PRENTICE HALL

Design For Trustworthy Software

可信赖的软件开发

(美) Bijay K. Jayaswal 著
Peter C. Patton
杨 浩 译

清华大学出版社

可信赖的软件开发

(美) Bijay K. Jayaswal 著
Peter C. Patton
杨 浩 译

清华大学出版社
北 京

北京市版权局著作权合同登记号 图字：01-2006-7233

图书在版编目(CIP)数据

可信赖的软件开发/(美)杰斯沃(Jayaswal, B.K.)，(美)潘通(Patton, P.C.) 著；杨浩 译.
—北京：清华大学出版社，2008.5
书名原文：Design for Trustworthy Software
ISBN 978-7-302-17282-6
I.可… II.①杰… ②潘… ③杨 … III.软件开发 IV.TP311.52
中国版本图书馆 CIP 数据核字(2008)第 042075 号

责任编辑：王 军 徐燕萍
装帧设计：孔祥丰
责任校对：成凤进
责任印制：何 芊
出版发行：清华大学出版社 **地 址**：北京清华大学学研大厦 A 座
http://www.tup.com.cn **邮 编**：100084
社 总 机：010-62770175 **邮 购**：010-62786544
投稿与读者服务：010-62776969，c-service@tup.tsinghua.edu.cn
质 量 反 馈：010-62772015，zhiliang@tup.tsinghua.edu.cn
印 装 者：北京鑫海金澳胶印有限公司
经 销：全国新华书店
开 本：185×260 **印 张**：33 **字 数**：803 千字
版 次：2008 年 5 月第 1 版 **印 次**：2008 年 5 月第1 次印刷
印 数：1～4000
定 价：68.00 元

本书如存在文字不清、漏印、缺页、倒页、脱页等印装质量问题，请与清华大学出版社出版部联系调换。联系电话：(010)62770177 转 3103 产品编号：023665－01

前　言

目前，世界上增长最快的是计算机终端用户的欲望。计算机革命是从《纽约时报》在1946年情人节宣布ENIAC(电子数字积分计算机)的问世开始的，而这场革命彻底改变了世界。用硅微芯片制造计算机硬件已经变得非常可靠，甚至可以嵌入其他机器。我们假定，如果硬件安全地度过了其“婴儿死亡”期，就永远不需要修理，其他机器也是这样(也许需要频繁地升级，以满足人们不断增长的要求)。同样，软件也已走了一段较长的路，但它始终有一个致命的弱点：可信赖的计算能力。今天，耐用品制造商肯定不会把有已知缺陷的产品投放到高技术市场上，但这对于软件经销商来说是家常便饭。面对计算机终端用户的苛刻要求、软件固有的复杂性和“质量文化”在软件业的普遍缺乏(但这种对质量的不懈追求在高技术含量的耐用品行业却非常普遍)，软件经销商别无选择。

本书作者以30余年的质量工作经验和50多年的软件开发经验为基础，探讨了设计可信赖软件的问题。我们受到Microsoft公司中Craig Mundie的可信赖计算活动的启发，查阅了有关软件质量的文献，召开了无数的会议后，我们相信，Taguchi方法提供了许多有用的东西。我们进一步发现，Taguchi方法不是由Taguchi博士本人推荐应用于可信赖软件的开发的。Taguchi方法只应用于6个案例，但全部成功了。本书的主旨是，尽管软件的设计与硬件类似，但软件的开发过程与硬件的制造过程没有丝毫雷同之处。因此，用于提高软件可靠性和可信赖程度的所有质量方法都必须尽可能地在上游阶段应用。Taguchi方法的天才之处在于，它可以在设计期间处理可控制的因素(内因)和不可控制的因素(外因)。通过使用矩形矩阵或Latin Square的统计试验技术，Taguchi方法可以同时考虑所有的因素。这意味着结束了下游阶段的测试、瓶颈分析、一次查找并修改一个错误等方式。目前，软件的质量目标是防止在实施过程中出错，而不是在实施过程中和实施之后查找和消除错误。与其他质量方法一样，Taguchi方法并不是一种可以直接插入软件开发过程的“黑盒子”，也不能单独使用。它必须放在其他在上游阶段使用的、面向客户的方法中，如层次分析过程(AHP)、质量功能展开(QFD)、TRIZ、Pugh概念选择、故障模式与效果分析(FMEA)，这些方法都可以直接使用，不需要编写任何代码。

Taguchi方法的真谛是聆听“顾客的呼声”。通过仔细的聆听，软件构建师或设计师可以了解计算机终端用户的期望，开发出能获得认可的可靠产品。这样，计算机终端用户就不会被拖入产品“修复再修复”的无休止循环中，却永远看不到成功的希望。本书为开发健壮软件提供了一个包含工具、技术和方法的框架，这个框架是一个集成技术、基于领导层的改革原则、学习型企业的最佳实践方式、管理基础体系及质量战略和系统，所有这些都揉合到软件开发的独特环境中，我们称之为可信赖软件的设计(Design for Trustworthy Software，DFTS)。

本书旨在满足软件开发企业的需要，这些或大或小的开发企业希望建立可信赖的或非常可靠的软件，以满足目前越来越专业的计算机用户的要求。本书适合整个公司学习，可以帮助理解、实施、提高和维护可信赖的软件开发系统。有远见的领导层可以凭借本书，

理解和评价用户的这些需求，并准备领导公司开发出这种健壮的软件。尽管我们强调的是企业软件，但凡是软件开发占很大份量的企业，如开发专用软件，提供内部的软件支持，或提供外包服务的企业，都可以使用本书。企业可以将本书用于获得正式的 DFTS 黑带、高级黑带或其他证书。这种官方证书可以极大地提高整个公司的 DFTS 学习热情和 DFTS 活动的开展。本书还可以用作软件开发人员、质量人员和高级管理人员(他们在企业中有着举足轻重的作用)的实践参考。

本书也可以供软件开发技术、MIS、产品设计与开发、操作、质量管理，以及技术管理等专业的大学生及研究生使用。本书特别补充了理科硕士课程中的工程、MIS、IT、计算机科学及 MBA 课程，主要探讨了操作、产品开发和技术。本书也可以用做 American Society for Quality (ASQ)软件质量认证工程师(CAQE)考试用书。

本书包含大量的示例、补充内容和案例，还有许多要点、复习题、讨论题、项目、练习和习题。在 Internet 上还有其他学习资料，为公司职员、学生和自学人员提供了更多、更新的内容。

本书并不是一本传统意义上的“手册”，而是详细介绍了几个已被证明为有效的质量方法的理论和实践，它们适合于软件开发，可以很好地交互使用。尤其是这些方法可以在实施阶段开始之前的设计阶段使用。本书提供了大量的小软件和其他工程设计案例与示例来演示理论的应用。软件构建师可以找到支持其设计理念的例子，软件工程师可以找到能在详细设计阶段提高质量的例子。虽然所有的 DFTS 技术都可以在整个开发过程中应用，但就终端用户需要的产品而言，重点应是概念、体系结构、工程设计、实施、测试和最终支持等领域。这 5 个部分为成功学习和应用 DFTS 技术建立了相关的领导和管理基础架构。

本书的组织方式

本书分为 5 部分。第 I 部分包含第 1~5 章，介绍了目前的软件开发情况，探讨了其缺陷，提出了开发可信赖软件的挑战及框架。这由两个主要的软件质量问题构成，分别是软件质量的量度标准和可信赖软件的金融远景，在第 2 章和第 3 章论述。第 II 部分包含第 6~14 章，介绍了作者为开发可信赖软件而推荐使用的工具和技术，是本书的核心。第III部分包含第 15~19 章，说明了如何在程序实现阶段开始之前的设计过程中，在上游阶段应用这些工具和技术。第Ⅳ部分包含第 20 章和第 21 章，为在企业中开展 DFTS 活动打基础。与所有的质量活动一样，DFTS 必须得到高层的支持才能成功，而且必须成为企业文化的一部分。第Ⅴ部分包含第 22~27 章，列举了 6 个主要的案例，应用了第 I ~Ⅳ部分介绍的各种软件质量技术。我们挑选出这些技术的世界级高手，他们慷慨地贡献出了最得意的例子，供读者思考和学习。

有用的软件

使用几个软件包，可以轻松地学习和应用质量方法，如 AHP、Taguchi 方法和 QFD。可以从许多网站上免费下载限制使用或限制时间的软件。下面的软件可以免费下载：

- AHP：在 http://www.expertchoice.com/software/grouptrialreg.htm 上可以免费下载 Expert Choice 的 15 天试用版本。学生、教师和公司团体购买可以享受特价，详情请致电 1-888-259-6400。
- QFD：Microsoft Excel 的 Modern Blitz QFD 模板包含在 QFD 协会的培训课程中，详情请访问 http://www.qfdi.org 网站。
- Taguchi 方法：Qualitek-4 DEMO 软件提供了 50 多个示例，允许使用 L_8 数组设计自己的试验。该软件可以从 http://www.nutek-us.com/wp-q4w.html 上下载。
  也可以访问如下有用的网站：
  http://www.nutek-us.com/wp-q4w-screen.html
  http://www.nutek-us.com/wp-q4w-eval.html
  涉及 L_8 数组的试验可以使用 DEMP 版本。完整版本需要向经销商购买。

本书的网站

本书的网站包含了本书的最新版本，为学生和教师提供了新的资料、示例和案例分析。该网站还为本书的其他读者提供了资料，如质量人员及在 DFTS 过程中起重要作用的公司领导。本书的两个网站是：

http://www.prenhallprefessional.com/title/0131872508

http://www.agilenty.com/publications

序

我从业以来，一直在编写商用企业软件，但可以预见，将来应用程序软件不再由程序员编写。二十多年以来，高级开发团队逐渐认识到，编程的最高境界其实是基于规范的软件。这种应用程序软件是根据非常精确的规范自动生成的，而精确的规范是由特定领域的专家编写的，而不是系统分析员或程序员编写的。目前的商用应用程序员将成为特定领域的专家或系统程序员，为规范语言或特定领域专用的设计语言(Domain-Specific Dedign Languages，DSDL)编写元编译器，以自动生成完整的应用程序系统。经过多年的研究，Lawson 公司发布了这样一个工具，叫作 Landmark™，主要用于准备发布新的应用程序软件。

以可靠、可重复的方式自动完成所有不能用手工方式实现的过程是不可能的。多年来，计算机软件的不可靠拖了自动生成软件的后腿。合并排序生成器已出现 50 多年了，但这个进步并没有在更复杂的应用程序中再现。其原因是，我们已经为合并排序程序编写出了准确、清晰的规范，而对于更复杂的应用程序，需要为哪怕一小段 HR 或供给/链应用程序编写规范。第一个问题是，需要开发出一种规范语言，它必须为任意应用程序提供非常清晰的表达能力，就像合并排序规范为其应用程序提供的表达能力一样。近年来，随着模式语言(Pattern Languages)及实现该语言的 DSDL 的问世，这个问题已经取得了相当大的进展。第二个问题是不应单纯以描述的方式理解软件开发过程。本书探讨的理论和示例提出了 5 个设计技术，就是对软件开发过程在这方面的一种尝试。在硬件的产品设计和制造过程中已在试用和测试这些技术，但它们还没有以系统的方式应用于软件的开发过程。本书将进行这方面的尝试，所以可作为软件开发过程的入门级图书和手册。实际上，本书囊括了这些设计技术在软件设计与开发上的所有应用，因此也是这方面的一个先锋。

我同意本书作者的观点：商用应用程序软件的未来依赖于基于规范的语言。本书将是从当今质量不高、手工创建的软件过渡到未来自动生成的、可完全信赖的软件的一座桥梁。

H. Richard Lawson，Lawson 软件公司副总裁

目　录

第Ⅴ部分　6个案例分析

第Ⅰ部分

当今的软件开发过程及其缺点，可信赖软件的挑战

第 1 章

当前的软件开发方法

停止对检验的依赖，就会提高质量。

——W. 爱德华兹·戴明

质量涉及许多方面，每个方面的改进都是一个进步。

——C.V.Ramamoorthy

简介

人员的能力和企业的服务器软件一般都会给用户带来缺陷，在计算时代的早期，这称为 bug。这个错误率及其给操作带来的故障，在今天销售的制成品或“硬件”成品中是无法容忍的。但软件不是一个像机械设备、家用器具或台式计算机那样生产出来的产品。自从 1946 年 ENIAC 问世以来，编程就是一个混合了智力和经济的活动，为了使软件程序像运行它们的计算机硬件一样可靠，人们投入了极大的精力。与大多数制成品不同，软件不断地重新设计和升级，因为系统组件要使一般用途的计算机适应各种不断变化的、有特殊用途的应用程序。需求在不断变化，软件程序也必须不断变化，以满足这些需求。在过去的 50 年中，人们开发出了大量的技术使软件更可靠，更可信赖。本章将回顾软件开发的主要模型，根据过去的最佳实践方式，找出一个健壮的软件开发模型，同时融合最近推出的编程技术。健壮软件开发模型(Robust Software Development Model，RSDM)承认，尽管软件是设计和“制造”出来的，但并不是一般意义上的“制造”。而且，软件开发更迫切地需要在上游阶段解决质量问题，因为几乎所有的软件缺陷都是在上游阶段引入的。DFTS 用健壮软件开发模型、软件设计优化工程和面向对象的设计技术解决了生产可信赖软件的问题。

本章内容

- 软件开发：需要一种新的模式
- 软件开发战略和生命周期模型
- 软件过程改进
- ADR 方法
- 健壮软件开发过程的 7 个要素
- 健壮软件开发模型
- 要点
- 其他资源