JS

计算机系统的高可靠性技术

[日] 猪濑 博 编著

尤国峻 肖俊远 译
高铭学 肖兴权 校

国防工业出版社

计算机系统的高可靠性技术

〔日〕猪濑　博　编著
尤国峻　肖俊远　译
高铭学　肖兴权　校

国防工业出版社

内 容 简 介

本书是日本信息处理学会为纪念该会成立二十周年而出版的第一本书。全书分别由该书编委会的十五名具有实际经验的专家执笔，由东京大学教授猪濑　博主编。

本书较系统地介绍了计算机系统高可靠性技术。全书共分十二章：前七章论述了提高计算机系统可靠性的主要技术内容；第八、九、十、十一章分别介绍了可靠性技术在成批处理系统、银行业务联机系统、分时系统和电子交换机中的应用；第十二章是对该项技术的展望。

本书可供从事计算机系统研究、设计、制造、使用和维护的科技人员、大专院校师生参考。

コンピュータ・システムの高信頼化
東京大学教授　猪濑　博　編著
情報処理学会　1977年

*

计算机系统的高可靠性技术

〔日〕猪濑　博　编著
尤国峻　肖俊远　译
高铭学　肖兴权　校

*

国防工业出版社出版
新华书店北京发行所发行　　各地新华书店经售
国防工业出版社印刷厂印装

*

850×1168 1/32　印张 14 1/4　374 千字
1985年3月第一版　1985年3月第一次印刷　印数：00,001—13,000册
统一书号：15034·2746　　定价：2.10元

译者的话

随着广泛的应用领域对电子计算机的要求越来越高，计算机系统的高可靠性技术越来越为人们所重视。为了有助于电子计算机的推广应用，特翻译此书，以供参考。

为了提高计算机的可靠性，一般有两个途径：一是在工艺上提高构成计算机的元、器件的可靠性；二是在系统结构方面提高计算机系统的可靠性。本书便是从后者的角度出发来论述高可靠性技术的。原书是日本信息处理学会为纪念该会成立二十周年而组织出版的第一本书。为此，专门成立了编委会，由东京大学猪濑　博教授担任主编，本书的十五名执笔者都是在有关技术方面具有丰富实践经验的专家。全书共分十二章，第一至第七章论述了提高计算机系统可靠性的主要技术内容，第八至第十一章分别介绍了几种典型的计算机系统实例，从而进一步阐明了计算机系统高可靠性技术的应用情况。第十二章是对计算机系统可靠性技术的展望。本书是一本既较全面又较系统、既有理论又有实践的很有价值的参考书。

本书可供从事计算机研究、设计、制造、使用和维护的科技人员，以及有关大专院校师生阅读。

本书的第一至第九章和第十一章由尤国峻翻译，第十、十二章由肖俊远翻译，尤国峻负责全书的统一。全书由高铭学、肖兴权审校。吕景瑜同志提出了很多宝贵意见，在此谨致谢忱。

尽管译校者作了努力，但因水平所限，译文仍可能存在错误和不足之处，恳请批评指正。

目　录

第一章　高可靠性技术基础

1.1　计算机系统的高可靠性技术

1.1.1　计算机与可靠性

计算机实际应用的历史，即使说成是可靠性技术发展的历史也并非言过其实。在世界上第一台电子计算机 ENIAC 中，由于使用了多达一万八千只电子管，因而其可靠性不能满足实际应用的要求。由于发明晶体管后，半导体技术突飞猛进，故器件可靠性迅速提高；在系统可靠性方面，冗余技术、错误控制、自动故障诊断等可靠性技术也取得了一定进展。于是，计算机终于持续稳定地发挥其强大的威力，从而很快在社会经济的各个领域得到了应用。

计算机最初主要是应用在事务处理、科学技术计算等所谓脱机成批处理方面，但随着计算机的可靠性不断提高，很快就应用到存款汇兑业务、座位预约、交通管制、生产及库存管理、分时计算等所谓联机实时处理方面了。例如，日本的计算机设置台数以每年增加30%的速度发展（如图1-1 *a* 所示）；而联机系统则增长得更快，1964年以前一台也没有，此后却以每年递增60%的速度发展（如图1-1 *b* 所示）。这就说明，不仅在硬件方面，而且在软件和使用方面的高可靠性技术也取得了显著进展。不过，考虑到今后联机系统的规模还要扩大，其功能还将更强，考虑到数据库的出现，并且预计发展很快，考虑到计算机在行政、医疗、教育、交通、防灾、防止犯罪、流通、福利等方面的应用，所有这些因素对计算机可靠性的要求将越来越高。

今天，很多生产活动、经济活动和社会活动都在使用着计算机。计算机刚问世时，人们的注意力主要放在计算机优点上，当

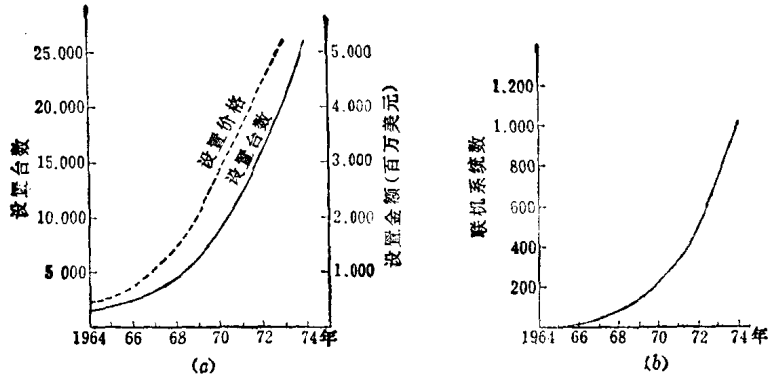

图1-1 日本计算机和联机系统的发展

（a）计算机的设置台数及设置价格；（b）联机系统数。

时在社会应用方面尚处在试行阶段。由于计算机逐渐渗透到社会中，并且其规模越来越大，因而形成了迅速发展中的社会经济活动全面依赖计算机的局面。与此同时，对于计算机可靠性的要求也日趋严格。这是因为，在这种状况下，如果计算机系统发生故障，则其效益就会大幅度削减，甚至完全丧失，从而使社会经济活动陷入不可收拾的混乱状态。对此必须严肃追究其技术责任。另外，随着计算机为个人、企业、行政机关等处理数量越来越大的更为重要的信息，人们更加担心会因操作失误或有意破坏而造成信息泄漏、信息破坏、信息窃取乃至信息恶用等事故。由此可见，计算机系统的高可靠性技术是实现信息化社会的关键。

尽管有待解决的可靠性问题不少，但实现高可靠性计算机的技术途径也非常多。大体上可分为下述两类：提高器件本身可靠性的技术；使用给定器件构成高可靠性系统的技术。如表1-1所列。

提高器件可靠性的技术包括下述一些内容：查明失效的物理机理，发现引起失效的现象，研究消除这些现象的制造工艺；利用大规模、超大规模集成电路技术，提高电路或子系统的可靠性；建立器件的性能老化模型（失效模型），由模型拟定加速试

表1-1 计算机系统的高可靠性技术

计算机的高可靠性技术

- （一）提高器件可靠性的技术（不属于本书内容）
  - 1. 高可靠性器件的研制
    - 1）查明失效的物理机理，按照失效机理加以改进
    - 2）利用大规模集成电路技术提高可靠度
    - 3）其他
  - 2. 改善环境条件
    - 1）改善温度、湿度、振动、冲击等物理条件
    - 2）降级使用
    - 3）培训维修人员和使用人员
    - 4）其他
- （二）计算机系统的高可靠性技术
  - 1. 提高系统的可靠性
    - 1）冗余结构设计（并行、备用、部分备用等）……第一、二、四章
    - 2）缩短修理时间（自动故障诊断、提高可维性等）……第七章
    - 3）系统恢复技术……第五章
    - 4）提高软件的可靠性
    - 5）其他
  - 2. 提高信息的可靠性
    - 1）在信息中附加冗余码（检错、纠错等）……第三章
    - 2）信息保护……第六章
    - 3）采用多数表决方式……第一章
    - 4）其他

验的方法，为系统设计提供失效率数据或提供有效的器件筛选方法；掌握物理的和人为的环境条件；规定使用条件；等等。在提高器件的可靠性方面已经取得出色成果，例如，十年前半导体器件失效率的数量级为10^{-6}/时，而今天已提高到10^{-9}/时了。

使用给定器件构成高可靠性系统的技术包括下述一些内容：采用冗余技术使系统在出故障时仍能维持正常功能；研究缩短修理时间的自动故障诊断技术；研究使系统能顺利地从故障状态恢

复成正常状态的恢复技术；研制错误少或易于检测错误的软件；利用附加在信息上的冗余码自动检错、纠错；保护计算机系统中正在处理的信息和存储着的信息不被破坏或泄漏；采用多数表决方式提高系统输出信息的可靠性；等等。在用给定器件构成高可靠性系统方面也取得了很大进展，以利用率为例，最初低于50%，而现在却达到了下述水平：二十年的累计停机时间在几小时以下。

由于本书旨在阐述计算机系统的高可靠性技术，所以不涉及第一方面的内容，而专门介绍第二方面所包括的各种技术的基础知识及其应用。第一至七章介绍计算机系统高可靠性技术的现状；第十二章展望有关的未来技术；第八至十一章以成批处理系统、联机银行业务系统、分时系统和电子交换机为实例，具体说明相应的高可靠性技术。

1.1.2 提高可靠性的方法

计算机系统在外部因素和内部因素的作用下，其正常工作状态可能受到种种干扰。外部因素包括：温度、湿度、振动、冲击、噪声、停电等物理因素及操作人员过失和局外人恶意破坏等人为因素；内部因素包括：器件的偶发性失效，器件在长时间使用后性能老化，以及经过试验未能发现的软件与硬件缺陷等等。由这些因素引起的系统异常状态，有的是瞬时性的，不修理也能恢复成正常状态，我们称之为错误（error）；有的是固定性的，只有通过修理才能恢复成正常状态，我们称之为故障（failure）。

错误除可能由操作失误、噪声等系统的外部因素引起外，还可能由磁介质不均匀、硬件接触不良、误动作、电路及软件不完善等内部因素引起。对于由内部因素引起的错误，由于不进行修理，系统的功能也能自动恢复，所以未能查明原因的情况是很多的。使错误不影响系统功能的方法有：在信息上附加冗余码进行检错、纠错；设置硬件功能和软件功能，防止信息破坏或泄漏。

我们把在信息上附加冗余码实现自动检错、纠错的方法称作错误控制（error control）。显然，自动纠错比自动检错需要附

加更多的冗余码。现以传送信息和存储信息作为典型实例，看看进行错误控制的情况。在传送信息时，由于在发送端和接收端预先规定了传输控制过程（transmission control procedure），所以接收端一旦检出错误就能通知发送端重新发送信息。此外，通常的传输线路上误码率是比较小（10^{-5}～10^{-6}）的。因此，这时自动检错的效率高。为了自动检错，可以采用种种附加冗余码的方式，其中包括：以字母为单位的垂直奇偶校验（vertical parity）和以字组为单位的水平奇偶校验（horizontal parity）等检错的低级方式；采用循环冗余码（cyclic redundancy code）等能检出多个突发错误（burst error）的高级方式；等等。但是，在存储信息时，由于不具备重新发送的手段，因而需要采用海明码（Hamming code）等实现自动纠错。本书第三章将讨论这方面的内容。

保护信息的方法很多。在计算机外部，可以采取确认用户身份或限制向计算机存取等措施；在计算机内部，可以使用只读存储器，给用户指定写入读出区域等手段。但是，要想既放心使用计算机，而所采取的保护措施又便于使用，则是一个极其困难的课题。本书第六章讨论这个问题。

故障按其发生时期通常分为早期故障、偶发故障与耗损故障三种。对于不同时期发生的故障，应当采取不同的措施。图 1-2 示出从系统制成后故障发生次数与使用时间的关系曲线，以及在各个时期所采取的维护方法。图中曲线呈船形（或浴盆形）。

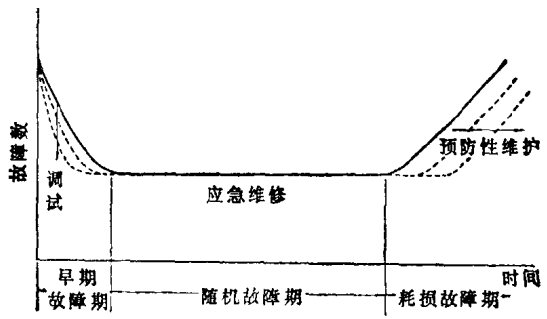

图1-2　故障次数与维护方案曲线

系统刚制成时，由于元器件质量差，软件不完善，设计欠佳等原因而发生早期故障（initial failure）。为了排除早期故障，要让系统试运行（test run），在试运行期间换掉质量不好的元器件，修正软件错误，修改设计。由于采取了这些措施，所以故障次数渐渐减少。当故障次数基本上稳定时，系统便可交付使用。系统在实际使用期间发生的故障大体上是均匀的。

系统经长时间使用后故障次数又渐渐增多，这是由于元、器件使用寿命已到所致，故称作耗损故障（wearout failure）。如果能够知道元、器件寿命的统计分布规律，那么，预先更换元、器件，就可以防止发生耗损故障。这种预先更换元器件的维护方法称之为预防性维护（preventive maintenance）。显然，进行预防性维护能够延长系统的实际使用期。

系统实际使用期位于早期故障期与耗损故障期之间，在此期间发生的故障完全是随机的偶发故障（chance failure），因此称这个期间为偶发故障期。在偶发故障期，由于不可能预先知道故障何时在何处发生，所以只能在故障发生后着手进行修理、更换元、器件等应急维修工作，因而这个期间的维护工作称为事后维修（aposteriori maintenance）或应急维修（emergency maintenance）。偶发故障期是高可靠性技术发挥作用的期间。

在偶发故障期，由于维修是在故障发生后才开始的，所以在修理、更换完毕之前，系统是不能使用的。为了在修理期间使系统的功能不停止，必须同时准备多个系统，这种系统结构称作冗余结构（redundant configuration）。冗余结构在宇宙飞船计算机等不能修理或修理时间极长的系统中是必不可少的，而在可维系统（如一般使用的计算机）中，用恰当的应急维修措施与之配合则能大幅度提高可靠性。本书的第二章和第四章将讨论这些问题。

图 1-3 示出了冗余系统的应急维修步骤。第一步是故障检测。由两台计算机组成的并联系统（parallel system）中，从两机输出的不一致便能立即发现故障；在由现用机与备用机组

成的备用系统（standby system）中，检测故障是通过让现用机定期执行结果已知的检验程序进行的。第二步是切离故障计算机。对于两台计算机组成的并联系统来说，在切离之前必须先判别哪一台出了故障，为此可采用执行检验程序等方法。在由三台计算机组成的并联系统中，判别是通过多数表决直接做出的。切离时，将现用机执行的程序和数据的现场保存起来，以及对备用机输入等操作，它们是同时进行的。

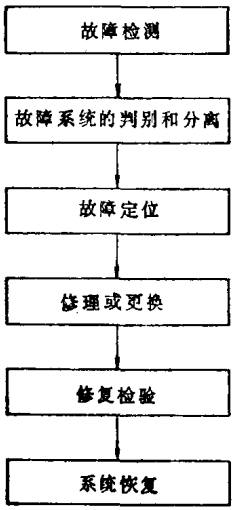

图1-3 应急维修步骤

第三步是故障定位。要求把故障定位到印制板这样的可更换单元。由于计算机中通常有几百个以上的可更换单元，所以故障定位花费的时间占了应急维修时间的主要部分。通常，在诊断前，先利用模拟等方法确定故障位置与输入/输出的对应关系。诊断时，输入一系列测试信号，观察输出，按照对应关系就可确定出故障位置。这一过程若是自动进行的，就叫做自动诊断（automatic diagnosis）。第七章将讨论这些问题。第四步是故障件的修理或更换，多数情况下只用备用印制板更换即可。第五步是修复检验，通过执行检验程序等方法验证故障是否已完全被修复。第六步是系统恢复，为使修理完毕的计算机重新返回正常工作状态而进行必要的处置。本书将在第五章讨论这些问题。

本章以下各节介绍与系统可靠性技术有关的基本内容，着重以可靠度和利用率的概念为中心进行说明。

1.2 与系统可靠性有关的基本参量

系统故障是按统计分布规律发生的概率事件；修理系统时，由于修理的难易程度不同，故修理时间也服从统计分布规律。因