



CRC Press
Taylor & Francis Group



国防电子信息技术丛书

Developing Safety-Critical Software

A Practical Guide for Aviation Software and DO-178C Compliance

安全关键软件 开发与审定

——DO-178C标准实践指南

[美] Leanna Rierson 著

崔晓峰 译



中国工信出版集团



电子工业出版社
PUBLISHING HOUSE OF ELECTRONICS INDUSTRY
<http://www.phei.com.cn>

国防电子信息技术丛书

安全关键软件开发与审定

—— DO-178C标准实践指南

Developing Safety-Critical Software

A Practical Guide for Aviation Software
and DO-178C Compliance

[美] Leanna Rierson 著

崔晓峰 译

电子工业出版社

Publishing House of Electronics Industry

内容简介

本书作者是DO-178系列标准的直接制定者之一。书中详细介绍了如何基于最新版本的DO-178C标准进行高安全软件开发，既包括对标准的全面介绍，又包括依据该标准进行开发和审定的实用指南；既包含多年从事高安全软件研制、管理、审定工作的经验，又包含相关最新软件技术的深入讲解。主要内容有：在系统与安全性大视野中的软件；DO-178C标准的具体解释及如何有效使用；DO-178C相关的工具鉴定、基于模型的开发、面向对象技术、形式化方法；成功开发高安全软件及审定的实用建议；以及和高安全软件开发和验证相关的深入专题。

本书读者群为民航软件研发和管理人员，尤其是从事DO-178B/178C审定的相关人员，同时包括其他高安全软件（包括军用和民用，例如航天、航空、电子等行业）研发和管理人员，以及按照CMMI（或其他等同标准）开展软件过程改进的单位和个人。

Developing Safety-Critical Software: A Practical Guide for Aviation Software and DO-178C Compliance, Leanna Rierson

ISBN: 978-1-4398-1368-3

Copyright © 2013 by Taylor & Francis Group, LLC

Authorized translation from English language edition published by CRC Press, part of Taylor & Francis Group LLC; All rights reserved.

Publishing House of Electronics Industry is authorized to publish and distribute exclusively the Chinese (Simplified Characters) language edition. This edition is authorized for sale throughout Mainland of China. No part of the publication may be reproduced or distributed by any means, or stored in a database or retrieval system, without the prior written permission of the publisher.

Copies of this book sold without a Taylor & Francis sticker on the cover are unauthorized and illegal.

本书原版由Taylor & Francis出版集团旗下，CRC出版公司出版，并经其授权翻译出版。版权所有，侵权必究。本书中文简体翻译版授权由电子工业出版社独家出版并限在中国大陆地区销售。未经出版者书面许可，不得以任何方式复制或发行本书的任何部分。

本书封面贴有Taylor & Francis公司防伪标签，无标签者不得销售。

版权贸易合同登记号 图字：01-2013-7215

图书在版编目（CIP）数据

安全关键软件开发与审定——DO-178C标准实践指南/（美）里埃森（Rierson, L.）著；崔晓峰译。

北京：电子工业出版社，2015.6

（国防电子信息技术丛书）

书名原文：Developing Safety-Critical Software: A Practical Guide for Aviation Software and DO-178C Compliance

ISBN 978-7-121-25992-0

I. ①安… II. ①里… ②崔… III. ①安全技术—软件开发—指南 IV. ①TP311.52-62

中国版本图书馆CIP数据核字（2015）第094008号

策划编辑：马 岚

责任编辑：马 岚 特约编辑：姚 旭

印 刷：三河市鑫金马印装有限公司

装 订：三河市鑫金马印装有限公司

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：787×1092 1/16 印张：22.5 字数：561千字

版 次：2015年6月第1版

印 次：2015年6月第1次印刷

定 价：89.00元

凡所购买电子工业出版社的图书有缺损问题，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zlt@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

安全关键软件 (safety-critical software) 是指应用于航空、航天、交通、能源、医疗、军事等领域, 其运行情况会影响到人身和设施安危的软件系统。该类软件无疑应当被投以格外的关注、施以有效的方法, 为追求“万无一失”而极尽所能。

在这一目标下, 基于“高质量的过程产生高质量的产品”这一理念, 出现了一系列“以过程为中心”的软件工程方法、标准和实践, 广为人知的“能力成熟度模型集成 (CMMI)”和本书将要介绍的“民航机载软件适航标准 (DO-178)”均属此列。CMMI 影响之大不必多说, 而 DO-178 的成熟和成功同样卓著。实际上可以说在近 30 年间, 每个有过飞行经历的人都已在不知不觉中, 获得过包含 DO-178 一份贡献的安全保障。

DO-178 是民航领域用于保证机载软件符合飞行安全要求 (即“适航性”) 的规范性文件, 它由美、欧航空组织建立, 已成为在全球航空领域 (包括中国) 得到广泛认可和使用的事实标准。该系列标准起始于 20 世纪 80 年代初, 最新版本 (DO-178C) 于 2011 年 12 月发布。DO-178C 继承了上一版本 (DO-178B) 的主体, 这本身就是对上一版本 1992 年以来近 20 年成功运用的最好肯定。新版在概念和结构的清晰性、与系统过程以及新技术发展的协调性方面进行了积极有益的改进, 将会进一步提升其实践的效能。

DO-178C 在作用和思想上与 CMMI (及其衍生的一些类似标准) 有一定的可比性, 但是也存在很大的实质不同。CMMI 最终评判的是一个组织 (企业) 的“能力”; DO-178C 最终评判的是一个产品是否合格。CMMI 涵盖工程活动和辅助活动、项目管理、过程管理; DO-178C 聚焦于工程及其直接相关的管理活动。此外, 即使在二者的交集上, DO-178C 的特色也十分突出。CMMI 是一个“模型”、“框架”, 以抽象原则为主 (除了明确的“目标”和“实践”), 没有强制特定做法, 更不提供系统化的实施途径。这种方式为实践者针对具体情况创造具体方法保留了灵活性, 但是也时常令一些实施者和评价者无所适从。与之不同的是, DO-178C 从头到脚都极具实践性、操作性, 它所规定的每一件事、每一个要求都更直截了当、更清晰明确, 此外还尽可能地针对各种可能用到的新技术和特殊技术, 给出专门的使用指导和要求。这种方式体现了—一个高安全领域对产品近似“刻板”的限定, 而事实也雄辩地证明了它的卓越成效。使用 DO-178C 无论开展研制还是检查, 可能会牺牲一些“发挥”的空间, 但是更强的可依据性、易判定性也将避免不少疑问与纠结的可能。对于许多正为难以驾驭 CMMI 而困扰的实践者, DO-178C 恰似一份难得的“消化药”和“实战图”, 在过程改进的道路上正好可以与 CMMI 相辅相成, 相得益彰。

作为一个行业标准, DO-178C 对于航空软件工作者自然是必修与必从的“法典”。但实际上对于其他领域软件而言, DO-178C 同样具有宝贵的指导作用。软件工程难题的根源是软件状态空间超大、需求抽象漂移、人为因素交织等内在特征, 而与软件应用的领域并无太大关联。

DO-178C 所针对和解决的各种问题，其实就是软件工程的基本和普遍问题。因此，对外界而言“深山人未知”的 DO-178C，作为一套成熟的工程准则和指南，完全可以在更广阔的空间发挥积极作用，尤其是那些具有高安全性要求的领域，无论天上还是地面，无论民用还是军事，无论是否以通过审定为目的。事实上，他山之石，可以攻玉，有机会深入了解一下不同领域的成功经验和不同背景的专家思维，往往可以获得超出预想的裨益。当然这种学习应当是启发式的而不是拘泥不化的，软件工程这门特殊的学科应当格外崇尚向实践学习、向成功学习，同时也应当格外谨记不存在“一只鞋子适合所有的脚”。

本书是在最新版的 DO-178C 推出之际，给出的一份对该系列规范的全面、深入的解读。本书作者是直接参与 DO-178C 文件修订的资深专家，以其对标准的把握，来传递标准原本的思想、方法、制定者的观点甚至争议。同时，本书还是作者作为航空软件审定的官方代表和权威专家，以其 20 年的研发、审定、授课经历，对其积累的宝贵经验的汇聚。这些经验和建议来自实践、用于实践，对于让规范真正发挥实效可谓一语千金。

国际上，软件过程和质量方面的标准早已在关键应用领域中发挥出重要作用。在国内，相关概念、模型、标准的重视和推行也已有相当时日。但是抽象的标准并不能完全传授如何在实际中实施和见效，包括如何有效地进行审查和评价，这也许是过程改进道路上常常遇到的最大困难。从这个意义上，本书将成熟领域中的成熟经验和盘托出，不拒其繁、不舍其微，没有玄奥的理论和华丽的铺陈，却也许正是尤为难得的良师益教。

由于译者的知识不足和时间仓促，翻译中难免有不当或谬误之处，敬请读者原谅和指正。任何意见、建议和探讨都欢迎致信：qualitysoftware@yeah.net。

崔晓峰

2014 年 5 月

前 言

我深感重任又忐忑不安地将这本书呈现给您。经过两年的研究和写作，我感到完成的还只是浮光掠影。我希望自己的经验和分享会对您的职业生涯带来帮助。

我很早就热衷于关注安全性及其现实的实现。在高中时代，我为一家本地报纸撰写一个关于安全性小建议的专栏，深入地研究了（作为互联网时代之前的美国乡镇所能做到的极致）：浴盆安全、拖拉机安全、电力安全，以及其他许多方面。在高中最后一年，我参加了州举办的说服力演讲比赛，主题是座椅安全带的安全性。对提高安全性的愿望引领我进入了美国联邦航空局（FAA），这个愿望也是撰写这本书的主要动因。

软件只是整个安全性链条中的一环，然而，它却是一个重要的环节，并且变得越来越关键。随着软件变得更加普及并且以更加关键的方式得到使用，它的风险和对安全性的作用日益增长。与软件相关的安全性增长的同时，许多公司的业务模型似乎也在变化——以少搏多、进度为王，软件工程师被看成如同棋盘上的棋子一样可以摆来摆去。

本书的意图是成为那些在业界奋斗的人们的有益工具。可能您是一位系统工程师或经理、软件经理、软件工程师、质量保证工程师，或者一位努力从他人那里汲取经验的学生。您想要做出色的工作，却被进度和预算的压力拖累。我希望这本书，基于我过去 20 年在航空工业中的经验，可以在您追求质量和卓越的时候助上一臂之力。

目 录

第一部分 引 言

第1章 引言和概览	2
1.1 安全关键软件的定义	2
1.2 安全性问题的重要性	2
1.3 本书目的和重要提示	4
1.4 本书概览	5

第二部分 安全关键软件开发的语境

第2章 系统语境中的软件	8
2.1 系统开发概览	8
2.2 系统需求	10
2.2.1 系统需求的重要性	10
2.2.2 系统需求的类型	10
2.2.3 良好需求的特性	10
2.2.4 系统需求考虑	11
2.2.5 需求假设	14
2.2.6 分配到软硬件项	14
2.3 系统需求确认与验证	14
2.3.1 需求确认	14
2.3.2 实现验证	15
2.3.3 确认与验证建议	15
2.4 系统工程师最佳实践	16
2.5 软件与系统的关系	18
第3章 系统安全性评估语境中的软件	20
3.1 航空器与系统安全性评估过程概览	20
3.1.1 安全性工作计划	20
3.1.2 功能危险评估	21
3.1.3 系统功能危险评估	22
3.1.4 初步航空器安全性评估	22
3.1.5 初步系统安全性评估	22

3.1.6	共同原因分析	23
3.1.7	航空器安全性评估和系统安全性评估	23
3.2	开发保证	24
3.2.1	开发保证级别	25
3.3	软件如何置入安全性过程	25
3.3.1	软件的独特性	25
3.3.2	软件开发保证	26
3.3.3	其他视点	27
3.3.4	在系统安全性过程关注软件的建议	28

第三部分 使用DO-178C开发安全关键软件

第4章	DO-178C及支持文件概览	31
4.1	DO-178历史	31
4.2	DO-178C和DO-278A核心文件	33
4.2.1	DO-278A与DO-178C的不同	37
4.2.2	DO-178C附件A目标表概览	38
4.3	DO-330: 软件工具鉴定考虑	41
4.4	DO-178C技术补充	41
4.4.1	DO-331: 基于模型的开发补充	42
4.4.2	DO-332: 面向对象技术补充	42
4.4.3	DO-333: 形式化方法补充	42
4.5	DO-248C: 支持材料	43
第5章	软件策划	44
5.1	引言	44
5.2	一般策划建议	44
5.3	5个软件计划	46
5.3.1	软件合格审定计划	46
5.3.2	软件开发计划	48
5.3.3	软件验证计划	49
5.3.4	软件配置管理计划	51
5.3.5	软件质量保证计划	53
5.4	3个开发标准	54
5.4.1	软件需求标准	55
5.4.2	软件设计标准	55
5.4.3	软件编码标准	56
5.5	工具鉴定计划	57
5.6	其他计划	57
5.6.1	项目管理计划	57

5.6.2	需求管理计划	57
5.6.3	测试计划	57
第6章	软件需求	58
6.1	引言	58
6.2	定义需求	58
6.3	良好软件需求的重要性	59
6.3.1	原因1: 需求是软件开发的基础	59
6.3.2	原因2: 好的需求节省时间和金钱	60
6.3.3	原因3: 好的需求对安全性至关重要	60
6.3.4	原因4: 好的需求对满足客户需要是必需的	61
6.3.5	原因5: 好的需求对测试很重要	61
6.4	软件需求工程师	61
6.5	软件需求开发概览	62
6.6	收集和分析软件需求的输入	63
6.6.1	需求收集活动	64
6.6.2	需求分析活动	64
6.7	编写软件需求	65
6.7.1	任务1: 确定方法	65
6.7.2	任务2: 确定软件需求文档版式	66
6.7.3	任务3: 将软件需求划分为子系统和/或特征	66
6.7.4	任务4: 确定需求优先级	67
6.7.5	一个简单迂回(不是一个任务): 要避免的斜坡	67
6.7.6	任务5: 编档需求	68
6.7.7	任务6: 提供系统需求的反馈	72
6.8	验证(评审)需求	73
6.8.1	同行评审推荐实践	74
6.9	管理需求	76
6.9.1	需求管理基础	76
6.9.2	需求管理工具	77
6.10	需求原型	78
6.11	可追踪性	79
6.11.1	可追踪性的重要性和好处	79
6.11.2	双向可追踪性	79
6.11.3	DO-178C和可追踪性	80
6.11.4	可追踪性挑战	81
第7章	软件设计	83
7.1	软件设计概览	83
7.1.1	软件体系结构	83

7.1.2	软件底层需求	83
7.1.3	设计打包	85
7.2	设计方法	85
7.2.1	基于结构的设计(传统)	85
7.2.2	面向对象的设计	86
7.3	良好设计的特性	86
7.4	设计验证	89
第8章	软件实现: 编码与集成	91
8.1	引言	91
8.2	编码	91
8.2.1	DO-178C编码指南概览	91
8.2.2	安全关键软件中使用的语言	92
8.2.3	选择一种语言和编译器	94
8.2.4	编程的一般建议	95
8.2.5	代码相关的特别话题	102
8.3	验证源代码	103
8.4	开发集成	104
8.4.1	构建过程	104
8.4.2	加载过程	105
8.5	验证开发集成	105
第9章	软件验证	106
9.1	引言	106
9.2	验证的重要性	106
9.3	独立性与验证	107
9.4	评审	108
9.4.1	软件计划评审	108
9.4.2	软件需求、设计和代码评审	108
9.4.3	测试资料评审	108
9.4.4	其他资料项评审	108
9.5	分析	109
9.5.1	最坏情况执行时间分析	109
9.5.2	内存余量分析	110
9.5.3	链接和内存映像分析	110
9.5.4	加载分析	111
9.5.5	中断分析	111
9.5.6	数学分析	111
9.5.7	错误和警告分析	112
9.5.8	分区分析	112

9.6	软件测试	112
9.6.1	软件测试的目的	112
9.6.2	DO-178C软件测试指南概览	114
9.6.3	测试策略综述	115
9.6.4	测试策划	119
9.6.5	测试开发	120
9.6.6	测试执行	122
9.6.7	测试报告	124
9.6.8	测试可追踪性	124
9.6.9	回归测试	124
9.6.10	易测试性	125
9.6.11	验证过程中的自动化	125
9.7	验证的验证	126
9.7.1	测试规程评审	127
9.7.2	测试结果的评审	127
9.7.3	需求覆盖分析	127
9.7.4	结构覆盖分析	128
9.8	问题报告	134
9.9	验证过程建议	136
第10章	软件配置管理	140
10.1	引言	140
10.1.1	什么是软件配置管理	140
10.1.2	为何需要软件配置管理	140
10.1.3	谁负责实现软件配置管理	141
10.1.4	软件配置管理涉及什么	142
10.2	SCM活动	142
10.2.1	配置标识	142
10.2.2	基线	143
10.2.3	可追踪性	143
10.2.4	问题报告	143
10.2.5	变更控制和评审	146
10.2.6	配置状态记录	147
10.2.7	发布	147
10.2.8	归档和提取	148
10.2.9	资料控制类	148
10.2.10	加载控制	149
10.2.11	软件生命周期环境控制	150
10.3	特别SCM技能	150
10.4	SCM资料	151
10.4.1	SCM计划	151

10.4.2	问题报告	151
10.4.3	软件生命周期环境配置索引	151
10.4.4	软件配置索引	151
10.4.5	SCM记录	152
10.5	SCM陷阱	152
10.6	变更影响分析	154
第11章	软件质量保证	157
11.1	引言: 软件质量和软件质量保证	157
11.1.1	定义软件质量	157
11.1.2	高质量软件的特性	157
11.1.3	软件质量保证	158
11.1.4	常见质量过程和产品问题的例子	159
11.2	有效和无效SQA的特征	159
11.2.1	有效的SQA	159
11.2.2	无效的SQA	160
11.3	SQA活动	161
第12章	合格审定联络	164
12.1	什么是合格审定联络	164
12.2	与合格审定机构的沟通	164
12.2.1	与合格审定机构协调的最佳实践	165
12.3	软件完成总结	167
12.4	介入阶段审核	168
12.4.1	SOI审核概览	168
12.4.2	软件作业辅助概览	169
12.4.3	使用软件作业辅助	171
12.4.4	对审核者的一般建议	171
12.4.5	对被审核者的一般建议	176
12.4.6	SOI评审细节	177
12.5	合格审定飞行测试之前的软件成熟度	184

第四部分 工具鉴定和DO-178C补充

第13章	DO-330和软件工具鉴定	186
13.1	引言	186
13.2	确定工具鉴定需要和级别 (DO-178C的12.2节)	187
13.3	鉴定一个工具 (DO-330概览)	190
13.3.1	DO-330的需要	190
13.3.2	DO-330工具鉴定过程	190
13.4	工具鉴定特别话题	197

13.4.1	FAA规定8110.49	197
13.4.2	工具确定性	197
13.4.3	额外的工具鉴定考虑	198
13.4.4	工具鉴定陷阱	199
13.4.5	DO-330和DO-178C补充	200
13.4.6	DO-330用于其他领域	200
第14章	DO-331和基于模型的开发与验证	201
14.1	引言	201
14.2	基于模型开发的潜在好处	202
14.3	基于模型开发的潜在风险	204
14.4	DO-331概览	206
14.5	合格审定机构对DO-331的认识	210
第15章	DO-332和面向对象技术及相关技术	211
15.1	面向对象技术介绍	211
15.2	OOT在航空中的使用	211
15.3	航空手册中的OOT	212
15.4	FAA资助的OOT和结构覆盖研究	212
15.5	DO-332概览	213
15.5.1	策划	213
15.5.2	开发	213
15.5.3	验证	213
15.5.4	脆弱性	214
15.5.5	类型安全	214
15.5.6	相关技术	214
15.5.7	常见问题	214
15.6	OOT建议	215
15.7	结论	215
第16章	DO-333和形式化方法	216
16.1	形式化方法介绍	216
16.2	什么是形式化方法	217
16.3	形式化方法的潜在好处	218
16.4	形式化方法的挑战	219
16.5	DO-333概览	220
16.5.1	DO-333的目的	220
16.5.2	DO-333与DO-178C的比较	220
16.6	其他资源	222

第五部分 特别专题

第17章 未覆盖代码（无关、无效和非激活代码）	224
17.1 引言	224
17.2 无关和无效代码	224
17.2.1 避免无关和无效代码的晚发现	225
17.2.2 评价无关或无效代码	225
17.3 非激活代码	227
17.3.1 策划	229
17.3.2 开发	229
17.3.3 验证	230
第18章 现场可加载软件	231
18.1 引言	231
18.2 什么是现场可加载软件	231
18.3 现场可加载软件的好处	231
18.4 现场可加载软件的挑战	232
18.5 开发和加载现场可加载软件	232
18.5.1 开发系统成为现场可加载的	232
18.5.2 开发现场可加载软件	233
18.5.3 加载现场可加载软件	233
18.5.4 修改现场可加载软件	234
18.6 总结	234
第19章 用户可修改软件	235
19.1 引言	235
19.2 什么是用户可修改软件	235
19.3 UMS例子	236
19.4 为UMS设计系统	236
19.5 修改和维护UMS	238
第20章 实时操作系统	240
20.1 引言	240
20.2 什么是RTOS	240
20.3 为什么使用RTOS	241
20.4 RTOS内核及其支持软件	241
20.4.1 RTOS内核	242
20.4.2 应用编程接口	242
20.4.3 主板支持包	243
20.4.4 设备驱动	243

20.4.5	支持库	244
20.5	安全关键系统中使用的RTOS的特性	244
20.5.1	确定性	244
20.5.2	可靠的性能	244
20.5.3	硬件兼容	244
20.5.4	环境兼容	244
20.5.5	容错	244
20.5.6	健康监控	245
20.5.7	可审定	245
20.5.8	可维护	245
20.5.9	可复用	246
20.6	安全关键系统中使用的RTOS的特征	246
20.6.1	多任务	246
20.6.2	有保证和确定性的可调度性	246
20.6.3	确定性的任务间通信	248
20.6.4	可靠的内存管理	248
20.6.5	中断处理	248
20.6.6	钩子函数	249
20.6.7	健壮性检查	249
20.6.8	文件系统	249
20.6.9	健壮分区	249
20.7	需考虑的RTOS问题	250
20.7.1	要考虑的技术问题	250
20.7.2	要考虑的合格审定问题	252
20.8	其他的RTOS相关话题	254
20.8.1	ARINC 653概览	254
20.8.2	工具支持	256
20.8.3	开源RTOS	256
20.8.4	多核处理器、虚拟化和虚拟机管理器	257
20.8.5	保密性	257
20.8.6	RTOS选择问题	257
第21章	软件分区	258
21.1	引言	258
21.1.1	分区：保护的一个子集	258
21.1.2	DO-178C和分区	258
21.1.3	健壮分区	259
21.2	共享内存（空间分区）	260
21.3	共享中央处理器（时间分区）	261
21.4	共享输入/输出	262
21.5	一些与分区相关的挑战	262

21.5.1	直接内存访问	262
21.5.2	高速缓存	263
21.5.3	中断	263
21.5.4	分区之间通信	263
21.6	分区的建议	264
第22章	配置数据	268
22.1	引言	268
22.2	术语和例子	268
22.3	DO-178C关于参数数据的指南总结	269
22.4	建议	270
第23章	航空数据	274
23.1	引言	274
23.2	DO-200A: 航空数据处理标准	274
23.3	FAA咨询通告AC 20-153A	277
23.4	用于处理航空数据的工具	278
23.5	与航空数据相关的其他工业文件	278
23.5.1	DO-201A: 航空信息标准	279
23.5.2	DO-236B: 航空系统性能最低标准: 区域导航要求的导航性能	279
23.5.3	DO-272C: 机场地图信息的用户需求	279
23.5.4	DO-276A: 地形和障碍数据的用户需求	279
23.5.5	DO-291B: 地形、障碍和机场地图数据互换标准	279
23.5.6	ARINC 424: 导航系统数据库标准	279
23.5.7	ARINC 816-1: 机场地图数据库的嵌入式互换格式	280
第24章	软件复用	281
24.1	引言	281
24.2	设计可复用构件	282
24.3	复用先前开发的软件	285
24.3.1	为在民用航空产品中使用而评价PDS	285
24.3.2	复用未使用DO-178[]开发的PDS	289
24.3.3	COTS软件的额外考虑	290
24.4	产品服役历史	292
24.4.1	产品服役历史的定义	292
24.4.2	使用产品服役历史寻求置信度的困难	292
24.4.3	使用产品服役历史声明置信度时考虑的因素	292
第25章	逆向工程	294
25.1	引言	294

25.2	什么是逆向工程	294
25.3	逆向工程的例子	295
25.4	逆向工程时要考虑的问题	295
25.5	逆向工程的建议	296
第26章	外包和离岸外包软件生命周期活动	301
26.1	引言	301
26.2	外包的原因	302
26.3	外包的挑战和风险	302
26.4	克服挑战和风险的建议	305
26.5	总结	311
附录A	转换准则举例	312
附录B	实时操作系统关注点	318
附录C	为安全关键系统选择实时操作系统时考虑的问题	321
附录D	软件服役历史问题	324
	缩略语	327
	参考文献	332