基于双主机冗余的显示控制系统设计

0 引言

随着航空电子设备的不断发展，对可靠性的要求越来越高。显示控制系统应用在航空电子控制系统中，主要完成数据通信、数据处理、图形显示和系统控制等功能，是人机交互的窗口，是重要的系统控制部件之一。由于显示控制系统的特殊功能地位，要求显示控制系统具有连续、稳定、可靠的工作特性。为了提高显示控制系统的可靠性，本文采用余度技术，即对系统进行双冗余设计来提高系统的可靠性、稳定性。

1 冗余理论

冗余理论来源于自动控制系统可靠性研究，其核心内容是如何最大限度地提高系统的可靠性。自动控制系统是由许多元部件组成的，元部件的组合方式与系统可靠性有十分密切的关系，冗余设计就是在控制系统中增加备用的关键元部件，当系统发生故障时，控制系统通过故障控制策略启动备用部件，来保证系统的正常运行，避免了单点故障造成的系统部分或全部功能的失效。

但冗余设计也不是一味地增加备份部件，备份部件的增加一方面增加了系统的复杂度、控制的复杂度，另一方面也增加了系统成本、功耗、重量，而且冗余设计的不合理，也可能降低系统的可靠性。

2 显示控制系统

2.1 系统构成

显示控制系统的主要功能是完成数据通信、数据处理、图形显示和系统控制。系统构成包括：控制模块、I/O 模块、A/D 模块、电源模块、液晶显示器以及键盘。系统各模块的主要功能：控制模块是系统的控制中心，和 I/O 模块，A/D 模块进行通信，并且完成数据的处理和系统控制，同时负责数据的显示和接收键盘指令完成相应的动作;I/O 模块主要完成数据的处理和数据的通信功能;A/D 模块主要完成数据的装换和数据的采集功能;电源模块主要完成电压的转换功能;液晶显示主要完成图形的显示功能;键盘主要完成用户按键指令的接收功能。

2.2 双主机冗余设计

依据冗余理论，对显示控制系统进行了详细的分析，控制模块和 I/O 模块，A/D 模块和显示器以及键盘都有交联关系，是系统的控制中心，属于系统的关键部件，因此控制模块也采用双余度设计来保证系统的可靠性。同时综合考虑系统的功耗、重量以及成本等因素，I/O 模块、A/D 模块、电源模块由于工作任务单一，交联关系简单，因此采用单余度设计。双主机冗余显示控制系统硬件架构如图 1 所示。

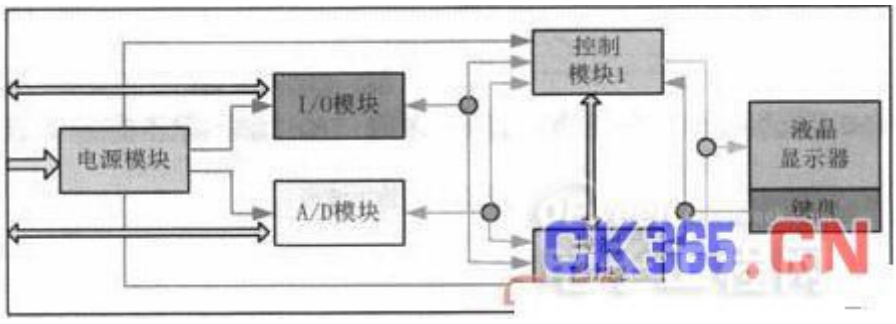

图1 双余度显示控制系统硬件结构

控制模块是整个显示控制系统的核心单元，绝大多数的控制任务都由它来完成。控制模块可以冗余配置，也可单模块工作。如果是冗余配置，一个模块作为主控模块，另一个作为备控模块;如果是单模块配置，不管是配置那一个通道的模块都作为主控模块工作。两个控制模块具有相同的硬件配置和运行同样的软件程序。

冗余配置的两块控制模块，一个运行在主控模式，另外一个运行在备控模式，它们是一个热备份的关系。它们都能访问 I/O 模块和 A/D 模块，但主控模式下的控制模块起着控制系统、图形显示、接收键盘指令等决定性的作用;备控模式下的控制模块执行诊断和监视主控模块状态的好坏，通过周期查询运行中的主控模块的状态并且实时接收主控模块发送的全部运行信息，但是它不输出图形信息，不接收键盘指令。备控模块实时保存最新的系统控制数据，以保证主/备切换的无缝连接。

3 冗余管理

3.1 优先权确定

冗余系统优先权设置通常采用三种方法：软件设置、通道竞争和外部硬件设置。在设计中一般不采用软件设置，因为软件的决策周期长、实时性差、可靠性较低，并且通道之间的互换性降低;第二种方法是通过通道竞争电路获取通道优先权，但是双余度系统没有必要设置此竞争逻辑;第三种方法直接采用外部硬件设置决定优先权，此方法简单可靠。本设计中控制器采用外部硬件设置优先权的方法，机箱中通道 A 设置为主控通道，通道 B 设置为热备份通道。

3.2 故障检测

3.2.1 在位状态检测

冗余配置的两个控制模块，插入机箱通电正常工作后，会通过硬连线互相报告在位状态。如果主控模块未在位或者未正常工作，则备控模块上电正常工作后可以检测到主控模块故障，自动切换成主控模块，行使主控模块的角色。如果是备控模块未在位或者未正常工作，则主控模块上电正常工作后可以检测到备控模块故障，并且将故障状态显示到显示器上，上报用户。

3.2.2 硬件状态检测

两个控制模块，正常工作后都周期性地运行检测程序，对模块的硬件资源、外围接口等状态周期性地检测，一旦发现故障，就将故障信息上报给主备切换控制逻辑，由主备切换控制逻辑来决策是否进行主备切换。

3.2.3 软件状态检测

通过看门狗来检测主备模块的软件运行状态，软件任务周期性地进行喂狗操作，如果软件运行出现故障，则会触发看门狗狗叫，一旦主控模块发生狗叫，则立即切换到备控模块工作。

3.3 主备切换

主备模块的切换是由硬件逻辑来控制完成的，具有快速性和稳定性。两个控制模块之间通过硬件连线互通状态信息，当主控模块发生故障时，由硬件逻辑控制自动完成切换，并且通过硬件连线把状态信息上报给当前的主控模块。切换方式包括自动切换和强制切换。自动

切换是由模块内部的逻辑控制，根据模块运行的状态信息来判断，自动完成切换，不需要外部干预。强制切换是由操作人员根据自身对当前系统运行状态的判断，通过离散量开关的方式强制执行切换。主备切换状态转换图如图 2 所示。

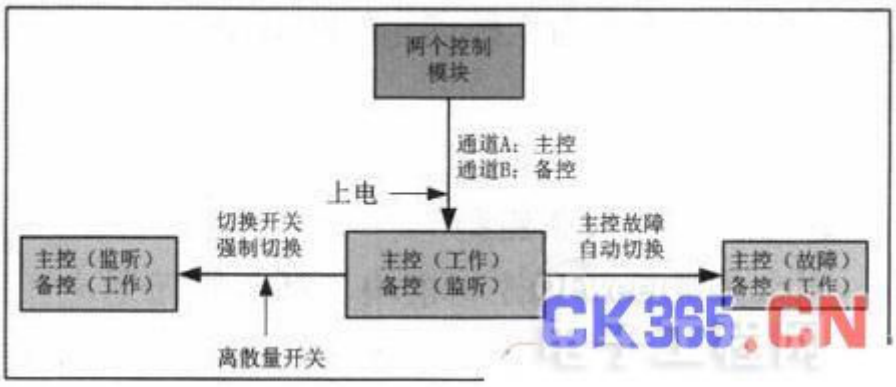

图 2 主设备切换状态转换图

4 总结

采用双主机冗余的显示控制系统，具有故障检测、自动故障切换控制的能力，提高了系统的可靠性。双主机冗余设计在一定程度上增加了系统的复杂度、功耗、重量以及成本，但是能够换来相对较高的可靠性，系统工作的连续性，能够满足航空电子设备的高可靠性要求。