容错与故障可测性系统设计

〔美〕P·K·拉拉 著
孟永炎 申晓留 成煜中 译

中国铁道出版社

容错与故障可测性系统设计

〔美〕P.K.拉拉 著

孟永炎 申晓留 成煜中 译

中国铁道出版社

1989年·北京

内 容 简 介

本书全面地论述了数字系统可靠性的基本概念和故障诊断及容错的基本原理，其中以一半以上的篇幅对容错计算的基本概念、基本技术和最新成就作了较为详细的介绍，很有参考价值。

本书可供从事数字系统研究、设计和维护的大学生、研究生及广大科技人员使用。

FAULT TOLERANT AND
FAULT TESTABLE HARDWARE DESIGN
Parag K.Lala
Prentice-Hall International,Inc.,London
1985
容错与故障可测性系统设计
〔美〕 P.K.拉拉 著
孟永炎 申晓留 成煜中 译
中国铁道出版社出版、发行
责任编辑 郝晓英 封面设计 安宏
各地新华书店经售
中国铁道出版社印刷厂印
开本：787×1092毫米 1/32 印张：10 字数：223 千
1989年3月 第1版 第1次印刷
印数：1—3000册 定价：3.95元

序

目前计算机的应用日益广泛地深入到各个领域，对计算机可靠性的要求越来越高。不但象航空、航天这样的高技术部门要求高可靠性的计算机，而且象银行、交通等部门也都要求高可靠的计算机。因此容错计算技术越来越受到人们的重视。

近二十年来，我国不少高等学校和科研单位先后开展了容错计算技术的研究，取得了一批理论上和实际应用上的成果，有些论文还被国际容错计算会议和其他一些国际会议所接受。在国内也先后召开了两次全国性的容错计算会议。1987年初还成立了直属于中国计算机学会的容错计算专业学组。总之，在我国已初步形成了一支容错计算技术研究的科技队伍。近年来国内虽已出版了几本编著和翻译的关于故障诊断和容错计算的书籍，但内容一般偏重于故障诊断和可测性设计，容错计算方面的内容比较少，到目前为止还缺乏一本内容全面和新颖的专著。孟永炎等同志翻译的这本书以一半多的篇幅比较详细地介绍了容错计算的基本概念、基本技术和最新成就，对我国容错计算的科研人员和教学人员无疑是一本很好的参考书，对广大从事计算机设计和应用的人员也是值得一读的。因此本书的出版将会受到有关科技人员的欢迎。

魏道政

1988年4月19日

译者的话

今天，对数字系统工作可靠性的重视已不再局限于宇航及军事部门。其他部门，诸如能源、铁道、邮电和化工等，对可靠性的要求也在日益增加。

一个完善的数字系统，它不仅应能满足生产过程提出的要求，而且应该是故障可测的和失效安全的。如何设计这样一种具有容错及自检能力的系统，已成为人们普遍感兴趣的课题。

本书全面地论述了数字系统可靠性的概念、故障诊断和容错的基本原理，尤其对容错的论述深入而且广泛。书中每讲解一种方法时，都附有实例以助理解。本书各章内容对最新科技成果均有反应（如特征码分析、内测试等），每章结尾列出了大量参考文献。我们认为这是一本较好的教材，可供从事数字系统设计及维护的大学生、研究生及广大科技人员使用。

本书第1、6和7章由成煜中翻译，第2、3和5章由申晓留翻译，第4章的翻译及全书的校核由孟永炎承担。本书原文中的错误，凡发现的已在译文中更正。在选译此书期间，曾得到魏道政教授和梁业伟教授的大力支持；黄刚同志对促进本书出版起了重要作用，太原计算机技术服务公司张万管总经理也鼎力相助，王继业、范亚玲和方燕虹等同志帮助抄写了部分书稿，在此一并致谢。

由于译者水平有限，错误和不妥之处在所难免，恳请批评指正。

译　者

1988年3月于北京

前　言

容错与可测性的共同目标是改善计算机硬件的可靠性。容错是关于对故障效果的屏蔽与恢复的学科，而可测性则包含了各种有利于故障检出的设计方法。哪种方法适用于哪种环境取决于它们的成本高低。近来在这两个方面的成果很多。这些成果形成了不同的设计思想和方法。遗憾的是许多工程技术人员尚不熟悉这些，因此急需向工程技术人员提供阐述容错与可测性一般原理及专题的大学课本及教科书。

本书主要为电机工程与计算机科学系的研究生编写，它也适合作为大学最后一年的教科书，不过读者必须在开关理论与逻辑设计方面具备一定的基础知识。这本书对于想了解硬件可靠性设计最新成果的实践工程师也同样是有用的。在每章结尾都列出了参考文献。

第1章涉及可靠性理论的基础。对可靠性度量中常用的术语（比如平均无故障时间和有效度）下了定义，并强调了维修性的重要意义。

第2章概括了数字电路中可能遇到的各种主要故障。先讨论了经典的固1和固0故障，然后介绍了非经典的故障（比如桥接和固定断开故障）。还讨论了间歇故障与暂时性故障的区别，以及阐述了间歇故障的几种模型。

第3章包含了组合电路与时序电路的故障检出原理。结合实例阐明了组合电路中故障检出的基本测试方法，还考虑了多重故障带来的问题。时序电路的测试仍是个主要问题，目前尚无公认的一般解决方法。在本章内详细地讨论了测试

时序电路的状态表校核法。后面介绍了尚未普遍应用但十分有效的逻辑电路测试方法，比如随机测试和跳变计数测试。最后结合特征码格式及它们的生成过程实例详细地讲述了采用线性移位寄存器的逻辑电路特征码测试方法。

第4章详细地讨论了多种硬件容错方法，还包括故障检出和恢复方法的具体分析。也谈到纠错码在时序电路和计算机存储系统容错设计中的应用。此外，简单介绍了软件冗余和时间冗余方法。阐述了“软失效”运行的概念，并介绍了几种实际的容错系统。最后给出了VLSI芯片的一种容错设计方案。

第5章展示了在自校验和失效保险电路的设计领域中的最新发展。分析了利用硬件设计中用过的各种检错码来进行自校验检测器的具体电路设计。还考虑了时序电路自校验和失效保险的设计方法。最后一节谈到近期完成的自校验可编程逻辑阵列（PLA）的设计方案。

第6章集中论述各种能用来提高组合与时序逻辑电路可测性的设计方法。讲述了为改善VLSI芯片可测性而建议采纳的若干设计方法。阐明了内测试和自治自测试概念。此外，讨论了几种无需考虑逻辑板测试而改善它们可测性的方法。

第7章讨论了在高可靠计算系统设计中当前正在研究的课题。

附录中包含了研究暂时故障时广泛用到的马尔可夫模型的介绍。（以下从略）

P.K.拉拉

目　录

1　可靠性的基本概念……1

1.1　可靠性的定义 ……1
1.2　可靠度和故障率 ……1
1.3　可靠度与平均故障间隔时间的关系 ……4
1.4　可维修度 ……6
1.5　有 效 度 ……7
1.6　串联系统与并联系统 ……8
1.7　参考文献 ……11

2　数字电路的故障……12

2.1　失效与故障 ……12
2.2　故障模型 ……12
2.3　暂时性故障 ……21
2.4　参考文献 ……25

3　测试生成……27

3.1　数字系统的故障诊断 ……27
3.2　组合逻辑电路的测试生成 ……28
3.3　组合电路中的多故障检测 ……53
3.4　时序电路的测试生成 ……55
3.5　随机测试…… ……68
3.6　跳变计数测试 ……69

3.7 特征码分析 ……71
3.8 参考文献 ……77

4 数字系统的容错设计……79

4.1 容错的重要性 ……79
4.2 容错的基本概念 ……80
4.3 静态冗余 ……81
4.4 动态冗余 ……89
4.5 混合冗余 ……92
4.6 自清除冗余方式 ……97
4.7 筛模冗余……100
4.8 5MR重构方案 ……102
4.9 利用纠错码进行存储系统的容错设计……107
4.10 时间冗余……121
4.11 软件冗余……122
4.12 软失效运行……124
4.13 实用的容错系统……124
4.14 针对VLSI芯片的一种容错设计方案 ……151
4.15 参考文献……158

5 自校验与故障安全逻辑 ……162

5.1 引 言……162
5.2 完全自校验检测器的设计……164
5.3 自校验时序机……205
5.4 部分自校验电路……213
5.5 强故障安全电路……215
5.6 失效保险设计……216
5.7 完全自校验PLA设计 ……228

5.8 参考文献……234

6 可测性设计 ……237

6.1 何谓可测性……237
6.2 可控性和可观察性……238
6.3 组合逻辑电路的可测性设计……239
6.4 时序电路的可测性设计……253
6.5 时序电路可测性设计中的路径扫描技术……256
6.6 电平灵敏扫描设计（LSSD）……261
6.7 随机存取扫描法……270
6.8 内 测 试……274
6.9 自治自测试设计……280
6.10 逻辑板内的可测性设计……287
6.11 参考文献……294

7 结 论 ……297

7.1 参考文献……304

附录 马尔可夫模型 ……307

1 可靠性的基本概念

1.1 可靠性的定义

近年来，数字系统的复杂性有了惊人的增加。尽管半导体厂商试图确保其产品是可靠的，但是，要保证在任意给定的时间内系统无故障发生，这几乎是不可能的。因此，可靠性已成为系统设计师和用户共同关注的主要课题[1.1, 1.2]。在特定的环境和给定的时间内，系统是否能按照预定的方式运行，是评价可靠性时遇到的一个基本问题。当然，这取决于许多因素，诸如系统设计、所用零部件和环境等。在给定条件下和给定时间内，某一特定系统的性能可看成是一个随机事件——即该事件的后果在其真正出现以前是未知的。因而，我们自然地把系统的可靠性看成一个未知参量，其定义为“给定系统在规定的工作条件下和预定的时间内持续完成规定功能的概率”。

通过按最坏情况设计、采用高质量元件及在装配阶段进行严密的质量控制等方法，可以提高系统的可靠性。然而，采用上述方法也会大大增加系统成本。可靠系统设计的另一方案是在系统中引入“冗余”（即附加的资源），以达到屏蔽故障影响的目的。这里，高质量元件并不是必不可少的，而可以代之以具有冗余和可重构的标准元件（参见第 4 章）。考虑到硬件费用的降低，显然采用第 2 种方法设计可靠系统花费较少。

1.2 可靠度和故障率

考虑在“恶劣”条件（温度、湿度等等）下N个相同元

件的失效过程。设$S(t)$为幸存元件数，即“寿命试验”开始后 t 时刻仍在运行的元件数；$F(t)$为到t时刻已失效的元件数，则元件的生存概率（又称可靠度$R(t)$）为

$$R(t)=\frac{S(t)}{N}$$

元件的失效概率（又称不可靠度$Q(t)$）为

$$Q(t)=\frac{F(t)}{N}$$

由于$S(t)+F(t)=N$，故有

$$R(t)+Q(t)=1$$

故障率$Z(t)$（也称事故率）可定义为“每单位时间内失效元件数与幸存元件数之比”，即

$$Z(t)=\frac{1}{S(t)}\frac{\mathrm{d}F(t)}{\mathrm{d}t} \qquad (1.1)$$

对电子元件的研究表明，在正常条件下，其故障率的变化特性如图1.1所示。图中有一段高故障率的初始区域，这

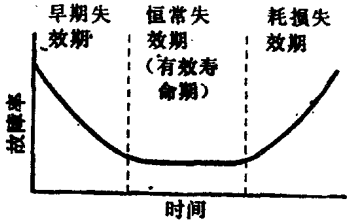

图1.1 故障率随时间变化曲线

是因为：在任何一批筛选出的元件中，都存在一些固有缺陷元件（即它们不能按人们预期的要求工作），它们在投入使用后迅速失效。因此，称第一段为有缺陷元件的“早期失效”阶段。中间段内故障率相对恒定，故障的出现时刻是随机的，称之为“有效寿命期”。在最后一段内，故障率开始随时间迅速增长，称之为“耗损期”。通常将图 1.1 所示形

状的曲线称作“浴盆”曲线。

在“有效寿命期”，故障率是恒定的，因而可以假设

$$Z(t)=\lambda \tag{1.2}$$

由前面定义，有

$$R(t)=\frac{S(t)}{N}=\frac{N-F(t)}{N}=1-\frac{F(t)}{N}$$

故

$$\frac{\mathrm{d}R(t)}{\mathrm{d}t}=-\frac{1}{N}\cdot\frac{\mathrm{d}F(t)}{\mathrm{d}t}$$

或

$$\frac{\mathrm{d}F(t)}{\mathrm{d}t}=-N\frac{\mathrm{d}R(t)}{\mathrm{d}t} \tag{1.3}$$

将式（1.2）和式（1.3）代入式（1.1）中，有

$$\lambda=-\frac{N}{S(t)}\cdot\frac{\mathrm{d}R(t)}{\mathrm{d}t}$$

$$=-\frac{1}{R(t)}\cdot\frac{\mathrm{d}R(t)}{\mathrm{d}t}$$

$$\left(\because\ R(t)=\frac{S(t)}{N}\right)$$

或

$$\lambda\cdot\mathrm{d}t=-\frac{\mathrm{d}R(t)}{R(t)}$$

对上式两边积分，有

$$\lambda\int_0^t\mathrm{d}t=-\int_1^{R(t)}\frac{\mathrm{d}R(t)}{R(t)}$$

上式的积分限按如下方式确定：$t=0$ 时 $R(t)$ 为 1；在时刻 t 时，由定义知，可靠度为 $R(t)$。

积分，有

$$\lambda[t]_0^t=-[\log_e R(t)]_1^{R(t)}$$

$$\lambda t=-[\log_e R(t)-\log_e 1]$$

$$-\lambda t=\log_e R(t)$$

故

$$R(t)=\exp(-\lambda t) \tag{1.4}$$

通常称上述关系为指数律故障。λ一般表示为每千小时百分比故障或每小时百分比故障。当乘积λt较小时，

$$R(t)=1-\lambda t \tag{1.5}$$

象元件故障一样，系统故障也可分为三个阶段。早期的系统故障，诸如布线错误、虚焊、误连等等，正常情况下都可消除在厂家的检验过程中。有效寿命期内发生的系统失效完全由元件故障引起。

设某系统内包含有k种元件，其故障率为λ_k，则系统故障率λ_{OV}为

$$\lambda_{OV}=\sum_{1}^{k}N_k\lambda_k$$

这里，N_k为每种元件的数目。

1.3 可靠度与平均故障间隔时间的关系

可靠度$R(t)$在不同的运行时间内取值不同。由于系统运行成功的概率取决于其运行条件和运行时间，因此，$R(t)$在实用上并不理想。对用户来说，更为有用的是系统发生故障的平均时间间隔，即平均故障间隔时间(MTBF)。一个系统的MTBF通常用小时表示，它可由$\int_0^\infty R(t)\mathrm{d}t$求出，即它等于可靠度曲线$R(t)$与时间轴$t$之间的面积。这个结论对任意故障分布都是成立的。对于指数故障律有

$$\begin{aligned}\mathrm{MTBF}&=\int_0^\infty\exp(-\lambda t)\mathrm{d}t\\&=-\frac{1}{\lambda}\Big|\exp(-\lambda t)\Big|_0^\infty=\frac{1}{\lambda}\end{aligned} \tag{1.6}$$

换句话说，系统的MTBF是其故障率的倒数。如果 λ 为每小时故障数，则MTBF用小时表示。举例来说，设有4000个元件，其故障率均为每千小时0.02%，则每小时平均故障数为

$$\frac{0.02}{100}\times\frac{1}{1000}\times 4000 = 8\times 10^{-4}\text{次/h}$$

因而，该系统的MTBF等于 $1/(8\times10^{-4})$，即1250h。将式（1.6）代入可靠度表达式（1.4）中，有

$$\begin{aligned} R(t) &= \exp(-\lambda t) \\ &= \exp(-t/\text{MTBF}) \end{aligned} \qquad (1.7)$$

可靠度与时间的关系曲线如图1.2所示。当时间增加时，可靠度减小。当 $t=$MTBF时，可靠度只有36.8%。这样，假如一个系统的MTBF为100h，它无故障运行100h的几率只有36.8%。

合并式（1.5）和（1.6），有

$$\begin{aligned} R(t) &= 1-\lambda t \\ &= 1-\frac{t}{\text{MTBF}} \end{aligned}$$

因此，

$$\text{MTBF}=\frac{t}{1-R(t)}$$

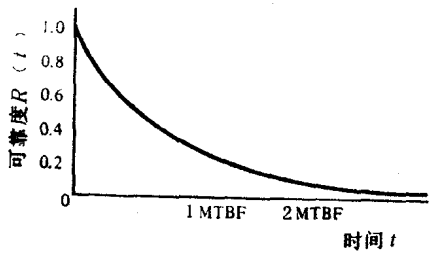

图1.2 可靠度曲线

例题 某第一代计算机包含有10000个电子管，$\lambda=0.5$

$\times 10^{-2}$/kh。可靠度为99%的时间是多少?

$$\begin{aligned} \mathrm{MTBF} &= \frac{t}{1-0.99} \\ t &= \mathrm{MTBF} \times 0.01 \\ &= \frac{0.01}{\lambda_{OV}} \end{aligned} \tag{1.8}$$

N = 电子管数 = 10000

λ = 电子管故障率

= 0.005/kh

= 5×10^{-6}/h

故

$$\lambda_{OV} = N\lambda = 10^4 \times 5 \times 10^{-6} = 5 \times 10^{-2}/\mathrm{h}$$

由式(1.8)有

$$t = \frac{0.01}{5 \times 10^{-2}} = \frac{10^{-2}}{5 \times 10^{-2}} = 0.2\mathrm{h} = 12\mathrm{min}$$

该结果通常具有代表性!

1.4 可维修度

当系统发生故障时,通常要进行修理以便使该系统恢复到运行状态。在指定时间内将一个失效系统恢复到运行状态的概率称为该系统的可维修度。或者说可维修度是在一定时间内对系统中的故障完成隔离和修复的概率(参见第2章)。这样,可维修度和修复率μ之间就存在一定的关系,因而也就与平均修复时间(MTTR)存在一定关系。MTTR与μ之间总有[1.3]

$$\mu = \frac{1}{\mathrm{MTTR}}$$

可维修度$M(t)$与MTTR和μ的关系如下:

$$M(t)=1-\exp(-\mu t)=1-\exp\left(-\frac{t}{\mathrm{MTTR}}\right)$$

其中，t 为限定的维修活动时间。

为了设计和制造一个可维修系统，有必要对可能发生在系统内的各种各样故障情况下的MTTR进行预测。这些预测通常都是建立在设计者和有经验的修理人员过去经验的基础上的。

系统修复时间由两个独立的部分组成——被动修复时间和主动修复时间〔1.3〕。被动修复时间主要由维修工程师到达用户所在地花费的时间来决定。在很多情况下，旅途时间超过了实际维修所需时间。而主动修复时间直接受系统设计的影响，它又可细分如下：

1. 从故障发生到系统用户发现故障的时间间隔。
2. 故障检测和找到可更换部件所需的时间。
3. 更换故障部件所用时间。
4. 确认故障已被清除和系统被完全修复所用时间。

依靠采用故障检测及快速隔离的系统设计，可使主动修复时间大大缩短。设计的系统越复杂，故障隔离越困难。然而，如果能使系统的可更换部分具有适当的自测试能力，则故障检测及其隔离将变得较为容易，这也有利于修复〔1.4〕。

1.5 有 效 度

系统的有效度是系统正常运行的概率，即系统在规定工作期间在任意时刻完成预期功能的概率〔1.3〕。

$$\text{有效度}=\frac{\text{系统正常运行时间}}{\text{系统正常运行时间}+\text{系统停机时间}}$$

$$=\frac{\text{系统正常运行时间}}{\text{系统正常运行时间}+(\text{故障数}\times\mathrm{MTTR})}$$