<<容错计算系统>>

图书基本信息

书名：<<容错计算系统>>

13位ISBN编号：9787307076600

10位ISBN编号：7307076608

出版时间：2010-6

出版时间：徐拾义 武汉大学出版社 (2010-06出版)

作者：徐拾义 编

页数：396

前言

自从第一台电子计算机问世以来，计算机系统（包括软件和硬件）就是在同数字系统的故障和错误的斗争中发展、成长的。
可以说，数字系统的成长史也是一部同系统内外故障的斗争史。
早期的计算机由于故障多而复杂，大量的计算错误使得系统无法正常运行。
1944年贝尔（Bell）的继电器计算机虽然使用了纠错编码，但是每次运算都必须运行两次，并将两次运行结果经过比对和检查后才能得出最后的结果：1951年世界上公认的第一台商业化电子计算机UNIVACI，使用了大量的奇偶校验技术和双算逻部件（ALU）并进行所谓的匹配一比较运算（match.and-compare）来应付各种可能的故障。
当前，随着信息技术和微电子技术研究开发的飞速发展，人们对数字系统以及相关微电子产品的依赖程度愈来愈大。
这些技术和产品，不仅需要应用于航空航天、原子核反应堆、军事科学、国防建设以及国民经济各种尖端科技领域，而且还直接涉及人们的生活，甚至是生命安全和人类生存等问题。
因此，当前人们在应用这些产品的同时必然会提出更高的要求，即除了传统意义上的要求和标准以外，还提出了更重要的评价体系——系统所提供服务的“可信性”（Dependability）标准问题。
事实上，对任何一件产品（一个系统）来说，能否为人类提供一种“可信”的服务是衡量其总体质量最重要的标准之一。
那么，什么叫可信的结果？
简而言之，就是在经过可行的确切论证以后，认为系统所提供的服务是正确无误，而且是可以信赖的结果。
问题在于什么叫可行的确切的论证，又由谁来完成这样的论证等。
对于这一系列问题，在过去，由于受到各种条件的限制，几乎是无法实现的。
因此，“可信计算”对数字计算系统领域中的一般科研人员和一般用户来说，只是高不可攀的“阳春白雪”，世界上只有极少数发达国家在某些特殊要求下，才会开发和应用它们，比如在航天飞机飞行姿态控制系统、原子核反应堆控制系统、导弹防御系统、铁路运输信号控制系统以及一些重症病人监护系统等需要提供十分可靠，而且只有可信的服务才能完成其所承担的任务的系统中。
这些控制系统中的任何隐患、故障和错误都将对系统和环境带来严重后果，甚至给人类造成深重灾难。
当前，随着数字计算系统日新月异的发展，原来的阳春白雪已经愈来愈普及，甚至渗透到了社会各个阶层，走进了寻常百姓的生活，使人类社会更多地享受由信息技术创造的成果。
但是，人类在享受着高新技术提供的各种前所未有的服务和乐趣的同时，却不可避免地会经受由于这些系统的不可靠和不可信所带来的种种险恶后果和严峻挑战。
事实上，这样的例子已经不胜枚举了，例如，当你将银行卡插入一台ATM机后得不到任何服务，或者得到错误的服务，甚至银行卡被“吞掉”，或者你在网上预订好的机票，在登机时竟然发现是无效机票……这些正是人们在普通的日常生活中随时可能遇到的不可靠和不可信服务的例子。
并且有些故障或错误是不可逆转的，往往使人们遭受极为严重的损失。
因此，当今“可信计算”已经不再神秘，人们应该研究和开发各种新理论、新技术，来规避所有可能产生的不可靠和不可信的结果。
“容错计算”的概念是直接提高数字系统的可靠性和可信性最重要的理念之一。
事实上，“容错计算”的概念已经逐渐步入人类社会，甚至已经和人们的日常工作及生活有了紧密的联系，因此，人们渴望着有一天可以从真正可靠和可信的数字系统中获得更加便捷、优秀的服务，而避免遇到种种不良的后果。

<<容错计算系统>>

内容概要

当前，数字计算系统已经渗透到社会的各个领域，容错计算理念以及与容错计算相关的理论和应用问题也将迅速深入到人类赖以生存的各个领域和环境中去。
同时，人们期待着所应用的，或者将应用的各种数字计算系统都是“ 诚信 ”的愿望必将实现。
因此，对容错计算系统的设计理论和实践环节的深入研究和开拓必将成为当今数字系统研究和开发的热点。

《容错计算系统》共10章，可以分成两大部分：第一部分对容错计算以及可信系统各类属性的定义和基本知识作详细的介绍和分析（从第1章至第4章），其中包括对软件和硬件系统的故障，错误和失效的定义和性质的形式化描述，并对软件和硬件系统中的故障和错误作了分析和比较；第二部分则是在对故障、错误和失效等主要属性作深入研究的基础上，阐述了提高系统可信性和可靠性以及容错计算的基本理论、主要技术和实施方法，并且介绍了其他相关的知识（从第5章至第10章）。
其中按照软件和硬件系统的开发生命周期各个阶段应采取的各种策略和措施进行详细的分析讨论，包括阐明了避错技术和防错技术、软件和硬件系统测试技术、可测性设计技术（包括冗余与编码技术）、容错系统的设计以及故障安全技术等在数字系统中的实施策略和实际应用。

《容错计算系统》是专为计算机科学与技术专业和信息工程专业高年级本科生和研究生以及从事容错计算理论和应用的有关专业人士撰写的，是一本集数字计算软件和硬件系统于一体的容错计算理论研究和应用与实践并重的教材，书中吸收并介绍了大量国内外关于容错计算理论和技术方面的信息。
《容错计算系统》与当前其他教材相比较，从具体内容上来看具有一定的先进性和前瞻性，对学习和了解数字系统的可靠性和容错计算系统的设计具有重要的意义。

<<容错计算系统>>

书籍目录

第1章 容错计算的基本概念1.1 故障的定义及性质1.1.1 故障的定义1.1.2 故障的产生1.1.3 故障的基本性质1.2 故障模型1.2.1 硬件故障模型1.2.2 软件故障模型1.3 故障模型的建立1.3.1 建立故障模型的重要性和标准1.3.2 故障模型的局限性1.4 错误的定义1.4.1 错误的定义1.4.2 错误的分类及其传递性1.5 失效的定义1.6 数字系统的可信性1.7 容错计算的定义及其重要功能1.8 本章小结1.9 思考题第2章 数字系统的可靠性2.1 数字系统可信性的定义2.2 数字系统的可靠性2.2.1 基本的可靠性函数和失效函数2.2.2 可靠性的重要参数及定义2.3 组合系统的可靠性2.3.1 串行组合系统的可靠性评估2.3.2 并行组合系统的可靠性2.3.3 串并行／并串行系统的可靠性2.3.4 非串行／非并行系统的可靠性2.4 数字系统的可测性2.5 数字系统的可维护性2.5.1 维护的定义2.5.2 可维护性的定义2.6 数字系统的可用性2.7 数字系统的安全性2.8 数字系统的信息安全2.9 数字系统可信性综合分析2.10 本章小结2.11 思考题第3章 冗余技术和编码原理3.1 功能性冗余技术的基本原理3.1.1 静态功能性冗余3.1.2 动态功能性冗余技术3.2 结构性冗余技术3.2.1 数字系统的结构性冗余技术3.2.2 主动冗余技术3.2.3 被动冗余技术3.2.4 混合冗余3.2.5 时间冗余技术3.3 纠错编码原理3.3.1 纠错编码的基本原理3.3.2 线性分组编码原理3.3.3 纠一／检二海明编码3.4 萧码——实用的纠一脸二编码3.5 循环码基本原理3.5.1 循环码基础和码多项式3.5.2 循环码多项式的性质3.5.3 循环码的系统码格式3.5.4 使用（n-k）级线性移位寄存器编码3.5.5 使用七级线性移位寄存器编码3.6 本章小结3.7 思考题第4章 自校验逻辑设计4.1 完全自校验电路的基本概念4.2 分离码电路及相关定义4.2.1 强／弱分离码电路4.2.2 自校验电路中的术语及基本定义4.3 无双向错误的组合逻辑设计4.4 检测由输入端故障产生的双向错误4.5 双向错误排除技术4.5.1 输入编码4.5.2 输出编码4.6 自对偶奇偶校验4.7 模3（mod 3）留数码自校验电路4.8 本章小结4.9 思考题第5章 故障避免和防止技术5.1 需求分析和规格说明阶段的故障避免措施5.1.1 确信技术5.1.2 验证技术5.2 设计阶段的故障避免措施5.2.1 故障预防——设计过程中的确信技术5.2.2 故障检测——设计过程中的验证技术5.3 设计阶段应用的功能测试5.4 故障防止措施5.4.1 应用故障防止应注意的事项5.4.2 应用于硬件系统的故障防止措施5.4.3 应用于软件系统的故障防止措施5.5 本章小结5.6 思考题第6章 软件可靠性模型和软件测试6.1 软件可靠性的研究意义6.2 软件开发的生命周期6.2.1 项目的初始阶段6.2.2 样本设计及定型阶段6.2.3 编程阶段6.2.4 测试阶段6.2.5 变异测试6.3 软件可靠性及其测度6.4 软件测试对软件可靠性模型的影响6.4.1 软件错误与检错曲线6.4.2 软件错误与检错模型6.5 软件可靠性模型6.5.1 常数检错率的软件可靠性模型6.5.2 线性递减型检错率的软件可靠性模型6.5.3 指数递减型检错率的软件可靠性模型6.6 软件可靠性模型中的常数估算6.6.1 参数估算方法（1）——常数型检错率6.6.2 参数估算方法（2）——线性递减型检错率6.6.3 参数估算方法（3）——指数递减型检错率6.7 本章小结6.8 思考题第7章 数字电路故障诊断7.1 数字电路故障诊断的基本概念7.1.1 故障等价7.1.2 故障控制7.2 数字电路的故障测试7.2.1 逻辑测试的基本类型7.2.2 逻辑测试的基本参数7.2.3 逻辑测试的层次分类7.2.4 逻辑测试的具体实施7.3 组合电路的测试生成7.3.1 逻辑电路的可控性和可观察性7.3.2 单固定故障测试生成7.4 特征分析测试法7.4.1 计“1”测试法7.4.2 跳变计数测试法7.4.3 征兆测试法7.5 时序电路测试生成7.5.1 时序电路测试的基本概念7.5.2 状态表验证和I／O校验序列7.5.3 利用鉴别序列生成校验序列7.5.4 无鉴别序列时序电路的校验序列7.6 桥接故障测试生成7.6.1 桥接故障模型7.6.2 非反馈型桥接故障的测试生成方法7.6.3 反馈型桥接故障的测试生成7.7 本章小结7.8 思考题第8章 可测试性设计技术8.1 可测试性设计思想的重要性8.2 可测试性设计的基本原理8.2.1 测试质量和可测试性属性8.2.2 可测试性设计的意义8.3 特定测试法8.3.1 设置附加测试点8.3.2 便于初始化设置8.3.3 将大规模组合电路分解为松散型连接的小规模模块8.3.4 提高时序电路的可控性8.3.5 软件可测试性设计中的测试点技术和异常检测技术8.4 专用可测试性电路及可测试性软件设计方法8.4.1 Reed-Muller电路扩展技术8.4.2 控制逻辑插入技术8.4.3 专用可测试性设计在软件中的应用8.5 组合电路内建测试（BIT）设计方法8.5.1 PLA电路的结构及基本故障模型8.5.2 PLA电路的可测试性设计——PLA的奇偶校验BIT技术8.6 时序电路内建测试（BIT）设计方法8.6.1 扫描通路设计思想8.6.2 隔离（切换）部件的设计8.6.3 电平触发扫描设计（LSSD）8.6.4 应用扫描设计技术的成本和对系统开发的影响8.7 边界扫描内建测试（BIT）技术8.7.1 边界扫描问题的提出8.7.2 边界扫描设计的基本原理8.8 内建自测试（BIST）方法8.8.1 内建自测试的基本概念8.8.2 线性反馈移位寄存器与特征多项式8.8.3 一个可测试性设计的实例——伪穷举奇偶校验法及奇偶校验可测试性设计8.9 本章小结8.10 思考题第9章 容错计算技术和容错系统9.1 软件系统的结构性冗

<<容错计算系统>>

余技术9.1.1 N-版本（模）冗余技术的基本概念9.1.2 软件系统N-版本冗余的实现方法9.1.3 指令复抽.技术9.2 卷回和向后恢复技术9.2.1 向后恢复技术9.2.2 向后恢复技术中的高速缓存9.2.3 向后恢复技术中恢复点的确定9.2.4 向后恢复技术中运行环境的恢复9.3 向前恢复技术9.3.1 恢复模块式9.3.2 终结模式技术9.4 N模冗余系统的可靠性评估9.4.1 系统裁决9.4.2 模块分级裁决9.4.3 裁决器的可靠性问题9.4.4 可修复的NMR系统9.5 容错系统的性能和成本关系的评估9.6 各种容错技术的比较9.6.1 容错设计技术的相似性9.6.2 容错设计的差异性9.7 容错计算技术与系统可靠性的关系9.8 本章小结9.9 思考题第10章 安全保障技术10.1 安全保障的基本概念10.1.1 固有安全设计确保系统的安全性10.1.2 冗余结构及故障安全技术提高系统的安全性10.1.3 基于冗余结构技术的安全保障系统例子10.2 安全保障系统与完全自校验技术10.2.1 双轨校验器实现自校验功能10.2.2 基于n取m码完全自校验及校验器的设计和构造10.2.3 基于n取1码完全自校验及校验器的设计和构造10.3 基于伯格码的完全自校验及校验器10.4 基于低耗留数码完全自校验及校验器的设计10.5 完全自校验PLA电路的设计10.5.1 强故障安全PLA电路的设计10.5.2 完全自校验PLA电路的设计10.6 最终安全保障组合电路的设计10.7 自校验时序电路的设计10.7.1 时序电路中的冗余故障10.7.2 自校验时序电路的设计10.8 安全保障时序机的设计10.9 安全保障系统与完全自校验技术的关系10.10 本章小结10.11 思考题参考文献

章节摘录

插图：对可信性的测度评估主要可以分为两个方面，即可信性的数量测度和质量测度。
从数量测度观点来评价一个数字系统的可信性，可以对系统可信性的多个属性进行全面的评估，这些评估的基础就是系统在各个属性上所提供服务的可“依赖程度”。
由于这些属性的不确定因素，这些依赖程度都是以概率的形式来衡量和农示的。
从宏观上来看，一个系统在整个生命周期中可能在一个阶段需要接受评估：第一阶段为需求分析和规格说明阶段，第二阶段为设计阶段，第三阶段则是系统的运行阶段。
第一阶段的评估是在系统建立之前，即在对其作规格说明阶段中进行的。
主要是根据它的规格说明来分析和预测该系统在将来作为产品的可信性。
即根据用户对可信性的要求和设计者对系统成本和需求分析来预测系统的可信性，并且确保系统在运行时的可信性应该在可接受的范围之内。
第二阶段的评估是在设计阶段进行。
在设计阶段应注意要运用必要的技术、可靠的元器件或模块以保证系统在运行时达到应有的可信性。
如在硬件系统中应该尽量避免使用不可靠的元器件，因为它们会带来许多隐患，导致系统不稳定。
同样在软件系统中应尽可能避免过多使用转向语句等结构，因为这些语句结构的使用可能使程序运行和程序调试变得十分复杂，难以控制，因而使程序容易发生错误。
第三阶段的评估是在系统运行阶段进行的。
这个阶段的评估主要是通过大量试验性的运行来得到应有的实验结果，以确定该系统的可信性是否在原有的设计范围内，是否达到了应有的标准。
如对同一个程序，应使用不同的数据输入，并需要运行上百次乃至几千次，直到得到一个明确的统计值为止。
第一阶段的评估和第二阶段的部分评估工作称为预测性评估，而第三阶段和第二阶段剩余部分的评估工作则称为运行性评估。
不管哪一种评估都存在一定的难度，因为它们都无法提供一个确定的数值，通常只是一个概率统计值。
因此，在一般情况下对可信性的数量评估只是一个概率值，很多情况必须视具体的系统而定。
从质量测度来评价一个数字系统的可信性，主要是根据在系统中检测到的致命性故障和错误的情况对系统可信性引起的后果的严重情况来测定。
事实上，这种测度只是对系统可信性可能受到损害的严重程度做出的评估，而并不是对故障或错误造成的严重后果的直接测量。
这种的评估可以有两种不同的方法：顺推法和逆推法。
顺推法是从已经检测到的致命性故障和错误推导出系统可能出现的失效及其后果的严重性，典型方法是故障树法。
逆推法则是从可能出现的失效及其严重后果推算出可能引起系统失效的致命性的故障和错误，常用的逆推法是失效模式分析法。
本章将分别对数字系统可信性的几个重要属性分别作系统的定量分析及讨论，主要将讨论数字系统可靠性测度的分析和评估，因为可靠性测度是衡量和保证系统能够提供可信服务最重要的因素。
对其他属性，如可测性、可用性、安全性、保密性等测度的分析将仅作简单的介绍，以飨读者。

<<容错计算系统>>

编辑推荐

《容错计算系统》是信息安全系列教材。

版权说明