可靠性与可测性分析设计

丁 瑾 编著

北京邮电大学出版社

可靠性与可测性分析设计

（博士后基金资助项目）

丁　瑾　编著

北京邮电大学出版社

图书在版编目（CIP）

可靠性与可测性分析设计/丁瑾编著. —北京：北京邮电大学出版社，1996. 7

ISBN 7-5635-0245-9

Ⅰ. 可… Ⅱ. 丁… Ⅲ. ①电子电路-可靠性设计 ②电子电路-可测函数-设计 Ⅳ. TN702

中国版本图书馆 CIP 数据核字（96）第 07945 号

内 容 提 要

本书对系统与数字电路的可靠性和可测性作了完整的叙述及讨论。书中很多部分是作者多年科学研究和教学实践的结果。全书共八章。第一、二章介绍可靠性与可测性的一些基础知识和基本概念。第三、四章讨论系统的可靠性分析及其设计，并介绍了冗余对系统可靠性的影响。第五、六、七章分别讨论了数字电路的测试及其可测性分析设计，重点介绍了概率可测性分析和结构可测性设计。第八章介绍了可维性设计，主要叙述了失效率与修复率的分配。

本书对电子、系统工程、自动控制、动力、通信及信息等学科领域有关的高年级大学生、研究生和工程技术人员是一本有益的参考书。

可靠性与可测性分析设计

丁 瑾 编著

责任编辑 王履镕 詹汉强

*

北京邮电大学出版社出版

（北京市海淀区西土城路 10 号）

新华书店北京发行所发行 各地新华书店经销

河北高碑店市印刷厂印刷

*

787×1092 毫米 1/16 印张 14 字数 352 千字

1996 年 7 月第一版 1996 年 7 月第一次印刷

印数：1—1000 册

ISBN 7-5635-0245-9/TN・106 定价：17.80 元

前　言

随着电路集成度的提高，系统的复杂及其应用的推广，电路的可测性与系统的可靠性问题日益受到广泛的重视。

提高系统的可靠性可从两个方面着手，一是从系统结构方面着手，降低整个系统的失效率，二是从系统维修方面着手，提高整个系统的修复率。降低系统的失效率主要采用容错技术，提高系统的修复率在很大程度上依赖于测试技术。为了完整地介绍与讨论容错技术和测试技术的传统方法和最新发展，作者向相关专业的大学生、研究生和工程技术人员奉献此书。

本书从理论和实践两个方面全面地介绍了系统的可靠性分析与设计以及数字电路的测试与可测性。在编写过程中，既强调基础理论、基本概念，又注重工程实践、实际应用；既具有系统性，又不失重点；既具有一定的深度，又能深入浅出，便于理解，特别注意近期新成果的出现，其中很多部分是作者多年科研经验与教学实践的结晶。但由于作者水平有限，错误和不妥之处在所难免，敬请同行们批评指正。

本书承蒙北京大学谢柏青教授和宁林副教授审阅，在编写过程中，得到胡健栋教授，张志美老师和纪蓉同志的很多帮助，在此一并表示衷心地感谢！

作者

一九九五年三月

目　　录

第一章　基础知识

第二章　基本概念

第三章 系统的可靠性分析

第四章 系统的可靠性设计

第五章 测试码的产生

第六章 可测性分析

第七章 可测性设计

第八章 系统的可维性设计

第一章　基础知识

在进行可靠性与可测性分析和设计时，经常使用一些基本的数学工具，包括概率论、布尔代数、随机过程等。本章将简要介绍有关这方面的数学基础知识。

1.1　概率基础[1,2]

1.1.1　事件

在科学试验中，人们把得到的结果称作事件，事件发生的规律可以通过观察归纳出来。通常把事件分成如下三类：

(1) 偶然事件。在一定条件下，某一事件可能发生，也可能不发生，则称此事件为偶然事件（或随机事件）。例如，抽取两件产品，观察其质量合格与否，“两件产品都合格”是一个事件，“两件产品都不合格”是一个事件，“至少一件合格”也是一个事件，上述事件都是偶然事件。

(2) 必然事件。在一定条件下，某一事件必然发生，则称该事件为必然事件。譬如，“两件产品的合格数小于等于两件”为必然事件。概率论中，必然事件通常用 Ω 来表示。

(3) 不可能事件。在一定条件下，某一事件不可能发生，则称该事件为不可能事件。例如，“两件产品的不合格数大于 2”是不可能事件。概率论中，不可能事件通常用 Φ 来表示。

事件间存在如下关系：

(1) 对立事件。在基本空间 Ω 中，由一切不属于 A 事件的基本事件组成的事件，称为 A 事件的对立事件，以 $\overline{A}$ 表示。

(2) 包含事件。若事件 A 的每一个基本事件都包含在事件 B 中，则称事件 B 包含事件 A，以 $B \supset A$ 表示。

(3) 相等事件。若 $B \supset A$ 和 $A \supset B$ 同时成立，则称 A 事件与 B 事件相等，以 $A=B$ 表示。

(4) 并事件。由属于事件 A 或属于事件 B 的全部基本事件组成的事件，称为事件 A 与事件 B 的并，以 $A \cup B$ 表示之。

(5) 交事件。由事件 A 与事件 B 中所有共同的基本事件组成的事件，称为事件 A 与事件 B 的交，记为 $A \cap B$。

(6) 相容不相容事件。若事件 A 与事件 B 没有公共的基本事件，则称 A 与 B 事件互不相容。反之，称为相容。例如，A 和 $\overline{A}$ 为互不相容事件，而“至少一件产品合格”与“两件产品合格”是相容事件。

(7) 差事件。由所有属于 A，但不属于 B 的基本事件组成的事件，称为事件 A 对 B 的差，记作 $A-B$。例如，$\overline{A}=\Omega-A$。

1.1.2　事件的频率与概率

定义：在相同条件下进行 n 次试验，事件 A 出现的次数 m 与 n 之比，称为事件 A 出现的

频率 $\hat{P}\{A\}$，可表示为

$$\hat{P}\{A\}=\frac{m}{n} \tag{1-1}$$

定义：在相同条件下进行试验，当试验次数 n 逐渐增大时，事件 A 出现的频率逐渐趋于一常数，我们称此常数为事件 A 发生的概率 $P\{A\}$，可表示成

$$P\{A\}=\lim_{n\to\infty}\frac{m}{n} \tag{1-2}$$

从事件及概率的定义中，我们可以看出概率具有如下性质：

(1) 任何事件 A 的概率 $P\{A\}$ 总是在 0 和 1 之间，即

$$0\leqslant P\{A\}\leqslant 1$$

(2) 必然事件 Ω 的概率等于 1，即

$$P\{\Omega\}=1$$

(3) 不可能事件的概率等于 0，亦即

$$P\{\Phi\}=0$$

1.1.3 排列与组合

在概率计算中，排列与组合占有重要的位置。我们把 n 个不同单元按某种次序排成一列，称为**排列**。若在排列中只考虑排列不同的单元，而不考虑先后次序，我们称其为**组合**。

(1) **全排列** 有 n 个单元，将它们进行排列，若所有单元均要排入，并且每个列中，每个单元仅仅出现一次，那么这种排列称为**全排列**。全排列总数为

$$P_n=n! \tag{1-3}$$

(2) **选排列** 从 n 个单元之中任取 m 个单元进行排列，称为**选排列**。其排列总数为

$$A_n^m=\frac{n!}{(n-m)!} \tag{1-4}$$

(3) **组合** 从 n 个单元中，每次取 m 个单元进行组合，其组合总数为

$$C_n^m=\frac{n!}{(n-m)!\ m!} \tag{1-5}$$

1.1.4 非独立事件与条件概率

定义：如果事件 A 是否发生与事件 B 是否发生没有关系，则称事件 A 与事件 B 相互独立。可用概率表示为

$$P\{AB\}=P\{A\}\cdot P\{B\} \tag{1-6}$$

事件的独立性概念，在可靠性和可测性理论中起着重要作用，可靠性与可测性分析中很多结论，均是在假设事件间独立的情形下获得的。

定义：在事件 B 发生的条件下，事件 A 发生的概率称为**条件概率**，记为 $P\{A/B\}$，且

$$P\{A/B\}=\frac{P\{AB\}}{P\{B\}} \tag{1-7}$$

并称事件 A 和事件 B 为**非独立事件**。

设事件 A_1，A_2，…，A_n 两两互不相容，且

$$\begin{cases}P\{A_i\}>0,\ i=1,\ 2,\ \cdots,\ n\\ \sum\limits_{i=1}^{n}A_i=\Omega\end{cases}$$

现考虑事件 B，只有当事件 A_1，A_2，…，A_n 中任一个发生时，它才发生，这时，我们有[2]

$$P\{B\}=\sum_{i=1}^{n}P\{A_i\}P\{B/A_i\} \tag{1-8}$$

(1-8)式称为全概率公式，是概率论中的一个基本公式，在可靠性和可测性分析中也经常用到。

1.2 布尔代数的基本定律[3,4]

布尔代数又称逻辑代数，是用来进行事件之间的逻辑运算的。设 A、B、C 均为逻辑变量(即取值为 0 或 1)，则有下述表达式成立：

(1) 交换律 $A+B=B+A$，$AB=BA$

(2) 结合律 $A+(B+C)=(A+B)+C$，$A(BC)=(AB)C$

(3) 吸收律 $(A+B)A=A$，$A+AB=A$

(4) 分配律 $A(B+C)=AB+AC$，$A+BC=(A+B)(A+C)$

(5) 等幅律 $A+A=A$，$AA=A$

(6) 互补律 $\bar{A}+A=1$，$\bar{A}A=0$

(7) 双重否定律 $\bar{\bar{A}}=A$

(8) 反演律 $\overline{A+B}=\bar{A}\,\bar{B}$，$\overline{AB}=\bar{A}+\bar{B}$

(9) 不交并律 $A+B+C=A+\bar{A}B+\overline{(A+\bar{A}B)}C$

布尔代数的运算定律，在可靠性与可测性分析和设计中，对系统和电路内各状态之间的化简和转换起着有益的作用。

1.3 随机变量及其数字特征[5]

1.3.1 随机变量

许多随机现象的结果表现为一定的数量，这个量可用 X 来表示，它是随一些偶然因素而随机改变的，因此，我们称 X 为随机变量。

例如，设备工作的基本结果（即状态）用 X 来表示，那么可得：

$$\begin{cases} X=0 & \text{工作状态；} \\ X=1 & \text{失效状态。} \end{cases}$$

又如打靶时子弹着落点离靶心的距离用 X 表示，可有：

$$\begin{cases} X=0 & \text{子弹着落点离靶心距离为0cm；} \\ X=10 & \text{子弹着落点离靶心距离为10cm；} \\ 20\leqslant X\leqslant 50 & \text{子弹着落点离靶心距离在20到50cm之间。} \end{cases}$$

可见随机变量种类很多，它可以是离散的，也可以是连续的，是有限的，也可以是无限的。例如，上面的设备工作基本状态是离散型的，而打靶时子弹着落点离靶心距离是连续型的，抽取6个产品的次品数为有限型的，而自然数为无限型的。

尽管随机变量 X 的取值是随机的，但它遵从一定的概率分布规律。

1.3.2 随机变量分布及密度函数

设 X 为一离散型随机变量，它可能的取值有 x_1，x_2，…，x_n，它们分别取这些值的概率为

$$P\{X=x_i\}=p_i \qquad i=1,\ 2,\ \cdots,\ n \tag{1-9}$$

可列表表示为

X	x_1	x_2	…	x_n
$P\{X=x_i\}$	p_1	p_2	…	p_n

p_i 具有如下性质：

(1) $p_i \geqslant 0$

(2) $\sum_{i=1}^{n} p_i = 1$

那么，我们可得 $X \leqslant x$ 的概率 $P\{X \leqslant x\}$ 为

$$Q(x) = P\{X \leqslant x\} = \sum_{x_i \leqslant x} p_i \tag{1-10}$$

设 X 为一连续型随机变量，它在 x 点处的概率为 $\Phi(x)$，那么 $\Phi(x)$ 应有下列性质：

(1) $\Phi(x) \geqslant 0$

(2) $\int_{-\infty}^{\infty} \Phi(x)\mathrm{d}x = 1$

依照离散型随机变量，我们可得 $X \leqslant x$ 的概率 $P\{X \leqslant x\}$ 为

$$Q(x)=P\{X \leqslant x\}=\int_{-\infty}^{x} \Phi(x)\mathrm{d}x \tag{1-11}$$

由上所述，我们可得随机变量的分布函数和密度函数的定义。

定义：设 X 是一个随机变量，x 是一个任意实数，“$X \leqslant x$”这一事件的概率即为随机变量 X 的分布函数 $Q(x)$，而随机变量分布函数曲线的斜率称为它的密度函数 $\Phi(x)$，可表示为

$$Q(x)=P\{X \leqslant x\} \tag{1-12}$$

$$\Phi(x)=\frac{\mathrm{d}Q(x)}{\mathrm{d}x} \tag{1-13}$$

1.3.3 随机变量的数学期望及方差

随机变量的分布函数和密度函数尽管能描述随机变量的统计特征，但难以得到随机变量的全面的数字特征，其中最有影响的是“数学期望”和“方差”。

定义：设 X 为一离散型随机变量，且级数 $\sum_{i=1}^{\infty} x_i p_i$ 绝对收敛，其中 x_i，p_i 分别是 X 的可能取值及相应的概率，则此级数就是随机变量 X 的数学期望 $E[X]$，即

$$E[X] = \sum_{i=1}^{\infty} x_i p_i \tag{1-14}$$

若 X 为一连续型随机变量，密度函数为 $\Phi(x)$，且 $\int_{-\infty}^{\infty} |x|\Phi(x)\mathrm{d}x$ 收敛，则

$$E[X] = \int_{-\infty}^{\infty} x\Phi(x)\mathrm{d}x \tag{1-15}$$

为连续型随机变量 X 的数学期望。

假若随机变量为一函数的话，那么离散型和连续型随机变量函数的数学期望为

$$E[g(X)] = \sum_{i=1}^{\infty} g(x_i)p_i \tag{1-16}$$

$$E[g(X)] = \int_{-\infty}^{\infty} g(x)\Phi(x)\mathrm{d}x \tag{1-17}$$

随机变量具有如下性质：

(1) 若 C 为常量，则

$$E[C] = C$$

(2) 设 X 为随机变量，C 为常量，则

$$E[CX] = CE[X]$$

(3) 设 X_1 和 X_2 为两随机变量，则有

$$E[X_1 + X_2] = E[X_1] + E[X_2]$$

定义：设 $E[X]$ 表示随机变量 X 的数字期望，那么其方差 $D[X]$ 定义为

$$D[X] = E[(X - E[X])^2] \tag{1-18}$$

从式(1-14) ～ (1-18) 可知，若 X 为离散型的，则

$$D[X] = \sum_{i=1}^{\infty} (x_i - E[X])^2 p_i \tag{1-19}$$

若随机变量 X 为连续型的，则有

$$D[X] = E[X^2] - (E[X])^2 \tag{1-20}$$

方差具有下列性质：

(1) 若 C 为常量，则

$$D[C] = 0$$

$$D[CX] = C^2 D[X]$$

(2) 若 X_1 和 X_2 为两个任意的随机变量，则有

$$D[X_1 + X_2] = D[X_1] + D[X_2] + 2E[(X_1 - E[X_1])(X_2 - E[X_2])]$$

(3) 若 X_1 和 X_2 为两个任意的互相独立的随机变量，C_1 和 C_2 为任意常量，则有

$$D[C_1X_1 + C_2X_2] = C_1^2 D[X_1] + C_2^2 D[X_2]$$

其实，在可靠性与可测性分析中，很多现象的结果都可用随机变量来表示，而只有使用诸如象分布函数、密度函数、数学期望、方差等数字特征，才能完整地描述这些现象的本质规律。

在本章中，只讲了一些概率与统计中的基本知识，还有很多象“大数定律”、“马尔柯夫过程”等没有触及，但它们在以后章节中将要用到，有兴趣的读者可查阅文献[5,6]。

第二章　基本概念

2.1　可靠性、可测性研究的必要性

2.1.1 研究的背景

可靠性概念对大家都不陌生，但它作为一门学问提出来，却是从第二次世界大战开始的。从四十年代起，由于战争的需要，一些新设备得到了发展。1939 年美国军械部队在监察贮存弹药的统计方法上取得成功，从而把统计数学理论和方法用于质量控制过程中。朝鲜战争开始以后，美国在战场上使用了当时看来性能先进但结构比较复杂的设备，但故障频繁，这就迫使美国大力开展可靠性研究。六十年代起，因空间科学和宇航技术的发展，可靠性研究水平得到进一步提高。现在可靠性研究已成为一门完整的、综合性很强的应用学科。

在我国，可靠性研究起步于五十年代，七十年代后，由于控制、测量卫星导弹等需要，可靠性研究也从探讨逐步进入了实践阶段。

可测性概念的提出始于七十年代。由于电路集成度的不断提高，经典的测试方法已不能适应要求，甚至出现测试成本与研制成本倒挂的局面。正是在这种情况下，人们提出了可测性设计概念，即在设计阶段就考虑测试问题，把降低测试难度的要求纳入设计规范，并通过可测性分析来检验和改进设计。

在我国，可测性研究起步晚，目前未见可测性设计方面的应用。因此，了解可测性知识是非常必要的。

2.1.2 研究的意义

质量是产品的生命，质量是企业的灵魂，可靠性则是评价产品质量的最主要指标。评价一个产品的好坏，主要看它的三大要素：可靠性、性能和价格。而可靠性则起着主要的作用[7,8]。为了提高系统的可靠性，人们进行了长期的研究，总结出了两种方法：容错和避错。所谓容错，就是指当系统中某些指定的部件出现故障时，系统仍能完成其规定的功能，并且执行结果不包含系统中的故障所引起的差错。容错的基本思想是在系统中加入冗余资源，来掩蔽故障的影响，从而达到提高系统可靠性的目的。所谓避错，就是试图构造出一个不包含故障的完美系统。要做到这一点，实际上是绝对不可能的。一旦出了故障，则就要通过检测手段来消除故障。一个系统的可靠性如何，从另一方面讲，就是看测试技术能否及时和准确地发现其内部的故障的水平。

近年来，人们逐渐认识到可靠性和可测性的重要性。从经济上说，一个部件的失效和不能修复，往往损坏整个设备和系统，这样将要花费很大的费用。从安全考虑，如果火车、汽车、飞机和宇宙飞船发生严重故障，将会造成人财物的重大损失。从日程推迟、不方便、顾客不满、信誉损失（可能对一个国家）直到严重危害国家安全等，也都可能是由不可靠性引起的。因此，不论从国防使用的军工产品上，还是从民用商品上，不论从政府工业上，还是从民用工业上，人们现

在越来越认识到可靠性与可测性的重要性，并且认识到研究可靠性与可测性的迫切性和必要性。

2.1.3 研究的内容及方法

可靠性与可测性研究的主要内容有：

(1) 明确系统在规定时间内完成任务的成功概率，这是可靠性研究的基本目标。

(2) 研究失效原因，找出防止和减少失效的方法，并且在失效后及时地通过测试技术来恢复系统工作。

(3) 为了达到高可靠性水平，可能会与产品性能、价格发生冲突，因此需要权衡这几方面的关系。

(4) 设备在使用阶段的维修性，设备的故障检测与诊断能力，设备是否容易检测，修复失效的时间等。因此，需研究设备可靠性与维修性的最佳组合。

在研究方法上，对于可靠性分析，主要分为可维修和不可维修两大类来研究，对于可靠性设计，主要是采用可靠度指标分配法、优化法和冗余法来提高可靠性指标。

对于可测性分析，主要采用静态可测性测度和动态可测性测度，在可测性设计上，主要采用结构可测性设计，以便能对时序电路进行测试。

2.2 可靠性函数

在研究可靠性函数之前，我们先看一下可靠性的定性定义。

定义：系统在规定条件下，在规定时间内，完成规定功能的能力，叫做可靠性。

自从把概率与统计引入可靠性之后，实现了可靠性由定性分析到定量分析的飞跃。

2.2.1 可靠度函数

定义：系统在规定条件和规定时间 t 内，完成指定功能的概率，叫做该系统的可靠度$R(t)$，可表示为

$$R(t) = P\{T > t\} \tag{2-1}$$

式中，T 表示系统正常工作时间这一随机变量。

当把时间 t 作为变量时，系统的可靠度就变为以 t 为变量的可靠度函数 $R(t)$。显然，当连续工作时间越长，发生故障的可能性越大，因而可靠度也就愈低，所以可靠度函数是一个递减函数。

可靠度函数，可以通过概率模型或统计定义来表示。设有 N 台产品，把它们进行正常的工作试验，到 t 时止，有 $n(t)$ 台失效，则按可靠度定义可得

$$R_{N(t)} = \lim_{N\to\infty} \frac{N - n(t)}{N} \tag{2-2}$$

如果运行试验的台数 N 有限时，那么以概率表示的可靠率函数 $R(t)$ 就蜕化为以频率表示的可靠度函数 $\hat{R}(t)$

$$\hat{R}_{N(t)} = \frac{N - n(t)}{N} \tag{2-3}$$

可靠度是产品可靠性的主要指标。它既能评价不能修复或难以修复的产品，如卫星等，也