基于力控组态环境双机容错控制系统的实现

张计科 王生铁 内蒙古工业大学信息工程学院(010062)

Abstract

Combining configuration software with the duplex fault-tolerant mode,the paper designs and implements the ForceControl´s configuration software-based duplex fault-tolerant system by means of handware redundancy for fault-tolerant, software´s reliability design,integration of Visual C++ and ForceControl and multi-level fault diagnosis.Test result shows that the system mentioned above is correct and practical.

Keywords:Reliability,duplex fault-tolerant system,configuration Software,integrative management and control

摘 要

本文将双机容错模式与组态软件相结合,通过硬件冗余容错、软件组态可靠设计、VC 与力控相嵌、多级故障诊断,设计实现基于力控组态环境的双机容错系统。实验验证了该系统的可行性和正确性。该系统具有低成本、高可靠性、管控一体化、易扩展的特点,有较高的实用价值。

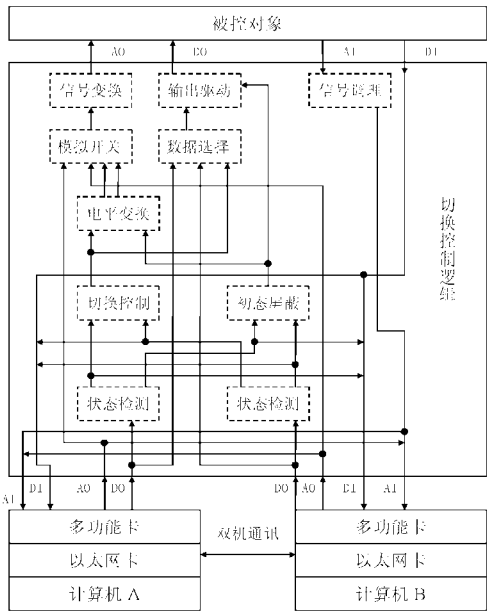
关键词:可靠性,双机容错系统,组态软件,管控一体化

组态软件由于具有友好的人机界面、先进的实时数据库及管理系统、丰富强大的功能、快速便捷的应用设计和灵活方便的扩展而在工业上得到了广泛应用,大大缩短了开发周期,突出了系统集成和通用性。着眼于低成本高可靠性、管控一体化的计算机控制系统的研究,在对各种冗余模式的可靠性静态指标、实现复杂度及经济性综合分析比较之后,硬件结构选用可用度较高的双机容错模式的热备份结构[1,3],软件选用性价比较高的力控组态软件,将组态软件和双机容错模式结合起来,构成基于组态环境双机容错系统,不仅可以提高系统可靠性,还可以增强系统的管控一体化功能。

1 双机容错系统硬件结构

双机容错系统的硬件结构如图 1 所示,主要包括计算机、切换控制逻辑和被控对象三个组成部分。系统基于模块化、标准化设计思想,具有简单、可靠、可维的特点。切换控制逻辑是一个独立单元,采用常规的模拟数字混合电路加以实现,接口采用标准模板,用于检测计算机工作状态、实现输入信号的调理、输出信号的切换、变换及驱动、初始随机状态屏蔽;计算机内插有多功能输入输出接口卡,实现数据采集、报表打印、实时控制、切换控制、界面控制、故障诊断等功能;两台计算机之间的信息交互通过切换控制逻辑、多功能输入输出接口卡及以太网通信接口实现[3]。

双机容错系统的工作过程为:当系统启动时,两机 Windows 自检成功后,实时输出本机状态信号并检测对方机状态信号,首先自检无误并标示本机状态的计算机成为主用机,另一台计算机自动成为备用机,两机开始各自的功能执行。被控对象的模拟量和开关量经切换控制逻辑进行信号调理后,无需切换直接接入两机的多功能数据采集卡上,进行数据采集,两机执行相应的数据处理、保存、备份、传送、维护等数据管理和图形显示、趋势输出、报表打印、报警记录等功能,根据系统设计的控制策略计算及输出相应的控制作用。与此同时,两机实时自检、互检,诊断故障,根据自己所处的状态、信息交互及故障诊断结果,发出实时切换命令,故障的主用机让权成为备用机,离线维修,修好后再投入系统备用;无故障的备用机夺权成为主用机,同时切换控制逻辑通过其中的转换控制电路将主用机的控制作用可靠地切换并作用到被控对象上去,接替原主用机工作,继续完成对被控对象的实时控制,而备用机的控制作用被屏蔽掉,保证了计算机的控制作用稳定地输出。如果主用机故障,再夺权切换,如此周而复始,从而有效地提高了控制系统的可靠性。



AI:模拟量输入;AO:模拟量输出;DI:开关量输入;DO:开关量输出

图 1 双机容错系统硬件结构框图

2 双机容错系统软件实现

双机容错系统是一个完全对称的体系结构,两台计算机结构完全相同,执行同样的任务。每个计算机都实现包括容错控制、实时控制、画面显示、报表打印、数据管理、故障诊断等功能。每台计算机的功能框图如图 2 所示。依据双机容错系统的硬件结构和功能描述,本着“实时可靠、界面友好、配置灵活、简单通用”的原则,基于力控组态环境利用 FIOS SDK 开发多功能板卡的驱动程序,实现组态环境和板卡之间的接口,将力控组态软件和 VC++有机结合,互为补充,设计实现双机容错系统的容错控制、实时控制、画面显示、趋势输出、数据管理、报表打印、故障诊断等功能。

2.1 力控环境下多功能板卡驱动程序的开发

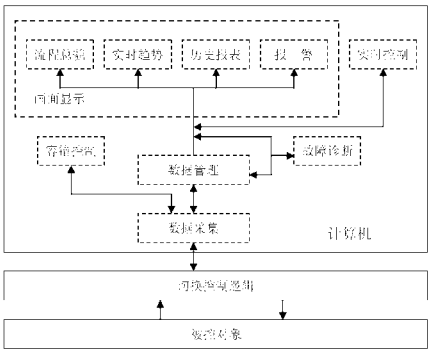


图 2 每台计算机的功能框图

计算机中的多功能卡采用北达众人 PS-2123 数据采集卡，该卡集 A/D、D/A、DI、DO 于一身，设有 8 路 8 位模入，2 路 8 位模出，8 路开入，8 路开出，符合 PC 总线标准，采用 I/O 译码方式，由 CPU 中的 A0~A10 决定板卡地址。

由于力控组态环境不支持所选多功能板卡，利用力控的 FIOS SDK 开发了多功能板卡的力控驱动程序(ForceControl I/O Server)。该驱动包括四部分：设备组态接口(Iodevui)、数据连接组态接口 (Ioitemui)、编程接口 (Ioapi) 和扫描程序 (Ioscan)。设备组态接口包括组态接口程序和 I/O 描述文件两部分，主要完成诸如定义设备的类别、厂商、型号、地址、通信方式、通信端口、端口参数等的设备组态过程；数据连接组态接口使数据库 DB 中的点参数与某种设备的具体通道建立逻辑连接关系，将这种连接关系保存在数据结构中以便于数据交换时正确地和通道连接；编程接口是 FIOS 最主要的接口，负责完成与 I/O 设备间的数据交换；扫描程序 Ioscan 完成对 Ioapi 部分的 dll 代码周期性扫描，把从 I/O 设备采集到的数据经 Ioapi 解析后提交给 DB，或将 DB 下置给 I/O 设备的数据经 Ioapi 解析转换后写入 I/O 设备，同时完成与 I/O 设备的底层通信、设备超时处理、设备故障诊断、与数据库 DB 之间的通信协作等[4]。限于篇幅，具体开发过程从略。

将开发好的驱动程序文件复制到力控安装目录下的 IO Servers 文件夹内，就可以在图形开发环境 Draw 的导航器中配置 I/O 设备，实现力控组态环境与板卡之间的接口。

2.2 容错控制

由于力控是基于 Windows 这种具有消息机制操作平台的分时多任务组态软件，不能保证双机切换的实时性和平稳性，因而引入了 VC++函数库中的高精度多媒体定时器和端口读写访问函数实现双机容错控制切换，流程图如图 3 所示。

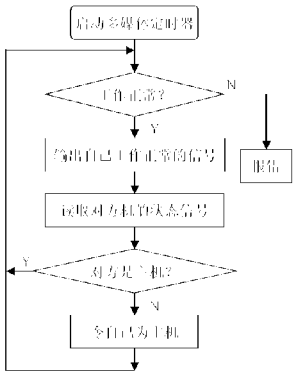


图 3 容错控制流程框图

2.3 数据管理

力控拥有强大的实时数据库系统，由实时数据库、实时数据库管理器、实时数据库运行系统和应用程序等几部分组成，可以方便地实现数据定义、实时数据采集与传送、历史数据存储与维护、数据运算、事务管理、调度、并发控制、数据检查和可靠性控制等。由于力控实时数据库将大部分技术细节都封装起来，展现在用户面前的数据管理组态环境是一个清晰明了的“表”，因此用户只需根据自身需要，进行必要的填表和参数设置，即可完成数据管理的组态，实现数据库与图形界面、控制策略、I/O 驱动、通信组件的互连。具体实现过程为：①启动数据库组态程序 DbManager；②新建数据点，指定区域和点类型；③设置点的基本参数，如名称、说明、初值、小数位、量程等④数据连接，包括连接类型和连接项两部分，实现点与指定设备的相应通道类型的某个通道建立逻辑映射关系；⑤参数报警设置，设定点的报警类型、优先级、报警值等参数；⑥历史参数设置，设定将点保存为历史数据的保存方式、保存时间间隔等参数。本文中在数据库中组了两个点，模入值 DEPRE 和模出值 ATVALVE。

为了保证双机数据的同步，两台计算机之间通过以太网相连，利用 VC++结合力控组态环境编程，实现了双机数据互备的功能。当两台计算机均正常工作时，两机通过网络实时访问对方数据库，获取对方的数据信息，并自动插入或更新数据；当有一台计算机发生故障时，该故障机被切离系统维修，修好后投入系统作为备用机工作，该机自动执行数据互备功能，更新数据，保证了数据的完整性和正确性。

2.4 画面显示

利用力控开发系统较为方便地开发了流程总貌、实时趋势、历史报表、报警的图形界面。在操作界面中用各种形象的图形表示工业现场运行设备，辅以脚本编程和动画效果，直观、形象、生动地显示现场工艺流程、运行参数的数值显示、实时趋势走向、报表和报警记录。其中，流程总貌图用来动态显示整个生产过程工序流程、检测数据、输出数据；实时趋势图实时显示工况的各种运行参数在不同时刻的变化曲线；历史报表可以浏览任何一天任一时刻的运行数据，随时以多种方式打印数据，进行分析和处理；报警图及时显示运行参数的报警记录，帮助操作人员判断和处理问题。各画面可相互切换，易于监视和操作，增强了人机交互的能力。

2.5 实时控制

为了便于研究和验证系统的性能，选取一个时间常数为 3 秒和 0.7 秒的二阶惯性环节作为被控对象进行研究，参考输入信号与对象实际输出之差作为切换控制逻辑的输入。采用等效连续设计方法设计控制器，系统设计为典 I 系统，求得连续控制器的传递函数。在力控控制策略生成器 StrategyBuilder 中，进行策略的组态。完成后的控制策略图如图 4 所示。图中输入变量 DEPRE.PV 和输出变量 ATVALVE 分别是由多功能板卡采集进来的数据(即切换控制逻辑的输入)和控制作用输出数据。线性变换模块 LNCH0 和 LNCH1 用于数码变换，分别实现输入电压由单极性到双极性的变换和输出电压由双极性到单极性的变换。一阶传递函数模块 TRANS0 实现控制器，限值模块 LIMIT0 完成限幅。

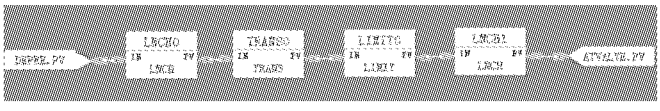


图 4 控制策略图

(下转第 31 页)

(上接第 20 页)

2.6 故障诊断

为了有效地提高控制系统的可靠性，系统设计实现了四级故障诊断机制。

第一级故障诊断：应用计算机的自检功能对计算机硬件进行初步诊断，如果自检失败，切离系统维修，如果自检成功，直接进入第二级。

第二级故障诊断：计算机操作系统本身具有一定故障诊断功能，可以初步检测和发现软硬件的各种错误，并可以修复部分软故障，如果发生不能修复故障且影响计算机正常功能运行时，则自动启动第三级故障诊断。

第三级故障诊断：这一级诊断在切换控制逻辑内完成，主要是根据计算机的工作状态信号 F、M，配合软件来判断计算机的工作正常和主从机状态，若是主机故障，则综合产生切换控制信号，双机切换，切离故障机马上维修；若是从机，马上切离维修。同时考虑到控制作用的特殊重要性，每台计算机的 D/A 输出都反馈到对方的 A/D 通道中，以此增加对 D/A 输出的故障诊断功能。

第四级故障诊断：利用力控实时数据库参数报警功能和力控 I/O 驱动程序的故障诊断功能，佐以事件记录，分别可以诊断出参数越限和 I/O 设备故障，便于操作人员查找故障、追忆事故、查询历史信息。

2.7 系统初始化

为了保证软件的系统性和操作的便利性，将 VC++开发的容错控制程序和力控应用程序有机地集成在一起，并利用 VC++开发了开机自启动、最小化托盘、隐藏窗口、自动执行容错切换和启动力控应用程序等系统初始化程序。

3 双机容错系统测试

根据图 1 的结构，构建完整的双机容错控制实验系统。采用两台联想 PⅢ-450 商用机作为容错计算机；选用众人公司 PS-2123 多功能输入输出卡实现模拟量和开关量的输入输出；利用运算放大器搭建模拟对象；方波发生器产生周期为 16 秒的方波作为参考输入信号；参考输入信号与对象实际输出之差作为切换控制逻辑的输入。软件安装完成后，对整个系统进行系统测试、功能测试、性能测试。系统测试包括多功能板卡测试和切换控制逻辑硬件的测试。功能测试包括容错切换、数据采集、实时控制、画面显示、报表打印、数据管理、故障诊断、系统初始化等功能的分项和总体测试。性能测试主要是对系统的双机切换时间、采样周期、数据刷新周期、动作执行周期等性能指标进行评价。

实验表明，该系统可靠实现容错控制功能，画面显示生动逼真，功能实现稳定可靠，维护扩充简单灵活，各项性能指标都达到了较好的预期效果，而且从控制性能上看，切换过程对被控对象输出未观察到任何影响，只是控制作用略有波动。

4 结束语

本着设计低成本、高可靠性、管控一体化、易扩展的计算机控制系统的原则，本文将双机容错模式与组态软件相结合，通过硬件冗余容错、软件组态可靠设计、VC 与力控结合、多级故障诊断，开发了基于力控组态环境的双机容错系统。实验验证了所设计系统的可行性和正确性。该系统结构简单、稳定可靠、功能多样、维护方便，具有较高的实用价值。

参考文献

1 疏松桂.控制系统可靠性分析与综合.北京：科学出版社，1992

2 马国华.监控组态软件及其应用.北京：清华大学出版社，2001

3 王生铁，侯晓坤，董志学. 双机容错系统切换控制逻辑的设计与实现. 第十三届中国过程控制会议论文集-过程控制科学技术与应用，珠海，澳门.2002

4 王生铁，张计科等.力控组态环境下数据采集卡驱动程序的开发. 内蒙古工业大学学报，2003，22(1)：57~61

[收稿日期：2004.5.24]