

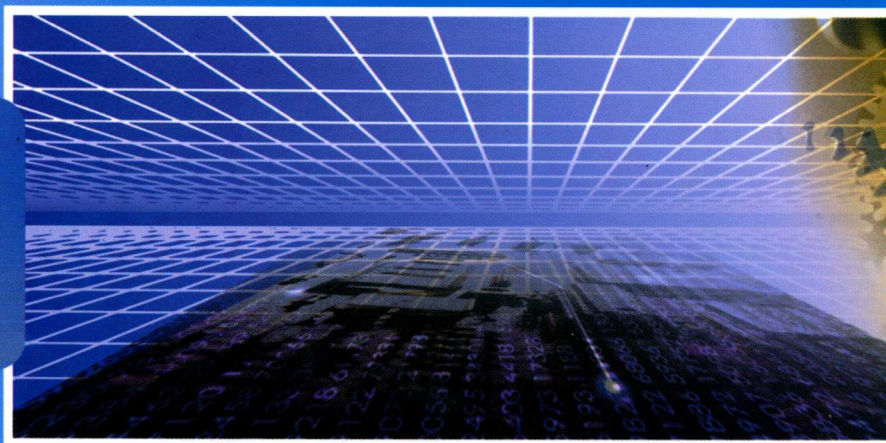


D-K-YT019-0D

空军航空机务系统教材

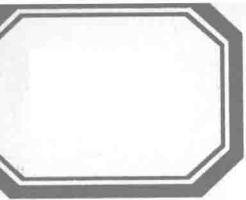
机载计算机软件

王勇 丛伟 主编



国防工业出版社

National Defense Industry Press



D-K-Y1019-0D

空军航空机务系统教材

机载计算机软件

王 勇 丛 伟 主 编

国防工业出版社

· 北京 ·

内 容 简 介

本书系统介绍了机载计算机软件结构、操作系统、开发环境、开发语言和发展趋势。全书共分6章,第1章介绍机载计算机软件结构,第2章主要从软件工程的角度论述机载计算机的系统设计思想、软件设计原理、软件结构以及常用的软件设计方法,第3章和第4章以 VxWorks 和 Tornado 为例介绍机载计算机使用的操作系统和软件开发环境,第5章介绍机载计算机程序设计语言 Ada95,第6章介绍机载计算机软件系统的发展趋势。

本书语言通俗易懂,难度深浅适中,内容组织循序渐进,示例丰富,每章后面备有形式多样的习题。本书可作为航空工程类院校的相关专业本科生和研究生的教材,同时也可作为航空兵部队、军事指挥机关、民航的工程技术和管理人员,以及航空计算机软件爱好者的自学指导书和参考书。

图书在版编目(CIP)数据

机载计算机软件 / 王勇, 丛伟主编. —北京: 国防工业出版社, 2008. 7
(空军航空机务系统教材)
ISBN 978 - 7 - 118 - 05418 - 7

I. 机... II. ①王... ②丛... III. 机载计算机 - 软件 - 教材 IV. V247

中国版本图书馆 CIP 数据核字(2007)第 196139 号

※

国防工业出版社出版发行

(北京市海淀区紫竹院南路 23 号 邮政编码 100044)

四季青印刷厂印刷

新华书店经售

*

开本 787 × 1092 1/16 印张 19 字数 460 千字

2008 年 7 月第 1 版第 1 次印刷 印数 1—5000 册 定价 49.00 元

(本书如有印装错误,我社负责调换)

国防书店:(010)68428422

发行邮购:(010)68414474

发行传真:(010)68411535

发行业务:(010)68472764

总 序

发生在世纪之交的几场局部战争表明,脱胎于 20 世纪工业文明的机械化战争正在被迅猛发展的信息文明催生的信息化战争所取代。信息化战争的一个显著特点,就是知识和技术密集,战争的成败越来越取决于各类高技术、高层次人才的质量和数量,以及人与武器的最佳配合。因此,作为人才培养基础工作的教材建设,就显得格外重要和十分紧迫。为了加快推进中国特色军事变革,贯彻执行军队人才战略工程规划,培养造就高素质新型航空机务人才,空军从 2003 年开始实施了航空机务系统教材体系工程。

实施航空机务系统教材体系工程是空军航空装备事业继往开来的大事,它是空军装备建设的一个重要组成部分,是航空装备保障人才培养的一个重要方面,也是体现空军航空装备技术保障水平的一个重要标志。两年来,空军航空机务系统近千名专家、教授和广大干部、教员积极参与教材编修工作,付出了艰辛的劳动,部分教材已经印发使用,效果显著。实践证明,实施教材体系工程,对于提高空军航空机务人才的现代科学文化水平和综合素质,进而提升航空机务保障力和战斗力,必将发挥重要作用和产生深远影响,是一项具有战略意义的工程。

空军航空机务系统教材体系工程,以邓小平理论和“三个代表”的重要思想为指导,以新时期军事战备方针为依据,以培养高素质新型航空机务人才为目标,着眼空军向攻防兼备型转变和航空装备发展需要,按照整体对应、系统配套、紧贴实际、适应发展,突出重点,解决急需的思路构建了一个较为完整的教材体系。教材体系的结构由部队、院校、训练机构教育训练教材三部分组成,分为航空机务军官教育训练教材和航空机务士兵教育训练教材两个系列十六个类别的教材组成。规划教材按照新编、修编、再版等不同方式组织编修。新编和修编的教材,充实了新技术、新装备的内容,吸收了近年来航空维修理论研究的新成果,对高技术战争条件下航空机务保障的特点和规律进行了有益探索,院校的专业训练教材与国家人才培养规格接轨并具有鲜明的军事特色,部队训练教材与总参颁布的《空军军事训练与考核大纲》配套,能够适应不同层次、不同专业航空机务人员的教育训练需要,教材的系统性、先进性、科学性、针对性和实践性与原有教材相比有了明显提高。

此次大规模教材编修工作,系统整理总结了空军航空机务事业创业 50 多年来的宝贵经验,将诸多专家、教授、骨干的学识见解和实践经验总结继承下来,优化了航空机务保障教材体系,为装备保障人员提供了一套系统、全面的教科书,满足了人才培养对教材的急需。全航空机务系统一定要认真学习新教材,使其真正发挥对航空机务工作的指导作用。

同时,教材建设又是一项学术性很强的工作,教材反映的学术理论内容是随实践的发展而发展的。当前我军建设正处在一个跨越式发展的历史关键时期,航空装备的飞速发展和空军作战样式的深刻变化,使航空机务人才培养呈现出许多新特点,给航空机务系统教材建设带来许多新问题。因此,必须十分关注航空装备的发展和航空机务教育训练的改革,不断发展和完善具有时代特征和我军特色的航空机务系统教材体系,为航空机务人才建设提供知识信息和开发智力资源。

魏 钢

二〇〇五年十二月

空军航空机务系统教材体系工程编委会

主 任 魏 钢

副主任 周 迈 毕雁翎 王凤银 袁 强 韩云涛

吴辉建 王洪国 王晓朝 常 远 蔡风震

李绍敏 李瑞迁 张凤鸣 张建华 许志良

委 员 刘千里 陆阿坤 李 明 郦 卫 沙云松

关相春 吴 鸿 朱小军 许家闻 夏利民

陈 涛 谢 军 严利华 高 俊 戴震球

王力军 曾庆阳 王培森 杜元海

空军航空机务系统教材体系工程总编审组

组 长 刘桂茂

副组长 刘千里 郦 卫 张凤鸣

成 员 孙海涛 陈廷楠 周志刚 杨 军 陈德煌

韩跃敏 谢先觉 高 虹 彭家荣 富 强

郭汉堂 呼万丰 童止戈 张 弘

空军航空机务系统教材体系工程 军械专业编审组

组 长 周志刚

成 员 查国云 刘应忠 杨 鸿 李建斌 那忠凯
王更辰 旷艾喜

前 言

近年来,我国正在加强新型飞机的引进、研发和改型,以适应未来信息战的需要。当前,为了培养高素质的航空科技人才,各军事院校已经或计划在其专业课程规划中增加机载计算机的相关内容,以规划出一套面向 21 世纪的、具有中国高等军事院校计算机教育特色的课程计划。但由于我国在机载计算机技术方面起步较晚,缺乏相关的技术资料,给学习、开发和研究等工作造成了极大障碍。因此,我们引进国际上具有先进性、实用性和权威性的军用机载计算机软件,系统地介绍了机载计算机的软件结构、操作系统、开发环境、机载计算机语言和发展趋势,以更好地服务于国内各高等军事院校及广大读者。

本书共分 6 章:第 1 章,介绍机载计算机软件结构。重点介绍机载计算机的系统设计思想、软件设计原理、软件结构以及常用的软件设计方法。第 2 章,介绍与机载计算机有关的软件工程内容。重点介绍机载计算机软件生命周期及软件开发技术、软件可靠性分析、利用可靠性增长模型提高软件的质量水平以及软件测试方法等方面的内容。第 3 章,介绍机载计算机使用的操作系统。重点介绍嵌入式实时系统软件的开发模型、开发过程及常用的开发工具,并以机载实时嵌入式操作系统 VxWorks 为例,介绍 VxWorks 操作系统的特点、组成和基本配置,通过实例详细介绍 VxWorks 程序设计中的多任务设计、任务调度机制、任务间通信、中断处理以及计时器等方面的内容。第 4 章,介绍机载计算机的软件开发环境。以 Tornado 开发工具为例,详细介绍 Tornado 的核心工具、使用步骤、网络编程、建立调试环境等内容。第 5 章,介绍机载计算机程序设计语言。重点介绍 Ada95 语言规范、程序组成要素、基本程序结构、程序包、类属单元和任务等重要内容。第 6 章,介绍机载计算机软件系统的发展趋势。

第 1 章、第 6 章和附录由王勇编写,其余的 4 章由丛伟编写。本书在编写过程中得到了空军工程大学雷英杰教授、白振兴教授和朱参世教授的大力支持和帮助,在此表示衷心的感谢。

由于机载计算机的软件系统更新很快,相关资料特别是应用类文献较少,加之作者的水平 and 经验有限,书中难免存在错误和疏漏之处,敬请广大读者和同行批评、指正。

编者
2007 年 10 月

目 录

第1章 机载计算机软件结构	1
1.1 系统设计思想	1
1.1.1 系统描述	1
1.1.2 传统设计方法	1
1.1.3 顶层设计思想	2
1.2 软件设计原理	5
1.2.1 任务管理	5
1.2.2 时间管理	5
1.2.3 错误管理	9
1.3 软件结构及设计方法	11
1.3.1 作战飞行程序	13
1.3.2 执行程序	15
1.3.3 应用程序	19
习题	30
第2章 机载计算机软件工程	31
2.1 软件生命周期及软件开发支持技术	31
2.1.1 软件过程开发模型	31
2.1.2 系统建模方法	37
2.1.3 开发方法及设计方法	43
2.1.4 编码及测试	48
2.1.5 系统的验证及维护	56
2.2 软件的可靠性分析	62
2.2.1 可靠性参数	62
2.2.2 提高软件可靠性的方法	65
2.2.3 软件的可靠性验证	71
2.3 利用可靠性增长模型提高软件的质量水平	74
2.3.1 可靠性增长模型的含义	74
2.3.2 数学模型(公式)	75
2.3.3 数据分析	76
2.4 机载软件的测试方法	77
2.4.1 传统的测试方法	77
2.4.2 改进的测试方法	78

2.4.3	净室测试方法	78
2.4.4	应用实例分析	79
	习题	82
第3章	机载计算机操作系统	83
3.1	概述	83
3.1.1	嵌入式系统的特点	83
3.1.2	实时系统的特点	84
3.1.3	机载计算机操作系统的特点	84
3.1.4	机载计算机操作系统的比较	85
3.2	嵌入式实时系统软件开发设计	86
3.2.1	开发模型	86
3.2.2	开发过程	87
3.2.3	开发工具	97
3.3	VxWorks 操作系统的特点、组成及配置	100
3.3.1	VxWorks 操作系统的特点	100
3.3.2	VxWorks 操作系统的组成	102
3.3.3	VxWorks 操作系统的基本配置	103
3.4	VxWorks 的任务、任务编程接口及任务间通信	112
3.4.1	任务的含义及特征	112
3.4.2	Wind 系统调度机制	114
3.4.3	控制函数及通信方法	114
3.5	VxWorks 的信号、中断处理及定时机制	122
3.5.1	信号的含义及配置	122
3.5.2	中断服务程序的设置及特殊限制	125
3.5.3	POSIX 计时器的特点及实例分析	129
	习题	136
第4章	机载计算机软件开发环境	137
4.1	Tornado 集成开发环境简介	137
4.1.1	Tornado 的核心部件	137
4.1.2	Wind Power 工具集的作用	140
4.1.3	Tornado 的使用步骤	142
4.2	网络编程	154
4.2.1	VxWorks 的网络工具	154
4.2.2	客户/服务器编程	168
4.3	建立调试环境及实例分析	173
4.3.1	主机/目标机开发环境	174
4.3.2	x86 系列目标机调试环境的建立	178
4.3.3	编程实例分析	186
	习题	197

第5章 机载计算机软件开发语言	200
5.1 Ada语言概述	200
5.1.1 Ada语言简介	200
5.1.2 Ada语言与C语言和Java语言的比较	203
5.1.3 Ada语言的开发环境	204
5.2 语法成分及数据类型	206
5.2.1 基本语法成分	206
5.2.2 标量类型及复合类型	208
5.2.3 自定义类型及访问类型	214
5.2.4 字符及字符串类型	220
5.3 程序控制结构及子程序	222
5.3.1 3种程序结构	222
5.3.2 过程和函数	226
5.3.3 方法重载	228
5.3.4 程序包及私有类型	230
5.4 面向对象程序设计	233
5.4.1 标志类型及抽象类型的定义	234
5.4.2 继承及派生的实现	237
5.4.3 多态性及类属单元	240
5.5 并发程序设计	246
5.5.1 任务的含义及特征	246
5.5.2 任务的控制语句	255
5.5.3 任务的通信方式	259
5.5.4 保护类型	261
习题	269
第6章 机载计算机软件系统发展趋势	270
6.1 软件结构的发展趋势	270
6.2 设计方法的发展趋势	274
6.3 操作系统的发展趋势	276
6.4 开发环境的发展趋势	278
习题	280
附录	282
附录A Ada95语言的程序包	282
附录B Ada95语言的预定义属性	289
附录C Ada95语言的预定义编用	291
附录D Ada95语言的常用词汇	293
参考文献	294

第1章 机载计算机软件结构

1.1 系统设计思想

1.1.1 系统描述

在先进的飞机上,由于功能的增加,因而也要求其承载的电子设备的功能迅速地增强。在完成基本的飞行和战斗任务时,飞机所必需的基本电子设备如下:

(1) 按设备类型分类的电子子系统有雷达、接收机和发射机、导航、电源和配电管理、通信、控制和显示仪器仪表、敌我识别、瞄准/射击系统和地形回避及地形跟踪。

(2) 按飞行和作战任务分类的电子子系统有进攻系统、防御系统、武器投放系统、电子对抗、飞行控制、威胁报警、外挂物管理和激光报警。

(3) 按执行功能分类的电子子系统有电子干扰吊舱、威胁报警接收机、雷达高度表、联合战术信息系统接收机、数据处理器、平视显示器(简称平显)。

由此可以看出,在这样密集的电子系统中,必须采用新的设计方法,以改善由于电子设备的增加给飞机的航空电子系统(简称航电系统)带来的爆炸性局面。

1.1.2 传统设计方法

1.1.2.1 设计思想

传统的做法是:对上述各个功能部件或功能子系统自底向上地进行拼凑式的综合,对设计进行逐次划分的过程是从基本的子系统出发(这些子系统要么是已经制造出来的,要么是其他项目已经开发好或外购得到的);然后把这些子系统通过模拟信号传输电缆进行交联;最后集成为一个综合的系统。这种设计方法的最大优点是实现各个子系统所需的时间短;但其缺点是对系统的整体功能把握不定,完成整个系统功能所需的时间长,对设计人员间的协作有较高的要求。

1.1.2.2 存在问题

由于电子子系统的增加,其功能的复杂性也在增加,自底向上的设计方法已经陷入困境,因为这种设计方法不可能解决下面4方面的问题:

(1) 飞机总体设计中对电子子系统的功能要求苛刻,对体积、质量限制也十分严格,传统设计方法除子系统本身外,其间的传输电缆就占可观的质量和体积。

(2) 由于不是从系统工程学的观点进行设计,因此,即使子系统的性能很好,但组合之后的总体性能却很差。因为各电子子系统都有诸如信息采集、传输、处理和控制等环节不能共享资源和互为备份,加之没有故障隔离或防止故障蔓延的措施,严重降低了系统的可靠性。

(3) 人-机工程上,一是提供给飞行员数据的多样性和飞行员有限的反应能力之间的矛盾;二是各子系统并行独立发展,没有标准化的接口,导致设备的多样化和复杂化。

(4) 离散式的设计不利于飞机改型时电子系统的增删,由于飞机的服役期较长,

要对飞机做一些小的改型,就要对其电子设备做重大的改造或增删,这就要求整个设计思想要适应系统的扩展。自底向上的方法不利于系统的改型,这就势必影响飞机的服役期。

1.1.3 顶层设计思想

1.1.3.1 设计基础

自底向上的设计方法所产生的问题是可以解决的,解决的途径是用系统的观点对航电系统进行统筹设计,采用自顶向下的顶层设计方法。这种设计方法是建立在航电系统的基础上,该系统的特点如下:

- (1) 飞机所要执行的全部任务是预知的,可以将一个完整的飞行过程分解为若干个阶段,如起飞、巡航、格斗、进场(回收)等,在每一个阶段由于条件不同可形成各种相应的任务服务功能,这就产生了飞行功能智能化的程序要求。
- (2) 全部目标任务以及任务执行时间决定了对资源的要求是可以预先估计到的,对存储器容量的要求也是有界的,因此,可以确定系统的配置规模。
- (3) 大部分任务的输入/输出(I/O)过程都是周期性的,且周期的大小可以根据实时性的要求和所传输信息变化率的快慢而预先确定,因而,系统的负载分布和可扩展性也是可预知的。
- (4) 某些非周期性事件的出现,如系统对飞行员操作的响应或一旦出现某类故障从故障中恢复或系统重构的能力等,都可以通过精心设计满足系统的要求。

基于上述4点的可预知性,可以根据系统的要求自顶向下地进行航电系统设计。

1.1.3.2 开发过程

自顶向下的开发过程大体包括6个顺序执行的阶段,如图1-1所示。

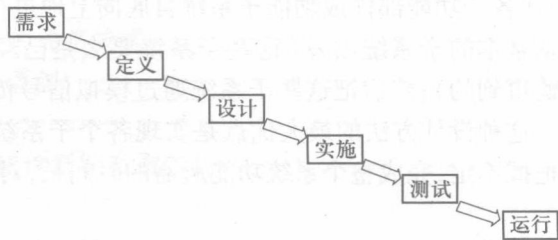


图1-1 自顶向下的顺序开发过程

整个系统的设计由硬件设计和软件设计两部分构成,为了密切地协调二者的关系,应在上述各个开发阶段完成时进行协调和设计评审,其过程如图1-2所示。在协调和设计评审时,不可避免地调整和修改本阶段甚至前一阶段的设计。因此,整个开发过程不仅是自顶向下的顺序开发过程,也是一个反复迭代的过程,如图1-3所示。通过反复验证、确认和修改设计的过程,使整个航电系统的性能达到总体性能指标。

1.1.3.3 性能指标

衡量航电系统性能的优劣,一般有下列技术指标:

- (1) 总线使用效率 是指在数据传输中,有效数据位传输时间与总传输时间(包括有效数据位传输时间(T_d)、指令字传输时间(T_0)、指令响应时间(T_r)和状态字间隔时间(T_g)的比值,即

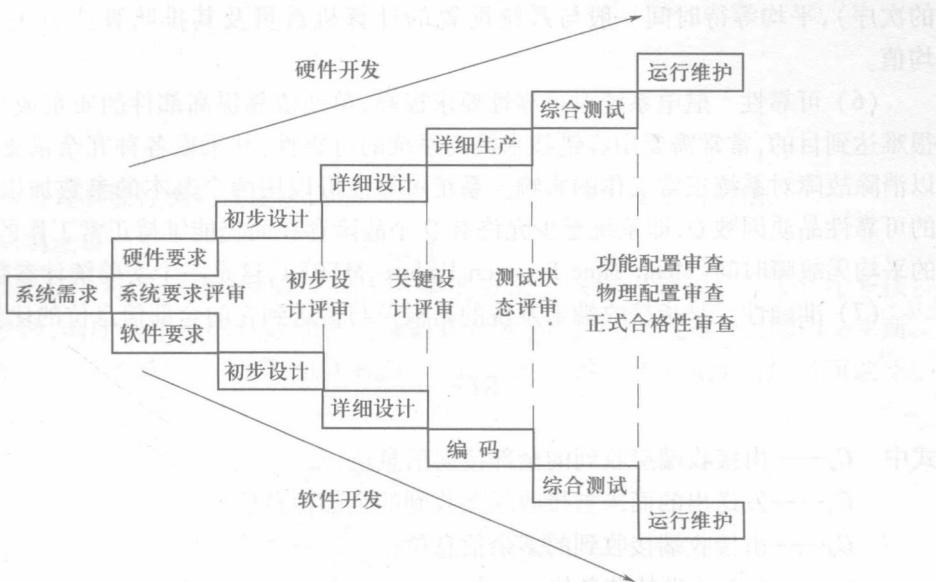


图 1-2 系统中的软件/硬件协调开发

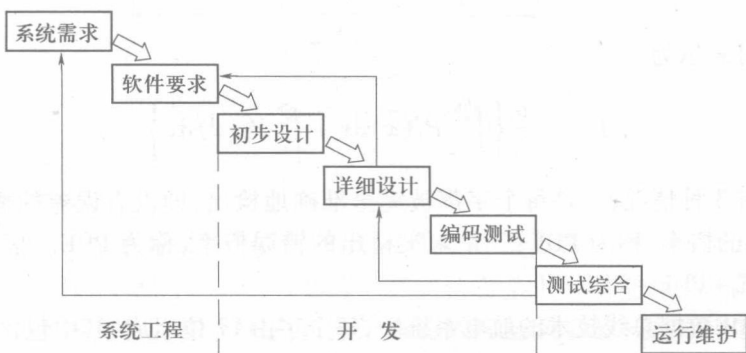


图 1-3 开发过程中的反复迭代

$$E = \frac{T_d}{T_d + T_0 + T_r + T_g} \quad (1-1)$$

(2) 总线负载 是指信息的实际传输量与最大允许传输量的比值。这个比值包括数据和内部开销两部分,反映系统允许扩充的余地。

(3) 总线利用率 与总线负载不同,它是指总线上信息传输的时间与全部时间的比值,反应总线上信息传输的拥挤程度。与总线负载相同的是,为支持分系统的扩展并防止总线堵塞,系统设计时对总线利用率也必须留有余地。

(4) 延迟时间 或称透明度,是指在信源处信息启动时间与吸收点处执行时间的差值。从动态的观点看,对周期性传输的数据,数据延迟时间即为数据刷新率的倒数或等于其传输的周期数。

(5) 平均等待时间 是指非周期性消息的传送等待的平均时间。一般说,异步消息的传送请求不可能立即得到服务,需要按照某种原则排队等待(如按优先级或异步请求到达

的次序),平均等待时间一般与系统配置的计算机数量及其排队算法有关,是一个统计平均值。

(6) 可靠性 航电系统对可靠性要求极高,单纯依靠提高部件的质量或装配的工艺质量很难达到目的,常常需要用容错技术提高系统的可靠性,并采取各种冗余措施,实现故障掩蔽以消除故障对系统正常工作的影响。系统可靠性可以用两个基本的参数加以衡量,一是系统的可靠性品质因数 Q ,即系统至少允许有 Q 个故障存在而仍能维持正常工作的能力;二是系统的平均无故障时间(Mean Time Between Failure, MTBF),这是一个实验统计参数。

(7) 准确性 是指接收端未发现的错误位与传送到它的全部信息位的比值,可表示为

$$\text{REF} = \frac{C_e + C_u + C_d}{C_t} \quad (1-2)$$

式中 C_e ——由接收端接收到的全部错误信息位;
 C_u ——发送出的而未被接收端接收到的全部信息位;
 C_d ——由接收端接收到的多余信息位;
 C_t ——全部传送的信息位。

实际上,衡量一个系统在信息传输过程中的准确性常常使用的指标是误码率、误字率和误块(数据块)率。

① 误码率可表示为

$$P_e = \frac{1}{2} \left\{ \int_{-\infty}^{U_b} P_1(x) dx + \int_{U_b}^{\infty} P_0(x) dx \right\} \quad (1-3)$$

② 误字率有 3 种情况:一是每个字都被完全准确地检出,即没有误差的概率,称为 PNE;二是被检出错误的概率,称为 PDE;三是未被检出的错误概率,称为 PUE。很明显,这三者之和等于 1,即 $PNE + PDE + PUE = 1$ 。

在采用 1553B 数据总线技术的航电系统中,每个字由 17 位组成,其中包含一个奇偶位,因此,误字率可表示为

$$\text{PNE} = (1 - P_e)^{17} \quad (1-4)$$

$$\text{PDE} = \sum_{n=1,3,5,\dots,17} \binom{17}{n} (1 - P_e)^{17-n} (P_e)^n \quad (1-5)$$

$$\text{PUE} = \sum_{n=2,4,6,\dots,16} \binom{17}{n} (1 - P_e)^{17-n} (P_e)^n \quad (1-6)$$

③ 误块率的计算式与消息长度有关,而消息长度取决于消息中的数据字数,因而,误块率是消息长度和消息中误字率的函数。如果在指令字(第 1 组)中存在错误或者任何数字(第 2 组)存在错误或者在上述二者中都存在错误,则认为检测出了消息(块)的错误。因此,误块率可表示为

$$\text{PBDE} = \Pr(d_1 \overline{d_2}) + \Pr(\overline{d_1} d_2) + \Pr(d_1 d_2) \quad (1-7)$$

式中 d_1 ——在第 1 组中检出的错误;

d_2 ——在第 2 组中检出的错误。

1.2 软件设计原理

1.2.1 任务管理

一般来说,任务管理有硬性编码调度法、表驱动调度法和排队调度法 3 种方法。

1.2.1.1 硬性编码调度法

硬性编码调度法是一种最基本、最简单的任务调度方法。系统设计时,把每个任务按照工作方式编码,调度程序根据有效的方式编码调度不同的任务,流程图如图 1-4 所示。这种方式的优点是任务简单、方式简单,但由于方式编码是系统事先确定的,因而缺乏灵活性。

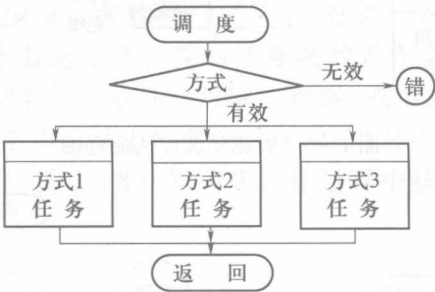


图 1-4 硬性编码调度法流程图

1.2.1.2 表驱动调度法

表驱动调度法是一种更灵活、功能更丰富的任务调度方法,但是系统开销较大。在表驱动调度法中,共有两个程序,即执行程序(建立任务表)和调度程序(使用任务表),其核心是任务表。任务表中的各个任务以优先级的顺序排列,每一项对应着该任务的状态和地址参数,状态参数是为解决多任务间并发而设置的,地址参数是该任务程序的起始地址。在执行任务程序的过程中,当时刻到达时,就调用调度程序,而调度程序则按一定的规则处理任务表中的任务。在表驱动调度法中,有一个定时机构,时间刻度的大小由执行任务的计算工作量和实时性要求两者共同决定。图 1-5 是表驱动调度法的流程图。

1.2.1.3 排队调度法

排队调度法比前两种调度法的功能更强、使用更灵活,但其系统开销较大,不适合应用在实时性要求很高的场合。其程序执行及调度过程如图 1-6 所示。

1.2.2 时间管理

在航电系统中,工作任务可以分为周期性任务和非周期性任务两类。对于周期性任务,系统必须按照任务要求的时间有规律地执行;对于非周期性任务,其执行时间和出现的次数无任何规律可循,属于随机事件。因此,必须采取有效的时间管理策略,以满足各种任务对时间的要求。对于周期性任务,系统采用大小周期的方法安排任务的运行;而对于非周期性任务,采用与周期性任务混合的方法安排任务的运行。

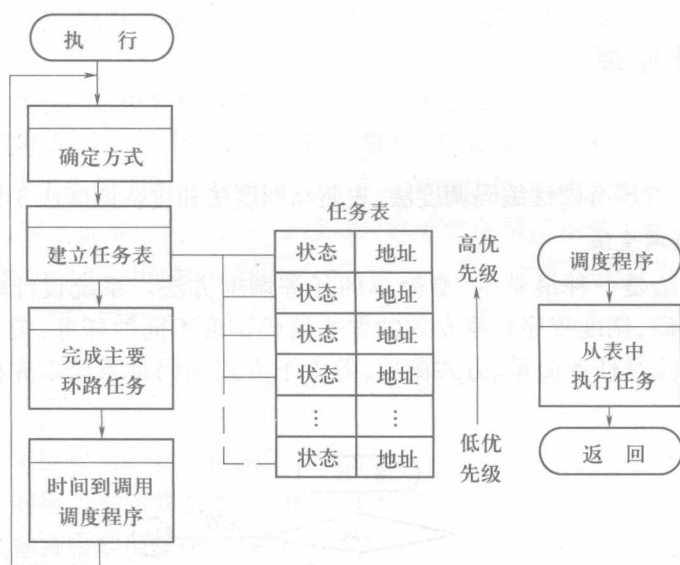


图 1-5 表驱动调度法流程图

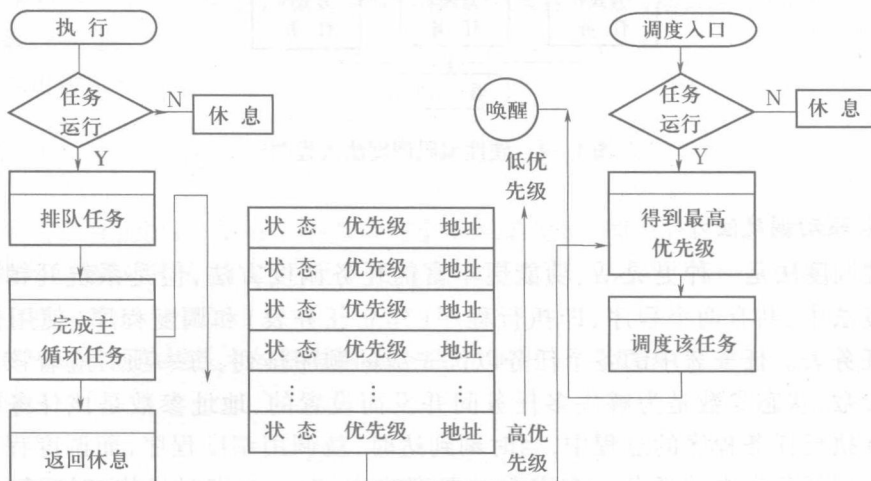


图 1-6 排队调度法流程图

1.2.2.1 同步信息传输

周期性任务有固定的执行周期,根据执行周期的不同,可以分为大周期和小周期两种形式。更新率最低(最大的执行周期)的工作周期称为大周期;更新率最高(最小的执行周期)的工作周期称为小周期。为了实现大、小周期任务的混合执行,把一个大周期分成 $N = 2^n$ 个小周期,如果 $n = 6$,则每个大周期共包括 64 个小周期。其示意图如图 1-7 所示。

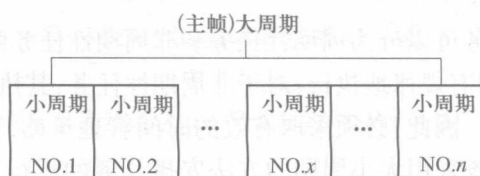


图 1-7 大、小周期时间安排关系