软件开发的过程模型	23
2.4.2 描述性过程建模	24
2.4.3 连续的过程改善	25
2.5 总结与展望	26
第 3 章 开发和测试的标准	29
3.1 引言	30
3.2 从标准到软件标准	30
3.2.1 为什么需要标准	31
3.2.2 为什么需要软件标准	31

3.3	软件开发的	标准	32
3.4	一般性	流程标准	32
3.5	IEC 61508	标准	33
3.5.1	对开发过程的一般性要求		34
3.5.2	安全监测		36
3.5.3	软件开发		36
3.6	Cenelec EN 50126、EN 50128 和 EN 50129	标准	39
3.7	总结		40
3.8	定义		40
第 4 章	与安全有关的软件系统的许可		42
4.1	引言		43
4.2	什么是许可		43
4.3	参与者		44
4.3.1	行政机关		44
4.3.2	鉴定人和检测机构		45
4.3.3	制造商		46
4.3.4	供应商		46
4.3.5	运营商和用户		47
4.4	获得许可		47
4.4.1	系统的复杂度		48
4.4.2	规划与约定（对规划的检验单）		48
4.4.3	人为因素		49
4.4.4	申请许可证过程中的风险处理		49
4.4.5	企业秘密的公开		50
第 5 章	嵌入式系统的法律问题		52
5.1	版权和专利权		53
5.1.1	版权		53
5.1.2	专利法		57
5.1.3	半导体保护		60
5.2	合同法		60
5.2.1	系统集成商与整体系统买主的合同关系		61
5.2.2	系统集成商与软件供应商的合同关系		62
5.2.3	整体系统的买主与软件供应商的合同关系		63
5.3	法律责任		63
5.3.1	机器制造商也是软件制造商		64

5.3.2	供应的软件	70
5.4	结论	72
第 6 章	嵌入式软件的需求工程	75
6.1	引言	76
6.2	RE 基础知识	77
6.3	RE 的框架体系	78
6.3.1	系统环境	78
6.3.2	RE 过程的三个维度	79
6.3.3	五个主要设计行为	80
6.3.4	早期和后期阶段的对比	81
6.4	对嵌入式系统复杂度的控制	83
6.5	三种需求模型	86
6.5.1	面向解决方案的需求建模	87
6.5.2	目标建模	88
6.5.3	场景与用例	89
6.5.4	建模种类的实例	90
6.6	基于场景和目标的系统开发的需求工程 (SEGOS-RE)	91
6.7	应用实例: 数码相机	95
6.8	总结与展望	99
第 7 章	软件结构和系统结构	105
7.1	定义和限制	106
7.1.1	嵌入式系统和软件结构	106
7.1.2	软件结构、系统结构的定义和视图	107
7.1.3	结构模型化的维度	110
7.2	嵌入式系统的结构模型	112
7.2.1	面向对象的元元结构	112
7.2.2	嵌入式系统的元结构	114
7.2.3	模型结构化的作用	118
7.3	模型结构和嵌入式系统的结构风格	119
7.3.1	操作方法	119
7.3.2	CIP 结构	119
7.3.3	面向角色结构	121
7.3.4	双服务器结构	122
7.3.5	X-By-Wire 结构	124
7.4	结构模板和框架	126

7.4.1	模板和框架作为软件再利用的工具	126
7.4.2	模板和框架的候选项	127
7.4.3	嵌入式系统中的一个模板实例	128
7.5	基于结构的嵌入式系统结构设计	129
7.5.1	软件结构对于嵌入式系统的作用	129
7.5.2	基于结构的软件开发	130
第 8 章	嵌入式软件编程	133
8.1	引言	134
8.2	C 语言嵌入式软件编程	135
8.2.1	POSIX 1003.1b 标准	136
8.2.2	线程管理与定时器	136
8.3	Ada 语言嵌入式软件编程	138
8.3.1	Ada 任务	139
8.3.2	Ada 时间特性	139
8.3.3	Ada 同步和调度	140
8.4	Java 与嵌入式系统	141
8.4.1	Java 实时规范	141
8.4.2	调度	142
8.4.3	内存管理	143
8.4.4	例程	144
8.4.5	Java 2 Micro Edition	144
8.5	Microsoft.Net Compact Framework	145
8.6	应用程序和操作系统	147
8.7	总结	149
第 9 章	嵌入式软件测试	150
9.1	引言	151
9.2	传统软件测试中的技术水平	152
9.2.1	动态测试	152
9.2.2	静态分析	154
9.2.3	形式化技术: 符号测试和形式化验证方法	155
9.3	嵌入式软件测试: 情形分析	155
9.4	嵌入式软件系统动态测试	156
9.4.1	嵌入式软件特殊性能测试	157
9.4.2	动态测试适用于嵌入式软件特性——一个例子	158
9.4.3	通过测试结果的静态评价得到量化的可靠性说明	161

9.4.4 组织	162
9.5 总结	163
第 10 章 嵌入式 UML/实时 UML	165
10.1 导论	166
10.2 当前的需求和解决的可能性	166
10.3 所应用的开发过程	166
10.4 使用 UML 进行需求分析	168
10.5 设计中的需求	173
10.6 标准扩展和展望	179
10.7 结论	181
第 11 章 形式化开发方法与分析技术	182
11.1 形式化技术的分类	183
11.1.1 静态建模	184
11.1.2 动态建模	185
11.1.3 嵌入式系统的形式化技术	186
11.2 用方法 B 开发系统	187
11.2.1 抽象机器	187
11.2.2 抽象机器的兼容性	189
11.2.3 逐步改进	190
11.2.4 逐步改进的正确性	192
11.2.5 结构化规范	193
11.2.6 应用	194
11.3 动态过程的建模与分析	194
11.3.1 用过程演算 CSP 建模	194
11.3.2 过程表达式语法	196
11.3.3 过程系统的特征	196
11.3.4 模型检测	197
11.3.5 特征获取摘要	198
11.4 总结与展望	199
11.4.1 形式化技术及面向对象	199
11.4.2 开发过程中的形式化技术规则	200
11.4.3 展望	200
第 12 章 安全性和可靠性分析技术	204
12.1 引言	205

12.2	基础	206
12.2.1	定义和术语介绍	206
12.2.2	概率关系介绍	209
12.2.3	过程分类	212
12.3	方法和技术	214
12.3.1	关于风险和可操作性的研究 (HAZOP)	214
12.3.2	初级风险分析 (PHA)	215
12.3.3	功能性风险评估 (FHA)	215
12.3.4	失效模式效应分析 (FMEA)	216
12.3.5	可靠性结构图 (RBD)	217
12.3.6	事件树分析法 (ETA)	218
12.3.7	故障树分析法 (FTA)	218
12.3.8	Markov 分析法	221
12.3.9	潜在通路分析技术	222
12.3.10	软件在方法和技术方面的相关扩展	222
12.4	适宜性和选择	222
12.5	可靠性检测和预测	224
12.6	总结	224
第 13 章	分布嵌入式系统	228
13.1	引言	229
13.2	分布嵌入式系统简介	230
13.3	一个简单的嵌入式系统	231
13.4	嵌入式系统的硬件存取	231
13.5	并发处理	234
13.6	分布式系统	236
13.6.1	简介	236
13.6.2	分布嵌入式系统的发展方向	237
13.6.3	ISO/OSI 层模型	238
13.6.4	分布式系统内部过程通信	240
13.7	基于 Ada 的分布式程序设计	244
13.8	总结	246
第 14 章	实时操作系统	248
14.1	实时系统	249
14.1.1	实时操作和实时体系结构	249
14.1.2	时间箱与时间保证	250

14.1.3	及时性	251
14.1.4	确知性	252
14.1.5	对操作系统的要求	253
14.2	独有特性	255
14.2.1	计划	255
14.2.2	协调	257
14.2.3	中断透明性	260
14.2.4	再入能力	262
14.2.5	可再入	263
14.3	软件技术观点	264
14.4	实例	266
14.4.1	QNX	267
14.4.2	VxWorks	267
14.4.3	OSEK/VDX	268
14.5	总结	269
第 15 章	反应式系统的建模: 同步语音和状态图	272
15.1	引言	273
15.1.1	反应式系统	273
15.1.2	同步语音和状态图——历史和概要	274
15.2	同步编程语言 Esterel	275
15.2.1	例子 ABRO	275
15.2.2	同步模型	276
15.2.3	用 Esterel 编写的 ABRO	278
15.2.4	代码组合	279
15.3	状态图	282
15.3.1	安全状态机 (SSM)	282
15.3.2	正确性和构建性	288
15.4	总结和前景	291
第 16 章	汽车中的软件技术	294
16.1	引言	295
16.2	一般趋势	295
16.2.1	在汽车中上升的软件份额	295
16.2.2	上升的系统复杂性	296
16.2.3	上升的质量要求	297
16.2.4	上升的期限和成本压力	297

16.2.5	快速的技术转变	298
16.3	对汽车制造商造成的影响	299
16.3.1	机会和优点	299
16.3.2	普通的挑战	299
16.3.3	技术挑战	300
16.3.4	必不可少的技术核心能力	301
16.4	技术状况与最新的研究结果	302
16.4.1	过程	302
16.4.2	方法与工具	303
16.4.3	软件结构	305
16.4.4	系统安全	307
16.5	总结与展望	309
第 17 章	安全软件在交通技术的嵌入式系统中的应用	311
17.1	引言	312
17.2	交通技术	312
17.3	安全性、风险的附属品	313
17.4	软件的安全性	315
17.4.1	CENELEC 标准规范的软件	315
17.4.2	角色	315
17.4.3	通过方法来保证正确性	316
17.4.4	通过过程来保证正确性	317
17.4.5	通过检测来保证正确性	317
17.5	案例研究	319
17.5.1	案例引言	319
17.5.2	系统描述	319
17.5.3	采用的方法	320
17.5.4	举例	321
17.5.5	试验项目的结果	322
17.6	总结和展望	323
第 18 章	航天应用领域嵌入式软件的开发	325
18.1	自动运输工具 (ATV)	326
18.2	推进驱动电子装置 (ATV-PDE)	326
18.3	宇航标准	328
18.3.1	作为开发基础的标准	328
18.3.2	适应性和临界状态	328

18.4	软件开发	329
18.4.1	团队建设和合作	329
18.4.2	计划完成	330
18.4.3	软件的临界状态	330
18.4.4	开发阶段	331
18.5	维护	336
18.6	总结	337
第 19 章	嵌入式软件在医疗技术中的应用	338
19.1	医疗设备的使用领域和分类	339
19.2	医疗设备类型及其应用	340
19.2.1	功能诊断与患者监护	340
19.2.2	造影诊断	341
19.2.3	治疗设备	345
19.2.4	生命维持系统	346
19.2.5	临床信息系统	346
19.3	医疗设备的设计	347
19.3.1	对医疗软件的特殊要求	348
19.3.2	数据管理与可视化	348
19.4	医疗技术中的软件标准	351
19.4.1	DICOM	351
19.4.2	HL7	352
19.5	医疗产品的开发过程	352
19.6	对医疗产品的风险管理	353
19.7	信息安全	354
19.8	医疗产品的投放市场	355
19.9	总结与展望	356
第 20 章	嵌入式软件在工业自动化领域的应用	358
20.1	引言	359
20.1.1	对工业自动化的一般要求	359
20.1.2	概况	360
20.2	技术过程	360
20.2.1	用于连续过程的嵌入式系统	360
20.2.2	用于离散过程的嵌入式系统	361
20.3	生命周期观察	361
20.4	对参与学科的集成	363

20.5	工业自动化中的结构和系统工程	364
20.5.1	工业自动化的层次划分	364
20.5.2	自动化元件的描述	367
20.6	对工业自动化中嵌入式系统的系统软件的要求	372
20.6.1	技术要求	372
20.6.2	经济要求	373
20.6.3	小结	373
20.7	优化和未来的系统变化	374
20.7.1	基于元件的系统	374
20.7.2	机电一体化	375
20.7.3	展望: 下一代思维变迁正在进行中	375
20.7.4	最后的评注	377
第 21 章	嵌入式通信软件的开发	378
21.1	专业通信系统中的软件需求	379
21.2	系统和软件生命周期——原则、过程、经验	379
21.2.1	产品生命周期中的标准开发过程	380
21.2.2	SDP 软件——软件开发过程	382
21.2.3	递归式渐进开发模型的复杂性概念	384
21.2.4	软件过程的改进	384
21.3	以 LambdaUnite MSS 系统为例介绍软件体系结构的作用	385
21.3.1	光纤传输技术应用领域	385
21.3.2	LambdaUnite 系统的产品介绍	386
21.3.3	系统开发: 一种挑战	387
21.3.4	软件体系结构: 任务	388
21.3.5	软件体系结构: 3 个例子展示的途径	389
21.3.6	软件体系结构: 结论	392
21.4	AnyMedia 系统中的软件体系结构及可执行软件	393
21.4.1	软件体系结构阶段的建模	394
21.4.2	层、框架和模式	397
21.4.3	实现阶段——体系结构模型的扩充	399
21.5	在 Node B 系统中的 UMTS 框架的面向功能的测试	401
21.5.1	UTRAN 简介	401
21.5.2	Node B	402
21.5.3	Node B 软件和硬件方面的需求	402
21.5.4	网络单元测试的定义和划分	403
21.5.5	已用的测试样例	404
21.5.6	对 UMTS 子层结构的测试	406

第1章

绪 论

全世界的绝大多数微处理器应用于嵌入式系统（如从家用电器到飞机）中。我们每天都在使用的许多设备都属于嵌入式系统。目前，嵌入式系统的许多功能是通过软件来实现的。因此，软件对于嵌入式系统具有很大的技术上和经济上的意义。此外，软件也持续和不可避免地影响着我们的日常生活。嵌入式系统软件工程是介于传统的软件工程和系统工程之间的一门重要的学科，它借助于这些领域里面的一些技术、方法和开发过程，并根据嵌入式系统的特点补充额外的求解方法。此外，各个不同应用领域的一些特定的性能要求和约束情况对于嵌入式系统的软件开发过程也有很大的影响。

本章主要内容

- 软件对于嵌入式系统的意义
- 软件工程的环境分析
- 用于嵌入式系统的软件工程
- 本书的主要内容