

机载机电管理计算机双余度设计

於二军, 吴 斌, 李 林, 向桂林

(中国航空计算技术研究所, 陕西 西安 710119)

摘 要: 机载机电管理计算机的任务可靠性对飞机飞行安全至关重要, 而提高任务可靠性的一个有效途径就是进行余度设计. 本文从研究两种常用的双余度容错模型出发, 将桥联模型应用于机电管理计算机的双余度设计. 通过对工作模型的故障容错机制的分析, 证明该双余度设计可有效提高机电管理计算机的任务可靠性, 具备一定的工程实用价值.

关键词: 机电管理计算机; 桥联模型; 任务可靠性

中图分类号: TP302.8

文献标识码: A

文章编号: 1000-7180(2012)12-0088-03

Design of Dual Redundancy Utility Management Computer

YU Er-jun, WU Bin, LI Lin, XIANG Gui-lin

(Aeronautics Computing Technique Research Institute, Xi'an 710119, China)

Abstract: The mission reliability of utility management computer is critical and essential to aircraft flight safety, an effective way to improving the mission reliability is dual redundancy design. Departure from the study of two commonly used reliability model, we use the bridging model for dual-redundant design of utility management computer. Fault-tolerant mechanism analysis of bridging model proves that the dual-redundant design can effectively improve the mission reliability of utility management computer, and has a certain practical value.

Key words: utility management computer; bridging model; mission reliability

1 引言

航空机电系统是那些保障飞机飞行及各系统功能实现的全机机、电、液压系统及功能设备, 它与先进航空电子系统、飞控系统和推进系统一起并列为飞机关键子系统. 航空机电系统包括有燃油系统、液压系统、电源及配电系统、刹车系统、环境控制系统、生命保障系统、弹射救生系统、辅助动力或第二动力系统及公共设备(如起落架、防火、制氧、舱盖、照明等子系统和设备). 航空机电系统的主要任务和目标是完成对上述机电系统及公共设备的综合控制、管理和故障监视的功能. 这些系统的性能直接影响着飞机的安全性、机动性、战斗力等多项战术技术指标. 机电管理计算机的可靠性直接关系到飞机飞行的安全性. 机载机电管理计算机设计的首要要求就是“一次故障工作、二次故障安全”. 要实现上述设计

要求, 就必须增加机电管理计算机的可靠性, 而增加可靠性的一个有效途径就是进行余度设计. 本文从研究两种常用的双余度容错模型出发, 将桥联模型应用于机电管理计算机的双余度设计. 通过对工作模型的故障容错机制的分析, 证明该双余度设计可有效提高机电管理计算机的任务可靠性.

2 双余度容错模型

对于双余度系统而言, 常用的两种双余度容错模型为并一串模型和串一并模型^[1], 分别如图 1(a) 和图 1(b)所示. A 和 B 代表两个余度通道, n 代表每个余度通道的 n 个分系统或分组件. 并一串模型和串一并模型在实践中被广泛应用, 极大提高了原有单余度系统的任务可靠性, 任何子系统和组件的故障均不会影响到系统工作的安全. 然而并一串模型和串一并模型在实际使用过程中也存在很多不足

的地方. 并一串模型由于过多考虑了系统维护和在线监控的需要, 系统成本较高, 而且在“串”的环节可能存在单点故障, 影响系统安全. 串一并模型从整个系统角度满足双余度容错的需要, 但是余度切换颗粒度太大, 任何单点故障将引起整个通道的故障切换. 为了克服上述缺点, 我们在不增加双余度系统资源的基础上, 将桥联模型(图 1(c)所示)应用于机电管理计算机的双余度设计, 该模型不仅避免了并一串模型中单点故障的影响, 又可以显著降低双余度切换颗粒度.

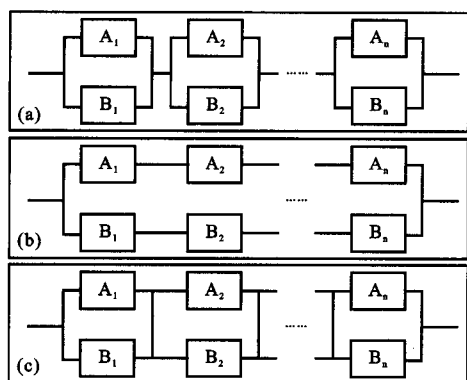


图 1 双余度容错模型

3 机电管理计算机双余度设计

机电管理计算机的功能需求主要是对飞机机电系统的各个子系统和设备进行综合控制、管理和故障监视. 其工作原理就是不断地从传感器中提取数据, 通过对控制率计算得出控制响应, 将这种响应送给执行器, 同时将机电系统的工作状态和品质通过数据线上信息显示系统. 基于上述需求, 机电管理计算机的内部功能可以分解为数据计算和信息处理单元(简称为 DPM)及接口采集和控制单元(简称为 IOM), 如图 2(a)所示. 数据计算机和信息处理单元主要用于对机电管理计算机控制率进行精确解算, 并将解算结果传送到接口采集与控制单元进行输出控制, 同时将机电管理计算机的工作状态和品质通过总线传送到信息显示系统进行显示. 接口采集和控制单元主要用于采集外部传感器的工作状态和性能, 并将采集到的外部数据通过背板总线传送到数据计算机和信息处理单元进行数据计算和控制率解算, 同时接收数据计算机和信息处理单元传送的控制数据进行输出控制. 另外, 接口采集和控制单元同时作为系统工作的监控器和模糊控制器, 当接口采集和控制单元采集到系统响应出现发散状态或没有按时获得数据计算机和信息处理单元的有效数据,

接口采集和控制单元启用逻辑控制或模糊规则控制, 确保系统工作安全.

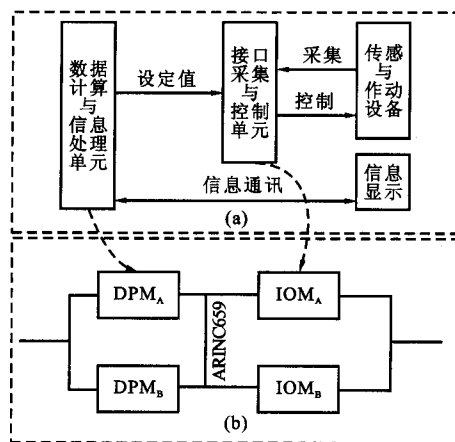


图 2 机电管理计算机双余度构型

结合机电管理计算机的功能需求和上文提出的混合结构的双余度容错模型, 可以得出机电管理计算机双余度构型原理如图 2(b)所示, 图中虚线箭头即表示功能的对应与分配情况. 由图 2(b)可以看出实现混合结构的双余度容错模型在机电管理计算机双余度设计中应用的关键“桥梁”就是 ARINC659 串行背板总线.

ARINC659 总线是一个线型多点串行通信总线^[2-3], 使用 4 条串行总线同时半双工传输和交叉校验的通信方式, 在时间上和空间上具有高容错性和坚固性划分的高完整性底板总线. ARINC659 串行总线总线接口单元 BIU 采用双重备份, 形成一对接口, 互连总线采用四重备份 (AX, AY, BX 和 BY). ARINC659 总线的大多数功能, 如时钟同步、信息调度和传输等都是接口上执行. 每对接口作为它伙伴的监控器, 控制它对互连介质的访问. 接口对中的每一个接口驱动一对不同的互连总线, 且能读取 4 个数据. 每个互连总线由两个数据线和—个时钟线组成, 当多个 BIU 同时驱动同一总线发生冲突时, 通过或门来解决. ARINC659 总线采用表驱动比例访问协议 (TDPA), 保证了数据时间和空间上的确定性. ARINC659 总线特有的主/备工作模式使双余度切换的颗粒度大大降低.

4 机电管理计算机工作模型与容错分析

双余度机电管理计算机的工作模型如图 3 所示. 双余度机电管理计算机采用独立双通道同构型结构, 通过比较监控原则, 实现内部故障监测的目标, 并通过对有效通道的选择和切换, 确保机电系统

可靠性的要求. 为抑制故障的蔓延和组合效应, 机电管理计算机采用通道间独立冗余和物理隔离模式. 正常情况下, 输入采集双通道同时工作, 输出控制 A 通道优先工作, B 通道热备份, 随时响应切换需求. 为了实现双余度容错, 我们设计了三级比较监控界面: 输入监控界面、处理器监控界面和输出监控界面.

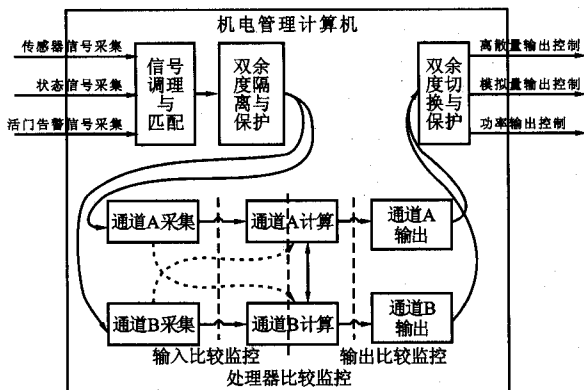


图3 机电管理计算机双余度工作模型

输入监控界面: 输入监控界面是用于对双通道输入信号容错管理. 当双通道完成输入信号采集和交叉传输后, 通过比较监控, 实现输入信号故障的监控、隔离和抑制, 并形成单余度输入信号提交给处理机.

处理机监控界面: 处理机监控界面是用于对双通道处理机输出信号的容错管理. 当双通道完成控制率计算结果(输出指令)和交叉传输后, 通过比较监控, 实现输出信号故障的监控、隔离和抑制, 并形成单余度输出信号提交给输出驱动电路.

输出监控界面: 输出监控界面是用于对双通道输出信号的容错管理. 当双通道驱动输出结果后, 通过在线信号的交叉传输, 进行比较监控, 实现输出信号故障的监控、隔离和抑制.

对于该双余度机电管理计算机的容错分析, 本

文主要从接口级故障、模块级故障和总线级故障来分析. 对于输入接口故障, 通过在线监控电路回绕测试进行故障定位, 将正确的输入采集结果传送到下级处理; 对于输出接口故障, 也是通过在线监控电路定位故障, 并通过通道故障逻辑电路进行接口电路电气切换, 保证机电管理计算机的正常工作; 对于模块级故障, 均启用 ARINC659 总线的主/备工作模式切换, 相关模块涉及比较监控界面降级为单余度工作, 不影响机电管理计算机的安全工作; 对于总线故障(仅针对 AX 和 BY、AY 和 BX 或三条及以上的背板总线故障, 其余故障 ARINC659 总线的容错机制可自我保障), 机电管理计算机采取第 3 节所描述的接口采集和控制模块(IOM)逻辑控制或模糊规则控制模式, 保证机电系统安全和飞机平台的飞行安全.

5 结束语

文中通过对双余度机载机电管理计算机的容错能力分析, 得出目前这种双余度模型. 可以有效解决可能存在的故障, 可以满足提高任务可靠性的目标, 该设计方法具备工程实用价值.

参考文献:

- [1] 熊峻江, 王甲峰, 袁立, 等. 余度设计中的系统可靠性最优分配模型[J]. 航空学报, 2004, 25(1): 26-31.
- [2] 任秀丽, 张翠华. 实时嵌入式系统总线的容错技术[J]. 仪器仪表学报, 2005, 26(8): 578-581.
- [3] Kenneth Hoyne, Kevin Driscoll. SAFEbus[J]. IEEE Aerospace and Electronic Systems Magazine, 1993, 8(3): 6-13.

作者简介:

於二军 男, (1981—), 硕士研究生. 研究方向为嵌入式计算机系统设