avionicstech@avic.com

DOI:10.12175/j.issn.1006-141X.2022.04.04

# 双总线通信架构的航电系统双机备份技术研究

谭 菲[1]，王金升[2]，朱剑锋[1]

（1. 中国航空无线电电子研究所，上海 200241;
2. 航空工业第一飞机设计研究院，西安 710089）

[摘 要] 针对采用两种通信总线作为主要通信的复杂航电系统，通过研究其体系结构，利用故障树对系统可能故障进行分析，优化了单总线通信系统中主备机表决算法，设计了一种双总线通信系统中主备机的同步和双机切换机制，提升了双机切换的性能，实现了系统故障时的平滑切换运行，提高了双机切换的实时性和双机备份系统的可靠性。

[关键词] 双总线通信；双机切换；故障树

[中图分类号]TP302.8 [文献标识码]A [文章编号]1006-141X(2022)04-0024-05

# Research on Dual-machine Backup Technology in Dual-bus Communication System

TAN Fei[1], WANG Jin-sheng[2], ZHU Jian-feng[1]

(1. China National Aeronautic Radio Electronics Research Institute, Shanghai 200241, China;
2. AVIC The First Aircraft Institute, Xi'an 710089, China)

**Abstract**: The architecture of complex system is studied, in which devices communicating via two types of bus, and fault analysis trees are built for the typical faults. Based on the optimized voting algorithm of the single bus system for switching the master and backup, a mechanism is designed to switch master-backup in the dual bus system and to synchronize the information. The mechanism can give a big improvement on the performance and reliability of the master-backup switching.

**Key words**: communicating via two types of bus; master-backup switching; fault analysis trees

随着计算机软硬件技术的持续发展，航空电子系统的研制在近十年时间内大踏步进入了数字化、总线网络互联、信息共享、综合显示控制、任务处理等系统集成化时代。在提高人机功效方面，飞机驾驶舱综合显示控制系统进行了综合化、信息化显示，在减轻空地勤人员工资负担的同时，也使飞机效能得到了更好的发挥。

先进的技术造就了先进的产品和系统，但是高度的集成化和多功能必然带来系统软硬件的复杂化，系统的工作可靠性和任务可靠性自然成为工程领域不能回避的现实问题。如何提高系统可靠性是业界针对每一个任务课题时必须首先清理的问题，合理

收稿日期：2021-09-11

引用格式：谭菲，王金升 , 朱剑锋 . 双总线通信架构的航电系统双机备份技术研究 [J]. 航空电子技术 ,2022,53(4)： 24-28.

而充裕的余度备份方案给了我们很好的解决思路。对关键领域采用双余度备份技术设计已经得到了一致的认可，但是双余度的处理节点如何协同工作，如何合理切换还有许多值得探讨的地方。

采用双节点对关键领域的处理设备进行备份，可以很大程度上提高系统的可靠性。在工程设计中，系统大多采用双机冗余系统来保障系统的可靠性。航空电子系统针对自身的特殊性，除采用双机冗余系统的设计外，亦采取将核心处理计算机设计为双机热备份的方式来提高系统的可靠性。传统双机备份的系统多为单一通信总线作为主要通信总线，系统在进行主备机表决、主备机同步、故障检测、故障分离以及系统重构时，仅需要考虑单一总线上的问题即可。但是单总线通信系统容易产生数据差异，一旦通信链路出现问题，故障检测机制就会失效，甚至会误判对侧机故障，造成两机都为主机，出现双机“抢权”的现象。

本文针对采用两种通信总线作为主要通信总线的复杂航电系统，通过故障树对系统故障进行分析，设计了该系统的双机备份模块，同时改进了单总线中主备机表决算法，实现主、备设备切换最高原则是不抢主控权，主控设备“主动”让出控制权。

为了保证系统的实时性要求，系统的双机备份采用热备份的设计，当系统发现故障进行主备机切换时，能够快速、平滑地切换到备机工作。系统同步过程在保证系统正确性运行的前提下，采用硬件或者软件的方法，使双机中应用程序的工作过程统一协调。

## 1　体系架构和故障模式分析

### 1.1 双总线通信系统体系结构

复杂航电系统抽象后的结构如图 1 所示，数据处理计算机 A 和数据处理计算机 B 互为备份，同时接收处理总线 A 和总线 B 上传来的数据。数据处理计算机通过 A 总线与综合显控系统相连，发送和接收综合显控系统内部用于显示和控制等数据；通过 B 总线连接组合导航、飞控等系统，获取飞控、导航等数据，经数据处理计算机解算处理，再经 A 总线发送给综合显控系统。两台数据处理计算机之间可以分别通过总线 A 和总线 B 共享数据。

为了保证该复杂航电系统的正确运行，其结构决定数据处理计算机中任意一个总线接口发生故障，数据处理计算机之间将发生主备切换。当作为主控设备的数据处理计算机发生其他影响系统完成正常工作的故障时，数据处理计算机之间也将发生主备切换。

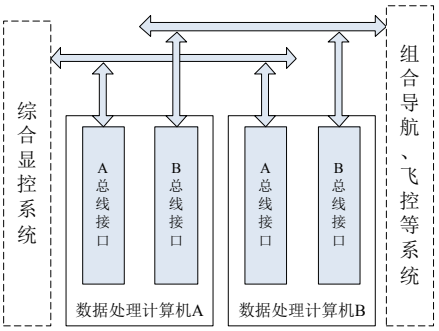


图 1 双总线通信系统体系结构

### 1.2 系统故障树分析法

使用故障树对系统进行故障分析是为了清晰刻画系统发生故障的条件（此处特指导致系统发生双机切换的故障事件）。通过罗列导致系统发生故障的事件，将这些事件作为叶子节点，再使用与门、或门作为中间节点，衍生出的根节点就是系统故障。图 2 为故障树模型。

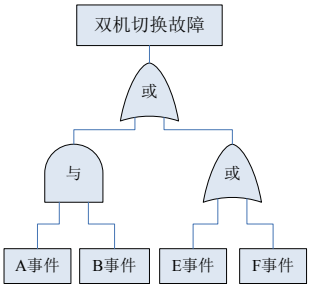


图 2 故障树模型

假设 A 事件和 B 事件同时满足，此时数据处理计算机将确定为已发生影响系统完成关键任务的故障，系统将进行双机切换工作（原主控设备降级，原备份设备升为主控设备代替原主控设备进行工作）；E 事件或者 F 事件两种事件，其一满足发生条件，则系统发生导致系统进行双机切换的故障。

表 1 为复杂系统引起双机切换的故障事件集。通过分析复杂系统的系统结构，可以暂时将故障罗列为 4 种可能故障类型，每种故障类型又存在着不同的表现形式，可以通过故障树的形式再详细列出。因此表 1 中给出的故障集都是引起双机切换的故障根节点，并不是底层的叶子节点。

表 1 引起双机切换的故障事件集

| 故障类型 | 故障内容 | 节点类型 |
|---|---|---|
| 通信故障 | A 总线故障 | 根节点 |
| | B 总线故障 | 根节点 |
| 应用故障 | 数据处理模块可被检测的应用程序调度故障集 | 根节点（需要分解） |
| 硬件故障 | 数据处理模块可被检测的硬件故障集 | 根节点（需要分解） |
| 通用故障 | 不可被检测故障 | 根节点 |

图 3 给出了通信故障中的 A 或者 B 总线故障的故障树模型，即故障可以表现为接收不到总线上的应答信号并且无法收到自回环数据，或者表现为总线接口硬件自检故障等叶子节点。实际系统的实现过程中需要对这些故障集的表现形式进行一一罗列，这些表现形式就是故障的叶子节点，他们通过与或逻辑确定故障类型，形成触发双机切换的前提条件。

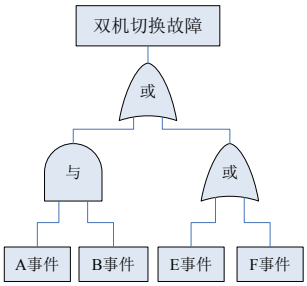


图 3 总线通信故障故障树

在获知系统的各种潜在故障信息后，可以更加便捷的对系统余度进行设计，如主控设备降级让出主控权，备份设备升级为主控并接管对系统的控制，使系统在故障时可平滑切换。

## 2 双机备份技术研究与设计

在现有体系结构下，双机备份技术的研究和实现需要完全依靠软件的功能，本文将从主备设备的表决规则、同步和切换三个步骤对双机备份技术进行研究。

### 2.1 主备设备表决规则

由于系统结构设计为数据处理模块全状态备份，在系统上电时，二者完全平等，因此必须设计规则控制两块数据处理模块中的只有一个能够成为主控设备（避免出现两个主控设备进行抢权的情形）。考虑传统单总线系统中，某总线需要通过总线控制器才能和总线上的设备进行通信，存在因时间差问题出现两个总线控制器，进而产生两个主控设备的问题。结合双总线的设计结构，利用总线之一（如航空电子全双工交换式以太网（AFDX：Avionics Full Duplex Switched Ethernet），不需要通过总线控制器进行设备间通信的特性，设计规则如下：

（1）A 和 B 同时上电时，预定数据处理模块 A 具备优先成为主控机的条件；

（2）模块 A 和 B 皆作为备份机启动；

（3）总线上不存在主控机时，备份机升级为主控机；

（4）A 和 B 之间通过总线通信获知对方模块的工作状态（主控机或者备份机状态）；

（5）A 和 B 之间通过总线通信获知模块启动优先顺序，再设定时间阈值 T，保证在时间上优先正常启动的模块成为主控设备。

规则（1）（2）（3）是双机备份中实现主备表决的基本规则，单总线系统基本采用此规则（单总线系统中为了保证主备表决的正确性，会增加硬线离散量的控制）；（4）（5）给出了一种方案性的规则，针对（1）（2）（3）实现过程中的不足和问题进行补强设计。与单总线系统相比，（4）和（5）通过双总线进行启动优先顺序的控制，同时基于不“抢主控权”的原则，可以有效解决单总线系统中偶发出现双主控机的情形。

### 2.2 主备设备同步

为了保证系统切换运行的实时性要求，系统采用双机热备份技术，其同步过程为在保证系统正确运行的前提下，通过软件执行流程和总线上数据收发同步的方法，使双机中应用程序的工作过程统一协调 [5]。

主备机同步包括任务同步和数据同步。主备机运行完全一样的应用程序，根据实际情况主控机执行主控状态下的流程，备份机执行备份状态下的流程；主控机和备份机同时接收总线上的数据，执行相同的逻辑流程，主控向总线上输出计算结果，备份机不进行数据计算和计算结果的输出；主控机和备份机任务同步向对方发送响应、应答命令，同步掌握对方状态；主控机周期向备份机发送响应和应答命令后，向备份机发送系统状态、核心数据等动态数据，备份机动态存储系统最新状态和数据信息。同时，主备机针对关键性数据（如系统中的各终端

设备的故障信息等）存储在各自的非易失存储器内，实现对关键数据的安全保护。

### 2.3 主备设备切换

数据处理模块使用双总线进行数据通信和控制，数据处理模块主备切换功能的设计原则是任何一种总线通信故障且故障所在模块为主控设备时，主控设备需要主动让出主控权；对于一些不可预知的故障造成程序无法正常运行或者硬件问题导致系统挂起等问题，依靠硬件看门狗设计将主控设备复位，实现主控数据处理模块让出主控权，通过主控设备的“主动”让出主控权，备份设备感知总线上无主控数据，进而接过控制权的方式实现在主控模块故障情况下仍能保证系统功能不降级。

表 1 中列出了引起双机切换的故障事件，对这些事件进行分析归类，可以分为两大类：可以通过应用软件“主动”检测到的故障和导致应用软件挂起的故障或者直接导致硬件宕机的故障。本文将这两类故障称之为可被程序检测的故障和不可被程序检测故障（不可被程序检测的故障是指导致硬件宕机的崩溃性软硬件故障）。

（1）可被程序检测故障

针对可被程序检测故障，程序主要逻辑仍然可以掌控 CPU 资源，能够进行部分任务调度和对部分外部接口的控制，主控可以根据设定的逻辑，“主动让出”主控权，实现双机的自动切换。图 4 描述系统主控机检测到故障后的流程框图，图中在出现双总线故障无法实现对外通信时，仍尝试对系统进行主备切换；而经过比较后，备份机不具备更加优良的资源状态时，不进行主备切换，提示故障，否则进行主备切换工作；至少一条通信总线正常工作的情形时，主控机首先停止主控机的工作，然后通过总线信息通知备份机进行主备切换。

在主控机出现对外通信故障（AB 总线全部通信故障）而进行强制出让控制权后，总线上将出现控制信息的真空期，此真空期内备份机的切换流程判断机制启动，待达到全部条件后，备份机升级为主控机，接管系统的控制权，对外进行数据的收发和控制。图 5 给出了备份机自动切换的示意图，图示中满足升级条件可以设计为：（a）n 个周期内无法收到主控机应答信息，通常 n=Tw/T+1，Tw 为看

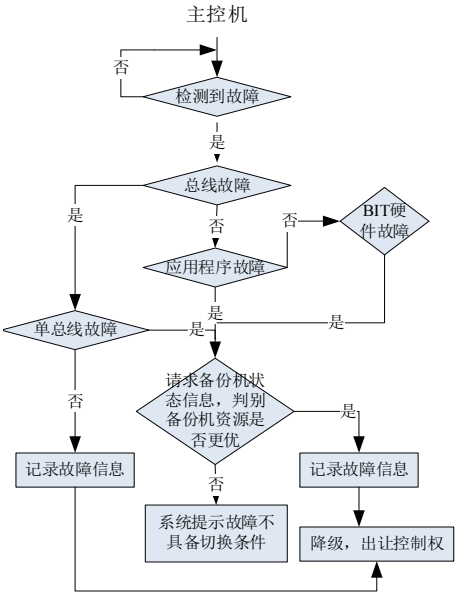


图 4 主控机“让权”的故障处理流程

门狗的阈值时间，T 为主控机和备份机之间进行请求、应答的周期时间，主控机在 T 周期内执行“喂狗”操作，此时可以设定总线上无主控设备；（b）BIT 结果全部通过。

（2）不可被程序检测故障

针对不可被程序检测故障的问题处理比较简单，通过在主控机内部的硬件看门狗电路设计来实现主控机的自动降权。主控机正常启动后，软件使能看门狗电路功能，设置周期任务对看门狗电路进行周期“喂狗”（周期发送数字信号）操作；当发生不可被程序检测故障时，主控机内所有应用崩溃，看门狗电路在指定时间内（阈值时间 Tw）未收到数字信号（“喂狗”信号），复位硬件（含控制器模块）实现降级功能。备份机的切换流程如图 5 所示。

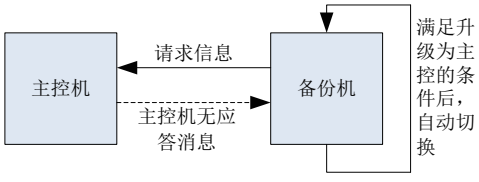


图 5 备份机自动切换示意图

## 3　双机切换性能分析

由于实时操作系统时间性要求，本文研究双机备份采用热备份的设计，当系统发现故障进行主备机切换时（或者手动切换时），能够快速、平滑地切换到备机工作。因此对双机切换的时间进行分析，

判断其切换过程中的时间消耗是否满足系统研制方案的要求。

表 2 双机切换的时间分析

| 故障类型 | 切换机制 | 时间消耗 |
|---|---|---|
| A\B 总线故障 | 通知备份机切换 | $0 < t \le 2T$ |
| 双总线故障 | 备份机主动切换 | $Tw < t \le Tw+2T$ |
| 应用程序可恢复性故障 | 通知备份机切换 | $0 < t \le 2T$ |
| BIT 硬件故障 | 通知备份机切换 | $0 < t \le 2T$ |
| 不可被程序检测故障 | 备份机主动切换 | $Tw < t \le Tw+2T$ |

由表 2 可知，双机切换时间最坏情况为 $Tw+2T$，即 $(n+1)T$。因为 Tw 是硬件特性比较大的值，将会影响系统的实时性要求，因此根据系统双机切换指标要求进行检查时间周期的优化方案设计。比如，设 n=5，当备份机 2T 时间内没有主控机响应消息，备份机首先尝试性向假想存在的主控机发送请求降级的信息，如果 5T 时间内，仍然无响应消息，假设总线上无主控设备，备份机进行升级主控机的工作（主控机此时无论是正常工作与否，都将根据流程失去主控权）。优化设计后，双机切换时间的最坏情况将为 $5T < t \le 6T$。n 值的优化设计可以根据 Tw 的实际情况和指标要求进行采用。

## 4 结论

本文的双机备份技术已经在采用 AFDX 网络和 GJB 289A 总线作为主要通信总线的系统中实现。通过不同故障的注入以及双机开启时间上的控制，主要优势体现在，该系统在发生双机切换的过程中，未出现双主控机“抢权”的情况。备份机可以在规定的时间内及时同步系统数据，保证双机切换顺利完成，正确的系统数据从而保障了飞行安全。

实践表明本文研究的双机备份技术，以通用的双总线通信系统体系结构为背景，适用于当前常用的如采用 1394 B、光纤（FC：Fibre Channel）、GJB 289A、AFDX 等总线的通信系统，其技术能够实现故障自检与隔离、主从切换与系统重构。而性能方面最快的双机切换时间小于 500 ms，能够满足双机切换的稳定性和实时性要求，系统的可靠性和安全性进一步得到提高。

## 参 考 文 献

[1] 苟冬荣 , 刘海清 . 双机容错计算机系统的设计与实现 [J]. 计算机工程 , 2008, 34(15): 255-258.

[2] 刘东 , 张春元 , 李瑞 . 基于任务同步的双机容错系统 [J]. 计算机工程 , 2007, 33(15): 224-226.

[3] 李宏亮 , 金士尧 , 胡华平 , 王志英 . 短事务、强实时双机容错系统的研究 [J], 计算机学报 , 2003, 26(2): 244-249.

[4] 吴娟 , 马永强 , 刘影 . 一种基于主备机快速切换的双机容错系统 [J]. 计算机应用 , 2005, 25(8): 1948-1951.

[5] 郑军 , 付强 , 李权 . 一种纯软件的双机热备份算法 [J]. 计算机应用 , 2002, 22(15): 99-100.