中国计算机学会
学术著作丛书

实时系统中的可靠性技术

袁由光 编著

清华大学出版社
广西科学技术出版社

中国计算机学会学术著作丛书

实时系统中的可靠性技术

袁由光　编著

清华大学出版社
广西科学技术出版社

（京）新登字 158 号

内 容 提 要

本书从理论和工程实践两个方面系统地介绍了提高实时系统可靠性的各种实用技术。全书共八章，首先从实时系统故障的来源、表现和分布规律出发，介绍了检测和纠正故障效应的编码技术，然后在此基础上详细地介绍了故障发生后确保系统正常运行的各种容错技术。最后给出了一个高可靠的实时容错计算机应用系统的设计实例。

本书可供从事可靠性技术研究和应用的工程技术人员及高等院校的有关专业师生作为参考。

图书在版编目(CIP)数据

实时系统中的可靠性技术/袁由光编著. —北京：清华大学出版社，1995.4
ISBN 7-302-01827-8

Ⅰ.实… Ⅱ.袁… Ⅲ.实时操作系统-系统可靠性 Ⅳ.TP316.2

中国版本图书馆 CIP 数据核字(95)第 04994 号

出版者：清华大学出版社（北京清华大学校内，邮编 100084）
广西科学技术出版社（南宁市河堤路 14 号，邮编 530021）
印刷者：人民文学印刷厂
发行者：新华书店总店北京科技发行所
开 本：787×1092 1/16 印张：12.5 字数：292 千字
版 次：1995 年 9 月第 1 版 1995 年 9 月第 1 次印刷
书 号：ISBN 7-302-01827-8/TP・819
印 数：0001—4000
定 价：12.80 元

The Reliability Techniques in Real-Time Systems

Yuan Youguang

Tsinghua University Press
Guangxi Science and Technology Publishing House

SUMMARY

This book presents systematically various practical techniques to improve reliability of real-time systems in both theory and engineering practice.

The volume is organized into 8 chapters. Taking the source, expression and distribution law of the real-time system's faults as the starting point, after reviewing the coding technology to detect and correct fault effection, the author devotes to the various fault-tolerant techniques which can guarantee the normal operation of the systems in fault events. Finally an application design of a high reliable real-time fault-tolerant computer is discussed.

This book is intended for technicians, scholars and college students who are concerned with the research and application of the reliability techniques.

清华大学出版社　广西科学技术出版社
计算机学术著作出版基金

评 审 委 员 会

主 任 委 员　张效祥

副主任委员　周远清　汪成为

委　　员　王鼎兴　杨芙清　李三立　施伯乐　徐家福
夏培肃　董韫美　张兴强　徐培忠

出 版 说 明

近年来，随着微电子和计算机技术渗透到各个技术领域，人类正在步入一个技术迅猛发展的新时期。这个新时期的主要标志是计算机和信息处理的广泛应用。计算机在改造传统产业，实现管理自动化，促进新兴产业的发展等方面都起着重要作用，它在现代化建设中的战略地位愈来愈明显。计算机科学与其它学科的交叉又产生了许多新学科，推动着科学技术向更广阔的领域发展，正在对人类社会产生深远的影响。

科学技术是第一生产力。计算机科学技术是我国高科技领域的一个重要方面。为了推动我国计算机科学及产业的发展，促进学术交流，使科研成果尽快转化为生产力，清华大学出版社与广西科学技术出版社联合设立了“计算机学术著作基金”，旨在支持和鼓励科技人员，撰写高水平的学术著作，以反映和推广我国在这一领域的最新成果。

计算机学术著作出版基金资助出版的著作范围包括：有重要理论价值或重要应用价值的学术专著；计算机学科前沿探索的论著；推动计算机技术及产业发展的专著；与计算机有关的交叉学科的论著；有较大应用价值的工具书；世界名著的优秀翻译作品。凡经作者本人申请，计算机学术著作出版基金评审委员会评审通过的著作，将由该基金资助出版，出版社将努力做好出版工作。

基金还支持两社列选的国家高科技重点图书和国家教委重点图书规划中计算机学科领域的学术著作的出版。为了做好选题工作，出版社特邀请中国计算机学会、中国中文信息学会帮助做好组织有关学术著作丛书的列选工作。

热诚希望得到广大计算机界同仁的支持和帮助。

清华大学出版社
广西科学技术出版社
计算机学术著作出版基金办公室

1992 年 4 月

序　言

计算机是当代发展最为迅猛的科学技术，其应用几乎已深入到人类社会活动和生活的一切领域，大大提高了社会生产力，引起了经济结构、社会结构和生活方式的深刻变化和变革，是最为活跃的生产力之一。计算机本身在国际范围内已成为年产值达2500亿美元的巨大产业，国际竞争异常剧烈，预计到本世纪末将发展为世界第一大产业。计算机科技具有极大的综合性质，与众多科学技术相交叉而反过来又渗入更多的科学技术，促进它们的发展。计算机科技内容十分丰富，学科分支生长尤为迅速，日新月异，层出不穷。因此在我国计算机科技尚比较落后的情况下，加强计算机科技的传播实为当务之急。

中国计算机学会一直把出版图书刊物作为学术活动的重要内容之一。我国计算机专家学者通过科学实践，做出了大量成果，积累了丰富经验与学识。他们有撰写著作的很大积极性，但相当时期以来计算机学术著作由于印数不多，出版往往遇到不少困难，专业性越强越有深度的著作，出版难度越大。最近清华大学出版社与广西科学技术出版社为促进我国计算机科学技术及产业的发展，推动计算机科技著作的出版工作，特设立“计算机学术著作出版基金”，以支持我国计算机科技工作者撰写高水平的学术著作，并将资助出版的著作列为中国计算机学会的学术著作丛书。我们十分重视这件事，并已把它列为学会本届理事会的工作要点之一。我们希望这一系列丛书能对传播学术成果、交流学术思想、促进科技转化为生产力起到良好作用，能对我国计算机科技发展具有有益的导向意义，也希望我国广大学会会员和计算机科技工作者，包括海外工作和学习的神州学人们能积极投稿，出好这一系列丛书。

中国计算机学会

1992年4月20日

前　言

随着计算机技术的高速发展，以计算机为基础的实时系统应用得越来越广泛。由于实时系统响应于外部发生的随机事件，并与外部世界作用的时间息息相关，因此实时系统的可靠性至关重要。

本书从理论和工程实践两个方面系统地介绍了提高实时系统可靠性的各种实用技术。第一章讨论了实时系统的特征；第二章介绍实时系统的故障来源、表现及可靠性参数；第三章介绍编码技术，编码技术是一种提高可靠性的信息冗余技术，同时也是理解以后各章介绍的各种容错技术的基础；第四章、第五章和第六章介绍的故障检测和诊断技术、故障屏蔽技术以及动态冗余技术等各种容错技术都统一在编码理论之下，把容错技术看着是对编码理论的实践，这对于系统地掌握可靠性技术十分重要；第七章讨论了当前研究的热门课题之一，分布计算机系统中的可靠性技术；最末一章介绍了一个实时容错计算机系统的实例，这不仅可以深化读者对理论知识的理解，也可以对工程技术人员的实践提供指导。

本书可作为从事实时系统研究以及可靠性研究的工程技术人员的参考书，也可作为有关专业大学生、研究生的教材或教学参考书。

作者领导的容错计算机研究室的同行们为本书作了大量的工程实践工作，余长芬同志参加了本书的部分整理工作，张雁同志为本书的录入花了许多心血，作者在此一并致谢。

由于作者水平有限，错误之处在所难免，恳请读者批评指正。

编著者

一九九四年八月

作者简介

袁由光，1941 年生，1965 年毕业于重庆大学无线电系，1982 年获得该校计算机系硕士学位。现任中国船舶工业总公司七院第七〇九研究所研究员、副总工程师兼容错计算机研究室主任，硕士生导师。主持国家“七五”和“八五”有关容错技术与容错计算机的重大预研和型号项目的研究，任项目负责人兼总设计师。1991 年获中国船舶工业总公司科技进步一等奖，1992 年获国家科技进步二等奖，1993 年获国家政府特殊津贴、光华科技基金奖等奖励，并获中国船舶工业总公司有突出贡献的中青年专家称号。

目　录

第一章　实时系统的特征

1.1　概　　述

一般来说，有两种不同的计算机应用模式。一种是围绕计算机来安排工作，即计算机开始工作前，把它所需要进行处理的所有数据转换成适合于机器可以利用的形式，一旦需要即可输入到计算机中进行处理，也就是说，被处理的数据完全处于计算机的控制之下；同样，计算机的输出也完全处于其控制之下，而与用户无关，这就是人们熟知的批处理方式。另一种应用模式是计算机围绕外部世界来工作，当外部世界需要向计算机输入数据时，计算机自动地由外部世界获取数据；同样，当且仅当外部世界请求输出时，计算机才输出被处理的数据。这种应用模式就是实时处理。实时处理响应于外部事件，并与外部世界作用的时间息息相关，因此这种系统叫做实时系统，或者叫做事件驱动系统。

更一般地说，实时系统是能及时响应外部发生的随机事件，并以足够快的速度完成对事件的处理的计算机应用系统。所谓外部事件是指与计算机相连接的设备（探测设备、控制对象、键盘等）提出的服务要求，如数据采集、情报检索、控制器输出等。

由此可见，实时系统具有如下特点：

（1）对外部事件的响应必须在一定时间内完成。例如，雇员上下班排队打卡时，计算机须在几秒钟内捕获卡片上的数据，如果在下一张卡片插入时未获取数据，该数据就会丢失。同样，要求的各种输出也须在一定时间内完成。事实上，数据的获取、处理、已处理数据的输出，都需在特定的时间内完成。这一时间的总和叫做系统的反应时间，其范围一般从几毫秒到几秒，缩短反应时间是设计实时系统的关键。

（2）必须满足一定的峰值负荷要求。一个实时系统的负荷可能是很不均匀的，有时负荷重，有时负荷轻，甚至有可能大部份时间没有被充分利用，但整个系统必须满足一定的峰值负荷要求。例如，实时雇员考勤系统，早上和晚上上下班时，该系统频繁的工作，从打卡机上捕获和处理数据的能力必须满足雇员上下班记录出勤情况的要求，而该系统在其余大部分时间没有被充分利用。

（3）与实时系统相关的另一个重要问题是，由于输入数据由系统本身捕获，因此，该数据只有在系统中才有效，而且只能通过系统来访问。也就是说，在故障发生时，不仅失去由系统执行的功能，而且也会失去有关的数据，使系统不可能恢复工作，因此实时系统的可靠性至关重要。

由于信息处理和过程控制都有一定的实时要求，我们可以把实时系统分为实时信息处理系统和实时过程控制系统。

（1）实时信息处理系统

信息是反映客观世界中各种事物的特征和变化的组合，是一种有用的知识，是知识的增量，信息的价值体现在信息的准确性、及时性和适用性。

利用电子计算机对信息进行采集、处理、存储、管理、检索和传输，必要时能向有关人员提供有用信息输出的系统，即称为信息处理系统。计算机进行信息处理就是对数字、符号、语言、文字、图形、图象、声音等各种信息源按一定法则进行处理以达到某种预定的目的。一般计算机进行信息处理的过程包括：(*a*)信息的采集；(*b*)信息的转换；(*c*)信息的存储；(*d*)信息的组织与检索；(*e*)信息的传输。

一个信息处理系统一般配有大型的文件和数据库，预先存有已知数据，能及时响应自身终端的服务请求，进行信息检索、修改、更新、加工、删除等功能，并在很短时间内对用户作出正确的回答。这类系统如电子数据处理系统、管理信息系统，决策支持系统、办公室自动化系统等。

(2) 实时过程控制系统

计算机过程控制系统是指计算机直接与其他机器、设备和仪器相连接，对它们的工作按照程序进行控制的系统，也就是计算机根据人们事先给定的指令序列(程序)，不断地、有序地加以执行，不断地、有序地给出控制信息，以实现对被控对象的控制。过程控制系统实时地采集被控制对象工作过程中发生的动态参数(如温度、频率、电压、压力、流量等)，这些参数经过变换处理以数字形式进入计算机，计算机对收集的信息进行处理，根据处理结果，再输出相应的信息调节被控制的有关机构(如电压、闸门、开关、加工机构等)，以控制生产过程平稳、均匀地按要求进行。

过程控制对实时性提出更高的要求，由于生产过程状态变化是随机的，但不管状态参数如何变化，都应对此“事件”作出及时响应，以保证系统能以最好的品质工作。“事件”和对事件的“响应”之间的时间延迟 t 是衡量系统的实时性的重要测度，不同的过程对该时间延迟的要求也不相同。例如，对于温度控制，t 为秒级就可以说是实时的；对调速系统毫秒级才算是实时的；而对于有些武器系统低于毫秒级才算是实时的。所以实时指标对具体过程才有意义。一般的实时过程控制系统有下列特征：(*a*)响应时间快；(*b*)中断能力强；(*c*)可靠性高；(*d*)要求有人机对话。

实时过程控制系统包括从最简单的自动检测和数据处理，到开环控制、闭环控制、直接数字控制、最佳控制直至多级分散集中控制等许多控制方式，随着计算机的向前发展，实时过程控制系统也发展到更高级的阶段，从而更加减轻人们的劳动并获得巨大的经济效益。

1.2 响应时间

前已述及，实时系统响应于外部事件，并与外部世界作用的时间息息相关，“事件”和对事件的“响应”之间的延迟时间叫做实时系统的响应时间。响应时间包括“事件”触发后，对数据的获取、数据的处理以及已处理数据的输出，直至驱动执行机构的所有时间的总和。响应时间是一个实时系统的重要特征。响应时间一般从几毫秒到几秒。有的快速反应系统甚至要求低于 1 个毫秒。

响应时间是设计一个实时应用系统的关键之一，不同的响应时间要求，对该系统中数据获取的速度、处理数据的速度、输出数据的速度都有不同的要求，特别是对系统中使用