分布式实时系统

张凤登　著

科学出版社

分布式实时系统

张凤登 著

科学出版社

北京

内 容 简 介

实时系统是在嵌入式系统、工业自动化系统和多媒体系统高度发展的基础上形成的一个新概念。本书采用认知领域的一些最新见解，以连贯、简洁、可理解的方式，系统地介绍了实时系统的产生背景、理论与技术基础，描述了分布式实时系统在架构层面的设计原理，并重点探讨了在预期负载和故障情况下强实时系统的设计、实现和评估方法。全书共分为10章，每章配有习题。

本书在编写过程中广泛吸取了实时系统设计方面的最新成果，全书内容自成体系，结构紧凑，前后呼应，具有一定的先进性、系统性和实用性。

本书可作为高等院校自动化、测控技术、信息工程、微电子、计算机、电气工程和机电一体化等专业高年级本科生、研究生的教材，也可作为从事嵌入式实时系统设计和应用的工程技术人员的参考书。

图书在版编目(CIP)数据

分布式实时系统/张凤登著. —北京：科学出版社，2014.3

ISBN 978-7-03-039313-5

Ⅰ.①分… Ⅱ.①张… Ⅲ.①分布式操作系统 Ⅳ.①TP316.4

中国版本图书馆CIP数据核字(2013)第299809号

策划编辑：王 哲/责任编辑：王 哲 邢宝钦/责任校对：钟 洋

责任印制：张 倩/封面设计：迷底书装

科 学 出 版 社 出版

北京东黄城根北街16号

邮政编码：100717

http://www.sciencep.com

北京市文林印务有限公司 印刷

科学出版社发行 各地新华书店经销

*

2014年3月第 一 版 开本：720×1 000 1/16

2014年3月第一次印刷 印张：21 1/2

字数：438 000

定价：96.00元

(如有印装质量问题，我社负责调换)

前　言

随着嵌入式系统、工业自动化系统和多媒体系统的不断发展，设备之间、人与系统之间的信息交换逐步实现网络化，各种网络化物理系统具备了自主获取和实时处理信息的能力，已被广泛应用于电力、冶金、化工、机械加工、食品加工和消费电子等领域，与人们的日常生产和生活息息相关。正因为如此，科技界已开始探索它们在安全性和可靠性要求极高的领域中的应用，如汽车、飞机、核电、交通、武器装备和航海航空等。学术界和工业界通过共同努力，逐步理解了很多应用实例的包含关系，并形成了一个新的科学概念——实时系统。这个概念与物理时间密切相关，不仅强调系统的控制运算、总线通信、错误诊断和结果预测能力，而且能够反映系统在预期负载和故障情况下的响应及时性和容错能力等，现已成为学术团体和工业组织的研究主题之一，也是当今网络化系统市场重要的技术促进因素。

为了确保实时系统安全可靠的运行，系统设计人员需要考虑很多因素，有时甚至颠覆了许多过去认为行之有效的系统设计原理。本书根据大量的工业实例，采用认知领域的一些最新见解，以连贯、简洁、可理解的方式，详细阐述了实时系统与时间之间的内在联系，从架构层面描述了这种系统的设计原理。

实时系统分为强实时系统和弱实时系统，本书侧重于讲述强实时系统方面的基本概念。全书共分为10章，第1、2章作为入门，主要介绍实时系统的基本概念，如实时环境、系统模型化；第3章着重描述Kopetz和Lamport在全局时钟同步和容错时钟同步方面的贡献；第4章给出实时系统的时间行为，如时间准确性、持久性、幂等性、复制确定性等；第5~8章利用故障、错误、失效和异常等概念，研究安全关键性系统的容错单元构造方法，探讨实时通信、实时操作系统、触发架构、CPU资源配置和实时调度算法等方面的重要见解；第9、10章讨论可依赖性实时系统的一般性设计和实现技术，并描述几种系统评估方法。围绕所讲内容，本书给出一些有代表性的设计实例。

本书的编写得到了资深学者、同事和科学出版社的大力支持。应启戛、张仁杰、缪学勤、吴勤勤为本书的组织结构和新术语的定义提出了很多宝贵意见；孟庆栋、周文杰、张勇、王闯、石秋蝉、廖振俭、华俊、尚雯雯、范科发、侯斌、王臻、张玮、胡羽、陈悫、张晓霞、张大庆、李红雨等仔细阅读了部分或全部书稿，并提出了许多宝

贵的改进建议；科学出版社的王哲编辑在本书的体例格式和易读性方面给予了许多帮助。在此谨向他们致以衷心的感谢。

由于作者水平有限，书中难免存在不足之处，敬请读者批评指正。

作　者

2013年8月

目　录

第1章 概 述

最近十多年里，嵌入式实时系统、工业自动化系统和多媒体系统的应用强劲增长，极大地推动了实时系统概念的形成和发展。本章从实时系统的定义出发，探讨实时系统的基本组成，以及系统在功能、时间和可依赖性方面的要求，并根据控制应用的特点，重点讲述在时间方面的概念和要求。实时系统的分类方法有多种，这里特别强调了弱实时(soft real time)系统和强实时(hard real time)系统之间的基本区别。本章还从经济角度分析实时系统的应用前景。

1.1 实时系统的定义

在介绍实时系统的定义之前，首先回顾一下“实时”和“系统”这两个术语。“实时”是一个不太容易理解的术语，许多人想当然地认为实时就是快。实际上，实时表示具有确定性的响应，即在给定的时间周期内，对某个事件做出可靠、准确的响应的能力。“系统”是指由相互制约的若干部分所构成的具有特定功能的整体。系统的状态由描述系统行为特征的变量来表示。随着时间的推移，系统会不断演化。外部环境的影响、内部组成的相互作用和人为的控制作用等，是导致系统状态和演化进程发生变化的主要因素。

很多文献给出了实时系统的定义，然而不同文献给出的定义不尽相同，至今也没有一个被人们广泛接受的定义。下面将从控制应用的角度，更加详细地讲述实时和实时系统的相关概念。

1.1.1 实时

简单地说，实时是用来描述实际应用的定时要求的。不同应用和不同用户的定时要求不尽相同，因此事物的实时性没有一个统一的时间限制。为了更加精确地定义系统的实时性能，经常使用弱实时和强实时两个术语。

实施弱实时的系统可以有不同的响应速率，而且不会影响整个系统的整体功能。例如，在温度监视系统中，温度不会快速改变，获取数据的速率相对较慢，可以每秒读数一次，读数间隔的轻微变化不会影响整个系统的功能。

然而，强实时的要求与前者不同，在一个绝对的时间内，它的响应速率必须是无差错的、准确的。例如，蒸馏过程的控制，必须以指定的时间间隔一致地采集压

力信号，以便及时做出开、关压力阀门的重要决策。如果不能在指定的时间周期内执行控制回路，那么压力可能增大到危险的程度。

1.1.2　实时系统

系统行为的正确性不仅取决于计算的逻辑结果，而且与产生这些结果的物理时间有关，这类系统称为实时系统[1]。其中，系统行为表示系统随时间推移的输出序列。实时计算机系统属于实时系统的一部分。

实时系统是随时间变化的。例如，在化学反应系统中，即使计算机控制系统已经停止运行，化学反应仍将继续改变状态。因此，将实时系统分解成一组自成体系(self-contained)的子系统是合理的，这种子系统通常称为簇。图1-1给出了一个实时系统实例，整个系统被分解成被控对象(被控簇)、实时计算机系统(计算簇)和操作员(操作员簇)三个子系统。

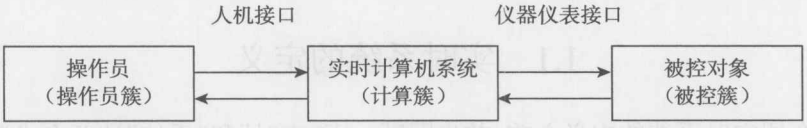

图1-1　实时系统实例

计算簇一般是分布式的，系统中的节点不只一个，各个节点通过实时通信网络相互连接，如图1-2所示，图中的A~F节点都是计算机节点。被控簇可以是物理设备或机器。操作员簇是指人机交互中的人类因素，但这里仅考虑操作员与计算簇之间的互动模式，并不关心操作终端的信息表示形式。通常，把被控簇和操作员簇统称为计算簇(实时计算机系统)的环境。

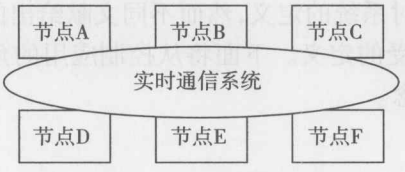

图1-2　分布式计算机系统

操作员与实时计算机系统之间的接口称为人机接口，被控对象与实时计算机系统之间的接口称为仪器仪表接口。人机接口是由输入设备(如键盘、鼠标)和输出设备(如显示器)组成的，用于实现与操作员的连接。仪器仪表接口是由传感器和执行器组成的，用于将被控簇中的物理信号(如电压、电流)变换成数字信号，或者将数字信号变换成被控簇中的物理信号。拥有仪器仪表接口的节点称为接口节点。

1.1.3 实时计算机系统

用从过去到未来的有向直线表示时间的进展,将时间线上的切口称为时刻(instant),发生在某一时刻的任何典型情况称为事件(event),描述事件的信息称为事件信息。当前时间点(现在)是一个非常特殊的事件,它将过去和未来分离开来(该时间模型建立在牛顿物理学基础上,忽略了相对论效应)。时间线上的间隔是由其起始事件和终止事件定义的,间隔的持续时间等于终止事件的时间减去起始事件的时间。数字时钟把时间线分割成一系列等长的持续时间,该等长的持续时间称为时钟粒度(granule),它们被特殊的周期性事件分隔开来,这些时间线上的特殊周期性事件称为时钟节拍(tick)。

实时计算机系统必须在指定的时间间隔内,对来自环境(被控簇或操作员簇)的激励做出反应,这里的指定时间间隔是由环境决定的,实时计算机系统必须产生结果的时刻称为截止时间(deadline)。如果截止时间已过,而产生的结果仍然有用,那么这个截止时间被定为弱截止时间。如果错过截止时间可能导致严重后果,那么该截止时间被定义为强截止时间。例如,一个有信号灯的铁路和公路交叉口,若信号灯没有在火车到达前变成"红"色,则可能导致意外事故。必须满足至少一个强截止时间的实时计算机系统称为强实时计算机系统,或安全关键性实时计算机系统。若系统不存在必须满足的强截止时间,则该系统称为弱实时计算机系统。

综上,实时计算机系统必须对给定的输入做出响应,而且强实时计算机系统的响应一定要在指定的截止时间之前完成。图1-3给出了实时计算机系统的时间概念模型[2]。

图1-3中,事件可能来自外界输入,如传感器的输入、硬件定时器中断等。一般情况下,系统要对事件做出响应,该响应可能会、也可能不会输出至外界。响应通常要在指定的截止时间之前发生。例如,如果给定输入是车轮的转动,那么截止时间是车轮转动一周的时间。从图中可以看出,事件发生后到开始处理之前有一段时间延迟(latency),产生响应的时间,除了包含该延迟,还包括一定的处理时间。一个实时计算机系统通常需要处理大量的事件。

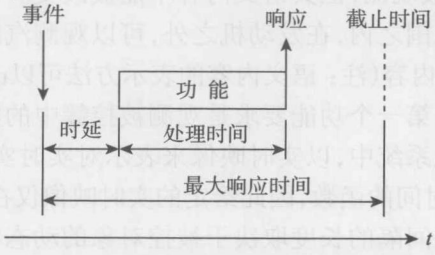

图1-3 实时计算机系统的时间概念模型