·测试、试验与仿真·

机载电子设备冗余设计与可靠性分析

张志伟

(中国电子科技集团公司光电研究院,天津 300308)

摘 要 阐述了冗余控制的概念和类型。针对冗余控制原理提出了一种机载电子设备冗余设计方法,包括硬冗余设计方法和软冗余设计方法,并分别对硬冗余和软冗余的工作原理进行了详细叙述。最后,对采用冗余设计的电子设备的可靠性进行了分析。结果表明,冗余设计方法能明显提升电子设备的任务可靠性,应用于机载电子设备,能适应机载电子设备高可靠性的作战要求。

关键词 机载电子设备 硬冗余 软冗余 冗余系统

中图分类号:TN709 **文献标识码**:A **文章编号**:1673-1255(2017)-03-0066-04

Redundancy Design and Reliability Analysis of Airborne Electronic Equipment

ZHANG Zhi-wei

(Academy of Opto-Electronics, China Electronics Technology Group Corporation (AOE CETC), Tianjin 300308*, China)*

Abstract: The concept and types of redundant control are described. Based on the principle of redundancy control, the design method of redundant system for airborne electronic equipments is put forward, including the design methods of hardware redundancy and software redundancy, and the principles of hardware redundancy and software redundancy are described respectively in detail. And the reliability of the electronic equipment adopting redundant design is analyzed. The results show that the design method of the redundant system can significantly improve the mission reliability of the electronic equipment, and can be applied to the airborne electronic equipment, which can meet operational reliability requirements of the airborne electronic equipment.

Key words: airborne electronic equipment; hardware redundancy; software redundancy; redundancy system

近年来,航空业发展突飞猛进,对机载电子设备的可靠性提出了越来越高的要求;同时,飞机上恶劣的工作环境和飞行安全要求也对机载设备的可靠性和稳定性提出了很高的要求。如何在空中复杂的环境条件下保证机载设备稳定、可靠的运行是机载电子设备面临的重要问题。提出了一种机载电子设备冗余设计方法,在满足机载设备功能、性能的同时能有效的提高机载电子设备的可靠性。

1 冗余控制原理

1.1 冗余控制的概念

冗余控制[1]理论来源于自动控制系统可靠性研究,其核心内容是如何最大限度地提高系统可靠性和稳定性。严格的讲冗余是采用一定成倍量的设备或元器件的方式组成控制系统来参加控制,当某一设备或元器件发生故障而损坏时,它可以通过硬件、软件或人为方式互相切换,作为后备设备或元器件替代因故障而损坏的设备或元器件,保持系统正常工作,使控制设备因意外而导致的损失降到最低。

冗余控制还涉及到一个概念——同步(synchronization)。它是指冗余系统的两个或多个处理器之间要经常比较各自的状态。根据一定的规则以决定系统是否工作在正常状态,这种状态比较和系统可靠性的判断被称为同步。

收稿日期:2017-04-06

作者简介:张志伟(1985-),河南省焦作市人,工学硕士,工程师,研究方向为光电工程.

1.2　冗余控制的类型

冗余控制的方式根据不同的需求有很多种方式，各种方式也不尽相同。

一般冗余控制可分为：处理器冗余（CPU冗余）、通信冗余（网络冗余）、I/O冗余和电源冗余[2]。

按冗余的实现方式来分大致可分为：

（1）硬冗余（hard-redundancy），即采用特殊的硬件模块来实现同类故障切换的冗余方式。

（2）软冗余（soft-redundancy），即采用编程的方式来实现故障切换的冗余方式，处理器成双使用，其中一个正常运行，一个处于备用状态。当主处理器故障失效时，通过事先在处理器程序中编制主/从处理器监控程序和主/从处理器数据交换程序来实时监控、判断主/从处理器的工作状态，采用软件方式将主处理器切换至从处理器，保证系统正常运行。

按冗余的切换方式来分大致可分为：

（1）热冗余，即硬冗余方式。当主设备故障时，通过特定硬件判断，备份方式，无间隙地自动切换到备用设备上，保持系统正常运行。

（2）暖冗余，即软冗余方式，主要通过编程方式来实现冗余。

（3）冷冗余，即一套或部分冗余的设备不通电工作，准备待命，当主设备故障时需要人工恢复系统运行。

一般的I/O冗余、电源冗余大多数属于硬件冗余的范畴，而处理器冗余，通信冗余既可以采用硬件冗余也可以采取软件冗余实现，一般硬冗余和软冗余比较，硬冗余投入较大，冗余实现相对简单，系统可靠性高，系统的切换速度快。软冗余不需要特殊的冗余模块和软件支持，系统切换速度比较慢，但是系统投入硬冗余少，成本较低。

2　机载电子设备冗余设计

2.1　硬冗余设计

硬冗余设计构成如图1所示。由图1可以看出，硬冗余设计由两套独立的控制模块和功能模块组成。控制模块主要完成与航电设备的数据交换和实时处理接收到的信息并下发给功能模块1、功能模块2；同时，对功能模块1、功能模块2的功能进行实时检测。功能模块主要完成控制模块下发的命令，将指令分配到执行模块。硬冗余设计中控制模块是数据处理分析、下发执行动作的执行单元，而功能模块1、功能模块2是控制模块与执行模块的连接单元，因此，选取控制模块、功能模块1、功能模块2作为一个冗余通道[5-6]进行备份。

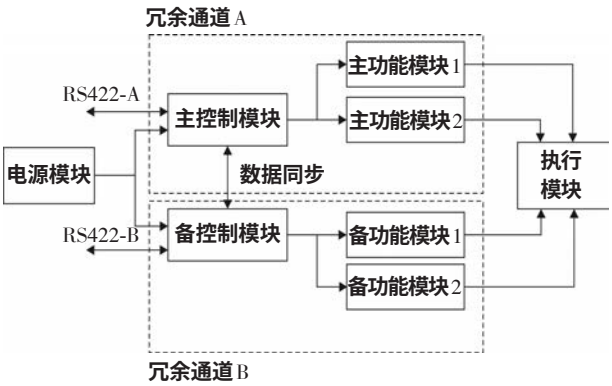

图1　硬冗余设计组成

硬冗余设计有3条通讯链路：（1）主控制模块与上位机通信，通过RS422通信总线进行数据交换；（2）备控制模块与上位机通信，通过RS422通信总线进行数据交换；（3）主控制模块与备控制模块的数据同步通讯链路，通过I^2C总线进行数据交换。

硬冗余设计采用“热备份”模式的主动冗余原理，通过串口通信进行主通道到冗余通道的切换，控制模块实时监控通道的故障，当发现故障时，通过串口将故障上报，通过主/备切换逻辑，实现主通道到备通道的切换。

为了保证主/备模块无扰动的切换，必须实现控制模块链路之间快速可靠的数据交换。两个控制模块采用相同的应用程序，自动的接收相同的数据。这样可以确保两个通道数据同步，当任意一个模块有故障时，另一个模块可以完成控制功能。

2.2　软冗余设计

软冗余设计程序框图如2所示。软冗余程序运行时，主/备通道（冗余通道A、冗余通道B）独立运行，由主控制模块掌握通讯控制权。主控制模块和备控制模块的应用程序由非冗余应用程序和冗余应用程序组成，主控制模块执行全部应用程序，备控制模块只执行非冗余应用程序，跳过应用程序。

软冗余设计中，主控制模块正常工作，备控制

模块处于备用状态。当主控制模块故障失效时，通过程序中的主/备控制模块监控程序和主/备控制模块数据交换处理程序来实时监控，判断主/备控制模块的工作状态，将主控制模块切换至备控制模块，实现备控制模块到主控制模块的切换。

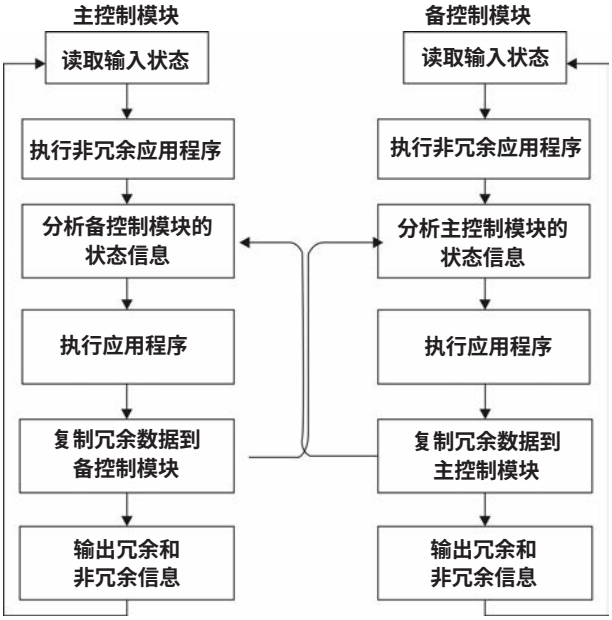

图2 软冗余设计程序框图

3 冗余设计的可靠性分析

冗余系统中冗余单元数与系统可靠度的关系如图3所示。

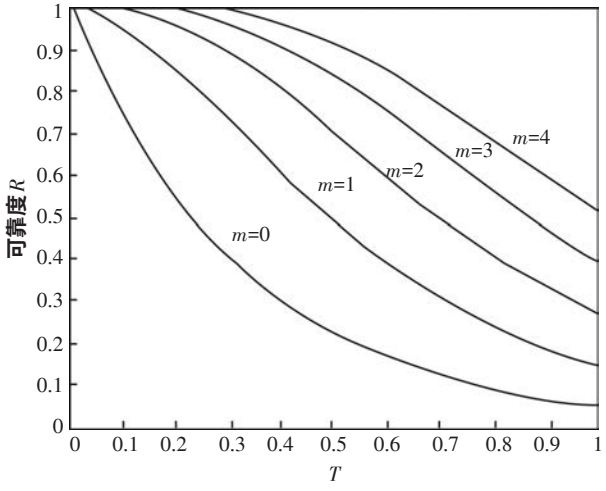

图3 可靠度R与冗余单元数的关系

由图中曲线可以看出，当冗余单元数由1增加到2时（m由0增加到1），系统的可靠度提升明显。随着冗余单元数的增加可靠度提升逐渐变慢，而且，冗余单元数越多，相应的硬件增加的就越多，系统越复杂，因此冗余设计采用控制模块、功能模块1、功能模块2为冗余备份的设计，以便保证系统的可靠性和稳定性[3-4]。

冗余系统的可靠性框图如图4所示。

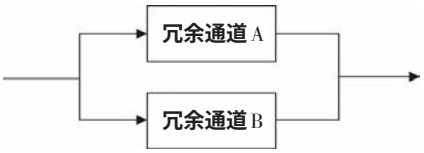

图4 冗余系统可靠性框图

假设冗余系统所包含单个通道的故障时间服从指数分布，则有

故障密度函数：$f(t)=\lambda e^{-\lambda t}$ （1）

不可靠度密度函数：$F(t)=1-e^{-\lambda t}$ （2）

可靠度密度函数：$R(t)=1\text{-}F(t)=e^{-\lambda t}$ （3）

系统故障率：$\lambda_s(t)=\sum_{i=0}^{n}\lambda_i(t)$ （4）

其中，$\lambda_s(t)$为系统故障率；$\lambda_i(t)$为第i个单元的故障率。

由图4根据并联系统定义，可靠性数学模型为

$$F_s(t)=\prod_{i=1}^{n}F_i(t) \quad (5)$$

其中，$F_s(t)$为系统不可靠度；$F_i(t)$为第i个单元的不可靠度。

冗余系统中通道A和通道B采用相同的硬件设计，因此，假设两个通道的故障率为λ，由式(2)可得其不可靠度分别为：$F_1(t)=1-e^{-\lambda t}$，$F_2(t)=1-e^{-\lambda t}$。

由式(2)、式(5)可得冗余系统两个通道的不可靠度和可靠度分别为

$$F_{冗}(t)=F_1(t)\times F_2(t)=(1-e^{-\lambda t})(1-e^{-\lambda t})$$

$$R_{冗}(t)=1\text{-}F_{冗}(t)=1\text{-}(1-e^{-\lambda t})(1-e^{-\lambda t})=2e^{-\lambda t}-e^{-2\lambda t} \quad (6)$$

由式(3)得单个通道的可靠度为

$$R_{单}(t)=e^{-\lambda t} \quad (7)$$

假设单通道故障率λ=0.000 06，工作时间2 000 h。由式(7)知，单通道工作2 000 h的可靠度为

$$R_{单}(t)=e^{-\lambda t}=e^{-2\,000\times 0.000\,06}=0.887 \quad (8)$$

由式(6)知,冗余系统工作2 000 h的可靠度为

$$R_{冗}(t)=2e^{-\lambda t}-e^{-2\lambda t}=2\times e^{-2\,000\times 0.000\,06}-e^{-2\times 2\,000\times 0.000\,06}=2\times 0.887-0.786\,6=0.987\,4 \quad (9)$$

由式(8)、式(9)可知,采用冗余设计的设备可靠度有明显提升,即系统的稳定性和系统的任务可靠性明显提升。

4 结　论

介绍了一种机载电子设备冗余设计方法,冗余设计从硬冗余和软冗余充分考虑了主/备通道切换实时性和可行性,通过同步的方法保证主备通道的一致性;同时,对冗余系统中主/备冗余通道的可靠度进行了分析。由结果可知,冗余设计能够有效的提升系统的任务可靠度,应用于机载电子设备,能适应机载电子设备高可靠性的作战要求,具有广泛的应用价值。

参考文献

[1] 陈子平.浅谈控制系统冗余控制的实现[J].自动化仪表,2005,26(9):4-5.

[2] 范丽云.硬件冗余在安全控制系统中的应用[J].计算机系统应用,1998.

[3] 高杜生,张玲霞.可靠性理论与工程应用[M].北京:国防工业出版社,2002.

[4] 白雪峰.惯性导航系统冗余设计与可靠性分析[J].自动化仪表,2005,26(9):4-6.

[5] 黄文君,金健祥.控制系统的冗余策略和实现准则[J].仪器仪表学报,2004,25(4):545-548.

[6] 王建虹.一种高可靠性双机冗余系统的设计[J].国外电子测量技术,2008.

[7] 蔡敬海,张振权.电子系统冗余设计及可靠性分析[J].光电技术应用,2016,31(1):64-68.

[8] 王珍熙.可靠性冗余及容错技术[M].北京:航空工业出版社,1991.

[9] 马银才,张兴媛.航空电子设备[M].北京:清华大学出版社,2012:1-28.

[10] 宋保维.系统可靠性设计与分析[M].西安:西北工业大学出版社,2000:12-56.