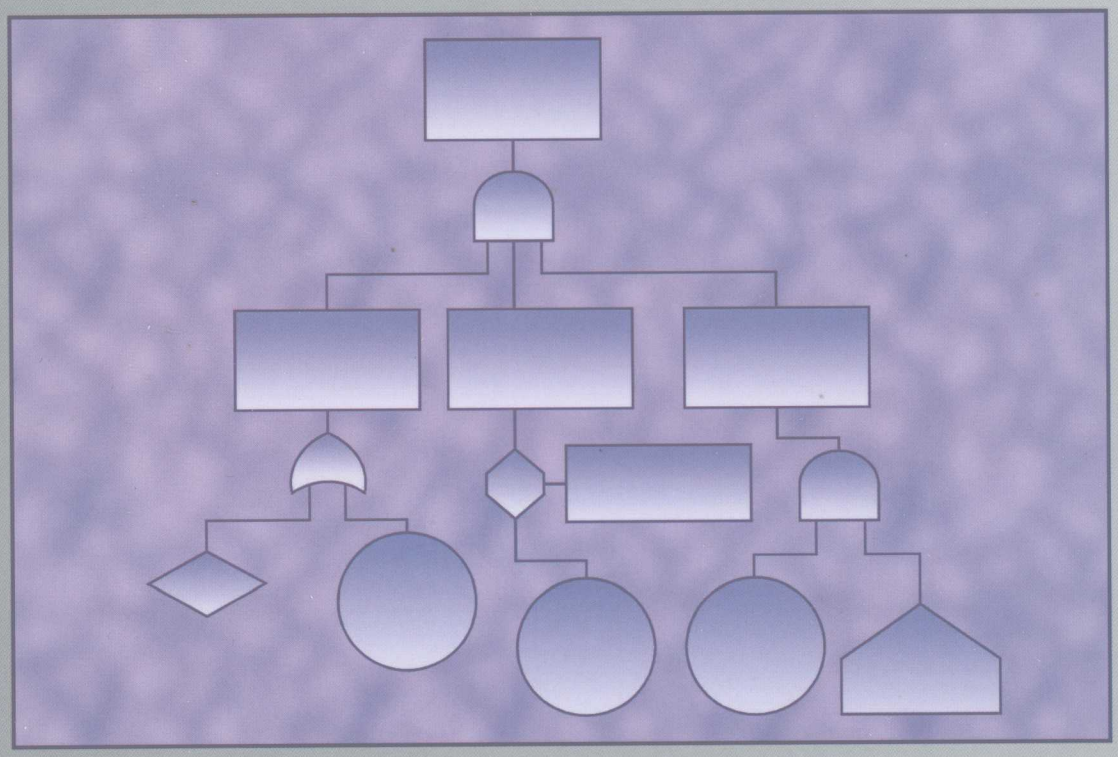
控制系统的安全评估与可靠性

威廉·戈布尔（美国）William M. Goble 著
白 焰 董 玲 杨国田 译



William M. Goble
Second Edition

中国电力出版社
www.cepp.com.cn

控制系统的安全评估与可靠性

威廉·戈布尔（美国）William M. Goble 著
白 焰 董 玲 杨国田 译

中国电力出版社
www.cepp.com.cn

内 容 提 要

本书介绍控制自动化系统的安全性与可靠性评估知识，内容主要包括故障树分析（FTA）、可靠性框图（RBD）、失效模式及影响分析（FMEA）以及马尔可夫模型。本书讨论了元件的失效模式、在线诊断、共因失效、软件可靠性以及运行安全等关键问题，并详细介绍了安全仪表系统（SIS）的各种分析技术，其中涵盖了从传感器到执行器的各种组成部件。书中包含了大量密切结合工程实际的例题和习题，并附有习题答案。

本书内容丰富、图文并茂、深入浅出，并且提供了大量的例题和习题。同时，该书又十分重视理论联系实际，介绍了许多工程化的方法。适合于广大从事自动控制系统研究、设计、管理及维护工作的工程技术人员，并且可作为自动化、测控技术与仪器及相关专业的大学本科生、研究生的课研参考用书。

图书在版编目（CIP）数据

控制系统的安全评估与可靠性／（美）戈布尔著；白焰，董玲，杨国田译．—北京：中国电力出版社，2008
书名原文：Control Systems Safety Evaluation & Reliability
ISBN 978-7-5083-7462-8

Ⅰ.控… Ⅱ.①戈…②白…③董…④杨… Ⅲ.①自动控制系统－安全技术－技术评估②自动控制系统－可靠性估计 Ⅳ.TP273

中国版本图书馆 CIP 数据核字（2008）第 109426 号

责任编辑：孙 芳
责任校对：崔燕菊
责任印制：郭华清

书 名：控制系统的安全评估与可靠性
译 者：白 焰 董 玲 杨国田
出版发行：中国电力出版社
地址：北京市三里河路 6 号 邮政编码：100044
电话：（010）68362602 传真：（010）68316497
印 刷：北京盛通印刷股份有限公司
开本尺寸：185mm × 260mm 印 张：30 字 数：586 千字
书 号：ISBN 978-7-5083-7462-8
版 次：2008 年 10 月北京第 1 版
印 次：2008 年 10 月第 1 次印刷
印 数：0001—3000 册
定 价：87.00 元

致　　谢

本书的出版得益于很多人的帮助。早期，我在 Villanova 大学 J. V. Bukowski 讲授的“可靠性工程”研究生课程中了解到这门学科。这门课程以及几年来的几次研修班为我着手写这本书提供了必要的帮助。

还有很多人协助研究了一些对控制系统安全性和可靠性很重要的问题。我要感谢我的合作者：John Grebe, John Cusimano, Ted Bell,Ted Tucker, Griff Francis, Dave Johnson, Glenn Bilane, Jim Kinney 和 Steve Duff。他们提出很多尖锐的问题，共同探讨关键点，给出了许多建议，并且提供了复杂问题的解决方法。特别感谢前任领导 Bob Adams，他提出了很苛刻的问题，并要求设计新产品时首先要考虑可靠性。

SP84 的同事们也为许多问题的研究提供了帮助。我要感谢 Vic Maggioli, Dimitrios Karydos, Tony Frederickson, Paris Stavrianidis, Paul Gruhn, Aarnout Brombacher, Ad Hamer, Rolf Spiker, Dan Sniezek 和 Steve Smith。在我们的辩论中我学到了很多知识。

本书的几位评审者提出了许多重要的建议。我要感谢 Tom Fisher, John Grebe, Griff Francis, Paul Gruhn, Dan Sniezek, Rainer Faller 和 Rachel Amkreutz。他们提出的评论和问题在很大程度上改进了本书。作者特别感谢 Villanova 大学的 Julia Bukowski 和 Eindhoven 大学的 Jan Rouvroye，他们为此书做了全面并且详尽的评审。作者还要特别感谢 Eindhoven 大学的 Iwan van Beurden，他详细地审阅并检查了本书的例题以及习题答案。我还要感谢我的好友，Rick Allen，他审阅了书稿，并对语法和标点的使用规则提出了建议。

最后我要感谢我的妻子 Sandy 和女儿 Tyree 和 Emily 的理解与帮助。她们帮忙校对、打字，并且检查数学公式。非常感谢她们为我所做出的一切，但最值得感谢的还是她们给我的鼓励和支持。

序　言

在控制系统设计中，为了在成本、性能和维护之间进行权衡，能够定量评估安全性和可靠性这样的控制系统设计参数历来非常重要。然而，除了考虑经济性之外，还要考虑人身保护和环境保护。由于国际法规要求安全保护系统的性能必须是可验证并且是可检测的，因此安全性和可靠性的定量分析就变得越来越重要了。

ISA 的 S84.01 标准定量地定义了安全仪表系统的性能等级。新的 IEC 安全标准和一些工业行业标准也同样如此。一般来说，这些标准都不是说明性的，它们不会详细地说明怎样设计系统，而是提出必须满足的、定量的安全性指标。设计人员要考虑各种设计方案，并从中找出哪一种设计方案能够满足指标。

安全系统设计的基本方法与从经济角度进行优化设计的设计人员所采用的方法非常一致。为了得到最优设计方案，必须综合考虑设计约束条件。在设计过程中，所有设计约束条件都会影响到最终的经济性。真正的设计优化需要在存在约束条件的情况下对备选设计方案进行评估。在优化过程中，需要考虑安全性和可靠性的量化指标和定量评估方法。

和许多其他工程领域一样，我们必须认识到：目前，系统的安全性和可靠性还不可能完全量化。为了简化问题，我们做了不同的假设。许多方法需要失效率数据和原始输入数据，但这些数据都是不准确的，或者是无法得到的。在工作条件与预期的使用条件一致的情况下，通过大量的寿命试验才能获得准确的失效率数据，但是有一些因素会阻碍这种试验。首先，从供货商采购来的控制系统元件普遍达到了比较高的可靠性级别，它们可以运行许多年。精确的寿命测试要求控制单元始终运行直至发生故障，因此测试所需要的时间远远超过了数据的有效期（在测试完成之前元件已经报废）。其次，控制系统的安装位置不同会使工作条件发生明显变化。某一个地点的失效率可能会比另一个地点的失效率高很多。最后，使用方法的不同也会影响元件的可靠性，在产品存在设计缺陷时更是如此。当今系统中使用的复杂元件很可能存在设计缺陷。在复杂的软件中也经常存在设计缺陷。

尽管有可变性、不精确性、假设简化性和方法多样性等局限，安全性和可靠性评估领域仍然在飞速发展。ISA 标准委员会正在该领域的各个方面开展工作。SP84 的一个委员会正在研究计算系统可靠性的方法。本书中提到了一些利用这些工具来计算可靠性的方法。

软件可靠性是十多年来重点研究的一个课题，这方面的研究成果也开始崭露头角。软件在控制系统中的发展极其迅速，因此软件的可靠性对控制系统来说非常重要。尽管软件工程技术提供了一些比较好的避免软件设计缺陷的方法，但是软件本身的发展速度远远超过了软件工程技术的发展速度，所以软件的可靠性可能会是未来控制系统可靠性的决定性因素。

控制系统的安全性和可靠性是重要的设计约束条件。当我们在控制系统设计中有了统一的安全性和可靠性术语，当我们充分理解了安全性和可靠性评估方法，其中包括如何考虑所有的环境因素，以及如何评估软件的可靠性时，安全性和可靠性就成了真正的设计参数，而这正是我们所追求的目标。

William M. Goble

Perkasie, PA

1998 年 1 月

译 者 序

随着全球特别是发展中国家工业化进程不断加快，生产过程不断强化，重大事故频繁发生。大工业在给人们带来舒适便捷生活的同时，也成为我们挥之不去的梦魇。1984 年印度博帕尔化工厂毒气外泄，1986 年前苏联切尔诺贝利核电站爆炸，这些至今仍然令人记忆犹新的灾难性事故不断地向我们昭示：安全生产是企业永恒的主题。

控制系统是企业生产过程的重要组成部分，是安全生产的关键要素之一，没有安全可靠的控制系统，就不可能有安全可靠的生产过程。因此，控制系统的安全性与可靠性评估就成为企业实现安全生产必须面对并且必须解决的问题。

近年来，一些国际组织相继公布了一系列有关控制系统安全性与可靠性的标准，例如：ISA 的 S84.01、IEC 的 61508 等，我们国家相关部门也陆续出台了一系列有关安全生产的国家标准，如 GB/T 20438《电气/电子/可编程电子安全相关系统的功能安全》等。随着国家对安全生产和环境保护方面监管力度的不断加大，将来可能会根据这些标准推出一系列企业必须执行的强制性法规。

流程工业中的控制系统在功能上可以分为基本过程控制系统（BPCS）和安全仪表系统（SIS）。BPCS 实现生产过程的连续调节和顺序控制等常规控制功能，而 SIS 则实现连锁保护和紧急停车等安全功能。过去，人们对于基本过程控制系统给予了较多的关注，形成了完整的理论体系、系统的设计方法以及成熟的工程方案；然而，对于安全仪表系统的研究则没有引起足够的重视，SIS 的设计往往凭借设计者的设计经验或照搬照抄以往的设计方案，没有系统化的设计方法和定量化的设计指标，造成了 SIS 设计的盲目性和随意性。

从 20 世纪 70 年代开始，欧美各国就开始用系统工程的理论和原理来研究解决 SIS 的功能安全问题，形成了系统化的分析和设计方法，这些方法贯穿于 SIS 系统的整个生命周期，从设计、制造、运行到管理，几乎囊括了与安全性和可靠性相关的各个方面。美国仪表、系统与自动化协会（ISA）也相继出版了一系列关于控制系统安全性与可靠性评估方面的书籍。为满足广大工程技术人员和在校学生学习控制系统安全性与可靠性评估知识的需要，我们翻译了 William M. Goble 所著的《控制系统安全评估与可靠性》（Control Systems Safety Evaluation and Reliability）一书。

该书作者 William M. Goble 博士是著名的可靠性与安全性方面的技术咨询与教育专家，发表了许多关于软硬件安全性与可靠性、质量改进以及定量建模方面的论文。

他在美国宾夕法尼亚大学从事工程可靠性研究生课程的教学工作，是美国仪表协会 ISA 安全性与可靠性方面的资深会员（Fellow），也是 IEEE 会员和 ISA SP84 委员会委员。

《控制系统安全评估与可靠性》一书是基于作者在该领域多年的教学与研究经验编写而成的。书中许多内容取材于作者在美国宾夕法尼亚大学开设的“工程可靠性”研究生课程，以及 ISA 的“系统安全性与可靠性评估”课程，部分内容取材于美国仪表协会 ISA TR84.02 草案，以及作者在荷兰爱因霍芬大学的研究成果。

该书为控制系统的设计者提供了必要的基本知识，使他们能够设计出满足安全性和可靠性要求的控制系统，并且帮助他们正确地评估控制系统的元件与结构，更好地与业主交换意见，提高生命周期成本估计的准确性。这本书也为可靠性与安全性工程师提供了大量来自控制系统制造工业的相关信息。

该书大量的例题和习题使得它十分适合作为可靠性工程方面的教科书。同时该书又十分重视理论联系实际，介绍了许多工程准则，具有广泛的应用价值。

该书主要分为两个部分：第一部分主要介绍一些基本知识，包括概率与统计、可靠性理论与定义以及基本的可靠性模型；第二部分专门论述安全仪表系统与控制系统的先进技术。

该书的主要特点是：

- 内容丰富。既包含了传统的安全性与可靠性分析方法又包含了近年来出现的一些先进分析方法，例如，马尔可夫分析方法等。
- 深入浅出。书中的论述循序渐进，通常由一个简单的问题出发，层层深入，不断提出新的问题，并逐步加深，最后形成一个完整的知识体系。
- 联系实际。书中除了阐述必要的基础理论之外，还密切结合控制系统工程实际，介绍了许多工程化的方法，这些方法简单有效，能够快速解决常见的工程问题，并且不需要繁杂的数学运算。
- 例题与习题。该书的例题与习题十分丰富，并且提供了习题答案，为读者自学或作为教科书提供了便利。
- 图文并茂。该书包含大量绘制精美的图表，生动直观，提高了该书的可读性和易读性。

本书由白焰、董玲、杨国田翻译，全书由白焰统稿并审校。华北电力大学崔彦波、张

健、江东泽、陶翠、鲁玺梦、黄从智、李玉凯、董玫参与了本书部分翻译、书稿整理和校对工作。译文在尊重原著的基础上，对原著中的一些错误做了更正。译者在翻译过程中尽可能遵循最新出版的国家标准，但由于安全性与可靠性名词术语尚存在一些不能统一、前后矛盾和争议之处，因此，译文难免会有一些措辞不当、理解偏颇甚至错误之处，敬请读者不吝指正。

译　者

于北京　华北电力大学

2008 年 4 月

关 于 本 书

本书取材广泛。多年来，作者发表了许多关于安全性和可靠性的论文。这些论文的前期准备、论文的成文过程以及读者的反馈信息都对本书的出版起到了巨大的推动作用。作者在宾夕法尼亚州立大学所讲授的课程“SYS506，工程可靠性”和在 ISA 所讲授的课程“ES35，评估系统的安全和可靠性”的笔记为本书提供了必要的组织架构。学生提出的问题使作者更加深刻地意识到，哪些地方需要更详尽的解释。

与 ISA 的 SP84 委员会共同协作进行的工作和讨论也为本书提供了主要素材，本书在编写过程中也使用了 ISA TR84.02 文件草案中的符号和方法，在荷兰爱因霍芬科技大学进行的研究和讨论也是本书的主要素材，还有一些素材来自作者在企业中开发和生产重要安全设备的经验。

本书适用于各种各样的读者。专业的控制系统设计者可以从本书中获得一些概要和详细的基础知识，这些内容对于更好地理解一个设计方案怎样才达到新的安全标准和可靠性工程目标是非常必要的。这将有助于对控制系统的部件进行合理地评估，对各种系统架构进行评估，更好地与卖方进行沟通，以及提高系统生命周期成本的估计精度。本书还将为那些希望得到控制系统生产厂家信息的可靠性和安全性工程师提供各种有用的信息。

本书也可作为大学可靠性课程的入门教材。书中许多例子和详细的解释将能够满足这种需求。贴近实际的论述有助于理解“工程评价”这一概念，即理论与实际应用的不同之处。本书的最终目的是为那些希望对安全仪表系统进行定量评估的专业人员提供背景知识。

本书分为两部分。第一部分是基础知识，包括概率、统计、可靠性理论的定义以及基本的可靠性建模方法。第二部分是专门针对安全仪表系统和控制系统的高级技术。熟悉可靠性理论的读者不妨简要地浏览一下第一部分，以便了解一些基本的表示方法。

可靠性工程这一学科正在不断发展。建模技术也将继续改进。希望读者通过 ISA 的杂志、会刊和技术论文集密切关注这一领域。

关 于 作 者

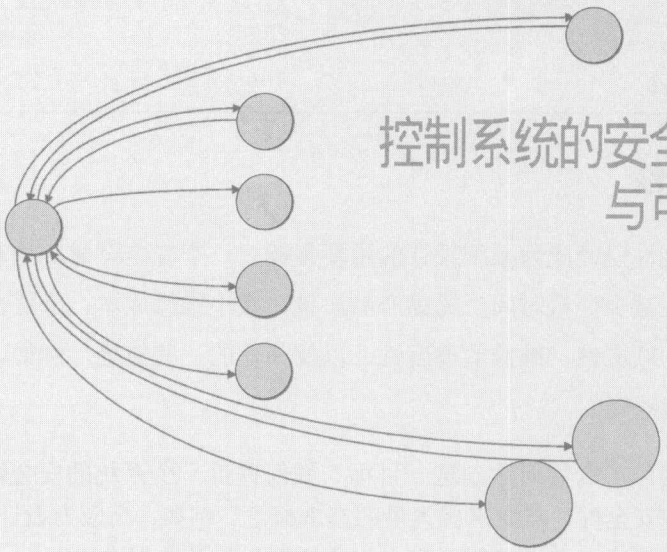
William M. Goble 博士在模拟与数字电子电路设计、软件开发、工程管理以及市场营销方面具有 25 年以上的经验。目前他是美国著名的、专门从事自动化系统安全性与可靠性研究与开发的 Exida 公司的总裁。

他分别在美国宾夕法尼亚州立大学和维拉诺瓦大学获得电气工程学士和硕士学位，在荷兰爱因霍芬大学机械系从事可编程电子系统安全性与可靠性建模方面的研究，并获得博士学位。他是宾夕法尼亚州的职业工程师，取得了 TÜV 颁发的注册功能安全专家证书。

他是著名的可靠性与安全性方面教育家与技术咨询专家，独撰或与他人共同发表过许多关于软硬件安全性与可靠性、质量改进以及定量建模方面的论文。

他作为宾夕法尼亚大学的客座教授，从事工程可靠性研究生课程的教学工作。他是 ISA 安全性与可靠性方面的资深会员（Fellow），并为其开设和讲授安全性和可靠性课程。他也是 IEEE 会员和 ISA SP84 委员会委员。

目　录



控制系统的安全评估
与可靠性

第1章

引　言

- ☑ 控制系统的安全性与可靠性
- ☑ 可靠性工程

控制系统的安全性与可靠性

自动控制系统的安全性和可靠性已经成为系统设计的重要指标。一个安全可靠的控制系统所带来的经济效益不仅体现在减少停机时间、提高产品质量、减小维修成本、降低投资风险等方面，而且包含了管理的顺应性，维修的调度性，以及其他的一些益处，例如，企业员工平和的心态和对工作的满意度。

既然安全性和可靠性如此重要，那么如何达到这一目标？如何评价一个系统的安全性和可靠性？要提高系统的可靠性和安全性，需要掌握大量的基本概念。例如，高应力设计，容错设计，在线故障诊断和高共因强度。在后续的章节中将要详细讨论这些概念。

可靠性和安全性使用了大量严格定义的参数，其中包括可靠性、安全性、*MTTF*（平均故障前时间）、*RRF*（风险降低因子）、*PFD*（需求失效概率）、安全可用性及其他一些参数。在过去的 50 年中，人们不断地提出这些术语，形成了可靠性和安全性工程这样一个研究领域。

基本过程控制系统 BPCS 和安全仪表系统 SIS

在控制系统中，安全保护设备一般是和控制设备分离的。控制设备被称为基本过程控制系统（BPCS），而保护设备则被称为安全仪表系统（SIS）。BPCS 读取过程传感器的数据，进行连续控制，或顺序控制计算，并向执行装置（阀门或电机）发出指令。SIS 读取传感器的数据，进行计算或实现判别潜在危险工况的逻辑，把输出送给执行机构，以避免出现危险工况。SIS 可以单独或同时保护人员、设备和环境。图 1-1 表示了这 2 类系统中的设备。

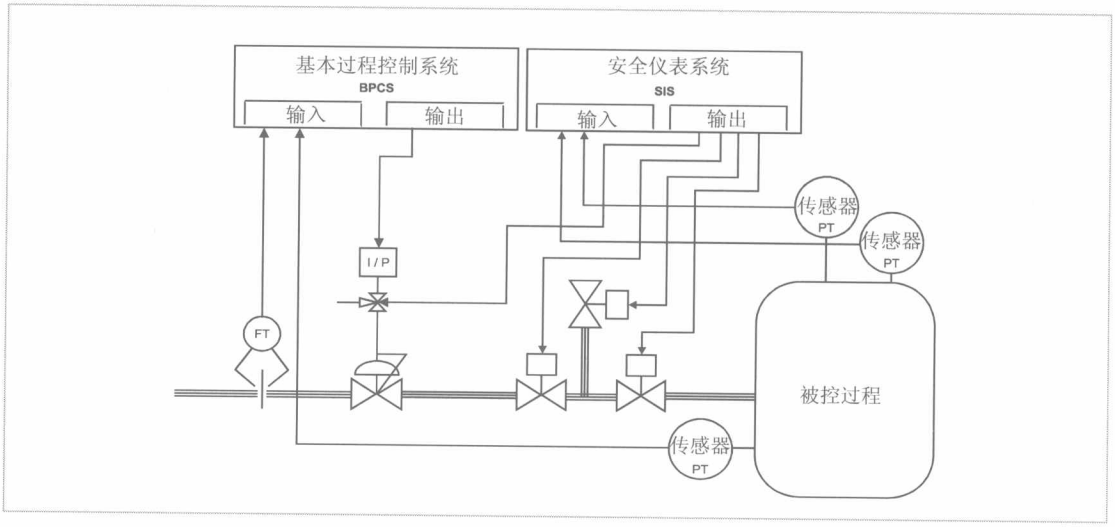


图1-1　BPCS和SIS