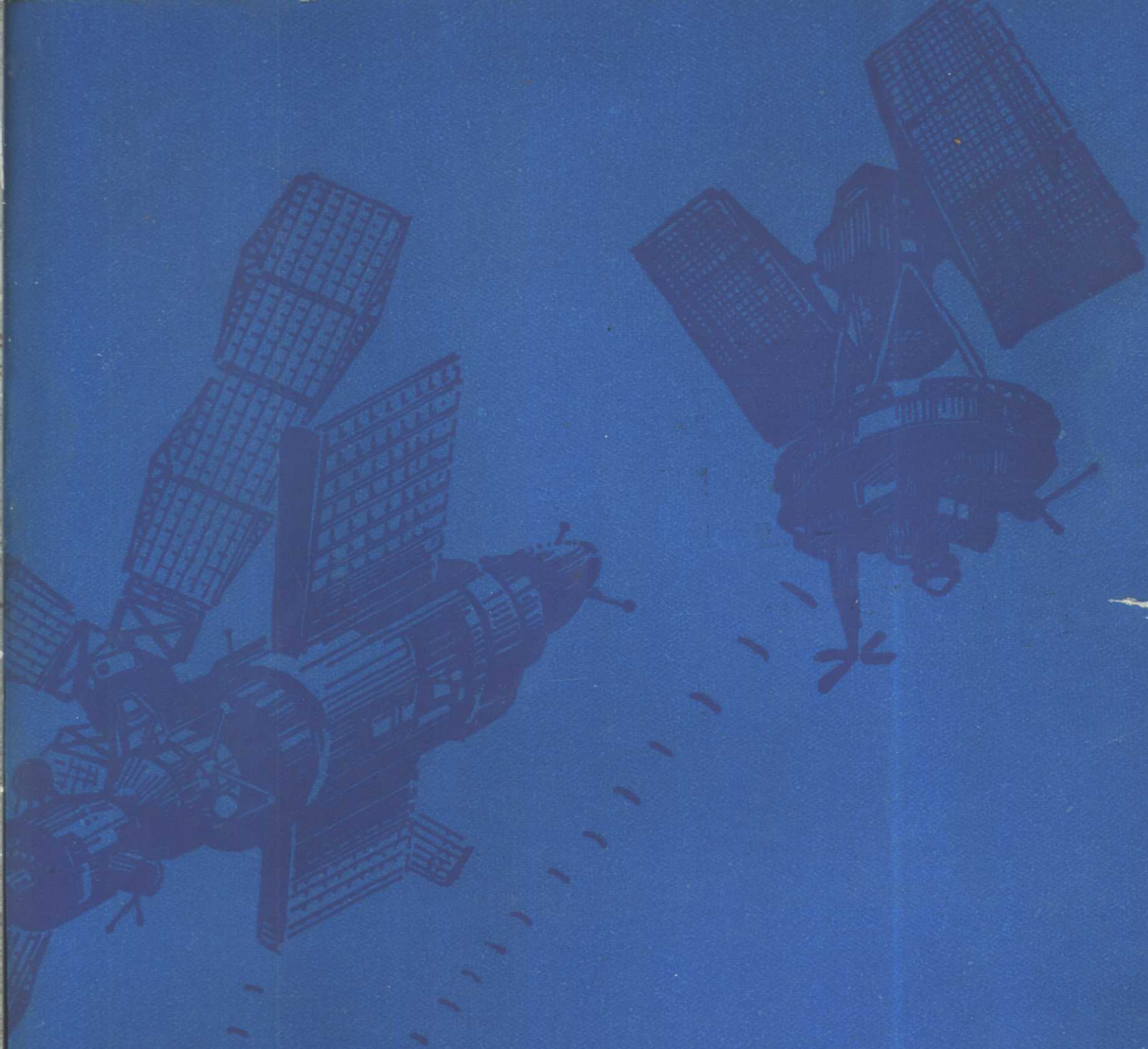

系统可靠性、故障诊断及容错

唐泳洪 编著

重庆大学出版社

系统可靠性、故障诊断及容错

唐泳洪　编著

重庆大学出版社

内 容 简 介

本书深入系统地阐述了与系统（包括软件系统）可靠性、故障诊断和容错等方面有关的数学模型和技术基础，并着重讨论了如何应用这些基本理论知识处理工程实际问题。其主要内容为：概率论基础，可靠性基本概念，常见分布型式及其应用，系统可靠度逻辑图的构造，不可修复型系统的可靠性数学模型，可修复型系统的可靠性数学模型，系统可靠度的最优配置，系统故障树的构造及分析，网络系统的可靠度，故障诊断技术，容错系统，软件可靠性，软件系统可靠性评价。

本书可供高等院校控制工程、自动化、计算机专业的师生使用，也可供机电一体化和机械制造等专业的大学生和研究生以及有关方面的工程技术人员、科研和设计人员、教学人员参考。

系统可靠性、故障诊断及容错

唐泳洪 编著

责任编辑 黄开植

*

重庆大学出版社出版发行

新华书店经销

中国人民解放军重庆通信学院印刷厂印刷

*

开本：787×1092 1/16 印张：20 字数：499 千

1990 年 2 月第 1 版 1990 年 2 月第 1 次印刷

印数：1—2700

标准书号：ISBN 7-5624-0264-7/TP·16 定价：3.97 元

序

长期以来，人们对可靠性的理解和描述一直都停留在模糊的定性概念上，没有精确地把握住它的数值量度。自从美国于1957年提出AGREE报告以后，可靠性才被当作一门单独的科学，开始应用概率论和统计学方法进行定量研究。至于故障诊断和容错技术的出现，则是70年代中期的事。

系统可靠性理论是以系统的寿命特征作为研究对象的一门综合性和交叉性学科，它涉及到基础科学、技术科学和管理科学中的许多领域。而故障诊断和容错，则是在系统可靠性理论指导下研究如何采用技术措施增加系统可靠性的一门科学，它涉及到的学科有：微电子技术、测试技术、自动控制技术、计算机和软件工程学等。

可靠性是产品的生命，随着我国四化建设的不断发展，系统可靠性问题已逐渐被人们所认识和重视，但由于我们过去的不重视和研究工作的薄弱，致使许多科技和管理人员在这一领域里的理论知识和实践技能远远不能满足当前形势的需要。现在《系统可靠性、故障诊断及容错》一书的问世，当可起着良好的作用。

书中，作者在总结研究成果和学习心得的基础上，深入而系统地阐述了有关系统可靠性、故障诊断和容错的基础理论、数学模型以及应用基本理论处理可靠性工程实际问题的方法和技巧。理论实际并重，研究、应用兼顾；内容翔实，材料新颖，结构严密，行文流畅；有一定学术水平和实用价值。乐于作序，以弁卷首。

张钟俊

于上海交通大学

1988年6月

前　言

系统可靠性是系统寿命指标的总称，它反映了一个系统在规定时间内和规定条件下完成规定功能的能力。系统可靠性理论是以系统寿命特征作为主要研究对象的一门综合性和边缘性学科，它涉及到基础学科、技术科学和管理科学中的许多领域，如概率论、数理统计、开关数学、运筹学、计算机、软件工程、机械、光学和电子学等。如果将系统可靠性理论应用于研究解决某一具体系统的可靠性问题，则还需对该系统所属学科中的某些理论问题和技术问题有一基本了解。

当尚未掌握某种产品时，该产品的开发或引进是主要矛盾，当已掌握了某种产品后，则主要矛盾将转为保证和提高该产品的可靠性质量指标和其它指标。可靠性是产品的生命，不能稳定可靠地工作的产品就不会拥有用户，就不能占有市场。随着我国“四化”建设事业的不断发展，可靠性问题的紧迫性已逐步被人们所认识，并愈来愈受到重视：有关部委已着手在科技人员中开展可靠性“扫盲”运动，并建立可靠性研究中心；全国机械工程学会决定成立“可靠性工程专业学会”。为了适应当前形势的需要并推动我国可靠性事业的前进，我们在总结自己的实践和学习他人的经验的基础上编写了《系统可靠性、故障诊断及容错》一书，目的在于帮助读者掌握系统可靠性的理论知识和提高这方面的实践能力，另一方面也是粗陈刍见，抛砖引玉。

虽然零部件是建立系统的基础，但最终出现并运行于工农业生产、科研、国防、航天、航海等各个领域和部门的则是具有各种功能的设备或装置（系统），而不是个别的、孤立的零部件。零部件的可靠性问题都是在某一具体的和特定的系统中以某种特定形式反映出来的，系统的可靠性并不唯一决定于零部件的可靠性，正确运用系统可靠性理论和技术可以设计出系统寿命远高于零部件寿命的系统。因此，单纯研究零部件的可靠性问题已不能满足当前各个领域在实践中对可靠性工作者所提出的要求。

学习和研究系统可靠性理论的最终目的是为了发展和完善这种理论并将其应用于系统的设计、制造、调试和维修的实践中以提高系统的运行可靠性，因此，本书还遵循“学以致用”原则，将理论紧密联系实际，并通过对较多的具体线路和工程项目的设计，叙述了应用可靠性理论处理实际问题的方法和技巧。

近年来，电子计算机已成为很多先进系统中的主要角色，因此，本书用了一定的篇幅讨论复杂系统（网络系统、容错系统、故障诊断系统）和软件的可靠性问题。

目前，提高系统可靠性的途径通常有两种：一是“避错”（*Fault-Avoidance*），另一是“容错”（*Fault-Tolerance*），然而，实践经验证明，要有效地达到提高系统可靠性的目的，必须尽可能地同时采用“避错”和“容错”两种技术措施。因此，本书用了适当篇幅介绍在系统中应用综合性措施提高系统可靠性的实例。

学习过程，不但是一个艰苦的脑力劳动过程，而且也是一个思维按规律活动的过程。为了便于读者掌握系统可靠性方面的知识，本书在内容安排、数学推导、理论分析和文字叙述方面均考虑了由浅入深，循序渐进，并力求语言通顺，条理清楚和层次分明。

本书共分十四章：第1～3章为基础部分；第4～7章从可靠性角度讲述各种系统的物理模型和教学模型；第8章讨论系统可靠性设计的优化问题；第9～12章讨论有关复杂系统的故障诊断和可靠性增长问题；第13～14章介绍软件可靠性问题，由于软件可靠性的研究国外也才刚刚开始，极不成熟，尚未形成一门学科，所以本书中对这一问题叙述得也很粗浅，只能算是向读者提供点滴有关这方面的信息罢了。

中国科学院学部委员张钟俊教授审阅了本书的有关章节和材料，并为之作序，重庆大学徐宗俊教授、重庆大学出版社杨世泽社长和李淑芳总编为本书的撰写和出版提供了宝贵而中肯的意见，并给予了热情的支持和帮助；各级领导同志给予了鼓励，作者在此一并表示衷心感谢。

为了克服书中的缺点和错误，敬请同行、专家和广大读者给予指正。

作者

目　录

第一章 绪 论

§1.1 可靠性发展史

朴素的“可靠性”概念在我国两千多年以前就已出现了，例如史记淮阴侯列传里就记载有与概率有关的话：“智者千虑必有一失，愚者千虑必有一得”。这不但用百分数描绘了智者和愚者这两种人谋划的失败和成功概率，而且还阐明了概率论中“不可忽视小概率事件”的思想，即尽管某一事件出现(成功)的概率虽小，但只要重复试验多次，其出现(成功)几乎是必然的。又如我们常说的“万无一失”就是指某一事物的可靠度大于0.9999。然而将可靠性作为单独的一门学科，有目的、有计划地对它进行研究，却是近代的事情。第二次世界大战发生后，美国运往远东的军用设备，由于可靠性方面的缺陷，有50%以上不能在作战中发挥作用，特别是电子通讯装置，情况则更为严重。当时美国海军部门对此曾作过调查、统计，结果表明，完好率仅占30%。这样，美国不得不于1943年最后下决心抽调军事部门、科学研究单位以及有关生产厂家的技术力量，组成一个联合体，来研究可靠性问题。与此同时，德国火箭专家 R.Lusser 也开始了对火箭制导系统可靠性的研究，他将一个整系统看成是由许多个分系统串联构成，并用概率乘法公式计算出 V-Ⅱ型火箭制导系统的可靠性仅为0.75。继后 Lusser 曾企图进一步建立可靠性数学模型，寻求提高 V-Ⅰ型火箭制导系统可靠性的措施，但不久由于战争的失败而中止。

朝鲜战场上的失利不但暴露了美国军用装备的可靠性指标低，也有力地说明了研究可靠性问题的必要性和紧迫性。有鉴于此，美国国防部于1952年成立了电子设备可靠性咨询小组 AGREE(Advisory Group on Reliability of Electronic Equipment)，对军用设备方面的可靠性问题进行调查研究，于1957年提出了“电子设备可靠性报告”，阐述了这一问题的现状以及研究这一问题的理论基础和方法，从而大体上确定了美国可靠性工程研究的方向。

继 AGREE 以后，日本于1958年以“东大”高木先生为首成立了可靠性研究委员会，1967年盐见弘先生出版了专著《可靠性工程基础》。

苏联于50年代初期主要是着重可靠性基础理论、概率论以及随机过程方面的研究，50年代中期开始在电子工程、自动控制以及人造地球卫星等领域内进行可靠性基础理论的应用研究。1958年 А.П. 符拉柔也夫斯基发表了巨著《机械制造自动线》，其中对自动线的可靠性、故障分布规律及其对生产率的影响都作了详细而精辟的分析。1968年在布达佩斯举行了苏联及东欧数国电子产品可靠性学会第二次年会。

我国对可靠性问题的关注大约开始于 60～70 年代，当时在第四机械工业部所属部门内将提高电子元器件的可靠性作为突出问题而提出，继后因机床数控装置常出故障，致使数控机床不能在生产中发挥应有作用，阻碍了数控技术的推广和发展，从而引起数控界对可靠性问题的重视。1961年参考文献[8]中对轴加工自动调节系统的联接型式和可靠性问题进行了探讨，并提出了从应用故障诊断技术、提高维修水平方面采取综合性措施，以减少排除故

障时间和提高可修复系统的广义可靠度和利用系数。1979～1980年一机部和八机部组织了一个调查组，对该两部所属的266条自动线进行了调查，发现能正常工作的只占44.7%，基本能用的占25.9%，因经常出故障而不能启用的占29.7%，从而开展可靠性问题研究在机械工业部门也被提上了议事日程。

近年来国内有不少专家、学者都在从事可靠性研究工作，发表了在理论或实践方面颇有参考价值的论文和专著，如：《概率论基础及其应用》（王梓坤著）、《数字系统的诊断与容错》（陈廷槐、陈光熙合著）、《可靠性统计》（茆诗松、王玲玲合著）、《可靠性数字引论》（曹晋华、程侃合著）、《可靠性工程概论》（王时任、陈继平合著）等就是。

§1.2 研究系统可靠性的意义

系统的质量指标一般应包括以下三个方面：

1） 性能指标，如精度、速度、强度、刚度、灵敏度、稳定度、分辨率、清晰度、自动化水平……等。

2） 经济指标，如价格、成本、功耗、煤耗、油耗……等。

3） 可靠性指标，它是反映系统能在多长时间内保持其性能指标和经济指标的一种能力。性能指标和经济指标是不包含时间因素的，而可靠性指标则是与时间紧密相联的。现在的产品，要求在出厂时，不但要提供性能指标和经济指标方面的确切数据，还要提供可靠性指标方面的保证，比如平均无故障工作时间（耐用度、可靠度等）。

性能指标和经济指标对系统或元件来说固然重要，但可靠性指标则更不容忽视。

某些军用设备，为了经常保持在可靠工作状态，每年所支付的费用往往是该设备本身价格的几倍或十几倍。这一严重事实充分说明了，即使纯粹从经济角度考虑，研究可靠性问题也是非常必要的。

如果从安全方面考虑，可靠性问题则更为重要。一个通讯网络或雷达系统在作战时发生故障会导致大量人员伤亡或失去战机；飞机着陆架不能可靠地下放会造成机毁人亡的严重事故；降落伞自动张伞装置的失灵会使跳伞人员粉身碎骨；汽阀漏气或安全阀发生故障会造成车间或整个工厂的爆炸、焚毁等灾难性后果；一个元件或部件在可靠性方面所存在的缺陷往往不仅殃及该元件或部件本身，而是会在更大范围内和更严重程度上给整个系统和装置造成不可估量的损失，比如由于开关、控制系统的失灵或固体燃料箱所存在的隐患会导致整个航天计划的失败。上次的“阿波罗”号事故使三名宇航员葬身火海，本次“挑战者号”的蒙难导致七名宇航员身亡，这些都充分说明了可靠性在保障安全方面所占有的重要地位。

§1.3 系统可靠性包含的内容

严格讲起来，系统可靠性应包括以下三个方面的内容：

1） 系统工作可靠性 R_0(*Operational Reliability of System*)。它是系统在运行时的可靠性，是一种综合性的可靠性指标。

2） 系统固有可靠性 R_I(*Inherent Reliability of System*)。它是系统生产厂在生产过程中就已确立了的一种可靠性，它和生产厂所选用的材料、零部件、设计方案、软件结

构、硬件结构、制造工艺、装配工艺有密切关系。它是系统的内在可靠性，当系统在生产厂一旦制造出来，固有可靠性便已确立。固有可靠性的具体数据可由生产厂将系统放在模拟的实际工作条件和标准环境下进行测试而求得，这是要求生产厂予以确立的一个产品可靠性指标。

3） 系统使用可靠性 R_U(*Use Reliability of System*)。它与系统在由制造厂转给用户过程中的包装、运输、保管以及在实际使用过程中的环境(温度、湿度、振动、冲击)、操作水平、维修技术等因素有关。

三种可靠性不是互不相关的，它们之间存在有一定的关系，这种关系可以用数学式子近似地表述如下

$$R_O \approx R_U \cdot R_I$$

此式说明，R_O是由 R_U和R_I共同决定的，在一定的系统固有可靠性R_I的情况下，通过精心包装、运输、保管、改善使用环境、提高操作和维修水平等措施可以获得较高的系统工作可靠性 R_O。

本书对以上三个方面的可靠性问题虽然都将有所述及，但重点将放在讨论有关 R_I和 R_U上，即重点讨论在设计系统时，在保证性能指标和经济指标的前提下，通过数学分析，从可靠性角度考虑，采取一些措施(如采用可靠性分配、冗余、容错技术等)以保证系统结构的合理性，并根据可靠性理论对现有系统进行分析，找出其可靠性方面的缺陷以便加以改进；以及在使用过程中采用故障诊断技术，提高操作、维修水平以提高系统的使用可靠性 R_U。

§1.4 系统可靠性定义

在给出“系统可靠性”确切定义之前，首先叙述一下什么是系统。按照信息论的观点，可将具有各种不同运动形态的系统抽象成是一个借助于信息获取、传递、加工、处理而实现某种目的的运动客体，如图 1.1 所示。我们现在所讨论的系统则是指一种由若干个或若干种元器件、部件按一定结构形式组成的，具有一定功能和质量指标的综合体，是一种具体的、规模较小的系统。

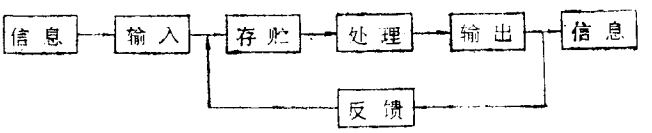

图 1.1

视叙述的方便和需要，我们有时亦将系统称之为产品(系统本身就是一种产品)，而将组成系统的元器件、部件称之为单元。在讨论可靠性基本理论和概念时，通常习惯于用“产品”或“元件”这一名词；而在讨论具体的系统可靠度问题时，通常习惯于用“系统”这一术语。

“系统”和“单元”本是相对的，比如当我们研究社会经济结构时，工厂只能算是其中的一个单元；当我们研究生产过程时，工厂本身就是系统，而车间则是单元；当我们研究工艺加工过程时，车间是一个系统，而车间内的各种加工设备则是单元；当我们研究某台具体设备时，则设备本身是系统，而组成设备的元器件、部件则是单元。

系统分“不可修复型系统”和“可修复型系统”两种。不可修复型系统如易耗品(灯泡、电池)、一次性使用品(炮弹、炸弹、爆破装置)、无人航空航天器(无人驾驶飞机、卫星、飞船)等。可修复型系统如交通运输工具、加工机床、动力机械、检测仪器、计算机、自动化装置……以及其它生产设备等。大多数地面上的设备和装置都是可修复型系统。

系统可靠度定义：系统在规定的条件下和规定的时间内，完成规定功能(无故障)的概率称之为系统可靠度(*System Reliability*)。

这一定义中包含五个部分：系统；规定的条件；规定的时间；规定的功能；概率。什么是系统，这在本节的前面已经叙述过了，不再重复。至于什么是概率，则将在第二章中介绍。这里仅就什么是规定的条件、时间、功能加以解释。

规定的条件。这通常指的是环境条件(如温度、湿度、振动、冲击、噪音、磁场、电场、油污、铁屑、灰尘……)、维修条件(如维护保养措施、修理技术水平等)和使用条件(使用者的操作技术熟练程度)，这三方面的条件对系统的可靠性有着直接影响。条件不同，虽是同一系统，其可靠性则大不一样。比如系统在实验条件下工作和在车间条件下工作，在室内工作和在野外工作，其可靠性可以相差十分悬殊。所以，不在规定的相同条件下讨论或比较系统的可靠性指标就没有意义。

规定的时间。前面曾提到，可靠性是包含时间因素的产品质量指标，撇开时间就失去了讨论可靠性的前提。在讨论可靠性时，依据系统及其功能的不同，“规定时间”的表示方法和长短亦随之而异，比如对一般的机器和仪器仪表来说用工作小时表示，对交通运输和运载工具(如汽车、火车、飞机、火箭等)来说用行驶或飞行公里表示，对齿轮、轴承和某些受弯曲载荷的产品来说用循环次数表示，对成功-失败型装置来说则用试验次数表示。导弹、火箭要求在几分几秒内可靠；灯泡、显象管要求几千上万小时内可靠；机器设备、桥梁建筑要求几十年几百年内可靠。产品可靠性随着时间的加长而逐渐降低，它是时间的非增函数。一定的可靠性是对一定的时间而言的，不在规定时间的前提下讨论可靠性同样是没有意义的。

规定的功能。通常用产品的各项性能指标(如精度、速度、稳定度……)来给出。在工作或试验中，通过检测，如确认产品达到了规定的性能指标，则称该产品完成了规定的功能，反之，则称该产品丧失了规定功能。今后我们将能完成规定功能的产品称之为“完好”产品，丧失了规定功能的产品称之为“失效”产品，将产品由完好状态向失效状态的转变称之为发生“失效”或“故障”，将此刻相应的各项性能指标称之为“失效判据”或“故障判据”。在讨论某种产品的可靠性时，明确而合理地给出定量的失效判据是非常重要的，否则就失去了讨论可靠性的准绳。

综上所述，可以认为：系统可靠性作为一门学科，其任务就是在规定时间、规定条件和规定功能的前提下研究系统(产品)发生故障的统计规律性，系统可靠性数学模型就是这种规律性的数学综合、分析与描述，借助于此，在设计和使用时便可为提高或预测系统的可靠性提供数量上的依据。

系统维修度定义：对发生故障的可修复系统在规定的条件下和规定的时间内完成修复的概率称之为系统维修度(*System Maintainability*)。维修度是表示通过维修活动将系统由不正常状态恢复到正常状态的一种恢复能力。

系统有效度定义：在某种维修条件下和规定的时间内将可修复系统的功能维持正常状态的概率称之为系统有效度(*System Availability*)。系统有效度是将系统可靠度和系统维