第34卷 第17期 计 算 机 工 程 2008年9月
Vol.34 No.17 Computer Engineering September 2008
·工程应用技术与实现· 文章编号：1000—3428(2008)17—0240—02 文献标识码：A 中图分类号：TP303

双模容错计算机的设计与实现

李 迅[1]，李洪峻[1]，刘庆敖[2]
(1. 国防科技大学自动控制系，长沙 410073；2. 空军第一航空学院，信阳 464000)

摘 要：高可靠性的计算机应用环境需要计算机具备容错功能，并要求采用高等级的处理器芯片。该文以高等级的Power PC处理器PC8245为基础，以FPGA为核心，设计双模容错的计算机。由于应用空间限制，该计算机采用了分布式冗余仲裁结构，仲裁逻辑同时运行在主计算机和备份计算机的FPGA中。分析了分布式冗余仲裁算法的有限状态机，论述了通信接口的冗余控制机制。

关键词：双模容错；PC8245处理器；分布式仲裁

Design and Implementation of Two Module Fault Tolerant Computer

LI Xun[1], LI Hong-jun[1], LIU Qing-ao[2]
(1. Department of Automatic Control, National University of Defense Techonology, Changsha 410073;
2. The First Aeronautic Institute of Air Force, Xinyang 464000)

【Abstract】 High reliability computer application needs the ability which the computer is fault tolerant, and requests high level CPU. This paper discusses a two module fault tolerant computer, which is based on PC8245 processor and FPGA. Because of the limited space, this computer uses distributed arbitration architecture, the arbitration logic runs in FPGA of the master computer and the backup computer. The finite state machine of the arbitration architecture and the mechanism of the communication interface redundancy control are discussed.

【Key words】 two module fault tolerant; PC8245; distributed arbitration

1 概述

在航空、航天、军事和工业控制领域，计算机的可靠性至关重要。可以通过器件选择和生产来控制提高计算机的可靠性，如航天领域选择宇航级的处理器，它具有抗辐射性能，温度范围高，但价格昂贵，性能有限，不能满足低成本和复杂应用的环境。也可以在设计时采用容错设计技术，如三模冗余技术[1]、双机冗余技术、降额设计技术等，这些可靠性设计技术对提高计算机的可靠性尤其重要。

低成本应用环境下，往往选择工业级COTS器件，如美国的TACSAT-1 战术卫星采用了MPC8260, MPC823 等Power PC系列工业级CPU[2]。在复杂应用环境下，要求丰富的通信接口和高的计算性能，这就需要高性能的CPU，而高性能CPU往往没有宇航级甚至军用等级器件，在这样的应用环境下，容错设计成为提高可靠性必不可少的技术。

目前，在星载环境下，Intel386EX[3]得到了大量的应用，但是Intel386EX性能相当有限，如最大工作频率为33 MHz，无浮点计算单元等，而本文设计的计算机需要实现丰富的通信接口，并且需要完成部分的浮点计算，安装空间、功耗都有限，根据这些需求本文选用了ATMEL公司的PC8245。PC8245 是Freescale公司的 Power PC 芯片MPC8245[4]的军温级芯片，在性能上和MPC8245 一致，完全兼容。PC8245功耗低，在330 MHz运行主频下，能够达到465 MIPS定点运算能力，芯片内部集成了单精度浮点计算单元FPU，以及8 KB的数据Cache和8 KB的指令Cache，较好地满足了计算机的计算能力要求。

2 计算机体系结构

PC8245集成了多种接口控制器，包括PCI接口控制器、两路UART接口控制器和I^2C接口控制器。根据计算机的任务要求，需要支持6路RS422接口和1路1553B端口，因此，需要扩充设计相应的端口。基于 PC8245 的计算机的体系结构如图1所示。

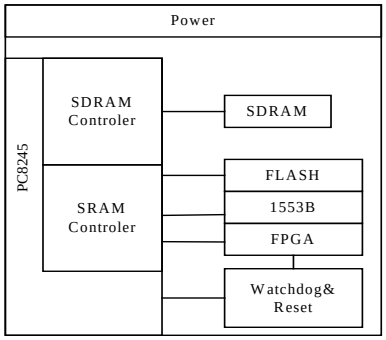

图1 计算机系统结构

系统的工作时钟采用33 MHz温度补偿时钟，CPU工作频率、SDRAM工作频率和PCI工作频率通过内部PLL倍频得到。从可靠性方面考虑，系统采用了降额设计的思想，CPU工作频率为266 MHz，SDRAM工作在99 MHz频率下，64 bit的数据带宽，128 MB的内存容量，充分满足系统的需要。复位部分采用MAX706T高等级器件，内置看门狗功能，看门狗控制信号由CPU通过FPGA生成。FPGA完成多种功能，包括仲裁判断逻辑、实现4路UART逻辑、看门狗控制逻辑以及地址译码等，FPGA和PC8245的接口为异步SRAM接口，其内部结构如图2所示。

作者简介：李 迅(1972－)，男，副教授、博士，主研方向：嵌入式计算，现场总线，控制网络；李洪峻，博士研究生；刘庆敖，讲师
收稿日期：2007-09-28 **E-mail：**wsan9200@yahoo.com.cn

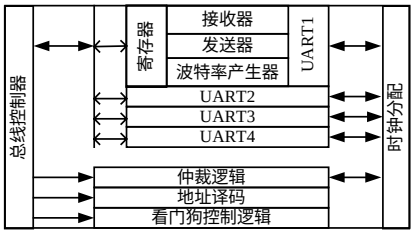

图 2　FPGA 逻辑结构

在FPGA中，通过总线控制器实现了UART的寄存器、仲裁逻辑的寄存器以及看门狗控制寄存器。FPGA采用Xilinx公司Virtex芯片XCV300[5]，30 万门逻辑容量。1553B总线采用DDC公司的DC-61580 高等级芯片实现，该芯片内置收发器，支持总线控制器(BC)、监控终端(MT)和远程终端(RT)的工作模式，工作模式通过软件设定。

计算机的 FLASH 为 16 bit 数据带宽，16 MB 容量，用于固化程序和配置参数，实现 FAT16 文件系统，可以在线更新用户程序。

3　分布式冗余仲裁结构

根据可靠性要求，计算机实现了双机容错设计。在设计性能上，设计要求实现双机动态热备冗余，即双机能够同时接收 RS422 接口和 1553B 总线的数据，同时进行计算，当双机切换时，只能影响在切换时刻发送的数据，不能影响数据接收。在空间上，实现小型化设计，不能设计独立的仲裁模块。因此，在容错设计实现上，该计算机没有采用常规的集中仲裁的方式，而是采用了分布式仲裁结构，将仲裁逻辑分布到了两个计算机模块上，冗余结构如图 3 所示。

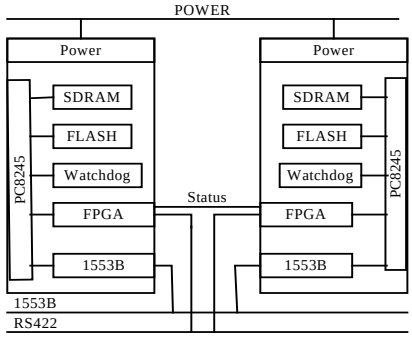

图 3　计算机冗余结构

可以看出，2 个计算机模块采用对称设计，在硬件和结构上一致，仲裁逻辑在 2 个计算机模块的 FPGA 上分别独立运行。系统上电时，通过缺省设置，选择一计算机作为主计算机运行，另一计算机作为备份机运行，一旦出现以下条件，则由主计算机切换到备份计算机运行：(1)主计算机 CPU 部分异常，包括 SDRAM 数据异常、FLASH 数据异常、CPU 工作异常、电源异常等；(2)总线接口异常，包括 RS422 接口异常和 1553B 接口异常；(3)手动切换。

第(1)个条件的判定是通过软件发送心跳信号给 FPGA 仲裁逻辑，仲裁逻辑根据心跳信号的好坏而决定是否切换，当主计算机 CPU 部分异常时，仲裁逻辑得到坏的心跳信号，否则，仲裁逻辑得到好的心跳信号。实现是通过软件定时器完成的，一旦软件定时器中断触发，则中断伺服程序向 FPGA 发送心跳信号，FPGA 通过硬件时钟，设置 3 个硬件定时器，定时器周期同软件定时器一样，每当硬件定时器触发，仲裁逻辑检测心跳信号，如果 3 个周期内连续监测到坏的心跳信号，则进行切换，并通过 IO 信号发送到备份计算机的 FPGA。

第(2)个条件的判定是通过应用程序完成的，应用程序通过周期性的握手来判定总线是否异常，一旦发现总线异常，如无法正常接收数据，应用程序向仲裁逻辑寄存器发送软切换指令，强制主计算机进行切换。

第(3)个条件是为了增加可靠性，用户可以通过地面遥控的控制命令完成双机的切换，这一切换的优先级最高。

从以上 3 个条件看到，双机冗余没有明确地对应用程序进行监控，而应用程序异常除了导致看门狗复位外，也应当产生切换的动作。在图 3 的冗余结构中，对应用程序的监控是通过隐含条件判断的，因为一旦应用程序发生故障，看门狗定时器溢出，造成系统复位，复位的计算机无法通过软件发送心跳信号到仲裁逻辑，仲裁逻辑的判据设定为，没有收到好的心跳，就认为是错误的心跳，从而产生切换动作。仲裁逻辑的有限状态机如图 4 所示。

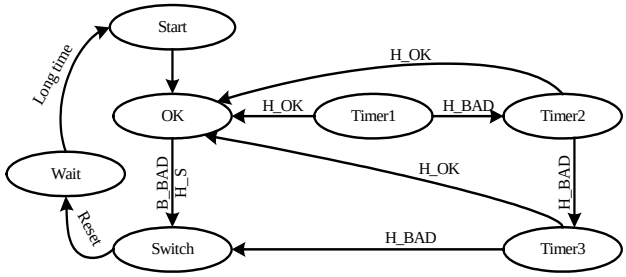

图 4　仲裁逻辑有限状态机

H_OK 和 H_BA 分别代表好的心跳信号和坏的心跳信号，B_BAD 代表总线故障，H_S 代表遥控切换命令，一旦发生切换动作，FPGA 控制看门狗使 CPU 部分复位。为了避免软件定时器开始之前就进行仲裁判定，仲裁逻辑在系统复位后，进入一个等待状态，等待的时间足够 CPU 部分复位并启动软件定时器。

4　总线冗余设计

计算机要求冗余的双机能够同时接收数据，并独立进行计算，如果一台计算机发生故障进行切换，也不会影响结果的输出。计算机主要包括 2 种接口：RS422 接口和 1553B 接口。RS422 接口是一种点到点或一点到多点的的通信接口，计算机内部冗余的 2 路 RS422 接口在机箱处连接在一起，对外表现为一路接口，冗余对外是透明的。由于 RS422 支持一点到多点的通信方式，因此在数据接收时，将 2 路接口连接在一起不存在问题。但是在数据发送时，连接在一起的 2 路接口会产生冲突，造成发送数据异常，甚至损坏接口。考虑到这个问题，RS422 接口的发送和接收采用了独立驱动的方式，发送驱动采用芯片 DS26F31，这一芯片有发送使能信号，当发送使能信号禁止数据发送时，发送端保持在高组状态，因此，通过控制 DS26F31 的使能信号，使得任意时刻主计算机使能发送，而备份计算机禁止发送，就避免了发送冲突。

1553B 是一种一对多的总线接口，采用硬件自动产生应答信息的命令/响应通信方式，总线上在任何时刻只能存在一个 BC，多个 RT 通过 RT 地址区分。计算机的 1553B 总线要求作为 RT 存在，如果冗余的 2 路 1553B 总线作为相同地址的 RT 存在，则能够同时接收到数据，但两者会同时产生硬件应答信息，而造成通信的异常。如果冗余的 2 路 1553B 总线作为不同地址的 RT 存在，则不会产生应答信息冲突，但

（下转第 247 页）