国外计算机科学教材系列

净室软件工程：技术与过程

Cleanroom Software Engineering

Technology and Process

[美] Stacy J. Prowell　Carmen J. Trammell　Richard C. Linger　Jesse H. Poore　著

贡可荣　张志祥　张秀山　等译

電子工業出版社
Publishing House of Electronics Industry
URL:http://www.phei.com.cn

国外计算机科学教材系列

净室软件工程：技术与过程

Cleanroom Software Engineering: Technology and Process

[美] Stacy J. Prowell　Carmen J. Trammell
Richard C. Linger　Jesse H. Poore　著

贲可荣　张志祥　张秀山　等译

電子工業出版社
Publishing House of Electronics Industry
北京·BEIJING

内 容 简 介

本书描述了由 IBM 公司开创的开发零缺陷或接近零缺陷的软件的成功做法。这个方法就是净室软件工程。产生净室软件工程的动机是提高软件的可靠性和费效比，并结合了项目管理的基于工程的技术、基于对象的系统认证、正确性验证和统计质量认证等技术。软件组织使用净室过程能够在其软件开发、性能方面有本质改进，在可靠性、生产率两方面形成竞争优势。作者根据他们在工业中应用的深刻体会，详细叙述了净室开发和认证过程，并阐述了这个过程是如何与 SEI 的 CMM 相吻合的。本书包含实例研究，并总结了应用于工业的关键净室实践，包含了可用于实际的许多技巧。本书可作为计算机专业高年级本科生、研究生的软件工程教材，亦可作为软件开发者、组织者和管理者的参考书。

Authorized translation from the English language edition published by Addison-Wesley. Copyright © 2000.
All rights reserved. No part of this book may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying, recording or by any information storage retrieval system, without permission from Publisher.
Simplified Chinese language edition published by Publishing House of Electronics Industry. Copyright © 2001.
本书中文简体专有翻译出版权由 Pearson 教育集团所属的 Addison-Wesley 授予电子工业出版社。其原文版权及中文翻译出版权受法律保护。未经许可，不得以任何形式或手段复制或抄袭本书内容。

图书在版编目(CIP)数据

净室软件工程：技术与过程 /(美)斯泰西(Stacy. J. P)等著；贲可荣等译. —北京：电子工业出版社，2001.6
(国外计算机科学教材系列)
书名原文：Cleanroom Software Engineering: Technology and Process
ISBN 7-5053-6726-9

Ⅰ.净… Ⅱ.①斯…②贲… Ⅲ.软件工程-高等学校-教材 Ⅳ.TP311.5

中国版本图书馆 CIP 数据核字(2001)第 036706 号

丛 书 名：国外计算机科学教材系列
书　　名：**净室软件工程：技术与过程**
原 书 名：Cleanroom Software Engineering: Technology and Process
著　　者：[美]Stacy J. Prowell　Carmen J. Trammell　Richard C. Linger　Jesse H. Poore
译　　者：贲可荣　张志祥　张秀山　等
责任编辑：宗　钢
排版制作：电子工业出版社计算机排版室监制
印 刷 者：北京东光印刷厂
出版发行：电子工业出版社　URL：http://www.phei.com.cn
　　北京市海淀区万寿路 173 信箱　邮编 100036　电话：68279077
经　　销：各地新华书店
开　　本：787×1092　1/16　印张：16.75 字数：428.8 千字
版　　次：2001 年 6 月第 1 版　2001 年 6 月第 1 次印刷
书　　号：ISBN 7-5053-6726-9 / TP·3758
定　　价：25.00 元
版权贸易合同登记号　图字：01-2000-3078

凡购买电子工业出版社的图书，如有缺页、倒页、脱页，请向购买书店调换。
若书店售缺，请与本社发行部联系调换。电话：88211980　68279077

出 版 说 明

随着21世纪的到来，计算机技术的发展更加迅猛，在各行各业的应用更加广泛，越来越多的高等院校增设了有关计算机科学的课程内容，或对现有计算机课程设置进行了适当调整，以紧跟前沿技术。在这个教学体系和学科结构变革的大环境下，对适合不同院系、不同专业、不同层次的教材的需求量与日俱增。此时，如果能够借鉴、学习国外一流大学的先进教学体系，引进具有先进性、实用性和权威性的国外一流大学计算机教材，汲取其精华，必能更好地促进中国高等院校教学的全面改革。

美国Prentice Hall出版公司是享誉世界的高校教材出版商，自1913年成立以来，一直致力于教材的出版，所出版的计算机教材为美国众多大学采用，其中有不少是专业领域中的经典名著，已翻译成多种文字在世界各地的大学中使用，成为全人类的共同财富。许多蜚声世界的教授、学者都是该公司的资深作者，如道格拉斯·科默（Douglas E. Comer）、威廉·斯大林（William Stallings）等。早在1997年，电子工业出版社就从Prentice Hall引进了一套计算机英文版专业教材，并将其翻译出版，同时定名为《国外计算机科学教材系列》（下称：第一轮教材）。截至2000年12月，该系列教材已出版23种，深受读者欢迎，被许多大学选为高年级学生和研究生教材或参考书。

4年过去了，已出版的教材中多数已经有了后续版本。因此，我们开始设计新一轮教材（第二轮教材）的出版，成立了由我国计算机界著名专家和教授组成的“教材出版委员会”，并结合第一轮教材的使用情况和师生反馈意见，组织了第二轮《国外计算机科学教材系列》出版工作。

第二轮教材的出版原则为：

1. 引进Prentice Hall出版公司2000年和2001年推出的新版教材，作为替换版本。
2. 在著名高校教授的建议下，除了从Prentice Hall新选了一些教材之外，还从McGraw-Hill和Addison Wesley Longman等著名专业教材出版社、麻省理工学院出版社和剑桥大学出版社等著名大学出版社引进了一些经典教材，作为增补版本。
3. 对于第一轮中无新版本的优秀教材，我们将其作为沿用版本，直接进入第二轮使用。
4. 对于第一轮中翻译质量较好且无新版本的教材，我们将其进行了修订，也作为沿用版本，进入第二轮使用。

这次推出的教材覆盖学科范围广、领域宽、层次多，既有本科专业课程教材，也有研究生课程教材，以适应不同院系、不同专业、不同层次的师生对教材的需求。广大师生可自由选择和自由组合使用。

按照计划，本轮教材规划出版37种，其中替换版本8种，新增版本14种，沿用版本15种。教材内容涉及的学科方向包括网络与通信、操作系统、计算机组织与结构、算法与数据结构、数据库与信息处理、编程语言、图形图像与多媒体、软件工程等。本轮教材计划于2001年7月前全部出版。教材的使用年限平均为3年。我们还将陆续推出一些教材的参考课件，希望能为授课老师提供帮助。

为了保证本轮教材的选题质量和翻译质量，我们约请了清华大学、北京大学、北京航空航天大学、复旦大学、上海交通大学、南京大学、浙江大学、哈尔滨工业大学、华中科技大学、西安交通

大学、国防科学技术大学、解放军理工大学等著名高校的教授和骨干教师参与了本轮教材的选题、翻译和审校工作。他们中既有讲授同类教材的骨干教师和博士，也有积累了几十年教学经验的教授和博士生导师。

在本轮教材的选题、翻译和编辑加工过程中，为提高教材质量，我们做了大量细致的工作，包括：

1. 对于新选题和新版本进行了全面论证。
2. 对于沿用版本，认真审查了前一版本教材，修改了其中的印刷错误。
3. 对于译者和编辑的选择，达到了专业对口。
4. 对于从英文原书中发现的错误，我们通过与作者联络、从网上下载勘误表等方式，一一做了修改。
5. 对于翻译、审校、编辑、排版、印刷质量进行了严格的审查把关。

通过这些工作，保证了本轮教材的质量较前一轮有明显的提高。相信读者一定能够从字里行间体会到我们的这些努力。

今后，我们将继续加强与各高校教师的密切联系，为广大师生引进更多的国外优秀教材和参考书，为我国计算机科学教学体系与国际教学体系的接轨做出努力。

由于我们对国际计算机科学、我国高校计算机教育的发展存在认识上的不足，在选题、翻译、出版等方面的工作中还有许多有待提高之处，恳请广大师生和读者提出批评和建议。

电子工业出版社

2001 年春

此为试读，需要完整PDF请访问：www.ertongbook.com

教材出版委员会

主　任　杨芙清　北京大学教授
中国科学院院士
北京大学信息与工程学部主任
北京大学软件工程研究所所长

委　员　王　珊　中国人民大学信息学院院长、教授

胡道元　清华大学计算机科学与技术系教授
国际信息处理联合会通信系统中国代表

钟玉琢　清华大学计算机科学与技术系教授
中国计算机学会多媒体专业委员会主任

谢希仁　中国人民解放军理工大学教授
全军网络技术研究中心主任、博士生导师

尤晋元　上海交通大学计算机科学与工程系教授
上海分布计算技术中心主任

施伯乐　上海国际数据库研究中心主任、复旦大学教授
中国计算机学会常务理事、上海市计算机学会理事长

邹　鹏　国防科学技术大学计算机学院教授、博士生导师
教育部计算机基础教学课程指导委员会副主任委员

张昆藏　青岛大学信息工程学院教授

译 者 序

随着社会对软件的日益依赖，软件故障的风险也越来越大，软件事实上已成为全球经济的中枢。但是，现今大部分的软件仍是由技术工人利用其掌握的技能和经验编制出来的，往往不能确保质量和进度，许多软件项目在一定的复杂度下便易于崩溃，根本不能作为有用系统，而且，这种系统若用于关键领域或要害部门，往往会带来严重的社会经济后果。

净室软件工程是一种具有坚实理论基础的软件工程技术。再好的管理也代替不了理论基础。净室理论基础由资深数学家 Harlan Mills 及其 IBM 的同仁于 20 世纪 80 年代初建立起来，首次提出了将函数理论和统计学应用于软件设计、测试和认证的软件工程领域，并集成了结构化编程、逐步求精、模块化设计的精髓。

20 世纪 90 年代初，IBM 运用净室方法开发了一种称为"海量存储控制单元适配器"的电子产品，售出了数千台，直至 1997 年超寿命使用后，仍未收到任何关于净室微码故障的报告！美国国家宇航局和国防部等大型机构均采用净室方法进行了大量实践，实践表明，采用净室方法可大大提高软件质量和生产力。

净室软件工程技术的引进势必为我国的软件产业提供一个更有效的设计和认证思路，为进一步落实软件质量保证政策提供有效途径。我们翻译此书的目的也就在此。

10 年前，贲可荣博士在陈火旺院士的指导下，开始从事软件工程的研究工作。近几年，在刘孟仁教授领导下，贲可荣博士开展了海军软件可靠性研究工作；与沈恩绍教授在国家自然科学基金方面的合作，开展了形式化方法应用研究。作为武汉大学软件工程国家重点实验室的访问学者，贲可荣博士与毋国庆教授、何炎祥教授、徐仁佐教授进行过深受教益的讨论。在齐治昌教授负责的 863 项目中，贲可荣博士开展了净室软件工程方面的学习和研究工作，与张志华博士、徐锡山博士、王戟博士经常性讨论，开阔了思路。

本书的序、前言、第 5、10 章和第 15 章由张秀山译校，第 4、8、9 章和第 16 章由张志祥译校，其余章节由贲可荣译校。全书由贲可荣审校。曾浩、张宇、曹方、苑青、舒畅、王德恒和徐荣花等参与了本书的翻译工作，在此表示感谢。

由于译者自身的知识局限和时间的仓促，译稿难免存在错误和疏漏。欢迎读者批评指正。

本书可作为计算机专业高年级本科生、研究生的软件工程教材，亦可作为软件开发者、组织者和管理者的参考书。

序

本书介绍了净室软件工程技术及管理，概述了净室在软件工程项目中的应用和软件管理、开发及测试的路线图(road map)。本书可作为未接触过净室软件人员的引论性教材，也可作为日渐增多的净室软件实践者的参考书。

本书分三大部分：

1. 第一部分：净室软件工程基础。介绍净室理论及工程实践。净室主要实践为：统计质量控制下的增量开发，基于功能的规范、开发及认证，以及基于使用模型的统计测试。净室参考模型(CRM)被作为整个净室工程过程的框架来介绍。在本部分中，举出一个小例子——安全警报以说明实践和产品。
2. 第二部分：净室软件工程参考模型。提供一种可被软件工程机构采用、剪裁和发挥的过程模型。CRM 用 14 个净室过程，20 个工作产品表示。每一过程按增强的 ETVX(入口，任务，验证，出口)模型定义。CRM 是净室项目性能及过程改进的指南。第 11 章叙述了软件能力成熟模型关键过程域与 CRM 之间的关系。
3. 第三部分：净室软件工程实例研究，讲述了一个大型实例——卫星控制系统，包括在净室项目中产生的关键技术工作产品：盒式结构规范及设计，使用模型及其分析。

通常，净室技术不需专门的工具就可使用。比如：盒式结构规范及设计可用传统的文字处理器和模板予以记录。然而，工具却常常可以简化和改进净室实践，有助于其升级为更大的系统。因此，本书中的主要实例都由净室工具产生输出，以做进一步分析和理解。

本书旨在使管理和技术人员对净室技术有所了解，提供管理净室项目的总的过程框架。第一部分讲述了净室理论及实践方法，适用于所有读者；第二部分定义了净室过程，既可用于管理活动的参考，又可作为其指南；第三部分中研究的实例将帮助读者对净室项目的产品有所了解，同时可看到如何将净室应用于自己的项目中去。

我们还将此书推荐给学习计算机科学及软件工程的本科生和研究生，使学生懂得大规模软件工程的智能控制的价值及必要性，以及为达到此目的而使用的技术和过程的重要性，对学生尤为重要的是理解增量开发的生命周期、精确规范设计和验证的方法和基于使用测试认证软件的应用。

前　言

我们的软件社会

计算机软件从它50年前的平凡起步，已经发展成为现代社会中的关键一环，影响着全球人类活动的各个领域。软件技术渗透到各种产品和服务中，成为贸易、企业、政府和国防的主要能动主体(agent)。每天，数以万亿的工作由软件来完成，从个人计算机应用到大规模、全球联网的极其复杂的系统，诸如生产、信贷和金融服务、通信、医疗服务；能源、交通、教育等经济部门及国防和政府部门无不依赖软件实现其日常运作。可以毫不夸张地说，现代社会的进步完全地、不可逆转地依赖于软件。

因此，软件已成为全球经济的中枢。计算机硬件产业依赖软件给其机器带来活力，各种产业及服务业要依赖软件来提高生产力，激发其员工的创造性。软件是变革的深层动力，使公司或工作能以前所未有的规模进行重组。通过脑力劳动的自动化及量的增加，软件正在促使全球经济发生着深刻的结构性变革，这种变革不亚于上个世纪通过手工劳作的自动化而产生的工业革命。总之，软件已成为一种关键资源——对致富和竞争力至关重要的资源。

随着社会对软件的日益依赖，软件失效的风险也越来越大。现今大部分的软件是由技术工人利用其掌握的技能编制出来的，不能产生一致的结果，这些技术完全不具备其他工程学科所具有的基于理论的严格的加工特点。结果，软件故障经常发生，常常带来严重的社会经济后果。许多软件项目在不能控制复杂度的重负下崩溃了，根本不能作为有用系统。

软件开发是一项挑战人类认知和控制极限的任务。不过，却有着一门科学和工程知识来指导软件工程走向有规则可寻的过程，这门知识就是建立在净室软件工程基础之上的。

净室软件工程

净室是一种以合理的成本开发高质量软件的基于理论、面向工作组的方法。净室是基于理论的，因为坚实的理论基础是任何工程学科所不可缺少的。再好的管理也代替不了理论基础。净室是面向工作组的，因为软件是由人开发出来的，并且理论必须简化到实际应用才能引导人的创造力和协作精神。净室是针对经济实用软件的生产的，因为在现实生活中，业务和资源的限制必须在软件工程中予以满足。最后，净室是针对高质量软件的生产的，因为高质量改进管理，降低风险及成本，满足用户需求，提供竞争优势。

开发与演示

净室理论基础建立于20世纪70年代末80年代初，资深数学家和IBM客座科学家Harlan Mills阐述了将数学、统计学及工程学上的基本概念应用到软件的设想。受Edsger Dijkstra关于结构化编程、Nicholas Wirth关于逐步求精、David Parnas关于模块化设计的影响，Mills为软件的工程方法奠定了科学基础。

两大基本观点促进了Mills的工作：首先，程序是数学函数规则，其次，潜在的程序执行是无穷的，质量认证必须进行统计采样。第一个观点使所有函数理论向软件开发敞开大门，导致

以下技术的产生:盒式结构规范及设计、函数理论正确性检验及增量开发,第二个观点使所有统计理论在软件测试方面得到应用,导致了统计使用测试和质量认证。

Mills 的观点在其与同仁 Alan Currit, Michael Dyer, Alan Hevner, Richard Linger, Bernard Witt 及 IBM 公司联邦系统部的其他同事的合作中得到了修改和演示。1979 年由 Addison-Wesley 出版的《结构化编程:理论与实践》(作者:Linger, Mills 和 Witt)介绍了软件规范、设计、认证及再工程中的函数理论方法。《信息系统分析和设计原理》(作者:Mills, Linger, Hevner, Academic 出版公司,1986)介绍了系统规范、设计和认证中的盒式结构方法,同时介绍了项目管理的增量开发。1987 年,净室将这些思想融合在一起。"净室"一词借自半导体业,强调"防患胜于除患"的思想。《净室软件工程》(作者:Mills, Dyer 和 Linger)刊登于《IEEE 软件》1987 年 5 月刊上。

第一项净室软件项目由 IBM 的 Richard Linger 于 20 世纪 80 年代中期负责实施。COBOL 结构化设施项目开发出一项商业软件再工程产品,该产品显示出了卓越的质量水平及用户使用可靠性,净室方法得到了初步确认。

确认和实践

1990 年,Richard Linger 创建了 IBM 净室软件技术中心,在此,净室方法、自动化及技术改变得到进一步改进。20 世纪 90 年代初,IBM 生产出运用净室方法开发的海量存储控制单元适配器,售出了数千单元,直至 1997 年产品超过使用寿命后,仍未收到任何反映净室微码现场故障的报告。这项开发由 Mike Brewer 领导,成员有 Paul Fisher, Dave Fuhrer, Karl Nielson 及其他一些工作组成员。认证测试由 Joe Ryan 和 Mike Houghtaling 领导。如今,IBM 公司存储系统部的测试实验室无可争议地成为统计使用测试方法的全球巨擎。

从 20 世纪 80 年代末到 90 年代初,享有盛名的国家宇航局(NASA)哥达德飞行控制中心(GSFC)软件工程实验室(SEL)在 Vic Basili, Scott Green, Rose Pajerski, Jon Valett 等人的领导下进行了一系列净室试验。这些试验被认为是迄今为止软件工程领域进行的一次最完整的研究。4 个规模依次扩大的地面控制软件系统按净室工程方法开发出来,结果表明,与 NASA GSFC 已足以让人佩服的底线相比,质量和生产力还有一致的提高。

20 世纪 80 年代中期,在美国国防部的 ARPA STARS 项目(自适应的可靠系统软件技术)的形成期,STARS 领导层选取净室作为开发和商业化的核心技术。领导层包括 Dave Ceely, Dick Drake, Bill Ett, Joe, Greene, John Foreman, Jim Moore 等。Mills 博士和 Arnie Beckhardt 为推动净室技术而建立的软件工程技术公司(SET)被选来推动净室技术的商业化,在 STARS 的支持下,SET 在净室的手段和工具方面取得了显著进展。

与此同时,Mills 博士正就使用净室建立一家名为 Q-Labs 的公司而同欧洲的 I. M. Ericsson AB 进行商谈,为软件工程新技术走出实验室,向 Ericsson(爱立信,译者注)进行转让。自两家公司成立之初,Q-Labs 和 SET 就是商业伙伴,以后两家公司于 1998 年合并为 Q-Labs 公司。

20 世纪 90 年代初,美国陆军 Picatinny Arsenal 执行了一个净室项目,并在这个项目中获得了 20 倍于引进净室技术所用的投资回报。1996 年国防部软件数据与分析中心在其所作的软件方法比较分析中,报告净室具有真实的价值和质量优势。其他留有软件生产和质量方面历史数据的机构也用净室进行了大型项目的研发,它们公开发表了其结果。净室实践明显改进了 IBM、Ericsson、NASA、DoD 及许多其他机构的软件项目产出。净室的数据表明而且将继续表明,采用净室学科有可能使软件成组性能得到很大的改善。

Carnegie Mellon 大学软件工程研究所(SEI)实际上已成为改进软件工程实践方面的领头羊。SEI 的软件能力成熟度模型(CMM)成为一项已被认可并广泛用于改善软件工程实践的管理模型。1996 年 SEI 完成了一个项目,该项目定义了净室参考模型并将净室的工程技术映射到 CMM 的管理过程中。这项工作的主要结论是净室与 CMM 是兼容的、相互支持的。该工作在 1996 年 2 份 SEI 技术报告中进行推广:净室软件工程参考模型(Linger, Trammell, 1996)和软件能力成熟度模型(CMM)的净室软件工程实践(Linger, Paulk, Trammell, 1996)。经 Carnegie Mellon 大学许可,本书将净室软件工程参考模型也纳入其中。

净室技术一直由 Mills 及其在全球各大学和工业界的同仁进行讲授,他们是 Vic Basili, Alan Hevner, Richard Linger, Jesse Poore, Dieter Rombach, Shirley Becker, Richard Cobb, Michael Deck, Chuck Engle, Philip Hausler, Ara Kouchakdjian, John Martin, Dave Pearson, Mark Pleszkoch, Stacy Prowell, Steve Rosen, Kirk Sayre, Alan Spangler, Carmen Trammell, Gwen Walton 和 James Whittaker。另外,还有很多人通过大量实地应用而推进净室实践,包括 Mike Brewer, John Gibson, Mike Houghtaling, David Kelly, Jenny Morales, Rob Oshana, Jason Selvidge, Wayne Sherer 和 Tom Swain。他们每个人都为净室成为真正的软件工程学科做出了各自的贡献。

不断发展

一项工程的发展是以其科学理论为基础的,实践中的改进从遵循源自实践的第一条原理开始并沿着科学的轨道向前发展。净室实践的改进和进展正是按照这种模式进行并将继续进行下去。

净室规范方法的精化的研究主流已经形成并在本书中予以说明。Mills 使用的函数理论,激发了 David Parnas 在序列(跟踪)分析和域划分方面的工作,这又激发了 Hailong Mao 在典型序列历史方面的研究,以上三者为本书中提到的 Stacy Prowell 和 Jesse Poore 基于序列规范的定义打下了基础。

另一项由 Gwen Walton 和 Jesse Poore 所从事的独立的研究,将基于 Markov 链使用模型应用到了运筹学的优化方法当中。他们的研究将基于约束的方法应用到使用建模中,该研究有望加强净室统计测试实践的控制,提高其价值。

其他在决策理论、先进统计设计、建模与仿真等有关理论和工程实践领域内开展的工作正在取得进展,净室软件工程也一定会随着得到进一步的改进。

此为试读,需要完整PDF请访问: www.ertongbook.com

目　　录

第一部分

净室软件工程基础

此为试读，需要完整PDF请访问：www.ertongbook.com