A-PDF Split DEMO : Purchase from www.A-PDF.com to remove the watermark

基于 IAP 功能单片机的远程更新系统设计

朱飞龙,杨 鸣*
(宁波大学 信息科学与工程学院,浙江 宁波 315211)

摘要:为了提高远程更新的可靠性和有效性,弥补传统更新系统的不足,设计了一种针对具有 IAP(In-Application Programming)功能单片机的远程更新系统。介绍了系统的整体实现框架,并着重描述了单片机内的程序结构、Flash 代码空间内用户代码区的划分和系统安全性的设计;并以 MSP430 单片机为例,利用 C 语言和汇编语言相结合,在 IAP 编程技术和 GPRS 通信技术的基础上,介绍了更新系统的具体实现。样机试验结果表明该系统达到了设计性能的要求,实现了预期的各种功能,能广泛应用于智能仪表等设计中。

关键词:单片机;远程更新系统;IAP;Flash;智能仪表
中图分类号:TH86;TP368.1 **文献标识码**:A **文章编号**:1001-4551(2010)09-0076-04

Design of remote update system based on the SCM with IAP function

ZHU Fei-long, YANG Ming
(College of Information Science and Engineering, Ningbo University, Ningbo 315211, China)

Abstract: Aiming at improving the reliability and validity of the remote update, making up the shortage of the traditional update system, a type of remote update system for single chip micyoco(SCM) with in-application programming(IAP) function was designed. The overall implementation framework of the system was introduced. The program structure within SCM, the subdivision of user code area in Flash code space and the design for system security were mainly described. And taking MSP430 SCM as an example, combining with C and assembly language, the concrete realization of the update system based on IAP technology and GPRS communication technology was further introduced. The test results of the prototype show that the system achieves the requirements of the design performance and realizes the desired functions, and it can be widely applied to various designs, such for intelligent instruments.

Key words: single chip micyoco(SCM); remote update system; in-application programming(IAP); Flash; intelligent instrument

0 引 言

目前,智能仪表的设计主要以单片机为控制核心[1],但是它的设计不可能一步到位,尤其是软件部分,需要不断地进行修改和完善。当程序出错或者用户的需求变更时,传统情况下就需要专业的维修服务人员亲自到设备现场[2],通过 JTAG 口连接笔记本等设备来重新在线烧制程序,整个过程效率低下。

在 IAP 编程技术的带动下[3],各种非现场烧制的程序更新方式逐步出现,如基于 GPRS 技术[4]或电话线技术的远程更新方式和基于 IC 卡技术或 USB 技术的现场更新方式等。其中通过 GPRS 技术来实现程序远程更新的方式,由于其操作方便、更新范围广阔等优点成为最实用的一种方式。因此,本研究通过 GPRS 技术设计一种基于 IAP 功能单片机的远程更新系统。

1 IAP 编程技术

IAP(in-application programming)[5-6]是应用在 Flash 程序存储器的一种编程模式,即在某段程序的控制下完成对 Flash 的读/写操作,可以控制对某段、某

收稿日期:2010-01-18
作者简介:朱飞龙(1986-),男,浙江奉化人,硕士研究生,主要从事嵌入式系统方面的研究. E-mail: zhfl1314@163.com
通信联系人:杨 鸣,男,研究员,硕士生导师. E-mail: yangming@nbu.edu.cn

页、甚至某个字节的读写操作。

在 IAP 编程模式中[7],Flash 存储器可以按照字或字节写入,但是不能按照字或字节来擦除,只能整段擦除,一段为 512 个字节。擦除的方式有段擦除和主存擦除(擦除全部的 Flash)两种,编程的方式有字/字节编程和块编程两种。由于 Flash 在写入和擦除时处于特殊的状态,不能接受访问,因此,擦除程序不能擦除程序本身被保存的段,同样编程的程序也不能向本身被保存的段内写数据,处于被编程或者被擦除过程中的段不能被读出。由于主存擦除指令擦除的是所有的保存程序的存储器,因此必然会擦除到擦除程序被保存的段,从而导致冲突。因此,执行主存擦除的程序只能存放在 RAM 中才能保证程序顺利执行,而段擦除只要被擦除的程序段和执行擦除的程序不在同一段即可。

2　远程更新系统框架的设计

用于智能化仪表的远程更新系统如图 1 所示。PC 机作为数据源,通过串口和 GPRS 模块[8-9]将准备好的更新数据发送出去;智能化仪表的处理器为 Flash 型,具有 IAP 编程模式的单片机,通过 GPRS 模块来接收更新数据[10]。当单片机程序需要更新时,PC 机就发送更新标志信号,单片机接收到更新标志信号之后,将该标志信号存储在 Flash 当中,然后马上复位;接着程序就会进入更新状态,开始接收更新数据并存储;数据接收完毕之后,用新代码将原代码覆盖,从而实现程序的远程更新。系统的数据源也可以是 U 盘,IC 卡等,只要能通过特定的数据收/发模块或数据传输接口将更新标志信号和更新数据传输给单片机,就可以实现程序的更新。本系统的单片机程序部分具有非常强的通用性,适用于各种程序更新系统。

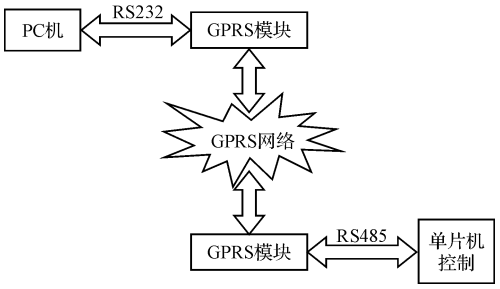

图 1　系统框图

2.1　程序结构设计

由于单片机的程序更新过程完全是自动进行,考虑到系统的可靠性和有效性,单片机内部程序结构就显得相当重要。一般的单片机系统启动之后,直接进入主程序,即应用程序,然后调用各个子程序,进行相应的操作。本系统如果采用一般的程序结构,将有两个不足:①程序更新的优先级和一般应用程序相当,不能保证程序更新的有效性,从而将造成不必要的时间浪费;②程序更新的独立性比较差,应用程序的故障往往也会影响到程序更新。因此就需要设计一种更合理的程序结构。

笔者从本系统所对应的单片机存储器结构中发现,整块 Flash 地址从低到高分别是:特殊功能寄存器、外围模块寄存器、数据存储器、程序存储器和中断向量表。程序存储器当中又可以分成用户代码区和系统 BOOT 区,系统 BOOT 区位于用户代码区之前,用户代码区用于存放用户的程序。单片机系统如无特殊操作,启动之后直接从 0 地址跳转到用户代码区执行应用程序,即主程序。而在本系统中,笔者设计了一种与一般单片机系统不同的程序结构。系统程序结构框图如图 2、图 3 所示。

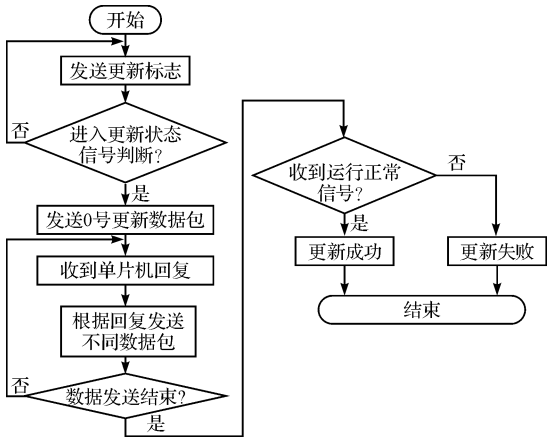

图 2　PC 机程序结构框图

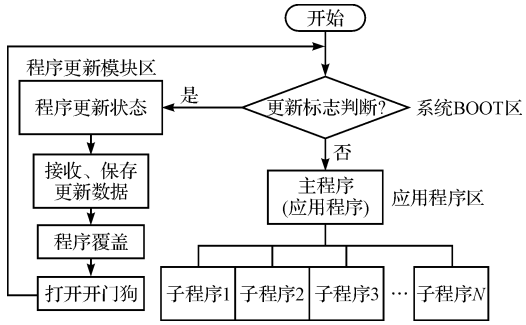

图 3　单片机程序结构框图

如图 2 所示,在本系统当中,PC 机首先通过 GPRS 模块发送更新标志信号[11],在收到单片机回复之后,进行是否收到进入更新状态信号的判断,如果没有,则继续发送更新标志;如果已经收到,则开始发送 0 号更新数据包。然后根据收到的单片机的不同回复发送不

同的数据包,直到数据发送结束。之后若收到运行正常信号,则表示更新成功,否则表示本次更新失败。而在单片机端,如图 3 所示,开始执行之后,首先在系统 BOOT 区内进行是否收到更新标志的判断,如果已经收到更新标志信号,则进入程序更新状态进行更新数据的接收保存,程序的覆盖,然后通过打开开门狗来复位系统;若没有收到更新标志信号,则进入主程序,即应用程序,执行相应的程序功能。一般情况下,程序都在应用程序中运行,当通过中断程序接收到更新标志信号,并通过校验时,就将该更新标志信号存储在 Flash 的某一地址上,并立即复位。复位之后根据前面所对应 Flash 地址上的信号来判断是否进入程序更新状态。这样就使得程序更新的优先级比一般应用程序更高。从逻辑上分析,也使程序更新和应用程序完全独立,互不影响。无论应用程序出现什么故障,都保证了程序更新工作正常,大大提高了系统的可靠性。其中图 3 当中所涉及到的主程序位于应用程序区,进入程序更新状态之后的操作都在程序更新模块区中进行,而应用程序区和程序更新模块区都处于用户代码区当中,具体情况将在 2.2 节中介绍。

2.2 Flash 空间划分

为了使程序更新和应用程序更加独立,方便操作 Flash,本系统将 Flash 空间中的用户代码区分成 4 个区,分别为应用程序区(主程序区)、更新数据区、备份区和程序更新模块区。

分区示意图如图 4 所示,将整个用户代码区的长度作为 L,从 0 位置开始到 $1/3L$ 位置处为应用程序区,即主程序区,存放的是用户的具体功能程序代码,也是程序升级中需要覆盖的主要部分;从 $1/3L$ 到$2/3L$ 处是更新数据区,用于存放接收到的并经过校验的更新数据;从 $2/3L$ 处开始为备份区,当数据代码接收完毕进行程序覆盖之前,考虑到系统的安全性,先将原程序进行备份;中断向量区为系统固有的 32 字节,在中断向量区所在段的正上方是程序更新模块区,主要包括数据的校验、收/发操作和执行 Flash 的擦除、写入操作。这两部分的程序代码分别放在不同的段,其中执行 Flash 擦除、写入操作的程序代码固定在 Flash 当中;执行数据校验、收/发的程序代码只有在需要对数据传输协议进行更新时才会进行覆盖。程序更新模块区的存在使得在理论上可以对具有 IAP 功能的单片机进行无限次的程序更新。上述所描写的 Flash 分区框架几乎适用所有具有 IAP 功能的 Flash 型单片机。

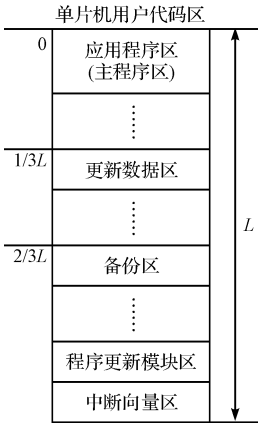

图 4 4 分区示意图

2.3 系统安全性设计

系统的安全性设计是整个设计的重点。本系统的程序更新失败有两种情况:一种是发生在程序覆盖之前,由于网络、数据传输错误等常规原因造成,通过数据校验或开门狗设置等手段,程序就会自动退出更新状态,执行原程序;另一种是发生在程序覆盖之后,由程序代码出错造成,造成代码出错的原因有两个:①传输的数据本身就有错误;②代码覆盖时发生错误。这时,程序就会进入死机或死循环状态。但由于开门狗的存在,系统会自动复位,重新运行之后由于相同的原因又会马上复位,造成频繁复位现象。当发生频繁复位时,系统就会进入备份区,恢复备份程序。

频繁复位的判断方法为:程序启动时,在 Flash 的某个位置作一个复位标记,在程序的末尾部分将此复位标记消除。如果发生频繁复位,程序就无法运行到末尾,复位标记就会逐渐增多。因此只需要在程序复位时,对复位标记的数量进行观察就可以确定是否发生了频繁复位。当程序覆盖完成、系统复位之后的执行流程如图 5 所示。程序覆盖完成,系统复位之后,先对是否发生频繁复位进行判断,如果没有发生,则直接运行新程序;否则就跳转到备份区,执行备份程序,用原来的程序来覆盖当前的新程序,最后打开开门狗使系统复位。

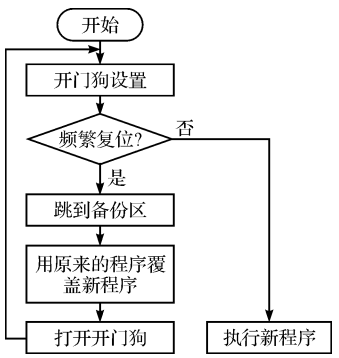

图 5 程序覆盖后流程图

3　系统的实现

在本系统当中,首先是对系统 BOOT 区进行操作。这部分的代码需要用汇编语言来编写,主要是对更新标志信号的判断,在实现过程中需注意地址的跳转。参数的传递采用通过固定存储区传递的方法[12]。其它部分都在用户代码区中进行,为了操作的方便,都用 C 语言来编写[13],下面是以 MSP430149 单片机为例的相关程序:

```
//*****************************************
    //BOOT 区的操作代码
    #include "msp430.h"
    ORG      000000h
    JMP      zhuan
    ORG      000A0h
    EXTERN main ;   //定义 C 语言函数的名称
    DC16     judge ;  //定义复位时的起始位置
    zhuan:          //此函数让 PC 顺利的进入 BOOT 区
    MOV.W   #0C00h,R10
    BR R10          //采用长跳转指令
    ORG 0C00h
    JMP judge
    ORG   0D00h
    judge:
    ……  //进行是否收到更新标志的判断
    JMP main     //跳转到用户代码区执行 C 语言代码
    ORG     1100h
    END
//*****************************************
    //main.c 文件
    #include <msp430x14x.h>
    #include"flash.h"
    ……
    int main( void )
    {
        ……
        m = updata(aRxBuff2,133);  //调用   updata 函数,实现更新数据的存储和程序的覆盖
        ……
    }
//*****************************************
    //flash.h 文件
    #ifndef __FLASH
    #define __FLASH
    ……
    unsigned char updata(unsigned char aRxBuff2[133], unsigned charNRxBuff2);
    //声明 updata 函数,供 main 函数调用
    ……
    #endif
```

4　结束语

本系统有机地结合了 IAP 编程技术和 GPRS 技术,在单片机内通过采用与一般方式所不同的程序框架结构、Flash 中用户代码区的 4 分区划分和系统安全性的设计,实现了智能仪表中程序的远程更新。研究结果表明,本系统相比于传统更新系统,性能更加优越,有效性和可靠性得到大大地提高,在实际工程应用当中具有一定的参考价值。本系统所提出的单片机程序框架结构适用于多种数据源,实际应用范围非常广阔。

参考文献(References):

[1] 彭华成,何岭松,许晓晖,等. 智能仪表软件远程升级的技术实现[J]. 机械与电子,2007(6):61 – 63.

[2] 王学虎,王少荣. 电力系统设备远程程序升级解决方案[J]. 电气应用,2007,26(7):39 – 42.

[3] 黄家升. 基于 IAP 的单片机软件远程升级[J]. 舰船电子对抗,2007(3):95 – 107.

[4] 胡静静. 实现基于 GPRS 的无线远程 IAP 功能[J]. 单片机与嵌入式系统应用,2005(6):21 – 24.

[5] 姜晓梅,李祥和,任朝荣,等. 基于 ARM 的 IAP 在线及远程升级技术[J]. 计算机应用,2008(2):519 – 521.

[6] 洪新旺,龙永华. P89C668 单片机 IAP 功能在淮氏硬度测量仪中的应用[J]. 机电工程技术,2008,37(8):48 – 50.

[7] 袁　璐,宋　华. 基于 Zigbee 和 IAP 的在线升级方案[J]. 测控技术,2008(10):79 – 82.

[8] 吕　鑫,王　忠. GPRS 数据传输模块的设计与实现[J]. 现代电子技术,2008(9):18 – 20.

[9] 侯益坤,熊春如,刘益标,等. 基于 ATmega128 与 GPRS 的远程数据采集系统的设计[J]. 机电工程技术,2009,38(6):50 – 51.

[10] PYLARINOS J, LOUVROS S, IOANNOU K, et al. Traffic analysis in GSM/GPRS networks using voice pre-emption priority[C]//Proceadings of the 7th WSEAS Interational Conference on Mathematical Methods and Computational Techniques in Electrical Englneering, Sofia Bulgaria,2005:120 – 123.

[11] STAEHLE D, LEIBNITZ K, TSIPOTIS K. QoS of internet access with GPRS[J]. **Wireless Networks**,2003(9):213 – 222.

[12] 秦　龙. MSP430 单片机常用模块与综合系统实例精讲[M]. 北京:电子工业出版社,2007.

[13] 张　晞,王德银,张　晨. MSP430 系列单片机实用 C 语言程序设计[M]. 北京:人民邮电出版社,2005.

[**编辑**:柴福莉]