基于 GPRS 网络的 MSP430 单片机 Flash 远程更新方法

陶维青，王付军
（合肥工业大学 电气与自动化工程学院，合肥 230009）

摘要：MSP430 单片机具有可在线编程的特点，通过嵌入式 GPRS 模块的通信功能和电力监控终端（TTU）自身具有的存储芯片（AT24C1024），实现了对基于 MSP430F449 的 TTU 程序的远程在线更新。详细介绍了远程更新的原理、上下位机编程方案及注意事项。实际检验表明，升级稳定、可靠。

关键词：MSP430 单片机；在线编程；串口；电力监控终端；GPRS
中图分类号：TN92 **文献标识码**：B **文章编号**：1001-1390（2007）07-0033-04

The method of updating flash of MSP430 microchip remotely based on GPRS network

TAO Wei-qing, WANG Fu-jun
（Institute of Electric Engineering and Automation, HeFei University of Technology, Hefei 230009,China）

Abstract: MSP430F449 microchip can program itself in-system. Because of the characteristic, updating programs of Transformer Terminal Unit （TTU) based on MSP430F449 remotely through GPRS communication module and a memorizer AT24C1024. Made detailed explanation for the principle of updating flash and providing the method of programming. Through practice, the updating is stable.

Key words: MSP430microcomputer; In-system programming; UART; TTU; GPRS

0 引 言

在很多嵌入式终端的应用系统中，自动化、智能化、便于维护是需要首要解决的问题。已经安装的设备，当程序出现缺陷，或者用户提出新的需求，则需要对单片机程序进行更新。通常的方式是取下设备，通过仿真器来更新程序。但这种方式效率低，特别是对于一些安装在高压、高空环境的设备，作业危险性大。考虑到很多设备具有通信信道，故远程更新程序是智能设备的必然趋势和要求。

MSP430 系列 Flash 型单片机，其 Flash 存储器可以在不外加编程电压的情况下，进行自擦写。通过 MSP430 的串口通信，设计了上下位机程序。借助嵌入式 GPRS 模块进行通信，接收上位机代码，实现了 MSP430 单片机程序远程在线更新。

1 MSP430Flash 的特点及自编程技术原理

MSP430 系列单片机的 Flash 都有两段信息段和 X 段 512 字节的主存和 2K 的 RAM 构成，不同型号 X 值不同。用来存放程序代码、数据表格以及用户信息，可多次擦除和写入，并且可在正常工作电压（2.7~3.6V）下擦写[1]，然后再以字或字节模式写入。

自编程技术就是在 Flash 主存中自定义一段，放置升级代码。即擦写 Flash、读取存储器或者通信程序。升级时运行这段代码擦写 Flash 的应用程序段，实现在线自编程。

2 系统升级通信路径

AT24C1024 是容量为 128K 的基于 I2C 总线协议的 EEPROM，不升级时用来存储历史和统计数据[2]，每页 256 个字节，共 256 页。用 MSP430 的两个 I/O 口模拟 I²C 总线实现对 AT24C1024 的读写。如图 1 所示，PC 先通过 Socket 资源和终端的 GPRS 模块通过 PPP 协议建立连接。然后通过 Internet 和移动的 GPRS 网络把升级代码发到 GPRS 嵌入式模块，接着再通过

RS232 总线传到 MSP430F449 的内部串口，把代码先存到 AT24C1024 中，经校验无误，才启动下位机升级程序。但实际的通信链路和通信协议可能有所差别。

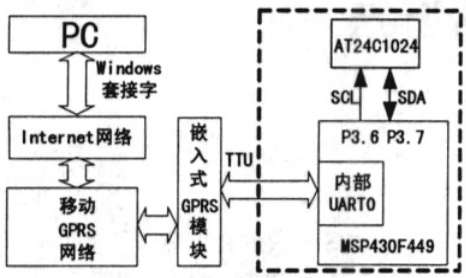

图 1 远程升级系统的通信路径

3 GPRS 模块设计

嵌入式 GPRS 模块设计包括无线发射模块和网络协议解析部分，我们采用西门子公司的 MC39I 作为发射模块。用以色列网络协议芯片 CO110 作为网络协议解析。MSP430F449 通过串口和 CO110 相连，MSP430F449 的数据在网络中是透明传输的。主站可以和多个终端建立多个 Socket 连接，终端上线后自动向主站发送地址标识。主站据此来区别是哪台终端上线。

4 升级操作步骤

4.1 改写.XCL 链接文件

在安装 MSP430 编译环境 IAR 的目录下，找到 lnk430F449.xcl，用 IAR 打开，修改为：

```
-Z(CONST)UPDATECODE=1100-18FF
-Z(CODE)CSTART=1900-FE00
-Z(CODE)CODE=1900-FE00
-Z (CONST)DATA16_C,DATA16_ID,DIFUNCT,CHECKSUM=1900-FE00
-Z(CONST)MYRESET=FFDE-FFDF
-Z(CONST)INTVEC=FFE0-FFFF
```

也就是从 Flash 的地址 0x1100-0x18FF，划出 2K 的空间，命名为 UPDATECODE 段，作为存放自己编写的烧写 Flash 和读 AT24C1024 存储器的代码。

4.2 生成 TXT 格式程序文件

在 IAR 工程的 options 中，选择 XLINK，然后在 Format 中选择 Other，输出格式选择 msp430-txt，这样经编译就生成了 TXT 格式的程序文件。在 Debug 下的 Exe 文件夹中可以看到生成的 TXT 程序文件。第一个 @1100 到第二个 @1900 之间的代码，是我们编写的升级程序，这部分代码只需第一次用 IAR 烧写进去，以后不需更新。第二个 @1900 到最后一行出现的 q 之间的代码，基本都是应用程序代码，这部分需要更新；校验和 CHECKSUM 代码，每次的长度和数值可能都不一样，是每次程序改动后要变化的代码，但这部分可以写入也可不写进 Flash；剩下的到最后一行 q 字符前面的是中断向量的在 Flash 中的地址和中断函数的入口地址，程序改动后，函数的入口地址可能发生变化，所以中断向量下的内容必须更新。

4.3 下位机升级代码的编写

4.3.1 编写引导函数

描述为：

```
void main()@"UPDATECODE"
{ If(*0XFFDE ==0XFFFF)update();
 Application(); }
```

@"UPDATECODE"作用是将该函数定位到 Flash 的 UPDATECODE 段，该函数内部所调用的函数也应定义为类似的形式。这样就保证了引导函数在自定义的 UPDATECODE 段，下次编译的时候这部分函数在 Flash 中的位置才不会变，函数的入口地址也不会变。

4.3.2 应用程序修改

在原有工程通信协议的基础上，添加传送 TXT 升级文件的代码，本设计采用 IEC60870-5-101 协议的帧格式，上位机起始帧包含 TXT 文件的 @ 个数 N，存到 AT24C1024 的信息页的第 0 个页内字节，N 可以用来作为读写 AT24C1024 的结束参数。信息帧包含 @ 后面的两个字节的要烧写的 Flash 的起始地址，和 @ 后面的十六进制代码的个数，以及计算好的要存入 AT24C1024 的起始页和结束页地址，最后一页的字节数和该帧的校验和。具体存储格式如图 2，并且每帧都包括要写到 AT24C1024 的页地址和页内地址，写多少个纯数据。以及每帧的校验和。如果本帧错误，最大重传三次。这是必要的，因为 GPRS 网络存在分组丢失，并可能引起 TCP 的拥塞控制 [3]。通信完成后从 AT24C1024 读上位机传下来所有数据，求其累加模 256 校验和，并将校验信息传回上位机。如果错误，在上位机界面提示错误信息。如总校验错，则不发升级

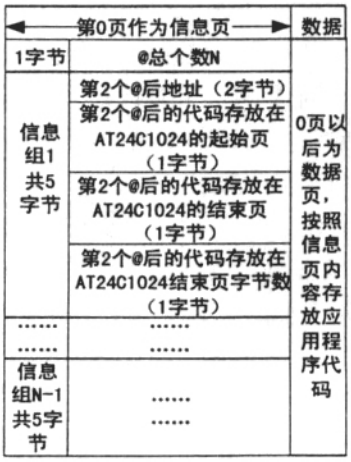

图 2 应用程序代码在 AT24C1204 存放格式

命令，接着重新传送。

4.3.3 升级代码编写

编写 __monitor void update ()@"UPDATECODE" 函数，__monitor 类型标识，定义为原子操作，函数执行的时候不会被打断[4]，并且函数调用时入口先入栈，返回时使用 RETI 返回，编译器根据进栈逐个弹出寄存器，这样函数的返回不会在升级空间以外的 Flash 空间。如图 3。接到上位机启动升级命令后，进入升级函数，根据 AT24C1024 的信息页中的要写入 Flash 的地址信息，读取后面的数据页的程序代码写入相应 Flash 地址空间。

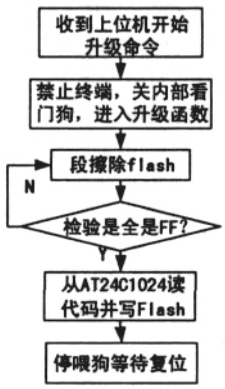

图 3 下位机升级程序过程

应注意：

(1) 首先字节模式擦除 0XFFFE 后两个字节，并把引导函数入口地址写入．并且擦除 MYRESET 后两个字节内容．而后用段擦除 [5] 模式，擦除 0x1900-0XFE00 中的所有段。最后写完所有的段之后，再把引导函数入口地址写入MYRESET 后的两个字节中，此地址可以在 IAR 编译环境软件仿真反汇编视图中看出。具体擦写 Flash 的代码请参考文献[4]、[5]。

(2) 连续擦除时，每擦除一段后，空写启动擦除的指针应该加 512，而最好不用采取乘的方式。避免乘法、移位等大量占用堆栈的操作导致程序跑飞．

(3) 应关闭内部看门狗，并且禁止中断，如果有外部硬件看门狗监控芯片，应擦除一段就喂一次外部看门狗。

4.4 上位机程序的编写

上位机采用 MFC 对话框编程，关键是对升级 TXT 文件的处理。升级文件中，每个 @ 后是要写入的十六进制的 Flash 首地址，所以升级是要把第二个 @ 后的代码（即程序段，校验和，以及中断向量）放入相应的 Flash 地址中，文本文件读取采用 ifstream 流十六进制输出，每帧的总字节为 256 个，纯 TXT 文件数据 235 个，具体如图 4 所示。开始时先写一个函数计算 @

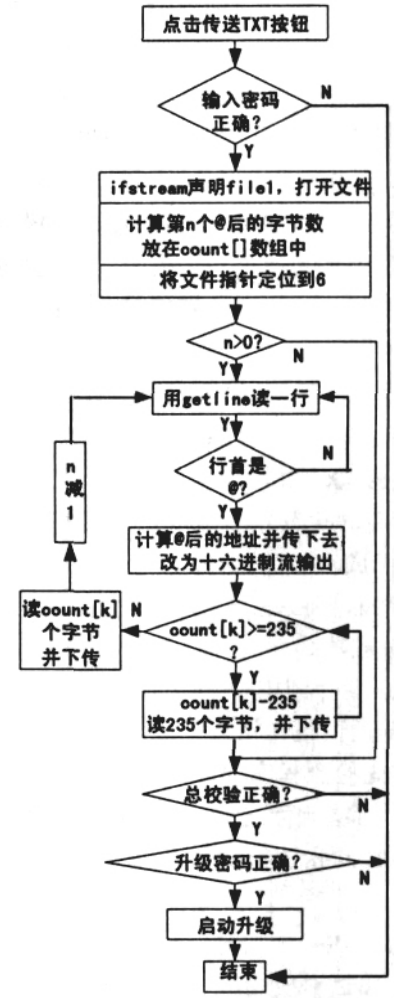

图 4 上位机读取升级文件流程图

的个数，作为文件结束的标志，@ 后的代码长度作为十六进制输出的计数，然后把文件的指针定位到 6，是为了跳过第一段不用更新的代码，因为从 @1100-@1900 之间的代码不用升级。具体帧结构可在用户数据域定义为如表 1 结构。不管什么协议，用户数据区都是可以自己定义的。这样可以在传输协议改变的情况下可方便的进行代码移植。

表 1 数据域帧结构

……
升级标识（如升级起时帧、数据帧、信息帧等）
满帧（235 纯数据）和非满帧标志
本帧要写入 AT24C1024 的页地址
本帧要写入 AT24C1024 的页内地址
TXT 文件数据
……

5 调 试

首次调试可以先在 IAR 仿真器环境下进行，先模

拟 TXT 升级文件的大概格式构造一个比较小的文件，然后传送，保证存储在 AT24C1024 里面的数据正确，然后在仿真器下设断点观察擦写，从 Memory 里面可以直接看到，正确后再验证从 AT24C1024 的读的数据。本系统每次读 256 个字节，也就是 AT24C1024 的一页，写 Flash 的时候字节写入，只要保证每段程序的首地址正确即可。写入速度快，50K 大小的程序大约半秒就可以完成。在 Memory 里面观察 Flash 里面的数据是否为你的预想格式。完成这些后可以再次烧写程序，如有外部看门狗，把跳针加上让外部看门狗工作。然后修改应用程序，如指示灯原来不亮改为亮等。重新编译，把生成的 TXT 文件放在上位机升级程序的目录下，观察升级后的状态并进行相关功能测试。

为确认升级成功，宏定义一个软件版本号，每次程序改动后改变软件版本，升级后，主站通过遥测软件版本确认升级成功。

如擦写 Flash 过程中停电或擦写失败，则重新上电或外部看门狗的监视作用会复位单片机，复位后进入引导程序，首先检测程序的入口地址，若为 0XFF，则调用升级函数，擦写函数会再次从 AT24C1024 中读取升级 TXT 文件，再次进行烧写。

6 应 用

在同一个工程中，添加升级代码，第一次通过仿真器烧入程序。以后对应用程序的改动都可以通过远程更新。利用上面的远程更新技术，已经实现了在带有 GPRS 通信终端的电力监控终端的程序的远程更新。50K 的程序代码大概需要 8 分钟更新完毕。该种方案适合所有的以 MSP430Flash 型单片机开发的嵌入式系统的程序升级。对其它能自编程的单片机也具有借鉴价值。如果代码较小，可以先把升级代码下载到 MSP430 本身的 Flash 中。随着通信技术和自编程处理器的不断发展，远程更新也会得到更广泛的应用。

参 考 文 献

[1] 沈建华,等. MSP430 系列 16 位超低功耗单片机原理与应用[M].清华大学出版社,2004.

[2] 陶维青,马小陆.基于 430 单片机的新型配电变压器远方终端的开发[J].继电器,2005,33(19).

[3] [美]里吉斯著,朱洪波等译.通用分组无线业务(GPRS)技术与应用[M].人民邮电出版社,2004.

[4] 张 晞,等.MSP430 系列单片机实用 C 语言程序设计[M].人民邮电出版社,2005.

[5] 美国德州仪器.MSP430 Flash Self-Programming Technique [Z], SLAA103.2004.

作者简介:

陶维青(1964-),男,合肥工业大学电气与自动化学院副教授,长期从事电力系统及其自动化方面的研究。

王付军(1984-),男,硕士研究生,研究方向为计算机控制与网络控制。
Email:wfj5126474@163.com

收稿日期:2007-04-12
(丘 源 编发)

(上接第 24 页)

实验表明该方法能有效地对机械转子实验台状态进行在线监测识别。当簇中部分传感节点出现异常时，该网络结构能监测识别其他机械转子实验台的工作状态。基于分簇结构的无线传感网络状态监测识别方法能适应监测环境的动态变化，对工业生产中的复杂流程设备工作状态识别是一种有效的识别方法。

参 考 文 献

[1] A.Willig, K.Matheus, A.Wolisz. Wireless technology in industrial networks[C]. Proceedings of IEEE.2005, 93(6):1130-1151.

[2] N. Ota, P. Wright. Trends in wireless sensor networks for manufacturing [J]. International Journal of Manufacturing Research, 2006, 1(1):3-17.

[3] L. Krishnamurthy, R. Adler, P. Buonadonna, et al. Design and deployment of industrial sensor networks: experiences from a semiconductor plant and the North Sea [C]. Proc. of the 3rd international conference on Embedded networked sensor systems, 2005:64-75.

[4] 郭前进, 于海斌, 徐皑冬. 基于状态维修的开放系统研究与实现[J]. 计算机集成制造系统. 2005, 11(3):416-421.

[5] 沈 波, 张世永, 钟亦平. 无线传感器网络分簇路由协议[J]. 软件学报. 2006, 17(7):1587-1600.

[6] J. Zhang, R.X. Li, P. Han. Wavelet packet feature extraction for vibration monitoring and fault diagnosis of turbo-generator[C]. Proc. of the Second International Conference on Machine Learning and Cybernetics. 2003: 76-80.

[7] C.W. Hsu, C.J. Lin. A comparison of methods for multi-class support vector machines [J]. IEEE Trans. on Neural Networks, 2002, 13:415-425.

作者简介:

毕道伟(1983-),男,硕士研究生,研究方向为无线传感网络技术和智能维护系统。

王 雪(1963-),男,博士,清华大学仪器科学与技术研究所所长,从事智能仪器、数据融合和无线传感网络等研究工作。
Email:wangxue@mail.tsinghua.edu.cn

王 晟(1981-),男,博士研究生,主要从事无线传感网络、协作信号处理等研究工作。

丁 梁(1985-),男,硕士研究生,主要从事无线传感网络、信号处理和智能计算等研究工作

收稿日期:2007-05-11
(丘 源 编发)