ITGOV LIBRARY

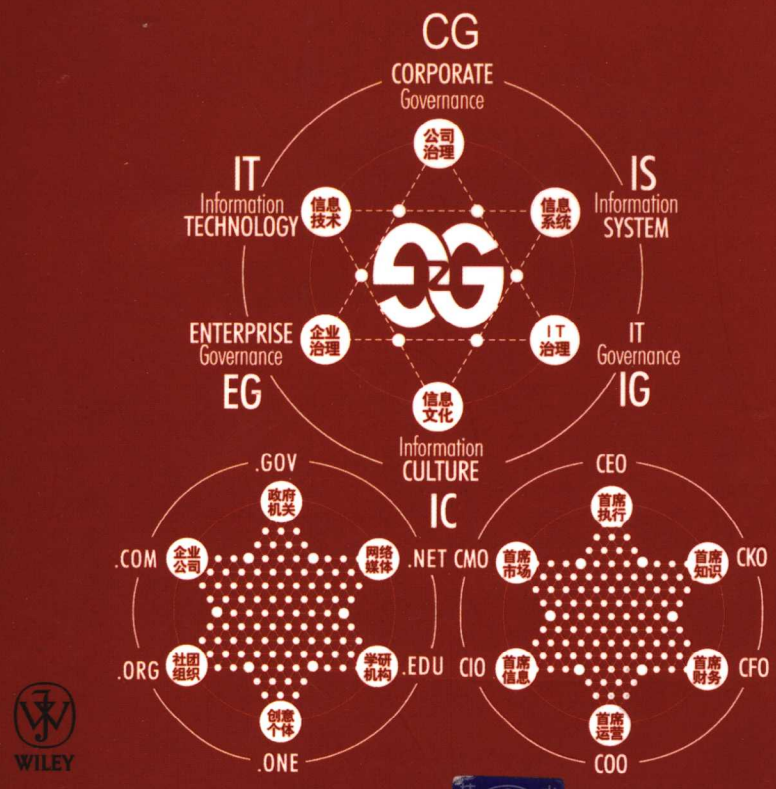
中国IT治理智库

ITGov.org.cn
中国IT治理研究中心

IT风险
基于IT治理的风险管理之道
Beating IT Risks

(英)Ernie Jordan　Luke Silcock　著
汤大马　译

ITGov中国IT治理研究中心　审校



WILEY

清华大学出版社

中国 IT 治理智库

IT 风险

—— 基于 IT 治理的风险管理之道

(英) Ernie Jordan 著
Luke Silcock
汤大马 译
ITGov中国IT治理研究中心 审校

清华大学出版社
北 京

Copyright © 2005 by Ernie Jordan and Luke Silcock. All Rights Reserved.

Beating IT Risks

All Rights Reserved. This translation published under license. Authorized translation from the English language edition published by John Wiley & Sons, Inc. company.

本书中文简体字翻译版由 John Wiley & Sons, Inc.授权清华大学出版社独家出版发行。此版本仅限在中华人民共和国境内(不包括中国香港、澳门特别行政区及中国台湾地区)销售。未经出版者预先书面许可，不得以任何方式复制或发行本书的任何部分。

北京市版权局著作权合同登记号　图字：01-2005-4072

本书封面贴有清华大学出版社防伪标签，无标签者不得销售。

版权所有，侵权必究。侵权举报电话：010-62782989　13501256678　13801310933

图书在版编目(CIP)数据

IT 风险—— 基于 IT 治理的风险管理之道/(英)乔丹，(英)赛尔库克著；汤大马译. —北京：清华大学出版社，2006.12

(中国 IT 治理智库)

书名原文：Beating IT Risks

ISBN 7-302-13947-4

Ⅰ.I…　Ⅱ.①乔…　②赛…　③汤…　Ⅲ.信息技术—高技术产业—风险管理　Ⅳ.F49

中国版本图书馆 CIP 数据核字(2006)第 120367 号

责任编辑：张立红(zlh-zlq@263.net)　陈　莉(clpear@163.com)

封面设计：王　岚

版式设计：孔祥丰

责任印制：孟凡玉

出版发行：清华大学出版社　　**地　　址**：北京清华大学学研大厦

http://www.tup.com.cn　　**邮　　编**：100084

c-service@tup.tsinghua.edu.cn

社 总 机：010-62770175　**邮购热线**：010-62786544

投稿咨询：010-62772015　**客户服务**：010-62776969

印 装 者：清华大学印刷厂

经　　销：全国新华书店

开　　本：169×240　**印　张**：21.5　**字　数**：375 千字

版　　次：2006 年 12 月第 1 版　　**印　　次**：2006 年 12 月第1 次印刷

印　　数：1～4000

定　　价：48.00 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：021583-01

内容简介

《IT风险》是一本机构或者企业IT管理和相关风险管理的指南。它为机构或者企业高级管理人员、IT经理和业务经理提供一套完整的有关IT管理和IT风险的实证模型和评价方法。结合具体案例和作者亲历的IT管理经验，本书从专家角度对各类IT风险以及应对策略进行了完整的阐述。本书的讨论涵盖了所有类型的IT风险。针对不同类型的机构和企业提出了最佳的IT风险管理方法。

本书适用于IT管理、业务管理人员；机构或企业的高级管理人员；风险管理人员；企业规划、咨询人员；相关专业学生。

作者简介

Ernie Jordan：澳大利亚悉尼麦考里大学商学院(世界商学院排名第50位)信息技术管理系管理学教授。从事IT治理、IT战略、操作风险和持续性方面的研究。在亚洲-澳大利亚地区，他是一名广受欢迎的演讲人。读者可以通过下列地址同Jordan博士取得联系：Ernie.Jordan@mq.edu.au

Luke Silcock：就职于PA咨询集团，为其全球众多重要客户提供有关IT管理方法的广泛咨询。在澳大利亚、英国和亚洲地区，他具有12年的管理咨询经验。主要集中在：总结和评估IT能力与成熟度；设计并领导IT效能改进措施；保证交付、降低风险、避免在IT驱动的业务项目中出现过度的费用膨胀。他还为伦敦和悉尼的毕马威管理咨询公司工作，专门从事IT咨询。

译者简介

汤大马：澳门某著名银行助理总经理，负责信息科技、电讯及产品规划工作。早年从事飞机机载计算机系统研究工作。20世纪90年代初加入中国银行，开始从事软件开发工作。先后参与、领导多项银行业务系统的开发、部署工作。负责省级分行的信息科技规划、管理工作。

主要工作方向：

A、银行IT基础设施建设与运营管理

B、IT宏观管理与企业应用架构

C、金融风险与企业技术风险管理

此为试读，需要完整PDF请访问：www.ertongbook.com

读者意见反馈卡

亲爱的读者：

感谢您购买了本书，希望它能为您的工作和学习带来帮助。为了今后能为您提供更优秀的图书，请您抽出宝贵的时间填写这份调查表，然后剪下寄到：北京清华大学出版社第五事业部(邮编 100084)；您也可以把意见反馈到 zlh-zlq@263.net。邮购咨询电话：010-62770175/77 转 3505。我们将充分考虑您的意见和建议，并尽可能地给您满意的答复。谢谢！

本 书 名：_____

个人资料：_____

姓　　名：_____ **性　别：**□男 □女 **出生年月(或年龄)：**_____

文化程度：_____ **职　业：**_____ **通讯地址：**_____

电话(或手机)：_____ **传　真：**_____ **电子信箱(E-mail)：**_____

您是如何得知本书的：_____

□别人推荐 □出版社图书目录 □网上信息 □书店

□杂志、报纸等的介绍(请指明)_____ □其他(请指明)_____

您从何处购得本书：□书店 □电脑商店 □软件销售处 □邮购 □商场 □其他

影响您购买本书的因素(可复选)：

□封面封底 □装帧设计 □价格 □内容提要、前言或目录 □书评广告

□出版社名声 □作者名声 □责任编辑

□其他：_____

您对本书封面设计的满意度：

□很满意 □比较满意 □一般 □较不满意 □不满意 □改进建议_____

您对本书印刷质量的满意度：

□很满意 □比较满意 □一般 □较不满意 □不满意 □改进建议_____

您对本书的总体满意度：

从文字角度：□很满意 □比较满意 □一般 □较不满意 □不满意

从技术角度：□很满意 □比较满意 □一般 □较不满意 □不满意

本书最令您满意的是：

□ 讲解浅显易懂 □内容充实详尽 □示例丰富到位

□ □指导明确合理 □其他：_____

您希望本书在哪些方面进行改进？_____

您希望增加什么系列的图书：_____

您最希望购买的其他图书：1._____ 2._____ 3._____ 4._____

您对使用中文版图书或外文版图书介意吗？更喜欢使用哪一种版本？

□介意 □无所谓 □中文版 □外文版

您的其他要求：_____

《中国IT治理智库》系列丛书专家委员会

（排名不分先后）

陈拂晓 国务院办公厅秘书局原局长、中国信息化推进联盟专家委员会副主席、中国信息化推进联盟IT治理专业委员会主任

李兆熙 国务院发展研究中心企业研究所副所长、研究员

杨立杰 中国人民银行内审司副司长

王智玉 审计署计算机中心主任

王东岩 劳动和社会保障部信息化工作领导小组副组长

李沁芳 中国金融电子化公司副总经理

汤大马 澳门大丰银行有限公司助理总经理

胡克瑾 同济大学经济与管理学院教授、博士生导师

丁　震 中国电信福建省电信有限公司副总经理、博士

仲安妮 中国工商银行稽核监督局副总经理

金磐石 中国建设银行股份有限公司监事、注册信息系统审计师

张　滨 中国移动通信集团公司管理信息系统部副总经理

张　艳 中国工商银行信息科技部副总经理

邹珊珊 中国光大银行稽核部副总经理

金　峰 新华人寿保险股份有限公司信息管理中心总经理

王　悦 振华石油控股有限公司总会计师

马卫国 中国北方工业公司信息资源部主任

文欣荣 中国铝业股份有限公司信息部副总经理

王继业 国电信息中心副主任

杜爱贞 信息产业部电子信息中心副主任

孙　强 ITGov 中国 IT 治理研究中心主任、注册信息系统审计师、认证信息安全管理专家

李文胜 新希望集团信息中心主任

王军民 奇正藏药集团信息管理部部长

李开祥 深圳市西乡人民医院信息科主任

胡丹露 中国人民解放军军事地理学会副秘书长

柳纯录 中国电子信息产业发展研究院总工程师

孟庆麟 ITGov 中国 IT 治理研究中心专家、注册 ISMS 主任审核员

吕本富 中国科学院研究生院管理学院副院长、教授

赵晓光 财政部信息中心运营维护处处长、高级工程师

李莞菁 中国网络通信集团公司企业信息化事业部副总经理

吴正宏 中国石油化工股份有限责任公司信息系统管理部副总工程师、教授级高工

陈淑平 中国联合通信有限公司计费、结算与信息系统部经理

李　东 北京大学光华管理学院教授、博士生导师，信息系统与物流管理系主任

董　焱 北京联合大学管理学院副院长、博士、教授

郝亚斌 中国电子视像行业协会副秘书长

刘　勤 上海国家会计学院信息部部长、教授

石宇良 北京市信息化工作办公室责任专家

刘复利 通信产业报社副社长

朱战备 上海贝尔阿尔卡特股份有限公司首席信息官、博士

王若讯 中海油信息技术中心主任

彭劲松 中国中化集团信息化部总经理

张明文 上海纽荷兰农机公司信息系统部经理

孙振鹏 VHP 出版集团中国地区首席代表 EXIN 中国区首席代表

李　新 北京大学数字中国研究院教育培训中心副主任、副教授

郭晓英 挪威船级社大中华区业务拓展总监、ISMS 主任审核员

赵大平 冠群电脑(中国)有限公司技术总监

辛儿伦 微软(中国)有限公司大中华区企业服务部总经理

朱伟星 中国惠普信息技术解决方案部总经理

隋成岩 思科系统(中国)网络技术有限公司企业事业部经理

Jan van Bon 国际 IT 服务管理门户网站(ITSMPORTAL.NET)首席主编、IT 服务管理资深专家

《中国 IT 治理智库》系列丛书

编委会

（排名不分先后）

主　编

孙　强　ITGov 中国 IT 治理研究中心主任

副主编

郝晓玲　上海财经大学讲师、博士，ITGov 中国 IT 治理研究中心绩效评估研究员

屈玉阁　中国网通（集团）有限公司河北省分公司企业信息化部高级工程师

戴志宏　上海市电信有限公司

李海风　北京大学国际会计与财务研究中心审计部主任

周凌波　东软电子出版社副总编辑

郑利强　北京华深科技发展有限公司监理咨询部经理、博士

阎振平　中国光大银行稽核部信息系统审计专家 注册信息系统审计师

孟秀转　ITGov 中国 IT 治理研究中心注册 BS15000 咨询师、博士

王东红　ITGov 中国 IT 治理研究中心信息系统审计专家

李长征　ITGov 中国 IT 治理研究中心 IT 服务管理专家

陈　涛　ITGov 中国 IT 治理研究中心 IT 内控专家

孟秀艳　ITGov 中国 IT 治理研究中心信息安全管理专家、博士

俞　静　ITGov 中国 IT 治理研究中心信息化绩效评价专家、博士

白　杨　ITGov 中国 IT 治理研究中心信息化绩效评价专家

李晓冬　ITGov 中国 IT 治理研究中心信息系统审计专家
徐　斌　中央财经大学会计学院博士
刘永久　国家图书馆
陈艳红　首都医科大学生工学院讲师
栾东庆　同济大学经济与管理学院博士
刘晓菲　ITGov 中国 IT 治理研究中心信息系统审计专家
邹志德　ITGov 中国 IT 治理研究中心信息系统审计专家
肖　沂　ITGov 中国 IT 治理研究中心信息化绩效评价专家
秦　勇　ITGov 中国 IT 治理研究中心信息系统审计专家

代　序

客观总结信息化实践，深入探索信息化理论

信息技术及其应用的飞速发展已将技术革命演变为产业革命和社会革命，由此带来的变革以及由这种变革造成的影响，已经超过以蒸汽机、电气化为代表的工业革命。信息产业已经成为规模最大、渗透性最强的支柱产业和战略产业。从冲绳宪章到罗马宣言，走向信息社会成为世界各国的共识。信息网络正成为最重要的基础设施，与信息技术、信息资源相结合，构成了最活跃的生产力。以信息技术创新能力、信息技术应用和信息资源开发利用广度和深度为标志的信息化能力，成为国家竞争力的主要标志。电子政务、电子商务、电子社区、远程教育和医疗成为广泛的实践。许多国家制定了应对这一历史机遇的国家战略。

党中央、国务院对信息化发展做出了一系列重大战略决策和部署。《中共中央关于制定国民经济和社会发展第十个五年计划的建议》中指出：信息化是当今世界经济和社会发展的大趋势，也是我国产业优化升级和实现工业化、现代化的关键环节。明确要求在“十五”计划中把推进国民经济和社会信息化放在优先位置。根据党中央的建议，“十五”计划把信息化作为一个重点部分，制定了“十五”信息化重点专项规划。2001年成立了由国务院总理任组长，中央、国务院和军队主要领导任副组长的国家信息化领导小组，成立了国务院信息化工作办公室作为其办事机构，加强了对推进信息化的领导和协调。在十六大报告中进一步提出了以信息化带动工业化，以工业化促进信息化，走出一条科技含量高、经济效益好、资源消耗低、环境污染少、人力资源优势得到充分

此为试读，需要完整PDF请访问：www.ertongbook.com

发挥的新型工业化道路。国家信息化领导小组对一系列信息化发展的战略和重大任务做出了决策和部署，要求紧紧抓住信息化发展的机遇，进一步增强加快信息化的紧迫感和使命感，推动经济社会全面、协调、可持续发展。

我国在数十年信息化发展中，各方面取得了十分显著的成绩，也存在不容忽视的困难、矛盾和问题。信息技术进展快、信息资源增长快、信息产业发展快、信息网络扩散快、信息技术应用渗透快、信息化环境变化快。实践促进理论研究、理论促进实践的成熟，面对信息化快速发展的形势，迫切需要客观总结实践经验、深入探索具有中国特色的发展规律，引导信息化走上科学、健康的轨道。

信息技术在经济和社会领域应用过程中逐渐改变着组织结构、管理制度和业务流程，并为制度创新和管理创新提供新的工具和平台，从而对建立现代企业制度、完善公司法人治理结构产生着不可忽视的重要作用。

《中国 IT 治理智库》系列丛书，引进经典专著和邀请专家学者编著相结合，从总结信息化经验、指导信息化实践，以及通过信息技术应用完善公司治理结构的两个方面，繁荣着我国信息化学术园地，将对我国信息化发展起到积极的引导作用。更希望，有更多的专家学者投身到信息化理论研究和实践总结，为我国信息化发展奠定坚实的理论基础。

是以为序。

杨学山

国务院信息化工作办公室副主任

2006 年 3 月 18 日

英文版序

以前，我们每个人面对的大多数风险通常都是局部的、个人性质的。随着时间的推移，新的技术不断地进入我们的生活，使我们面临的风险也变得越来越广泛。技术对我们的生活所产生的影响日渐加深。计算机—通讯系统现在已经触及我们日常生活的方方面面，不仅与民众的健康、安乐有关，也对机构[1]、政府乃至于全球的环境都构成了影响。

遗憾的是，随着我们越来越依赖计算机和网络系统，我们要面对的相关风险不是在逐渐减小，而是在迅速增大。发展中的一些新的应用严重地依赖于某些自动化系统。对企业的需求而言，这些系统自身的确定性如何并不是完全透明的。加之没有系统化地考虑系统复杂性问题，使得某些系统变得越来越庞杂。系统中出现新的缺陷和弱点的速度似乎总是快于老问题的解决速度。对系统进行的恶意攻击也有增多的趋势。可以预想，我们将来重要的国家基础设施也将会以不同的方式依赖于信息技术——实际上是互相依赖。

通常，风险总是会出现在旁观者的眼里。风险常常会被当事者所轻视，甚至于完全被忽视。对于每一个从事风险管理、风险预防或者风险处置的人来说，对风险具有深入的理解是非常重要的。幸运的是《信息技术风险》这本书为不同背景的读者带来了有关信息技术风险的很多新颖的观点。在信息技术风险管理领域，这是迄今为止最重要、最实用而又最切合实际的一本书，对信息技术管理者而言更是如此。

这本书所体现的智慧在某些人看来可能仅仅是一些“常识”。但是，常识往往并不普通。回忆一下历史上曾经出现过的那些带有缺陷的系统，回想一下

---

1 本书讨论的信息技术管理和风险涵盖了企业、机构和其他各种信息技术应用场所。原著先后使用了多个意义接近但又有一些区别的词来表达应用场所，如 organization、enterprise、company、firm 等。其实它们之间存在一些微妙的差别。译者将依照原著的用词，但其中意义相信读者结合上下文可以体会出来——译注。

曾经出现过的滥用、人为错误、操作失误、环境风险、管理不善以及发生过的各种事故(Neumann，1995)，我们可以发现，从常识上来看这些问题应该极为罕见，但现实却截然相反。业界普遍存在的一种现象是表现在系统管理和系统开发决策上的短视，常常忽略风险设施。造成的后果往往也是灾难性的——造成无可挽回的人身伤亡、巨大的经济损失以及秘密泄漏。

一个人所冒的风险对其他人来说也会是一场挑战。这本书为我们描述了可以彻底避免或者大幅减少上述错失的诸多选择。因为，重大的伤害一直伴随着计算机革命进程的始终。我本人希望读者能够仔细地阅读并留意作者的建议——相信通过持续不断地努力，我们能够避免再次遭受这些损失。当然，我们也不能指望采用一些简单的方法就能达到我们的目标，因为问题本身就非常复杂，问题的答案需要深思熟虑，需要谅解，需要远见，更需要大局观。请记住！避免风险没有容易的答案。对我们来说，风险总是如影随行。

把应对风险和“击鼓[2]”相比较是个非常不同的视角——“鼓声”是单音，而本书则是一部交响曲，所有的声音都会纠缠在一起发出共鸣。如果本书在使读者了解更多细节的同时还能看到这一幅巨大的图景，那么这就是它最大的贡献了。

Peter G. Neumann

加州，美国

2004 年 9 月 21 日

（斯坦福研究院国际计算机科学实验室首席科学家，ACM 风险论坛主持人，ACM 通讯杂志的联合编辑）

2 本书的原著名为“Beating IT Risks”，意有击鼓之义——译注

致　谢

作者对 PA 咨询集团给予本书的热忱帮助表示感谢。我们也要感谢 PA 咨询集团团队成员为本书提供的案例材料、鼓励和建议。特别要对 Clare Argent、John Burn、Jonathan Cooper-Bagnall、Karen Crothers、Frank Decker、Neil Douglas、Dean Evans、Polly Ferguson、Ian Foster、Guy Gybels、Kerry Harris、Greg Jones、Fons Kuijpers、Geoff Larbalestier、John Lunn、Nuala MacDermott,、Rob McMillan、Christian Nelissen、Bernie Robertson、Jason Robson、Dawn Whitmore 和 Nick Woodward 表达我们的谢意。

我们还要感谢澳大利亚悉尼麦考里大学商学院的 Bob Hunt 和 Dave Musson，他们审阅了本书的初稿并提出了很多有价值的建议。

我们非常欣赏 Wiley 职员的专业性和技能，尤其是 Sarah Booth、Lorna Skinner、Rachel Goodyear、Amelia Thompson 和 Trisha Dale。

Luke 要特别感谢他的妻子 Louise 和他的两个儿子 Sam 和 Rowan 对他在本书写作期间的支持和理解。

Ernie 要感谢 Amy 和 Alex，他们的爱和鼓励使这一切成为可能。

中文版序

技术在给人类带来巨大助益的同时，也使我们面对着巨大风险。信息技术也不例外。

信息技术的发展进程一直有风险相伴。信息技术自身的发展基本上可以看成是技术进步同风险管理与控制之间的互动与平衡。随着信息技术的快速发展，它日益渗透到了我们日常生活的方方面面，人类对信息技术的依赖日渐加深。随之而来的是信息技术可能会给人类带来的风险威胁也越来越大。信息技术风险给我们日常生活已经带来的或者将要带来的影响显得非常深刻。一方面信息技术正在深刻地影响着我们的人类，我们日益依赖于信息技术进步。另一方面，广泛的信息技术应用又使我们面对着更大的技术风险。这种正反馈系统机制的形成促使问题正在逐步走向复杂化。如何打破这种循环成为我们当今所面临的一个巨大挑战。

我们对信息技术发展规律的认识也经历了一个由简单到复杂，由局部到全局，由肤浅到深入的过程。从强调单一硬件系统的可靠到强调信息技术基础设施风险，从网络安全到强壮而灵活的系统架构体系，从软件开发质量保障到流程控制目标保障，从防范信息泄露到整体信息资产安全，从桌面系统病毒控制到全系统安全保障，从单一的系统运行监控到IT运营乃至IT服务连续性管理，从企业内部开发团队管理到外源性外包乃至多源风险控制策略，从单个项目的风险控制到企业信息技术战略制定，从盲从于新的流行技术到新兴技术与主流标准战略，一直发展成为融合了防范与应对IT应用、IT项目、信息资产、IT基础设施、业务服务连续性与IT服务连续性、IT服务及产品供应商等风险组合的信息技术风险管理体系。这些发展在充分反映了信息技术高速发展的同时，也折射出了信息技术给我们带来的巨大的风险挑战。

同其他风险研究领域相似，目前对信息技术风险的研究着重在两个方向

上：一是呼应现实信息技术应用的要求，讨论和总结信息技术风险组合的具体内涵。从信息、资源、规划、获取与实施、交付与支持、监控等多个方面制定具体的控制目标，提出应对信息技术风险的最佳实践方法。第二个方向是信息技术风险基础理论方面的探讨，即风险度量与模型化。这两方面的工作主要来源于几方面的驱动力，一是面对着日益复杂而广泛的信息技术风险，在实践上我们需要一套全面的，并且行之有效的标准和最佳实践指引。其次是基于资本配置的要求和因应量化的效能考核需要。这本书是信息技术风险管理最佳实践的开篇之作。它全面介绍了同信息技术相关的各种风险以及这些风险之间的相互关系。作者采用风险组合的方法来考察和分析信息技术风险，用系统性的方法来应对风险。这本书很好地总结了信息技术风险管理的最佳实践，使我们在对信息技术风险有了更加深入的认识的同时，也使我们对信息技术管理实践具有了更广阔视野。

我们相信这本书将会使我们对信息技术领域所面临的机遇与挑战有着更深刻的认识。它也将成为我们总结、分析、应对信息技术风险的新起点。

白　硕

上海证券交易所总工程师、博士生导师

2006年9月6日

此为试读，需要完整PDF请访问：www.ertongbook.com