工程系统可靠性分析基础

江荣汉 编著

湖南大学出版社

内容简介

可靠性研究是一个新兴的研究领域，内涵丰富，外延广泛。其核心是系统可靠性分析计算，即由元件的可靠性指标计算出系统可靠性指标。从这一特点出发，本书主要介绍工程系统可靠性分析的两种基本方法——解析法和模拟法。解析法中着重介绍了网络分析法、状态空间法和故障树分析法；模拟法中介绍了蒙特卡罗非时序模拟与时序模拟法。全书熔基本理论、计算方法和工程实例于一体。内容精炼，结构严谨，概念明确，通俗易懂。可供工科院校各类专业、各类研究班与培训班教学参考，也可供科研、设计及工程管理人员参考。

工程系统可靠性分析基础

江荣汉　编著

☆

湖南大学出版社出版发行

（长沙岳麓山）

湖南省新华书店经销　　湖南大学印刷厂印刷

☆

787×1092　32开　6印张　135千字

1987年12月第1版　1987年12月第1次印刷

印数：0001——3500册

ISBN 7—314—00177—4/TP·9

统一书号：15412·40　定价：1.45元

前　言

可靠性问题渗透于各个工程领域，贯穿于各个工程系统（或产品）的规划、设计、制造、安装和运行的各个环节。近二十多年来，国外在开展可靠性研究方面取得了很大进展。一些政府还公布和推行了有关可靠性的国家标准和准则。可靠性研究领域异常活跃。十多年来，我国在这个领域的研究也有较大发展。部份高等学校已开始设有可靠性课程，出版了一些专著与教材。为了适应这种形势，湖南大学电气工程系有关专业试对高年级本科生开设选修课。本教材即应此需要于1984年完成初稿。经几年的教学实践，进行了修改与补充。可靠性研究的内涵丰富，外延广泛。本书力图以最小的篇幅阐明最核心的问题——工程系统可靠性的分析计算方法，以引导初学者入门，并为深入具体工程领域的可靠性研究打下理论基础。

全书共分六章。第一章诸论，第二章元件的可靠性，为本书的基础；第三章网络分析法，第四章状态空间法，第五章其他分析方法与蒙特卡罗模拟法，为本书重点；第六章可靠性数据与估值方法的应用，为所述方法的工程系统应用实例。本书内容精炼，概念清晰，熔基本理论、计算方法和工程应用于一体。可供工科院校各类专业和各种培训班及研究班教学参考，也可供科研、设计及工程管理人员参考。

成书过程中得到教研室同志们及多方人士的支持与帮助，此外，还参阅了许多国内外作者的专著与论文，在此谨致谢忱。

由于水平所限，时间仓促，缺点与错漏在所难免，敬请读者批评指正。

编著者 1987年8月

目　录

第一章 绪 论

第一节 可靠性研究课题的提出与发展过程

一、问题的提出

可靠性课题的提出具有其深刻的原因。

首先，随着生产的发展和科学技术的进步，为人类的生产与生存的装备和系统越来越复杂。如军事工程系统，通讯系统，电力系统及其他系统都在迅速发展。在空间上，系统向极端方向发展。有向大方向发展的，如电力系统，现在世界上已出现了全国统一电力系统（苏联于1980年形成了装机容量为2.27亿千瓦的统一系统），也出现了跨国的联合电力系统（北美联合电力系统，西欧联合电力系统，苏联、东欧和西欧的两联合系统可能联成更大的系统）。也有向小方向发展的，如超大规模集成电路，集成度越来越高，元件体积越来越小。八十年代后期，一个芯片上将出现集成100万个晶体管的微电子系统。1990年至2000年将出现1千万个至1亿个晶体管的微电子器件[1]。

在时间上，系统也向极端方向发展。系统的无故障平均时间（即连续工作时间）越来越长，由几天增至几十年，即不需检修而可长期工作（如电力电压和电流互感器等）；系统的动作时间越来越短，即其运动速度越来越大，如计算机运算速

度，1990 年可望超过 1 千亿次/秒，2000 年以前可达到万亿次/秒[1]。

在环境方面，系统所处的条件也向极端方面变化。如高温、高压、高湿、高动态负载（机械的和电磁的振动和冲击）、强电磁干扰和极低温等。例如在炮弹上的元器件要承受 20 000g的冲击加速度。

同样，系统的运行也越来越复杂，若一元件有两种工作状态，即工作与故障状态（谓之两状态元件），n 个元件组成的系统，就有 2^n 个工作状态。100个元件组成的系统，则有 $2^{100}\approx10^{30}$ 个工作状态。对于三状态元件（即正常工作状态，短路故障状态和开路故障状态，如三极管），100个元件组成的系统，则有 $3^{100}\approx10^{40}$个工作状态。大型计算机有100万个元件；阿波罗宇宙飞船有 700 万个元件；一座核电站约有设备5000台，仪表9000种，阀门上万个，用管线连起来组成 170 个系统；一个电力系统的元件数更多，其工作状态也就更多了。这些工作状态中有的是系统正常工作状态，有的是系统故障状态。为分析这些复杂系统，以减少故障，凭过去的经验和直观定性分析已不适应要求。必须建立一门新的学科来分析其可靠性。

其次，建设现代大型系统需要大量投资。如电力工业，是产业部门中投资最多的一个，占国家总投资的20%～25%（日本），甚至三分之一（苏联）[2]。每年还要继续投入大量的人力、物力和财力，以保证其继续发展。这样大投资的系统的建设和运行，必须要有科学的可靠性论证作基础，才能保证其经济效益。

再次，现代大型系统的故障将引起一系列严重恶果，造成人们生活的混乱和国民经济的损失，以及严重的社会与环

境的影响。系统事故是灾难性的。例如1965年11月9日美国东北地区电网大停电，12分钟，2100万千瓦负荷失电，停电最长时间达13小时，受影响的地区达20万平方公里，居民达3千万人，损失1亿美元。又如，由于集成电路的失效而致的美国预警系统于1979年11月9日、1980年1月3日和6月3日三次误发核袭击警报。这些系统事故所带来的社会与环境方面的社会压力往往比经济损失导致的压力更大，所以系统事故的冲击往往成为系统可靠性研究的发展动力。

就这样，可靠性研究这门崭新的学科应运而生，形成了以概率统计为基础，集系统工程、运筹学、质量控制、生产管理多学科之大成的可靠性研究领域。

二、发展过程

可靠性的理论基础概率论与数理统计在本世纪三十年代开始得到迅速发展，而可靠性研究课题的本身，则源于三、四十年代用概率论分析机器维修问题，用更新论分析更换问题，以及用材料疲劳与极限理论来研究材料复合问题等。

可靠性的大量研究是应航空与军事工程的需要首先提出的。二次世界大战期间，德国人计算了他们的 V_1 与 V_2 型导弹的动作概率，以分析其可靠性。美国人是从军用电子设备可靠性分析开始的。当时美国有份报告提到：飞机运到东方时，其机载电子设备有60％发生了故障，军舰上的电子设备70％发生了故障，陆军通讯设备的电子备品是必须品的9倍，……。因此，迫使美国从40年代初开始对电子设备的可靠性进行全面的研究[3]。

紧接着，可靠性研究应核工业，即原子反应堆的可靠性与安全性的要求而发展。连续供电的要求，促进了电力系统可

靠性的研究。连续生产过程的工业（如钢铁工业、化学工业……）的减少损失和空闲的要求，促进其可靠性研究的发展。目前，可靠性研究已经进入了所有的工程领域。人们制订了一系列有关国家与国际标准，建立了可靠性研究试验中心及协调机构，发展了可靠性数据系统与交换网，以及创建了可靠性教育。

现在可靠性理论已得到了相当的发展，它除了提供定性的可靠性评价与一系列可靠性数量指标，说明系统如何故障和故障后果之外，还能提供一系列设计、试验与维修方法，以解决可靠性优化问题和提高系统可靠性；另外，它还将系统可靠性与其投资和运行经济性等联系起来，因而使人们得以适当地处理可靠性与经济性的矛盾，合理地作出规划和设计，以及解决运行管理中的决策问题。

可靠性是由于今天在世界范围内科学技术各个领域高层次的成就，人类社会生活各个领域的高层次要求，人类科学认识潜力、创造潜力的高层次萌动，……，诸如此类多股高层次有序性潮流的交汇而产生和发展的，是一定历史时期的产物；既依从整个社会发展的普遍规律，也依从科学发展的内在规律；经历着描述阶段、逻辑分析阶段和定性与定量统一的阶段。

第二节　可靠性研究的内容和方法

一、可靠性的概念

可靠性（Reliability）的老概念是关于人或事的可信赖的程度的定性描述。其新概念是关于用概率数学来精确地推导工程系统性能的量度的一门新学科。

例如，在电力系统中，可靠性与经济性的矛盾过去是用定性的设计和运行准则来解决的。这些准则中引用的确定性指标是有缺陷的，因为它们没有反映电力系统行为、用电需求和元件故障的概率或随机的性质。这是由于当时缺乏数据、计算工具和可靠性计算方法，以及缺乏对于概率数学和概率准则的意义的了解所致。现在上述情况完全改变了，因而建立在概率数学上的可靠性的新概念就很快地发展起来[4]。现在为人们公认的关于可靠性的定义是：一个元件或装置或系统，在规定条件下和预定时间内完成规定功能的概率。1985年，苏联国标对可靠性给以定义[5]："可靠性具有复合的属性。根据对象的用途与运行条件，它包括连续性、耐久性、可维修性和可保存性，或这些特性的组合。对于具体的对象与运行条件，这些特性有各自相关的意义。"这使可靠性的定义一般化了。对于电力系统可以找到简化的定义：可靠性是大电力系统把生产的电力供给到主要配电点上去的保证的程度。

由于研究的内容不一样，可靠性分为[2]：

静态可靠性（Static Reliability）：由系统元件所引起的系统故障，仅研究一次性故障发生的部分，不考虑此故障影响而形成多次故障所及的其他部分，也不考虑系统动态特性（如系统稳定性……），即数秒以内的暂态现象。

动态可靠性（Dynamic Reliability）：即一次性故障向周围波及，达到系统中健全部分，从而导致多次性的故障，此时要考虑形成系统破坏的二重及三重事故，即要有一系列事故发展的预想。

这是两种特性根本不同的问题，属于不同的学科分支，前者简称可靠性（Reliability），后者称安全性（Security）。但也有一些作者[5]用不同术语来描述类似分类方法，称前者

为系统充足性（System Adequacy），称后者为系统安全性（System Security），统称为系统可靠性（System Reliability）。

二、可靠性研究的内容和方法[7,8]

可靠性研究的内容丰富，方法很多，这里列举一种概括方式。

可靠性数学（Reliability Mathemetics），它是基础数学（代数学、分析学、概率论、统计学）和应用数学（数学规划、网络分析、网络模拟、随机过程、排队论、信息论、对策论）的综合应用，它们在经典数学中研究得不多，而是近几十年提炼与总结出来的。它是可靠性研究的理论基础。

可靠性分析（Reliability Analysis），它是用网络分析法、网络模拟法、状态空间法、故障树法和FMEA法等各种方法，根据系统组成元件的可靠性来分析系统的可靠性。

可靠性工程（Reliability Engineering），包括：

① 可靠性预测——在设计阶段，按元件→子系统→系统，自下而上地估算可靠性指标，从而找出其薄弱环节。

② 可靠性分配——根据系统与元件之间的可靠性功能关系，将系统可靠性指标在元件之间合理分配，也就是按系统→子系统→元件，自上而下地落实可靠性指标。

③ 可靠性优化——运用最佳备用设计、故障诊断技术和最佳预防措施来解决系统设计、制造和运行中的优化问题。

④ 可靠性试验——贯穿在系统的规划、设计、制造和运行的全过程，包括评价试验、证实试验、实用试验、生产试验和寿命试验。

可靠性管理（Reliability Management），包括全面的质量管理和安全管理，即包括系统（产品）的规划、设计、安装(制造)、运行和维护中可靠性指标的管理，故障数据的收集、分析和反馈，可靠性组织的建立，可靠性教育研究的发展等。它是科学、技术与艺术三结合的产物。

总之，可靠性研究是一个新兴的研究领域，是一门边缘科学，它的定义、术语与研究范围正在发展与完善过程中，并已应用于各个工程领域，贯穿于各个工程系统的规划、设计、运行和管理的各个阶段。它既有运用于各个工程系统的共同的理论基础和计算原理，又有涉及各个工程系统所特有的属性和特征。

可靠性研究的外延非常广泛，内涵非常丰富。但其中最基本的是可靠性分析计算，即由元件可靠性指标计算出系统可靠性指标。

可靠性分析计算现已成为任何工程系统与技术产品的设计（包括性能设计与可靠性设计）过程中必不可少的环节。从微电子电路到统一的国家通讯系统，从单台动力机组到国家联合电力系统，对拟采用的设计、建设与运行的技术方案都必须进行可靠性定量分析，算出量化的可靠性指标。这是由于已经发展了能为研制者（厂家）与使用者(用户)所共同接受的通用的可靠性计算方法。可靠性分析计算的基本方法虽然主要来自电子技术领域，但可以应用于其他的工程与国民经济各领域，并且为其他各个领域——无线电电子学、情报、机械制造、建筑和电力——形成具有各自特点的可靠性分析计算方法提供了基础。

此外，可靠性分析计算是可靠性预测（由元件到系统的合成计算）、可靠性分配（由系统到元件的分解计算）和可

靠性优化（在一个或多个约束条件下达到最大可靠度或最小耗量的优化计算）等其他可靠性研究环节的基础。

因此，本书着重讨论几种基本工程可靠性分析计算方法，以为读者进一步深入各个领域的可靠性研究作好理论准备。

第二章　元件的可靠性

确定元件、子系统或系统的可靠性模型与可靠性特征量（指标）是可靠性分析的基本任务。元件可靠性是系统可靠性的基础。

一个设备或系统通常由元件与子系统构成。为了研究方便，常将其分为元件与系统两级或多级，从而根据元件可靠性特征量，用可靠性估值方法算出系统的可靠性特征量。

根据研究对象的级别（元件、子系统与系统），可靠性特征量（指标）也可以分为运行特征量（指标）与技术特征量（指标）。前者可以方便地描述高级对象（如系统）的功能的质量，是用户所需要的；后者反映了“制造工艺”的特点，可以方便地描述低级对象（如元件）的可靠性，是估计高级对象（如系统）可靠性所需要的。

第一节　元件及其可靠性概念

在可靠性研究中，所谓元件，就是一个基本单元，在系统运行过程中其可靠性特征量保持不变。但并不意味着再不能从结构上将其分解。相对来说，元件可靠性特征量比较容易地从实际运行经验中得到。因此在系统可靠性分析中，元

件的可靠性指标是已知的。

元件与系统的概念是相对的。一个研究对象在一种研究中可以认为是系统，而在更大的研究范围内则可以认为是元件，取决于研究的目的、研究的精度、研究概念的水平以及研究对象在研究范围内的地位等。

元件按失效模式（失效是指元件丧失规定的功能，对可修复元件通常也称为故障）可分为两状态与三状态元件。前者是指元件有工作状态与失效状态。后者是指工作状态和两种失效状态。如继电器有拒绝动作和误动作两种失效状态。元件还有部分失效状态（如发电机在降低出力下运行）和公共失效状态（由于设计与制造缺陷、运行失误或自然灾害等引起的多元件同时发生的同种失效）。多种失效形式使可靠性问题复杂化，近来研究者给予特别重视。

元件按维修性可分为不可修复与可修复元件。前者是指失效后不能或不值得去修复的元件；后者是指失效后可以修复的元件。前者的寿命是指发生失效前的工作时间。后者寿命是指相邻两次故障间的工作时间，这也称为无故障时间。电力系统中的元件是可修复的。

元件可靠性用可靠性特征量（或可靠性指标或可靠性数据）即某种数量指标来表示，其真值是理论数值。在具体估算时，其值与所利用的数据，数据处理方法及某些特殊假定有关。据不同数据处理方法，有不同名称，如特征量估计值，特征量观测值，特征量外推值和特征量预测值[9]。

由于元件特性和环境条件的变化，可靠性特征量是一个随机数。常用某一个未知的固定数来代替其描述统计分布的特性。可靠性特征量必须从环境和元件特性不断变化条件下的多年的观察数据中得出。在实际中，在一定方式下一定时

间内某种故障的元件数目是容易确定的，然而在同一时间内没有故障的元件数目却很难准确统计，因而收集与统计可靠性特征量是比较困难的。统计所得元件可靠性特征量与其本身设计特点、构造特点以及环境条件有关，往往难于反映元件的实际可靠性特征。这是由于所取元件的运行条件和环境条件是不完全符合实际的，且统计的数目（或时间）是有限的缘故。

下边按元件的可修与否来分别研究其可靠性特征量。

第二节　不可修复元件的可靠性特征量

一、可靠度R(t)或不可靠度F(t)

不可修复元件的寿命T是从投入运行开始到灾变性失效发生为止的一段时间，是一个随机变量，决定于其概率分布。

$$F(t)=P(T\leqslant t) \qquad (2\text{-}1)$$

表示元件寿命T小于t的概率，称为积累概率分布函数。它表示从开始运行（$t=0$）到时刻t的所有时间内可能发生失效的概率之和，是t的函数。它必定在0与1之间，$F(0)=0$，即元件开始运行时，没有失效；$F(\infty)=1$，即元件运行无限长时间之后，完全失效。其概率密度为

$$f(t)=\lim_{\Delta t\to 0}\frac{1}{\Delta t}P(t<T\leqslant t+\Delta t) \qquad (2\text{-}2)$$

可以直接看出，（2-1）与（2-2）式有下述关系

$$F(t)=\int_0^t f(t)dt \qquad (2\text{-}3)$$

$$f(t)=\frac{dF(t)}{dt} \qquad (2\text{-}4)$$

根据定义，元件可靠性是在规定条件下和预定时间内完成规定功能的概率，它也是可靠性特征量，称为可靠度，即

$$R=P(T>t_m) \qquad (2\text{-}5)$$

式中 t_m ——时间段，或称任务期，在此时段内元件完成规定的功能。

显然，可靠度R是t_m的函数。故元件可靠度定义为

$$R(t)=P(T>t) \qquad (2\text{-}6)$$

根据概率论，并考虑到（2-1）式，有

$$P(T>t)+P(T\leqslant t)=1$$

即 $$P(T>t)=1-P(T\leqslant t)=1-F(t).$$

也就是 $$R(t)=1-F(t) \qquad (2\text{-}7)$$

根据分布函数的特性，元件可靠度$R(t)$必定在0与1之间，可靠度$R(0)=1$，即元件开始运行时完全可靠；可靠度$R(\infty)=0$，即元件运行无限长时间之后，完全失效。

由(2-7)式可见，$F(t)$表示元件损坏的程度，或者说是元件在规定条件下和规定时间内失效的概率，可以称为不可靠度（函数），或累积失效概率。

例2-1 对N个样品进行寿命试验，每经过 Δt 时间后检查一次，第 i 次有n_i个样品失效（图2-1）。求该样品的可靠度$R(t)$的观测值。

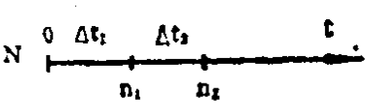

图2—1 N个样品寿命试验过程

解 据题意，可作出试验过程于图2-1。