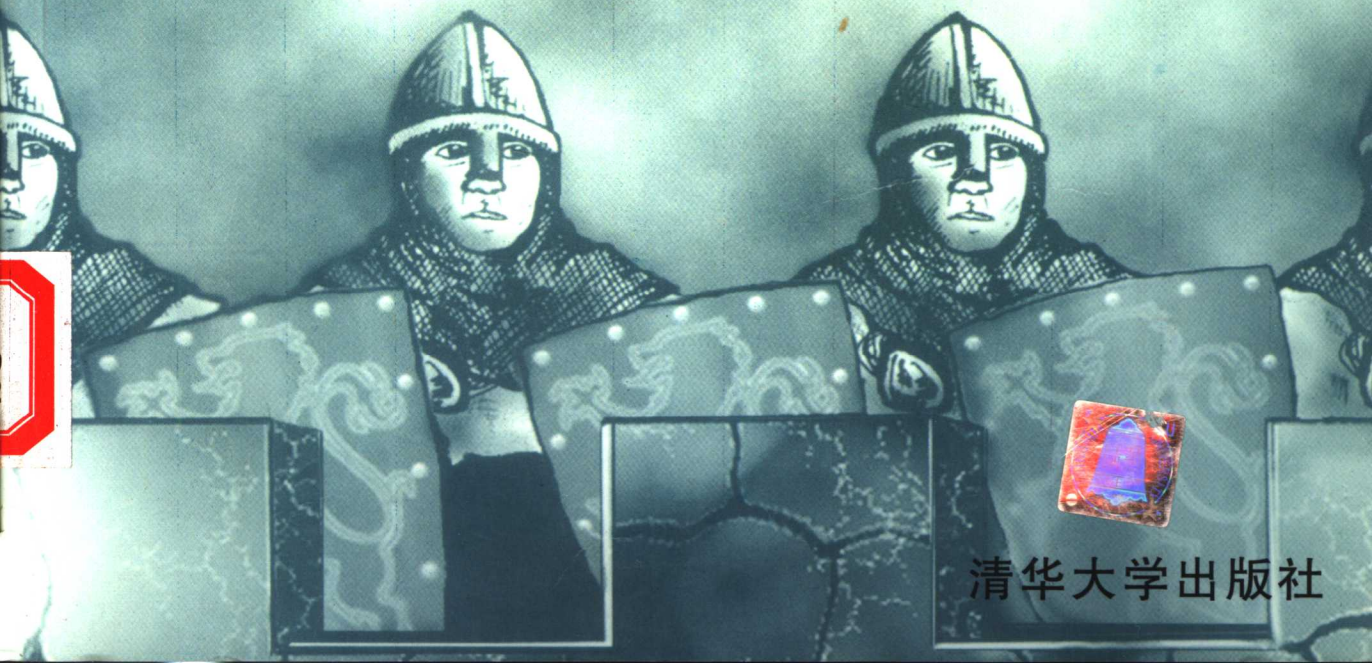
[英]Felix Redmill Chris Dale 编著
郑人杰 温以德 等译

# 计算机应用系统的可信性实践

## Life Cycle Management For Dependability



清华大学出版社

# 计算机应用系统的可信性实践

[英]Felix Redmill　Chris Dale　编著

郑人杰　温以德　等 译

清华大学出版社

北　京

## 内 容 简 介

本书讲述如何实现系统的可信性，以可信性的管理为核心内容，及时地提出各种忠告。各章节都包含一个特定的主题：从企业可信性、方针与风险，到开发与测试，运行与维护。每一章节都注重实践，提供实用的建议，用相关事例或案例来支持所要阐述的理论。

本书适用于与计算机系统有关的任何管理者。



北京市版权局著作权合同登记号　图字 01-2002-6318 号

**图书在版编目(CIP)数据**

计算机应用系统的可信性实践/(英)瑞得米尔，(英)德尔编著；郑人杰等译．—北京：清华大学出版社，2003.3
ISBN 7-302-06412-1

Ⅰ.计…　Ⅱ.①瑞…②德…③郑…　Ⅲ.计算机系统－系统管理　Ⅳ.TP338

中国版本图书馆 CIP 数据核字(2003)第 018767 号

**出 版 者**：清华大学出版社(北京清华大学学研大厦，邮编 100084)
http://www.tup.tsinghua.edu.cn
http://www.tup.com.cn
**责任编辑**：汤斌浩　丁朝欣　胡先福
**印 刷 者**：世界知识印刷厂
**发 行 者**：新华书店总店北京发行所
**开　　本**：787×960　1/16　**印张**：12.5　**字数**：281 千字
**版　　次**：2003 年 3 月第 1 版　2003 年 3 月第 1 次印刷
**书　　号**：ISBN 7-302-06412-1/TP·4831
**印　　数**：0001～3000
**定　　价**：30.00 元

# 序

用简单的语言描述什么是可信性系统是一件相对容易的事。可信性系统就是做人们希望它做的事，不做人们不希望它做的事，这样我们才可以有充分的理由信赖这样的系统。因此，“可信性”作为一个集合名词，它包含了一系列特定的系统特性，诸如“安全性”和“可靠性”等。

然而，建立一个可信性的系统远比提供简单的定义困难得多。从设计可信性的具体属性，到确定用户主要依赖的属性，以及在这些属性之间、在属性与开发成本与进度间取得平衡，每一步都不是一件容易的事。而且，随着需求、设计、实现或操作复杂性的增加，实现可信度的难度还会迅速攀升。但是，无可否认的是，数字计算机的出现已经使我们能够以相对低廉的成本建立复杂性极高的系统。

列举出有利于提高可信性的方法和技术是一件很容易的事。其中有一些是一般性的；一些着眼于系统的某一特定的层面、生命周期或工业部门；还有一些则追求完美，力图弥补现存的不足。这些方面的有关内容可以从相关会议的报道、期刊或书籍中获得，更具体的规定则以工业部门的标准、指南的形式出现。

比从技术上(常常是不完整地)描述实现可信度的方法更加困难的是：在系统开发(和运行)过程中建立和实施一种工作程序，以确保在特定系统中达到必要的可信性水平。这是首要的，并且是最重要的管理任务。然而，根本的问题是高层管理必须意识引并认可，为了实现可信性系统的需求需要在整个生命周期的开发过程中进行适当的投资。项目管理者必须利用和监督开发过程，按照可信性目标制定政策和开展工作。就本质而言，开发一个可信性系统最需要的就是有一个可信的机制。

目前，在可信性这一至关重要的领域仍缺乏管理方面的指导。对有效指导的需求非常明显而且迫切：缺乏可信性可以导致巨大的经济损失，如 1996 年 Ariane 5 型火箭发射时的爆炸所造成的惊人的灾难；缺乏可信性还可能引致生命的丧失，人类已在 1986 年美国 Therac 事件中经历了这一可怕的遭遇。

本书以可信性的管理为核心内容，及时地提出各种忠告。各章节都包含一个特定的主题：从企业可信性文化、方针与风险，到开发与测试，运行与维护。每一章节都注重实践，提供实用的建议，用相关事例或案例来支持所要阐述的理论。

本书源于英国安全与可靠性俱乐部，该俱乐部始终坚持从管理的角度来讨论可信性的问题。由于编辑和作者的共同努力，这一目标终于得以实现。在此，我郑重地推荐这本书，向所有希望建立和运行可信性系统的管理者，尤其是那些还没有形成可信性观念的管理者。

汤姆·安德森

# 前　言

本书讲述如何实现系统的可信性，适用于与计算机系统有关的任何管理者。本书所要论述的主要问题是“可信性”、“管理”和“系统”。在此，先对每一个概念作一个简单的阐述。

“可信性”被定义为“一个系统的可信赖性，这种可信赖性使系统在向用户提供服务时，用户所看到的系统行为，公正地说，也具有可靠性”。其实，用户的观点往往和他们的权益联系着，他们的权益又与系统运行的效果相关。这些就构成了可信性的一系列属性：安全性、可靠性、可获得性、机密性、完整性和可维护性。在某一特定系统中具体要求哪些要素具有可信性，这要由项目的提出者作出规定。

本书中所指的“系统”是以软件为基础的系统。我们在很大程度上依赖软件系统：不仅在工商业领域，甚至在政府部门、商务活动及人们的日常行为中。软件系统的可信性至关重要——这种重要性不仅表现在使用的可获得性、数据的完整性或机密性、服务的可信性，而且表现在软件系统所影响的事物的安全性等方面。然而，本书中所描述的原理不仅局限于计算机系统，它适用于任何系统，包括需要具有可信性的组织。

“管理”意味着承担可信性的责任，并采取必要的措施实现可信性。直到最近，还有很多人认为获得系统的可信性完全是技术问题，但同时，更多的人认识到系统的可信性是一个管理责任的问题。实际上，尤其是当安全性遭到破坏时，人们往往发现管理负有不可推卸的责任，不仅因为它没能确保系统的可信性，更因为它未能在组织中建立并保持可信性的企业文化。

在可信性要求很高的地方，仅仅力图达到可信性是不够的。管理上还必须建立可信性的标准，制定实行这一标准的计划，得到使人相信系统运行能够达到可信性标准的证据，并在实践中进行监控。这样，在系统生命周期的不同阶段，管理的重点也将随之变动：开发阶段适用的管理方法对运行、维护或变更阶段可能不再适用。

本书的第一章讲述可信性的一般概念、定义，为后面的章节作一些铺垫。第二章论述企业的可信性文化，讨论在生命周期各阶段中的管理问题，这些问题在其他技术类书籍中很少提及——但它对所有的现代管理者却是一个很重要的问题；第三章论述策略和计划；第四章论述检测及评估，首先讨论生命周期不同阶段中的关键问题，然后提出如何将它们应用于实践中的建议；第五章论述项目管理；第六章讨论运行管理；第七章讨论维护及变更管理，其中论及特定的生命周期，并区别其在管理上的不同点；第八章解释风险管理及简单的实际应用，与第二章相同，它适用于系统生命周期的各个阶段。

作为编辑，我们为每一章邀请了相关领域的专家编写。即使这样，我们仍然做了细致的编审，以确保讲解的清晰性和全书的一致性。我们不希望破坏每位作者的独特风格，但更希望融汇各位专家的意见，并保证全书写作风格的统一性。

Felix Redmill & Chris Dale

1997 年 1 月

# 致　谢

我们向新城堡大学(University of Newcastle upon Tyne)的汤姆·安德森(Tom Anderson)教授表达我们的谢意，因为是安德森教授第一次向我们提出了写作此书的建议，而且还亲自为本书作序。

我们同时感谢各章节的每一位作者，感谢他们在写作期间以及在本书出版期间需要解决问题时所给予的合作。我们还要感谢伊丽莎白·爱瑞(Elizabeth Avery)帮助我们作了校对及提供了索引。

本书各章节的内容只反映每位作者的个人观点，并不一定是其雇主的意见。因此，书中所示的信息仅具参考性，并不能照搬用于实际工作，也不担保随之带来的任何后果。在这里我们谨代表作者向曾经给本书提出建议的人表示感谢，他们是：Ian Wand 和 Andy Vickers (第四章)；Eric Gilchrist, Paul Lucas 和 Stuart Nunns(第六章)；Sophia Langley 和 Steve Gandy(第八章)。

# 作 者 小 传

**罗宾·库克(Robin Cook)**

*伦敦地铁公司,E&M 设计部 安全&ARM 组,南卡罗那得30 号,卡内里渥夫,伦敦E14 5ET*

罗宾·库克受雇于伦敦地铁有限公司,是 Jubilee Line Extension 项目组的一个成员。他在该项目组工作的四年中,负责为项目中的电子及机械小组和承包商提供关于可靠性问题的指导。系统的广度以及承包商的背景要求他使用多种不同的手段,但必须保持兼容性和目标的一致性。他的主要工作是制订策略和计划,以有效而及时地获得可接受的系统可信性。

罗宾的职业生涯从电子和编程系统的设计开始。当他被要求展示查错统计及诊断需求时,他表现出对可信性分析技术的独特兴趣。这种兴趣在他作为可信性及可维护性问题顾问的四年当中得到了充分的发展,而他目前的工作更有助于此兴趣的发展。

**克里斯·德尔(Chris Dale)**

*CSC 索引研究与咨询服务公司,Bloomsbury 广场12 号,伦敦WC1 A 2LL*

自 20 世纪 80 年代早期以来,克里斯·德尔就投身于可信性计算领域。他曾经在英国国际计算机公司(ICL)、英国宇航局(British Aerospace)和英国原子能委员会(UK Atomic Energy Authority)任职。他是软件可信性研究中心的元老,该中心的成员都是英国软件可信性领域的专家。1992—1996 年期间,克里斯还曾一度担任过该中心的主任。近几年,他的工作主要包括与英国软件可信性及测量俱乐部(UK software Reliability and Metrics Club)的合作,担任 ENCRESS(欧洲软件可信性及安全性俱乐部网——European Network of Clubs for Reliability and Safety of Software)的领导职务等。目前,克里斯在 CSC 索引研究与咨询服务公司工作。

**路易丝·李(Louise Lee)**

*CITI 股份有限公司,Challenge House , Sherwood Drive , Bletchley MK3 6DP*

路易丝·李非常成功地领导了一些突破传统组织界限的变革活动,包括在一个功能强大的组织中引入客户支持策略;在高校管理机制中有效地引入质量管理系统,以及在大型技术密集型组织中设计并实现资源管理系统。

她曾在几家大的咨询公司工作,负责开发和改进公司项目管理过程的能力。作为 IT

密集型项目的成功的管理者，她对战略性项目，以及需要用户参与和早期承诺的项目的管理有特别的兴趣。

**汤尼·莱文尼(Tony Levene)**

*Quality Projects, Norgrey, Lower Wokingham Road, Crowthorne, RG 45 6DB（电话及传真：01344 780399）*

汤尼·莱文尼，质量项目(Quality Projects)主任，在电子及计算机系统工业领域有25年的技术、咨询和管理经验。质量项目旨在协助组织机构通过必要的变革过程以获得并保持竞争的优势。这些变革包括在所有层次上的文化以及态度的变化所引起的业务过程的变化。它的中心内容是通过项目及项目管理达到变革的目的。

汤尼的许多不寻常的经验和技能使他能够根据第一手经验及独特的方法来引入组织及业绩的改革措施，他的这些措施极大地吸引了那些对理论没有兴趣而更注重如何获得实效的客户。

汤尼是1995英国质量奖(UK Quality Award)的顾问，该奖项由英国质量基金会(British Quality Foundation)授予有突出贡献的组织，称他们为"优秀单位"。

**约翰·A·迈克得米德(John A McDermid)**

*约克大学计算机科学系，约克YOI 5DD*

约翰·A·迈克得米德是约克大学软件工程教授，领导高集成系统工程组(High Integrity Systems Engineering)。他的主要兴趣在以安全性为系统核心的软件工程，并使之应用于航天领域；他还领导BAe可信性计算系统中心(DCSC)及Rolls-Royce大学技术中心(UTC)的系统及软件工程工作。同时，他还是约克软件工程有限公司的主管，该公司提供与高集成系统领域相关的工具及咨询。

**法立斯·瑞得米尔(Felix Redmill)**

*红磨房咨询公司，22 Onslow Gardens，伦敦N10 3 JU*

法立斯·瑞得米尔是质量改进、项目管理和软件工程领域的顾问及讲师。他曾有22年在远程通信及计算工业等领域担任工程师和管理者的经验。现在，他是英国安全关键系统俱乐部的协调员，撰写并编辑过若干著作。

**爱尔文·斯高兹(Erwin Schoitsch)**

*奥地利研究中心，Seibersdorf，A-2444 奥地利*

爱尔文·斯高兹是奥地利研究中心信息技术部主任，领导信息技术的应用研究，主攻系统可信性、软件质量以及过程改进。同时，他也从事咨询工作。他所在的部门与奥地利及欧洲的其他工业伙伴、当地及联邦政府机构在许多项目上都有合作。

他积极参与国际标准化组织的工作，如国际电工委员会(IEC)和国际标准化组织(ISO)，以及它们在奥地利的分支机构，并在其中担任工作组主席、培训研讨会组织者及讲师等职务。他在本国及国际学术刊物上曾发表过多篇论文。

**盖·文格特(Guy Wingate)**

*欧技工程股份有限公司, Belasis Hall Technical Park , 克利夫兰 TS23 4YS*

盖·文格特是 Good Manufacturing Practice at ICI's Eutech Engineering 的管理者。Eutech 提供化学及医药工业方面的服务。文格特博士带领的工作组向英国大部分医药生产商及供应商提供项目管理的支持、咨询、监督及培训服务，包括自动化及工程方面的实践。文格特博士经常主持本国或国际学术会议，并在会上宣读论文，他还是 Automated Manufacturing: Good Practices and Case Studies 的编辑。文格特博士曾获达累姆(Durham)大学计算机系工程学士学位、高等电子学工程硕士学位以及工程学博士学位。

**克里斯朵夫·沃斯里(Christopher Worsley)**

*CITI 股份有限公司, Challenge House , Sherwood Drive , Bletchely MK3 6DP*

克里斯朵夫·沃斯里是 CITI 有限公司的管理经理。自 1986 年以来，他一直任项目管理部门的经理，负责大型组织机构项目管理的改进工作。

他曾参与许多工程及大型项目的工作，并担任项目管理者、项目业务经理、项目经理指导者、项目管理者顾问及项目评估者等职务。他还承担一些更具专业性的职务，如担任大型变更项目设计委员会的评审者，在跨国组织机构中担任 IS 策略可行性评估者。同时，他还是 Lloyds 管理机构中现代系统开发方法的倡导者。他曾发表过许多论文，论述项目管理、风险管理以及技术解决方案对管理的影响。

# 目　录