

# 基于双机热备的航天发动机控制器设计

李 鹏<sup>1</sup>, 来新泉<sup>2</sup>

(1 西安航天动力研究所, 陕西 西安 710100;

2 西安电子科技大学 电子工程学院, 陕西 西安 710069)

**摘 要:** 为提高控制器乃至发动机系统工作的可靠性, 提出了基于双机热备控制器的冗余设计方案, 通过对双机热备关键技术的研究, 对技术难点进行攻关, 提出了具体的解决措施, 确保了双机的同步运行和主备机的可靠仲裁, 从而构建了一个可靠的控制器系统, 实现了双机热备控制器的自主研发技术储备, 可以满足工程应用需要。

**关键词:** 控制器; 双机热备; 仲裁; 同步

**中图分类号:** V434

**文献标识码:** A

**文章编号:** (2010) 03-0058-05

## Design of dual-processor hot standby aerospace engine controller

Li Peng<sup>1</sup>, Lai Xinquan<sup>2</sup>

(1 Xi'an Aerospace Propulsion Institute, Xi'an 710100, China;

2 Electronic Engineering School, Xidian University, Xi'an 710069, China)

**Abstract:** A controller is one of the core components of an aerospace engine system. In order to improve the reliability of the controller and aerospace engine system, a dual-processor of hot standby redundant design is used. The key components of the controller are dual-redundant design. The hot standby redundant key technology to ensure the synchronization of the dual-processor operation and reliable machine arbitration is presented. A reliable controller system to meet the needs of engineering applications is constructed.

**Key words:** controller; hot standby back-up; arbitration; synchronous

收稿日期: 2010-02-02; 修回日期: 2010-03-15。

作者简介: 李鹏 (1976—), 男, 工程师, 研究领域为航天发动机测控技术。

0 引言

航天技术的发展目前更趋向系统化、层次化、模块化的发展进程, 航天发动机拥有自身的控制单元已成为航天动力领域发展的新需求, 控制器作为航天发动机系统的控制驱动单元, 对其进行高可靠性设计是航天系统工程可靠性保障措施的要求。

因此, 控制器的设计需采用冗余容错技术, 对控制器的核心部件处理机单元和相关关键部件进行冗余容错设计, 来提高控制器的可靠性。

1 双机冗余方案设计

容错是指设备的一个或多个关键部分发生故障时, 能够自动地进行检测与诊断, 并采取相应措施, 保证设备维持其规定功能, 或牺牲性能来保证设备在可接受范围内继续工作。冗余容错技术就是利用硬件冗余法或软件冗余法来处理故障, 提高系统可靠性<sup>[1]</sup>。目前, 硬件冗余技术主要有以下几种实现方式: 单机线路冗余、双机冷备、双机热备和三重冗余<sup>[2,3]</sup>。

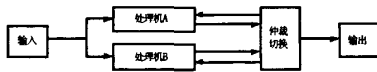


图 1 双机热备结构框图

Fig.1 Hot standby block diagram

由于单机线路冗余可靠性有限, 双机冷备存在控制实时性差, 三重冗余系统过于庞大, 取舍各种冗余方式的利弊, 结合具体工程实现情况, 本系统采用基于双机热备的硬件冗余设计方案, 即两套硬件、软件完全相同的处理机系统实现主备双机工作模式, 系统开机自检后默认处理机 A 为主机, 处理机 B 为备机, 主机的输出信号具有输出控制权。

当主机 A 出现故障时, 通过仲裁及切换电路, 将没收处理机 A 的控制权, 并将控制权转为处理机 B, 处理机 B 由备机状态变为主机状态, 接管控制任务, 实现控制权的无缝转换, 确保控制单元继续可靠工作, 双机热备的冗余设计结构框图如图 1 所示。

2 控制器系统介绍

控制器主要由双机热备的处理机部分、仲裁器、双路 CAN 总线接口线路、冗余电源、驱动线路、以及模拟量采集转换线路构成, 控制器系统图如图 2 所示。

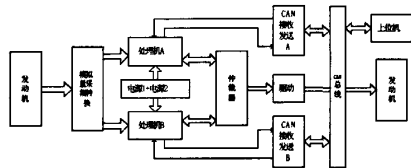


图 2 控制器系统图

Fig.2 Controller system diagram

控制器的处理机部分采用了双机热备设计, 处理机与上位机之间的通讯采用 CAN 总线<sup>[4]</sup>通讯, 采用双路 CAN 接口实现 CAN 接口的冗余; 控制器通过对 6 路 I/O 控制信号及驱动线路均进行双路并行冗余设计, 实现对发动机 6 路电磁阀的控制驱动; 控制器对 1 路 PWM 阀门进行流量调节, 1 路 PWM 阀门的控制需要 2 路 PWM 信号进行叠加控制, PWM 阀门的驱动线路采用单线路驱动; 数据采集部分采用单线路对 10 路模拟量进行采集, 采集到的数据同时送到两 DSP 的 ADC 接口, 实现双机同步采集, 采集数据通过 CAN 总线上传给上位机, 实现状态参数和遥测数据的上传。

2.1 处理机系统

处理机系统采用基于 DSP 控制芯片构建的处理系统, 采用 TI 公司的 TMS320C2812 控制芯片<sup>[5]</sup>, DSP 外扩存储器 E<sup>2</sup>PROM、晶振、复位电

路、JTAG、等外扩接口电路，构成硬件完全一样的两套处理机系统。两处理机均外扩 CAN 收发电路，构成双 CAN 通道，两 CAN 采用相同的 ID，能同时接收 CAN 数据，但只有主机能发送 CAN 数据。DSP-TMS320C2812 集成了增强型 CAN 总线通讯接口，接口芯片采用 PCA82C250，CAN 总线节点与处理机之间的电气隔离采用 ADuM1201 实现。

处理机系统以及接口电路的供电也采用双路电源设计，两路电源输出正向端串接保护二极管后并接在一起，两地线相连，构成双路电源的可靠冗余。

2.2 仲裁器

仲裁器可对两台处理机的工作状态及输出信号进行综合比对，判断并设置两处理机的主备状态，将控制输出的主权交给主机。

仲裁器对两处理器的仲裁通过硬件电路+软件判断来实现，仲裁器采用硬件电路对两路输出信号进行比对，若两信号相同则以主机的输出通过三态门使能输出，若两信号不一致，则需借助两处理机进行自检，通过中断自检子程序来确定两处理机工作是否正常，并反馈给仲裁器两机的工作状态，仲裁器再进行综合判断，确定两机的主备状态。

由于仲裁器对 12 路 I/O 和 2 路 PWM 信号均需进行状态比对，所以采用一片 FPGA 芯片，在片内实现主备双机的仲裁和输出权的转换。FPGA 选用 ALTERA 公司 APEX 20K 系列产品的 EP20K60E，带有 PLL。FPGA 与 DSP 之间接口关系见图 3 所示。

DSPA/B 与 FPGA 的接口信号有：两路 DSPA/B 的输出控制信号送入 FPGA 中，FPGA 分别向 DSPA 和 DSPB 送中断请求状态信号 INTERA 和 INTERB，以及处理机的主备状态信号 HA (HB)，处理机给 FPGA 的状态返回信号 ZA (ZB) 和 S A (SB)。

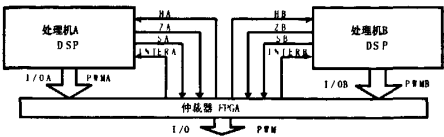


图 3 FPGA 与 DSP 的接口

Fig.3 Interface of FPGA and DSP

3 关键技术

在基于双机热备工作方式下，当出现双机输出信号不同或单机工作出现异常以及双机输出非同步等故障临界状态的情况下，实现主备机的选择以及实现主备机对输出控制的无缝切换就显得有些困难，而在工程应用中，要保证双机工作的可靠性就必须重点解决各种仲裁判断的临界状态，确保仲裁结果正确、可靠。

3.1 同步性问题的解决

双机热备的冗余工作方式是一种较为可靠、实用的应用方案，主备机同时工作可以进行无缝切换控制，但在工程应用中要真正做到进程的完全同步有着较大困难，通过以下措施可保证两机工作同步性问题。

3.1.1 输入输出同步

两处理机要达到进程完全同步，首先要保证输出信号为同步信号，CAN 总线采用双路总线接口，两处理机各用一路，双 CAN 同时接收数据，保证了两处理机输入信号的同步。

两套处理机系统采用相同的 DSP 器件以及外围扩展电路，做到两处理机硬件的对称，两处理机公用一个晶振时钟源，将两机的输入时钟保持一致，达到两机时钟同步；同时，两套处理机装订完全相同的软件，使得两处理机具有相同的硬件、软件，同时两处理的时钟也一致，两个完全对称的系统在同时接收到输入信号后，会输出同步输出信号。

### 3.1.2 定时仲裁方法

虽然对称的两处理机系统能实现输出信号的同步, 但如果输出信号间存在一定时间偏差会造成仲裁器的误判、错判现象, 在此采取定时仲裁的方法来解决此问题。

控制器对 PWM 输出控制的精度要求为 1ms, 对 I/O 口输出控制的精度要求为 10ms, 所以现在重点考虑 PWM 的输出同步的处理。在仲裁器中进行信号比较时, FPGA 的时钟源来自 DSP 的时钟输出 CLK\_OUT, 在仲裁器 FPGA 中通过 PLL 锁相环, 构成一个 100 $\mu$ s 的时钟周期, 即频率为 10kHz 的比较时钟, 在两路处理机输出信号比较时不进行实时比较, 而是通过上述构建的比较时钟触发器进行触发比较, 每间隔 100 $\mu$ s 进行一次状态比对, 这样仲裁频率为 10kHz, 单路 PWM 时钟触发时序见图 4。

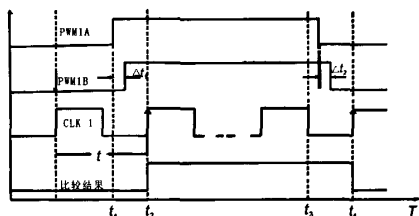


图 4 单路 PWM 时钟触发时序

Fig.4 Single PWM clock trigger timing

若两比较信号 PWM1A 和 PWM1B 在起始处存在时间差  $\Delta t_1$ , 在结束处存在时间差  $\Delta t_2$ , 在时钟的上升沿进行触发比较, 如果 CLK\_1 的上升沿时刻刚好处于  $\Delta t_1$  或  $\Delta t_2$  内, 将会出现两信号不一致, 为避免因小时间偏差造成的误判, 可以通过忽略首次比较结果, 对仲裁器提出的第一次的中断, 处理机只对赋值 Q (初值为 0) 值进行加 1, 返回给仲裁器的处理器工作状态 ZA (ZB) 为正常, 仲裁器清除中断 INTER 状态, 进入第二次信号的比较, 若第二次比较结果不同, 仲裁器送出中断标志, 处理机响应中断, 判断 Q 值  $\geq 2$  就进入中断自检子程序, 进行双机状态检查,

确定主备机及输出控制权, 这样既实现了对处理机输出的 PWM 信号的可靠判断, 又能避免因非同步小偏差比较带来的误判。

采取这种比较仲裁措施后, 输出信号的最大偏差时间  $< 2t$ , 即小于 200 $\mu$ s, 小于 PWM 的控制精度 1ms 的要求, 这样既可以解决 200 $\mu$ s 内的软件同步偏差和误判问题, 同时又满足对 PWM 控制精度的要求。

### 3.1.3 软件同步设计

为实现双机运行的同步, 两处理机装载相同软件, 但由于主备双机在工作过程中只有主机可以向 CAN 总线发数据, 备机不能发送数据, 因此, 主备双机在发送数据时, 存在非同步时刻, 为解决此问题, 在双机发送数据时查询处理机所处的主备状态, 主机发送数据而备机需延时等待, 这样保证双机的同步。

此外, 还可以利用软件在运行中存在一个关键的同步点, 即 CAN 通信的接收, 两处理机同步接收到 CAN 信号, 开始运行对应控制程序, 输出同步的控制信号, 使得双机同步, 同时这也就要求 CAN 信息的接收具有最高的中断优先级, 这就需要软件处理好各事件中断的优先权, 各事件优先权顺序为: CAN 接收中断优于控制输出, 优于 CAN 发送数据, 优于数据采集。

DSP 的主频率可达 150MHz, 时钟周期为 6.67ns, CPU 在单周期内执行寄存器到寄存器的操作, 所以, 两处理器在软件在运行中的时间偏差也处于 ns 级, 对于 200 $\mu$ s 的同步偏差来讲是可以忽略的, 同时, 通过上述采取的同步保证措施, 有效确保了双机工作的同步性。

### 3.2 故障仲裁

在仲裁过程中, 如果两处理机出现一处理机重启, 会造成两处理机工作的不同步, 会给仲裁带来困难, 若出现此现象, 为保证控制器的可靠工作, 避免工作不稳定的处理机对系统造成干扰, 此刻将双机热备工作模式转换为单机工作模式。

具体解决措施为：在双处理机的程序中设置位置标志，通过查找标志位可得知处理机所处的工作位置，如设置一位置量  $S$ ，开机时其初始值为 0，软件运行到一定阶段标志值就累加，当出现一处理机出现重启后，两处理机的输出不同，仲裁器提出中断自检请求，自检程序首先去读  $S$  值，若  $S$  值小于给定值就认为处理机已重启，处理机给仲裁器状态信号，仲裁器就将控制权交给工作正常的处理机，退出双机模式，运行单机模式。

## 4 结 论

航天发动机控制器为发动机系统的核心控制单元，按照航天产品的可靠性工程要求，对控制器的设计采用了容错冗余设计，控制器的处理机部分采用了双机热备冗余设计，通讯采用了双

CAN 总线接口，对电源以及控制驱动线路均进行了双路并行冗余设计，通过对双机热备技术难点的解决，认为基于双机热备的控制器方案是可行的，本设计方案可以应用到型号产品的研制中。

### 参考文献：

- [1] 孙秀娟. 基于双模冗余容错技术的数据采集系统设计[J]. 电测与仪表, 2008, 45 (512): 49-52.
- [2] 王建虹. 一种高可靠性双机冗余系统的设计[J]. 研究与开发, 2008, 27(4): 42-44.
- [3] 于增泽. TS3000 三重化冗余容错集成控制系统的应用[J]. 石油化工自动化, 2000, 44(4): 44-46.
- [4] 饶运涛, 邹继军. 现场总线 CAN 原理与应用 [M]. 北京: 北京航空航天大学出版社, 2007.
- [5] 苏奎峰. TMS320F2812 原理与开发[M]. 北京: 电子工业出版社, 2005.

(编辑: 王建喜)

(上接第 44 页)

- [13] Curnier A. On Three Modal Synthesis Variants[J]. Journal of Sound Vibration, Vol. 90(No.4), 1983: 527-540.
- [14] Qiu Jibao, Ying Zuguang, L H Yam. New Modal Synthesis Technique Using Mixed Modes[J]. AIAA Journal. 1997. Vol. 35. No.12, 1870-1875.
- [15] Qiu Jibao, Williams F W, Qiu Renxi. An Exact Substructure Method Using Mixed Modes[J]. Journal of sound and Vibration, 2003, 266: 737-757.
- [16] 黄道琼, 张继桐, 何洪庆. 四机并联发动机低频特性

分析[J]. 火箭推进, 2004, 39(4): 28-31.

- [17] 张正平, 邱吉宝, 王健民, 等. 航天器结构虚拟动态试验技术新进展[J]. 振动工程学报, 2008, 21(3): 210-221.
- [18] Thomas, G Carne, David R. Modal Analysis of a Shell-payload Structure Using Test Data [C]. 4th International Modal Analysis Conference; 1986. Los Angeles.
- [19] 向树红, 晏廷飞, 邱吉宝, 等. 40 吨振动台虚拟试验仿真技术研究[J]. 宇航学报, 2004, 25(4): 376-381.

(编辑: 王建喜)