文章编号：1672-2892(2010)03-0357-03

气球控制安全中的双机冗余设计

黄 翌[1]，陈丽娟[2]

(1.中国电子科技集团 第38研究所，安徽 合肥 230031；2.合肥工业大学 仪器科学与光电工程学院，安徽 合肥 230009)

摘 要：分析现代战争的特点和气球载雷达的功能，指出气球载雷达具有长时间浮空的特性。为了满足气球控制系统稳定可靠，能够长时间滞空工作的要求，提出了一种采用双计算机并行工作，热备份冗余切换的双机容错系统的设计方案。通过实际项目验证，气球可以数月系留工作，满足气球载雷达球控系统滞空工作的高可靠性要求。

关键词：气球载雷达；球控系统；双机容错；仲裁算法

中图分类号：TN957.52^{+}9 **文献标识码**：A

Dual-host redundancy design on safe control of balloon

HUANG Yi[1]，CHEN Li-juan[2]

(1.The 38th Research Institute of CETC，Hefei Anhui 230031，China；
2.School of Instrument Science and Opto-electronics Engineering，Hefei University of Technology，Hefei Anhui 230009，China)

Abstract：The floating time of aerostat-load-radar is very long in modern warfare. Therefore the high stable and reliable balloon control system is needed. A design scheme of dual-host redundancy system was put forward，which adopted two host computers working together and the two computers could switch in real time. The scheme was verified through actual project. The balloon can work for several months，which meet the reliability requirements of the balloon control system in aerostat-load-radar.

Key words：aerostat-load-radar；balloon control system；dual-host redundancy；arbitrating algorithm

现代战争的特点是全方位、多层次和大纵深立体化战争，战争的方式主要是对抗低空和超低空突防、反辐射导弹、隐身飞机和电子干扰等“四大威胁”。而低空和超低空飞行是现代飞行器(低空隐身飞机和掠海巡航导弹)实施突防的重要手段。近年来，随着电子和导航等技术的发展，低空飞行器能够用亚音速或超音速贴近地面高度近百米到数十米和海面高度十几米到几米机动飞行。它们可以穿过中、远程警戒雷达的防空网，从雷达探测盲区潜入，对敌方的防空系统实施偷袭和摧毁。气球载雷达的首要任务就是搜索远距离低空飞行器，探测海上舰船、地面目标、干扰机位置以及从水下潜艇发射的巡航导弹、战略导弹等，并指令跟踪和拦截，是有效地实施高空和远距离低空防御的战略武器。系留气球载警戒雷达系统利用地面或舰船上的系留设施，将载有警戒雷达的气球悬浮在空间的一定高度，以扩大雷达对地面或海面低空飞行器的探测范围。目前，系留气球载预警雷达系统已成为各国防空预警系统的重要组成部分。但是，由于气球在系留状态和升空工作中需要一直保持对气压、阀门等调节装置的控制，并且滞空时间长，即使在系留状态时也要保持控制系统的正常工作。如果球控系统死机，调节装置的误动作将会造成设备不可估量的损失，故球控系统要求通过容错或恢复处理等机制保障整个系统的可靠工作[1-2]。本文提出了一种采用双计算机并行工作，热备份冗余切换的双机容错系统设计方案，详细阐述了如何在FPGA中实现双机仲裁和软硬件协同设计的方法。

1 系统组成

球控系统由1块附有2个PC104计算机的插件组成，2个计算机同时运行，互为热备份。板上的FPGA对2个计算机进行总线仲裁和数据交换，在其中1个计算机跑飞后能够立即保存现场数据，实时热切换到另1个计算机继续工作，并复位飞的计算机。切换后的计算机将恢复现场数据，继续程序的运行。系统结构框图见图1，其

收稿日期：2009-10-09；修回日期：2010-03-08

中寄存器组 A 实时保存计算机 1 的工作数据和现场环境，计算机 2 可以读出寄存器组 A 中的数据；寄存器组 B 实时保存计算机 2 的工作数据和现场环境，计算机 1 可以读出寄存器组 B 中的数据。仲裁器通过每个计算机送出的看门狗信号 WD 来判断其工作状态，如果正在工作的计算机死机，就将对外设的控制权平滑地切换给另 1 台计算机，并将不正常的计算机复位。

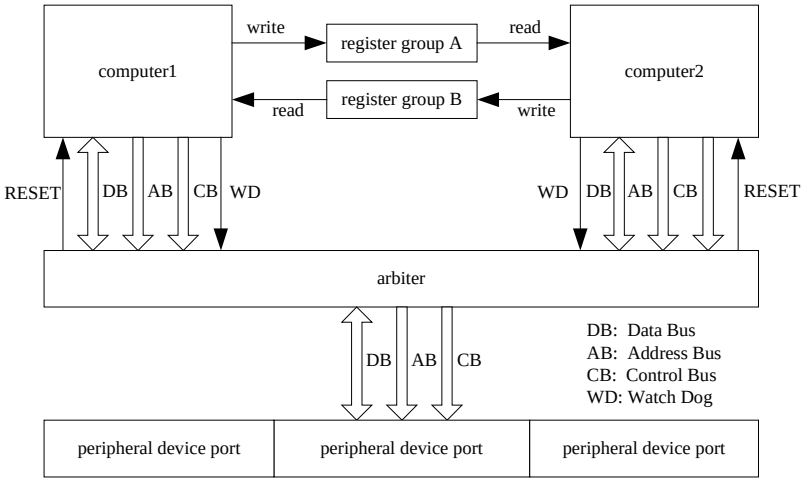


Fig.1 System block diagram
图 1 系统框图

2 仲裁器结构

仲裁器的结构见图 2，它需要完成以下功能：能够判断计算机的运行情况，并复位“跑飞”的计算机；根据计算机的运行情况，将总线赋给运行正常的计算机，转交控制权。

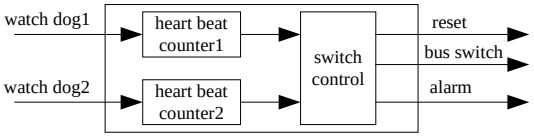


Fig.2 Arbiter architecture
图 2 仲裁器结构

2.1 仲裁算法

仲裁算法通常有 2 种：a) 固定优先级(fixed priority)算法；b) 循环优先级(rotator priority)算法。它们各有优缺点，但不管是哪一种仲裁算法，都必须满足每一时刻只能有 1 个计算机占用总线的要求。所谓固定优先级就是每个计算机的优先级是事先确定好的，在仲裁器进行仲裁的过程中固定不变；而循环优先级算法则不同，各计算机的优先级根据一定规律发生变化，某个计算机占用总线后，其优先级变为最高。采用固定优先级算法，需要将 2 台计算机标定固定的优先级，其优点是能够确定计算机的工作状态，判断计算机的损坏情况，其缺点是增加了系统的切换次数，造成计算机使用寿命不同。采用循环优先级算法的优点是可以减少计算机切换次数，计算机使用均匀，但是无法判断另 1 台计算机的工作状态，增加了控制系统失效的风险[3]。基于此原因，本系统采用固定优先级仲裁算法。

2.2 实现方案

实时双机冗余容错系统采用热备份技术。系统上电后，2 台计算机执行完全相同的程序，首先执行自检程序，将看门狗信号发给仲裁器，并且在运行时通过信号量实现 2 台计算机的软件同步。对于采用双机容错的系统，仲裁器不仅要负责控制 2 台计算机并行工作时关键数据共享和同步通信，而且也要负责计算机与外部端口之间的通信。当整个系统启动后，仲裁器复位内部所有的状态，随后 2 个心跳计数器开始计时，默认时长由计算机启动时间决定，同时开始监控整个系统状态[4]。2 台计算机开始工作后，在默认时长内不断发看门狗信号给仲裁器，清零心跳计数器。若在默认时长内计算机 1 发出看门狗信号给仲裁器，计算机 1 正常工作，仲裁器将总线授权给计算机 1，计算机控制执行件工作，计算机 2 只能获得外部状态和环境信息，并与计算机 1 在一定时间范围内同步运行。如果计算机 1 没有发出看门狗信号给仲裁器，标志计算机 1 跑飞，仲裁器将总线切换给计算机 2，并复位计算机 1。计算机 2 接管总线后，初始化外部端口，读取计算机 1 的工作数据和现场环境，获得对执行件的控制权，继续工作运行。

3 软件设计

容错系统的实现，除了要有可靠的硬件电路支持外，还要对监控软件进行周密设计。相对单机系统而言，双机系统的软件要复杂得多，除了完成其控制系统应有的功能外，还需要实现 2 方面功能：a) 满足双机同步的要求；b) 保证双机切换的可靠实现。

3.1 双机同步

在双机容错系统中,同步是整个系统的核心。容错系统的同步策略大致分为硬件同步和软件同步这 2 种方式。硬件同步方式需要专门的硬件装置,保证系统的各个模块按照完全相同的频率来运行,而且系统中各个模块在运行过程中不能有时钟丢失等现象的存在,因而实现起来比较困难。大多数双机容错系统都是采用软件同步的方式,根据具体的应用任务,取定一个合适的同步周期和最大同步阈值,严格在同步周期内实现各模块之间的任务执行、容错表决与比较处理等。为保证气球滞空时球控系统的不间断运行,球控系统软件采取任务级同步方式。在设定的同步周期和同步阈值内,备份计算机必须保证在时间、数据和运行状态方面与主机保持严格一致。同步机制参考操作系统中的进程同步,将其简单地建模为生产者–消费者模型[5],采用 P,V 操作的信号量机制解决同步问题。

P,V 原语描述:荷兰的著名计算机科学家 Dijkstra 把互斥的关键含义抽象成信号量(Semaphore)概念,并引入在信号量上的 P,V 操作作为同步原语。信号量是被保护的量,只有 P,V 操作和信号量初始化操作才能访问和改变它的值。P 操作和 V 操作分别定义如下:

```
P(semaphore)                          V(semaphore)
  {s.value=s.value-1;                   {s.value=s.value+1;
    if(s.value<0)                         if(s.value<=0)
      asleep(s->queue);}                    wakeup(s->queue);}
```

P,V 原语控制算法实现可以有效地保证生产者和消费者彼此交替、同步工作,从而避免了生产者速度过快导致数据丢失及消费者速度过快导致的数据重复读取。通过在球控系统软件的某些关键控制区,分别设置 P 操作和 V 操作,可以有效地保证 2 台计算机在运行过程中保持同步运行,在切换到备份计算机后不会出现重复操作和误操作。

3.2 双机切换

在程序运行过程中,2 台计算机都可以取到控制中心的控制信息和气球的状态,但是在控制时只有获得控制权的计算机能够对各个执行件进行控制,并将控制状态放在备份计算机可以访问的寄存器组中,由备份计算机获得控制状态。在切换控制权后,备份计算机获得控制权,根据获得的控制状态恢复现场,继续平滑运行。

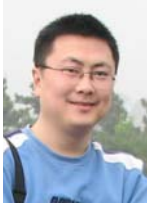
4　结论

气球载雷达的载体是系留气球,需要悬浮工作于空中,因此对气球阀门和气囊控制的可靠性和稳定性显得尤为重要。在实际的工程应用中,本文提供的双计算机并行工作和热备份冗余切换的设计技术,很好地满足了球控系统需要长时间滞空工作的要求。

参考文献:

[1] 王平. 小卫星星载容错计算机控制系统软硬件设计[J]. 宇航学报, 2006,27(3):412–415.
[2] 刘小熊. 电传飞行控制系统的余度设计技术[J]. 飞行设计, 2006(3):35–38.
[3] Suzuki Hideto. Space demonstration of a fault tolerant computer system using commercial MPU[J]. Space Technology, 2004, 24(1):35–41.
[4] 李平,俞承芳,李旦. 控制区域网络总线物理故障及冗余方案[J]. 信息与电子工程, 2009,7(1):61–65.
[5] 帖军. 进程同步中的生产者消费者模型分析[J]. 武汉科技学院学报, 2007,20(4):30–34.

作者简介:



黄　翌(1978–),男,合肥市人,工学硕士,主要从事雷达监控系统和任务电子系统的硬件和软件的设计与开发.email:huang2k@163.com.

陈丽娟(1978–),女,安徽省广德市人,工学硕士,主要从事光电系统的数据处理和硬件软件的设计与开发.