

无线动态重构系统的可靠性设计

陈梅, 邓胡滨, 李津发

(华东交通大学 信息工程学院, 江西 南昌 330013)

摘要: 以小气候环境监测系统的嵌入式移动前端设备无线动态重构应用为例, 给出了一种动态重构系统的硬件可靠性设计方案。

关键词: 动态重构 可靠性 冗余设计

无线动态重构系统用于地域分散、地形复杂、范围广、距离远且监测点移动的场合, 解决维护难度和工作量很大的问题。该项研究以江西省科技攻关项目《樟树道地中药材基地产业化建设 GAP 支撑系统的研究与设计》的中药材基地环境监测子系统为研究平台。在该项研究过程中, 要实现远程动态重构, 其至关重要的一项工作就是系统的可靠性研究与设计。与没有动态重构功能的系统相比较, 无论从硬件还是软件设计上都较之复杂, 而系统的复杂性与可靠性之间始终存在尖锐的矛盾。因此, 如何在复杂系统中提高其可靠性一直以来是研究的热点问题。

为了提高系统的可靠性, 提出了两种方法: 容错和避错。其中容错是指当系统中某些指定的部件出现故障时, 系统仍能完成其规定的功能, 并且执行结果不包含系统中的故障所引起的差错。其基本思想就是在系统中加入冗余资源来遮蔽故障的影响, 从而达到提高系统可靠性的目的。而避错只是试图构造出一个不包含故障的完美系统, 要做到这一点实际上是绝对不可能的^[1]。因此本文可靠性的研究主要是探讨如何使系统能容错。

1 无线动态重构系统的软硬件架构

该项研究中的动态重构系统是通过 Internet 实现对基于低端微处理器的嵌入式系统远程动态重构功能, 整个系统有四种运行模式: 系统硬件检测模式; 系统硬件重构模式; 正常工作模式; 软硬件升级模式。对装配到现场的嵌入式系统实现动态重构的基本流程为:

(1) 在系统正常工作模式下, 按系统内部定时或远端用户的需要, 调用系统硬件的检测程序, 进入系统硬件检测模式。

(2) 系统的检测结果通过 Internet 网络送往远端用户。

(3) 根据系统中的硬件错误报告, 或者应系统硬件功能扩展的需要, 用户在本机上生成系统重构的软件、驱动程序文件和硬件逻辑数据。

(4) 具有对系统操控权限的用户通过 Internet 网络, 下载相应文件到嵌入式前端系统中。

(5) 嵌入式前端系统接受并存储下载的文件数据。

(6) 进入系统软硬件升级模式, 对软硬件进行升级。

(7) 微处理器调用下载驱动程序, 进入对系统硬件重构模式。

(8) 系统重构完成后, 再调用自检程序检测系统重构后的状况, 并向远端用户报告系统重构的情况。

(9) 系统自检成功后进入正常的运行状态, 否则重新进行重构。

根据上述流程, 可将设计内容归结为以下几个重要方面: 嵌入式系统网络连接与系统软固件升级驱动设计、系统硬件资源重构的可靠性与安全性设计。

由于系统的远程重构是通过 Internet 网络进行, 因此首先要进行对低端微处理器的嵌入式系统的网络连接设计。对于嵌入式系统与 Internet 互联网的接入方式以及对协议的研究, 归结为两种不同处理方法: 即内部固化 TCP/IP 协议的单片机方法, 或是由 PC 机/网络芯片作为网关接入 TCP/IP 的网络方法。通过比较可得, 对于 8/16 位的低端微处理器的嵌入式系统建立无线网络则可采用内嵌有 TCP/IP 协议栈的 GPRS IP Modem 代替网络芯片作为网关处理与 Internet 连接的事务, 使 IRL 网络产品使用更灵活, 应用场合更广。在建立好网络后, 再根据对硬件状况检测的结果, 对系统硬件逻辑功能以及相应的软、硬件进行重构和升级的驱动程序设计。

由于系统被挂在网络上, 不可避免地存在对系统控制的安全性问题, 主要有以下几方面: 如对于断电这样的突发性事件, 采用对配置数据在系统上电时的重新配置机制; 对于在网络传输过程中数据的可靠性问题, 采用数据校验与传输应答机制可以解决; 对于下载到嵌入式前端的配置数据与上传到远端监控系统的采集数据的合法性问题, 可以采用对传送的数据进行加密/解密、数据校验、冗余发送、远端比较等方法, 并在各个前端嵌入式系统上设计一个身份标识, 必须保证只有具有权限的用户才能实现对系统的重新配置, 禁止系统被他人任意操控。

要实现嵌入式系统硬件资源重构的可靠性设计,必须在对系统硬件资源冗余设计与检测的前提下进行。对冗余资源的设计不仅包括在系统可编程器件等硬件的冗余,还要进行电路连线资源的冗余设计。针对不同的冗余资源,系统自检也分为两个方面,一是在可编程器件上的硬件检测,二是对系统功能电路及连线的检测。对系统硬件自检后,将自检结果上传给监控中心的上位机,根据自检结果确定系统运转的硬件故障以及系统可用硬件资源。因此,系统硬件资源冗余的可靠性设计是整个动态重构系统设计的基础。

2 嵌入式移动前端模块的可靠性硬件设计

基于 GPRS 的动态重构系统的嵌入式移动前端模块硬件结构如图 1 所示。

CPU 采用具有 ISP/IAP 功能的微处理器 μ PSD3234 提供动态重构时序。由图 1 可知,为使系统具有可重构性,硬件资源和线路的冗余设计主要考虑:(1)可控连接池的设计,实现器件与线路的冗余配套连接;三个传感器与三个放大器 AD620 间、三个放大器 AD620 与 ispPAC30 的两个 PAC 块间、以及 ispPAC30 与微处理器 μ PSD3234 中的 AD 转换器间;(2)ispPAC30 器件及其内部冗余配置。

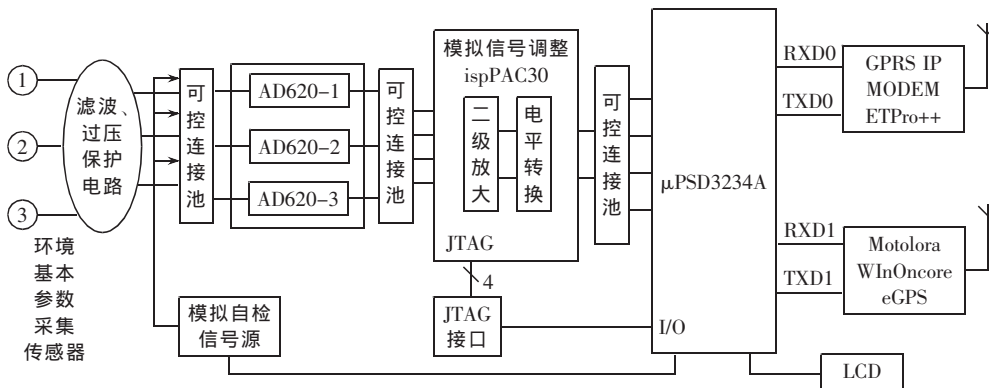


图 1 嵌入式移动前端模块硬件框图

2.1 可控连接池的设计

可控连接池采用 MAX 公司的可控开关矩阵芯片 MAX4573,该芯片具有 11 路单刀开关,每个开关都能在系统处理器控制下通过 SPI 串行总线实现开、合控制。

(1) 自检信号输入到前端环节矩阵

自检信号由前置放大器 AD620 端输入模拟采样电路中。自检信号由系统微处理器上的 I/O 提供,因此对信号的处理不需要进行差分输入处理以抑制共模噪声,采用单端输入即可。连接池如图 2 所示。

(2) 输入信号与前置放大器 AD620 的连接矩阵

三个传感器元件得到的三个信号 A、B、C 与前级放大环节的三个 AD620 进行连接,信号 A、B、C 采用差分输入形式。信号 A、B、C 能分别选择三个 AD620 中的任何一个。连接矩阵如图 3 所示。

(3) 前置放大器 AD620 与 ispPAC30 的连接矩阵

在前置放大器 AD620 与 ispPAC30 连接设计上,三个

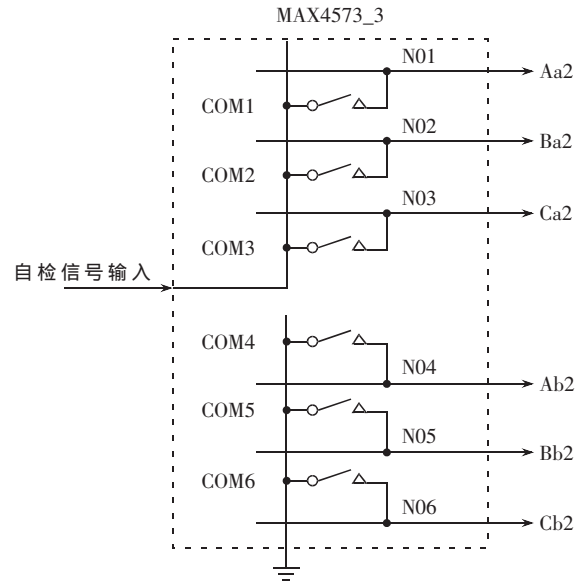


图 2 自检信号输入端矩阵

放大器实现与 ispPAC30 内部 4 个 IA 任何一个都能进行连接,以保障采样电路最灵活的冗余、修改。AD620 输出端与 ispPAC30 的连接矩阵见图 4 所示。

(4) ispPAC30 与 μ PSD3234 的 AD 转换器间的连接矩阵

经前级放大器件 ispPAC30 放大后的信号直接送入微处理器 μ PSD3234 的 4 通道 AD 转换器进行转换,其连接矩阵如图 5 所示。

由于系统微处理器 μ PSD3234 没有提供 SPI 总线接口电路,必须通过软件实现 SPI 总线驱动。因此,利用系统 I/O 口线通过软件来产生 SPI 接口协议的操作时序。在本系统中,通过 μ PSD3234 器件上的 P4.0、P4.1、P4.2 和电路上 6 个 MAX4573 各自对应的片选信号 A1、A2、A3、A4、A5、A6 来进行 SPI 驱动模拟。模拟驱动程序段如下:

MAX_1: CS BIT PA1
AJMP SPI
MAX_2: CS BIT PA2
AJMP SPI
MAX_3: CS BIT PA3
AJMP SPI
MAX_4: CS BIT PA4
AJMP SPI
MAX_5: CS BIT PA5
AJMP SPI
MAX_6: CS BIT PA6
AJMP SPI

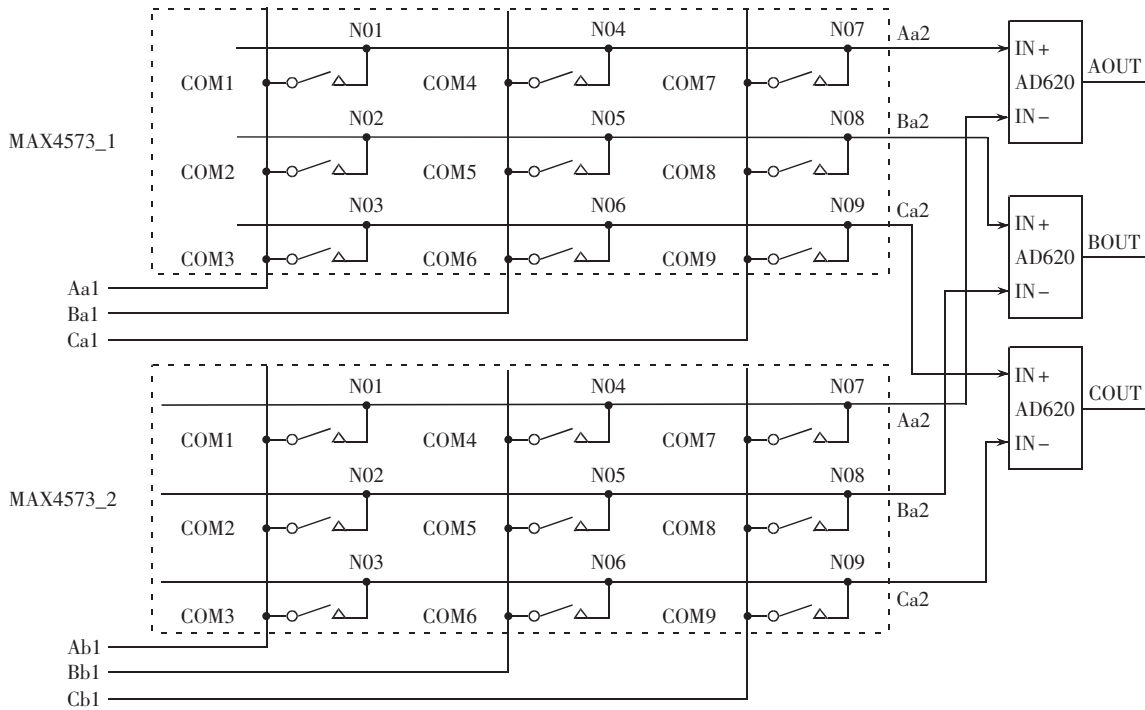


图 3 信号采样输入端与前置放大器 AD620 的连接矩阵

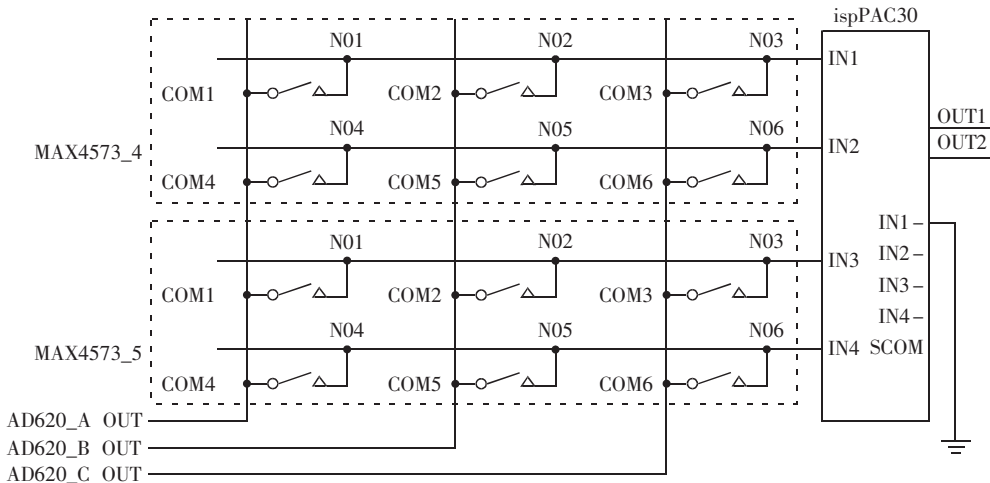


图 4 前置放大器 AD620 输出端与 ispPAC30 的连接矩阵

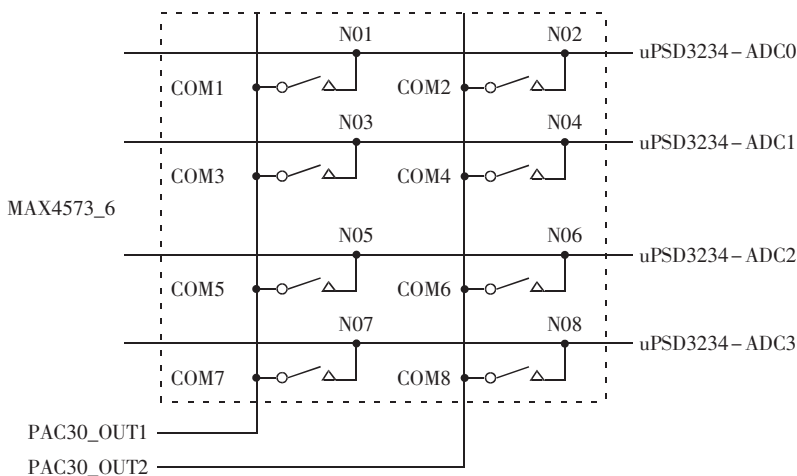


图 5 ispPAC30 与 μ PSD3234 间的连接矩阵

```

SPI: SO      BIT P4.0
          ;对 SPI 引脚进行定义
SI          BIT P4.1
SCK        BIT P4.2
OUTBYTE:   ;数据输出
            子程序
            MOV RO, #08H;
            RO 作计数器, 一个字节
            CLR C
            CLR SCK
OUT:       NOP SETB SCK
          ;产生 SCK 高电平
RLC A;累加器 A 中数据循
          ;环左移
MOV SO, C ;输出数据到 SO 引脚
CLR SCK ;时钟低电平, 数据从 SO 引
          ;脚输出到器件
DJNZ RO, OUT ;8 位数据未输出完,
          ;继续输出
RET
INBYTE: ; 数据输入子程序
MOV RO, #08H
CLR SCK ;产生 SCK 低电平
IN:     MOV C, SI
RLC A
SETB SCK ;产生 SCK 高电平
DJNZ RO, IN ;循环输入 8 位数
RET
    
```

嵌入式技术

2.2 ispPAC30 器件及内部冗余配置

ispPAC30 器件是 Lattice 半导体公司在 2001 年 10 月推出的一个高性能在系统可编程器件和具有动态可重构功能的模拟集成电路,是属于 ispPAC 在系统可编程模拟电路,其可编程性能包括:能对模拟信号进行放大、转换、滤波的功能;能把器件中的多个功能块进行互联,能对电路进行重构;能调整电路的增益、带宽和阈值,如图 6 所示。

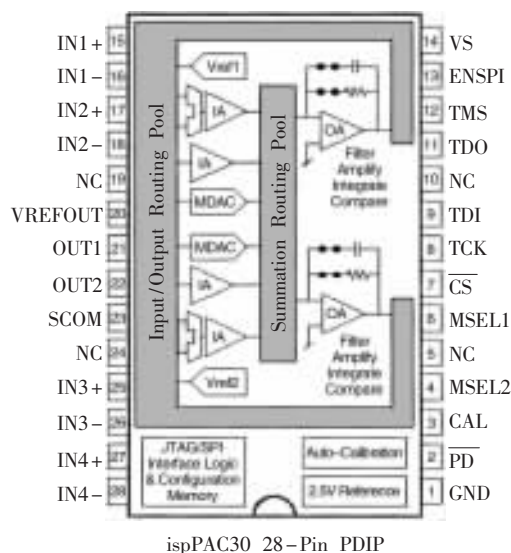


图 6 ispPAC30 内部结构

ispPAC30 内部由两个完全相同的功能块(PAC 块)、模拟布线池(ARP)、自动校准电路、片内参考电源及配置存储器件构成。ARP 实现器件内部互连及与输入、输出引脚之间的灵活连接,从而构成各种电路形式。ispPAC30 内部包含四个输入仪表放大器、两个独立的内部可控参考源(可分 7 级,64mV~2.5V)和两个增强型 DAC。此 DAC 为一种特殊 DAC,输入信号可以为外部模拟信号,也可以为内部模拟信号,还可以是内部 DC 信号,使用非常灵活。另外,ispPAC30 的模拟布线池非常完整,所有 I/O 均可与任何 IA 或 DAC 连接,所有 IA 和 DAC 的输出也可叠加到任何输出放大器上。ispPAC30 增益的调整还可以由内部多个 IA 进行级连实现。

在本设计中,因为需要采用 IA 冗余,因此采用 IA

与 MDAC 编译后的参考电压来实现 ispPAC30 脉冲增益的调整。由 IA1、IA2 和 OA1 构成的第一个 PAC 块,信号通道在起始工作状态下由 IA1 和 OA1 组成,其中 IA2 作为 IA1 的冗余处理。在 IA1 有故障时,通过 IRL 重新配置 IA1、IA2 与 OA1 的连线,用 IA2 取代 IA1,由 IA2 和 OA1 形成通道。同理,由 IA3、IA4 和 OA2 构成的第二个 PAC 块在通道配置上也一样。

ispPAC30 是在系统可编程模拟器件,对 ispPAC30 的配置由上位机的 PAC-Designer 工具产生 SVF 编程文件,直接用于 JTAG 串行链路中。要对 ispPAC30 进行内部配置,就要用 μ PSD3234 的通用 I/O 口与 ispPAC30 的 JTAG 接口相连,可通过软件模拟 JTAG 驱动。但为加快开发进度,在这两个芯片之间连接了一个 FLASHLink 接口模块,由硬件完成对上位监控中心下载来的 SVF 文件的解析及 JTAG 驱动功能。本文给出了一种动态重构系统的硬件可靠性设计的方案。从理论上说,采用冗余设计方案能够达到任何可靠性设计指标。但是,由于冗余元件的增加,相应地也就增加了系统的体积、重量、费用和功耗等。因此,冗余设计是一个可靠性和资源指标权衡的问题。

参考文献

- 1 丁瑾.可靠性与可测性分析设计.北京:北京邮电大学出版社,1996
- 2 汤琳宝,陈恒等.模拟数字可编程器件与电路设计.北京:科学出版社,2003
- 3 郑小军,胡道徐.一种通用的嵌入式系统 ISP 方法.电子技术应用,2005;(7):22~23
- 4 颜荣江.PSD8XXF 的在系统编程技术.电子技术应用,2000;(1):55~58
- 5 陈梅,张永贤.基于 GPRS 的无线动态重构技术的应用研究.微计算机信息,2006;3(3):203~205
- 6 陈梅,李津发.ISP 技术在远程数据采集电路中的应用.华东交通大学学报,2004;(1):60~63
- 7 Architecting Systems for Upgradability with IRL.USA;Xilinx Corp,2001.6
- 8 STMicroelectronics.Flash Programmable System Device with 8032 Microcontroller Core.2002.6
- 9 ispPAC30 Data Sheet.Lattice Corp,2001.8

(收稿日期:2006-05-24)