轨道交通安全计算机中倒机单元的设计

边 庆[1],单 冬[1,2]
(1. 北京交通大学 电子信息工程学院,北京 100044;
2. 北京交大微联科技有限公司,北京 100195)

摘 要:安全计算机被广泛应用于轨道交通信号系统中,其中倒机单元有效提高了安全计算机的可靠性。研究了二乘二取二安全计算机结构,介绍了基于通信的倒机方式,制定了安全通信协议。该方式硬件上利用 FPGA 实现,使整个设计紧凑、灵活、稳定且高速;软件上,讨论了主备状态的确定,分析了倒机基本原则和单系的状态转移。具有该倒机方式的安全计算机,已在多种轨道交通信号系统中得到了应用,应用结果表明,本方案切实可用,能够满足系统高可靠性的要求。

关键词:安全计算机;倒机单元;二乘二取二;通信
中图分类号:TP399;U231 **文献标识码**:A **文章编号**:1673-629X(2012)09-0153-04

Design of Switch Unit in Safety Computer of Railway Transportation

BIAN Qing[1], SHAN Dong[1,2]
(1. School of Electronics and Information Engineering, Beijing Jiaotong University, Beijing 100044, China;
2. Beijing Jiaoda Microunion Tech. Co. Ltd., Beijing 100195, China)

Abstract: Safety computers are widely used in railway signaling systems. Switch unit improves the reliability of safety computers effectively. The structure of double 2-vote-2 safety computer is researched. It introduces a design scheme of switch unit based on communication. The realization of switch unit is using FPGA in hardware, makes the whole design tighter, more flexible, more steady and high-speed. In software, the methods of selecting the host are discussed. The basic principle of switching and shift of working status are analyzed. Safety computers including the switch unit have been applied in several railway signaling systems. The application results show the scheme is practical and applicable to the work, and meets the needs of high reliability.

Key words: safety computers; switch unit; double 2-vote-2; communication

0 引 言

轨道交通信号系统是保证行车安全的实时控制系统,必须具有高可靠性和高安全性。二乘二取二安全计算机不但具有高可靠性和高安全性,而且维护方便和便于脱机测试的优点显得尤为重要[1]。因此,广泛应用于轨道交通信号设备中,如车站计算机联锁系统和列车运行控制系统等。

倒机单元是二乘二取二安全计算机的关键单元,实现了两系主备切换,有效提高了系统的可靠性和可用性。目前安全计算机中倒机单元主要是通过信号线连接,是基于独立的倒机模块实现,然而,这种方式很难采用冗余技术提高可靠性,并且存在由于倒机模块故障而导致系统不能正常工作的问题,当倒机模块故障时两系都不能成为主用,整个系统将停止工作,因此不能满足系统高可靠性的要求。

文中介绍一种基于通信的倒机方式,实现系统主备倒机不会因倒机单元故障而受到影响,提高系统的可靠性。

1 二乘二取二安全计算机的结构

如图 1 所示,二乘二取二安全计算机由功能完全相同的两套子系统(A 系和 B 系)构成,每个子系统是二取二(2oo2)结构,两个 CPU 同步运行,并进行实时比较,只有运行一致时才对外输出或传输运算结果,实现系统的高安全性[2,3]。

二乘就是两系构成热备冗余结构,可以称作双系热备,和双机热备原理相同,保证系统在其中一系故障情况下能够倒向备机工作,实现系统的高可靠性。

双系热备是基于主/备方式的机器热备,主备机都

收稿日期:2012-02-03;**修回日期**:2012-05-13
基金项目:铁道部科技研究开发计划项目(2011X009-E)
作者简介:边 庆(1986-),男,硕士研究生,研究方向为交通信息工程及控制;单 冬,副教授,硕士生导师,研究方向为交通信息工程及控制。

进行系统的数据输入输出、逻辑运算,并同步运行,但在同一时刻只有主机才有系统的最终控制权。当主机故障时,主机通知备机,或者备机通过双系热备模块软件的诊断将备机激活,保证在尽量短时间内恢复正常使用,达到无缝切换。

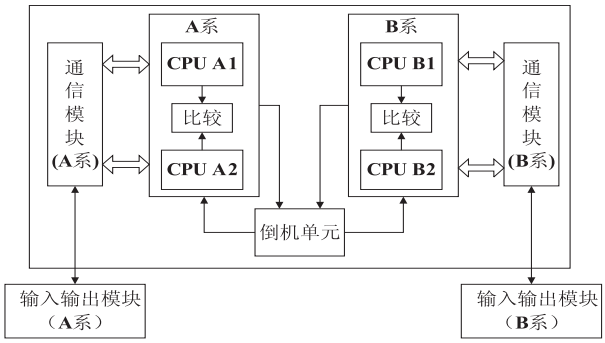

图 1 二乘二取二安全计算机结构图

2 基于通信的倒机方式

图 1 所示的系统是一种典型的基于独立倒机模块实现的二乘二取二安全计算机[4]。图 2 所示的是一种基于通信的倒机方式,即完全依赖两系间的通信,两系间信息交互的传输系统可以是通信接口电路,也可以是局部网络。为了使安全计算机平台具有较强的独立性、通用性,本设计采用通信接口电路。

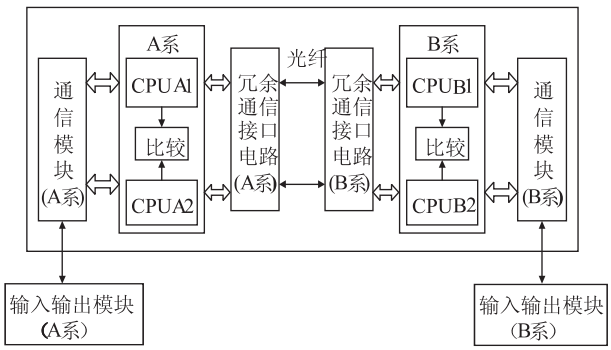

图 2 基于通信的倒机方式框图

安全计算机中两系是相同的,以其中 A 系为例,介绍工作过程:A 系 CPU A1 和 B 系 CPU B1 依靠一路通信链路,交换彼此的运行状态数据,进行比较并计算得到 A 系的预控制状态 1;同时 A 系 CPU A2 和 B 系 CPU B2 交互彼此的数据,计算得到 A 系的预控制状态 2,预控制状态 1 和预控制状态 2 相互比较并生成 A 系的最终控制状态,A 系根据最终控制状态判断是否进行倒机。

通信接口电路是冗余的,使得每一系可以通过两条数据通道获取另一系的运行状态,有效降低了由于某个通信模块的故障造成系统误动作,从而使基于通信的倒机方式达到高可靠性。当两条通信链路的一条故障时,A 系和 B 系将改变策略,正常的通信链路的功能只是两系同步。

假如 CPU A1 和 CPU B1 的通信链路故障,CPU A2 和 CPU B2 的通信链路正常,两系将利用正常的通信链路进行同步,CPU A2 和 CPU B2 利用通信交互彼此数据,CPU A1 和 CPU B1 不再交互数据,而每系内两 CPU 是二取二结构,同一系内两 CPU 是同步并且实时比较的,安全性不受影响。显然,整个系统仍可以继续工作,只是冗余的通信链路变为单个通信链路。

安全通信协议的制定:

欧洲电工标准化委员会(CENELEC)核准的 EN50159 标准提出在安全相关设备中的数据通信必须建立安全相关通信功能,因此两系之间的通信必须是安全通信[5]。安全通信最终都是体现在通信协议上,本设计中安全计算机使用的通信协议帧结构包含:帧头、标识符、序列号、时间戳、数据位、校验码和帧尾。

●帧头和帧尾。采用了带帧头帧尾的透明传输机制,能够防止数据接收不完整错误。

●标识符。通过源标识符(源 ID)、目的标识符(目标 ID)和数据类型标识符校验数据的真实性。

●序列号。序列号的使用能够减少消息重复、丢失、插入和以不正确序列发送消息产生的故障,还作为数据新旧标识。

●时间戳。可以检测消息重复和以不正确序列、太迟、太早发送消息产生的故障,用以说明数据的实时性。

●校验码。用于对传输错误进行检测,通过 16 位 CRC 校验数据的正确性,识别通信过程中可能产生的误码。如 CRC 校验不通过,则数据无效,丢弃该数据包。CRC 校验码根据帧序号、时间戳、信息类型和数据内容生成,不包括帧头。

安全通信协议是针对通信的安全风险制定的,对传输数据进行时效性、真实性、完整性和有序性的校验,降低了传输数据的误码率,从而使基于通信的倒机方式达到高安全性。

3 倒机单元的硬件设计

通信协议可采用软件编程或 FPGA 实现。软件编程方法灵活,通过修改程序就可以设计不同的通信协议,但程序运行占用处理器资源多,执行速度慢。现场可编程门阵列(Field Programmable Gate Array,FPGA)是采用硬件技术处理信号,又可以通过软件反复编程使用,能够兼顾速度和灵活性,实时性能够预测和仿真,另外,FPGA 内部资源丰富、低功耗、可靠性高、开发费用低等,因此采用 FPGA 设计安全通信协议是一种可行的方法。

本设计选用 Altera 公司 Cyclone II 系列芯片中 EP2C8Q208C8N,光发送器和光接收器分别是 HF-

BR1412 和 HFBR2412,光纤是单模光纤[6]。如图 3 或 4 所示,CPU 与通信接口电路的接口为总线形式,具体为双口随机存储器(DPRAM),可以看作 CPU 的一个外部存储器。本设计中双口 RAM 采用 FPGA 内嵌的 DPRAM,还集成有 FIFO、CRC 编码和解码、UART 发送和接收控制等,使整个设计紧凑、稳定、可靠。其中,DPRAM 和 FIFO 由 Quartus II 中的 MegaWizard plug-in Manager 工具产生,简化设计[7]。为了提高通信的速率和抗干扰性,传输介质采用光纤。

在硬件电路设计中,FPGA 内部模块的设计框图如图 3 和图 4 所示[8]。

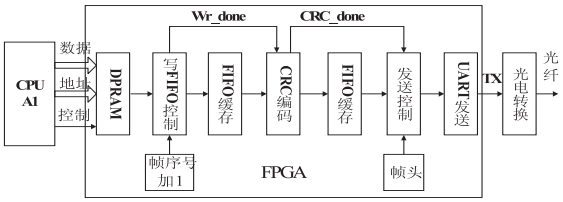

图 3　发送端 FPGA 内部模块框图

图 3 为发送端模块框图,CPU 向 DPRAM 写数据完成后,FPGA 读取 DPRAM 中数据,并且序列号加 1,经过 FIFO 缓存,进行 CRC 编码,编码完成后,向发送控制模块发送指示信号“CRC_done”,发送控制模块实现组帧,按照数据帧格式依次通过 UART 发送出去。

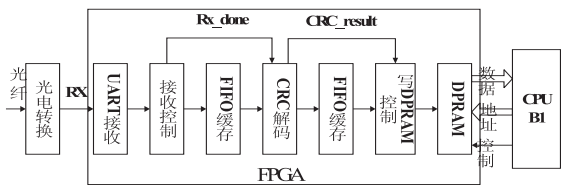

图 4　接收端 FPGA 内部模块框图

图 4 为接收端模块框图,接收模块接收线路上的数据,CRC 解码完成后,向写 DPRAM 控制模块发送指示信号,当 CRC 校验正确时,将数据写入 DPRAM;当校验不正确时,则丢弃该帧数据。

循环冗余校验码 CRC(Cyclic Redundancy Code)编译码方法简单,检错、纠错能力强,误判概率低,应用广泛。本设计采用 CRC-CCITT(由欧洲 CCITT 推荐),生成多项式为 $g(x) = x^{16} + x^{12} + x^5 + 1$,实现方法是基于字节运算的并行实现,该方法逻辑简单、处理速度高,一个时钟周期内完成一个字节的 CRC 计算,而且很方便地在 FPGA 中实现[9,10]。

光纤通信中一般传输速率较高,所以需要使用较高速度的 UART,要设计高速的 UART 必须使用 FPGA 内部的锁相环 PLL[11]。外部晶振提供的时钟通过 PLL 倍频后为波特率发生器提供较高的基准时钟,从而得到较高的发送速率和接收采样速率,提高收发速度。

4　倒机单元的软件设计

4.1　主备状态的确定

如图 5 所示,A 系启动时,首先启动软件的双系热备模块,将自己置于初始状态,然后读取 B 系的工作状态,假如读取到 B 系的工作状态已经是主机状态,则向主机发送同步请求,然后接收主机发来的数据并同步本系的数据,数据同步完毕后,将本系状态置于备机状态。假如读取到 B 系是备机状态或不能取得 B 系的工作状态,则将本系置于主机状态。

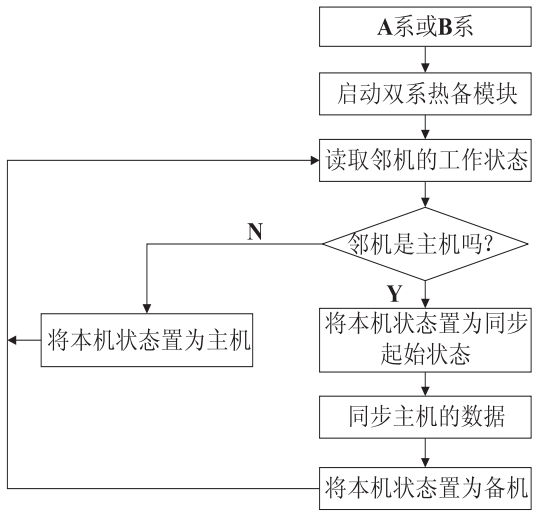

图 5　主备状态确定的软件流程图

在初始状态确定后,主机循环读取备机状态,若发现备机转为主机,则原主机将自己置于备机状态,此后不断地从主机获取数据并更新自己的数据。若备机不能取得主机状态或发现主机转为备机,则原备机转为主机状态。

4.2　倒机原则

双系之间的倒机有两种情况,一种是主机主动通知备机升为主机,主机在判定自身故障需要倒机时,在检查邻机确实在工作且故障等级低于本机时,主机将主动通知邻机或者停止与邻机的通信联系从而触发邻机升为主机;还有一种情况是备机依据检测手段发现主机发生故障了,而主动将自身状态升为主机。

4.3　单系状态转移

系统运行过程中,每系根据自己和对方的实际运行情况调整自身的工作状态,保证在单系出现故障情况下能及时主备倒机。二乘二取二系统正常运行时,每系的工作状态为主机、备机、同步或待机中的一种,如图 6 所示。用箭头线表示从一种状态变为另一种状态,箭头线上标有号码,如满足条件 8 时,某系从待机状态变为同步状态。

主备机之间通过两系之间的通信连接交互彼此的状态,并根据上述状态转移条件进行决策以确定相应的本机状态及邻机状态[12]。

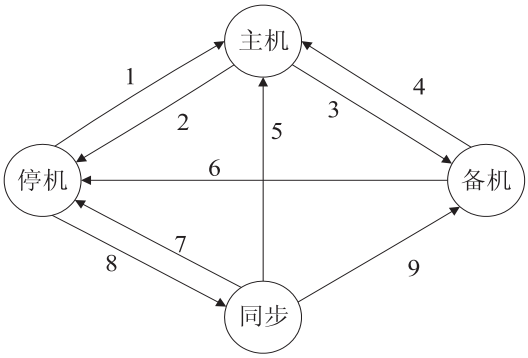

图 6 双系热备状态转移图

5 结束语

轨道交通信号系统的核心是安全计算机,对它的研究具有重要实践意义。文中介绍了二乘二取二安全计算机中倒机单元的设计方法,从硬件和软件上介绍了基于通信的倒机方式的实现。具有该倒机方式的安全计算机,已在列车运行控制系统和车站计算机联锁系统得到了应用。下步对关键技术及实现细节进一步改进和优化,以提高系统的安全性、可靠性和可用性。

参考文献:

[1] 赵志熙. 计算机联锁系统技术[M]. 北京:中国铁道出版社,1999.

[2] Wang Shuai, Ji Yindong, Dong Wei, et al. Design and RAMS Analysis of a Fault-tolerant Computer Control System[J]. Tsinghua Science and Technology, 2007, 12(z1): 116-121.

[3] Kim H, Lee H, Lee K. The design and analysis of AVTMR (all voting triple modular redundancy) and dual-duplex system [J]. Reliability Engineering and System Safety, 2005, 88(3): 291-300.

[4] 吴江娇,张松涛,张 源. 计算机联锁系统操作表示机双机热备的实现[J]. 北方交通大学学报,2003,27(5):69-72.

[5] 李开成. 现代铁路信号中的通信技术[M]. 北京:中国铁道出版社,2010.

[6] 李成钢,申 萍,聂晓波. 基于 FPGA 的 HDLC 与 RS485 通信网关的设计[J]. 机车电传动,2011(1):20-23.

[7] 张维旭,贺占庄. 基于 FPGA 的异步 FIFO 设计[J]. 计算机技术与发展,2006,16(7):168-170.

[8] 林 垚,于拓华. 基于 FPGA 的铁路远程通信系统的设计与实现[J]. 中国铁路,2008(5):41-44.

[9] 张 蓓,鲁新平,马 龙,等. 基于字节的循环冗余校验算法及 FPGA 实现[J]. 微处理机,2009,31(1):88-90.

[10] 张树刚,张遂南,黄士坦. CRC 校验码并行计算的 FPGA 实现[J]. 计算机技术与发展,2007,17(2):56-58.

[11] 王永州,范多旺. 基于 FPGA/CPLD 的高速和低速 UART 的设计及其应用[J]. 铁路计算机应用,2006,15(10):1-4.

[12] 王秀娟. 调度集中系统中双机热备机制的实现[J]. 北京交通大学学报(自然科学版),2009,33(2):26-29.

(上接第 152 页)

3 结束语

通过完成对系统的软件架构设计,实现基于. NET 气门尺寸检测系统。该系统已应用在实际生产中,使用该系统对气门尺寸进行检测,提高了生产效率,同时美观的人机交换界面,简单易懂的操作方式,使操作人员只需进行简单的培训就能掌握系统的使用。经实际使用验证,符合工厂使用要求,后续工作是连接自动加工生产线,实现自动加工、自动检测。

参考文献:

[1] 黄杰贤,徐 杜,蒋永平. 一种轴套类零件尺寸高精度图像检测方法的研究[J]. 光学与光电技术,2008,6(2):85-87.

[2] 郭伟华,徐 杜,蒋永平. 发动机气门尺寸计算机视觉检测软件系统的设计[J]. 光学与光电技术,2010,8(3):65-68.

[3] 胡小松,罗 芬. 基于. NET 平台的组织工作信息远程传输系统的设计与实现[J]. 计算机与现代化,2011(3):137-139.

[4] 张志杰. 基于分层结构的管理信息系统架构设计[J]. 计算机技术与发展,2010,20(10): 146-149.

[5] 徐 杜,蒋永平. 采用数字同步技术的轴类零件尺寸光电检测[J]. 光电工程,2004, 31(8):45-48.

[6] 高 阳. 基于. NET 平台的三层架构软件框架的设计与实现[J]. 计算机技术与发展,2011,21(2):77-80.

[7] 陶 徐. 机器视觉在烟盒包装检测中的应用[D]. 昆明:昆明理工大学,2007.

[8] 何 斌,马天宇,王运坚. Visual C++数字图像处理[M]. 北京:人民邮电出版社,2001.

[9] 姚峰林,詹海英,李元宗. 机器视觉中的边缘检测技术研究[J]. 机械工程与自动化,2005(1):25-29.

[10] 张绍堂,蒋 作,郑智捷. 机器视觉技术在烟草异物剔除系统中的应用[J]. 云南民族大学学报(自然科学版),2007,16(2):46-50.

[11] Kyasanur P, Jungmin S. Multichannel mesh networks: challenges and protocols[J]. IEEE Wireless Communications, 2006, 13(2):30-36.

[12] Shen Dongxu, Li V O K. Performance Analysis for A Stabilized Multi-channel Slotted ALOHA Algorithm[C]//Proceedings of the 14th IEEE 2003 International Symposium on Personal Indoor and Mobile Radio Communications. [s. l.]: [s. n.], 2003:249-253.