

基于 STM32 的在应用编程(IAP)开发*

雷卫延 敖振浪 周钦强

(广东省大气探测技术中心 广州 510080)

摘要: 针对嵌入式终端设备程序升级困难的问题,设计了一种基于 STM32 的远程升级方案。该方案系统深入地研究了 Ymodem 协议的通信流程,以及基于 STM32 的在应用编程(IAP)的技术原理和关键技术的实现,关键技术包括程序起始位置和中断向量表设置、APP 程序区 flash 擦除、APP 程序写入 flash、IAP 跳转到 APP 程序等 4 个部分,利用 RS232 标准串口实现了上位机与嵌入式终端设备之间基于 Ymodem 协议的通信,即嵌入式终端设备的远程在线即时更新功能,实际应用表明,该方案具有良好的应用价值和推广价值。

关键词: STM32; 在应用编程(IAP); 应用程序(APP); ymodem 协议; 程序更新

中图分类号: TP311.52 **文献标识码:** A **国家标准学科分类代码:** 510.99

In application programming(IAP) development based on STM32

Lei Weiyan Ao Zhenlang Zhou Qinqiang

(Guangdong Atmospheric Sounding Technology Center, Guangzhou 510080, China)

Abstract: About the embedded terminal equipment upgrade difficult problem, this paper designs a remote upgrading scheme based on STM32. The scheme study the communication flow of Ymodem protocol, and IAP technology principle and IAP function realization based on STM32, including set the initial position and the interrupt vector table, APP program area flash erase, APP program written in flash, IAP jumps to APP procedures and so on. This paper using the RS232 standard serial port realizes the communication between PC and embedded terminal equipment based on Ymodem Protocol, namely embedded terminal equipment real time updates by remote mode. Experiments show that, the design has good application value and extension value.

Keywords: STM32; in application programming(IAP); application(APP); ymodem protocol; program update

1 引言

STM32 系列基于专为要求高性能、低成本、低功耗的嵌入式应用专门设计的 ARM Cortex-M3 内核。随着业务的发展,气象部门新的观测要素不断涌现,采集器的程序代码也需要随之的升级。传统的代码升级方式通常采用 JTAG 或 ISP 接口,需要把采集器寄回厂家,升级过程较为复杂。基于 STM32 开发的新型自动气象站数据采集器,它运行速度快、功耗低、充足的存储空间、有丰富的接口(USB、标准 RS232 串口、以太网、SD 卡扩展口),能够适应业务不断发展的需要。

IAP 是 In Application Programming 的首字母缩写, IAP 是用户的程序在运行过程中对 User Flash 的部分区域进行烧写,目的是为了在产品发布后可以方便地通过预留的通信口对产品中的固件程序进行更新升级。通常在用户需要实现 IAP 功能时,需要在设计固件程序时

编写两个项目代码,第一个项目程序不执行正常的功能操作,而只是通过某种通信管道(如 USB、USART)接收程序或数据,执行对第二部分代码的更新,被称作引导程序,该部分代码必须通过 JTAG 或 ISP 烧入;第二个项目代码才是真正的功能代码,即 APP 程序,该部分代码可以使用 JTAG 或 ISP 烧入,也可以利用第一部分代码 IAP 功能写入。

2 Ymodem 协议

Ymodem 协议作为上位机和 STM32 通信的桥梁,它具有完善的握手机制和出错管理机制,可以大幅提高 IAP 的成功率。

Ymodem 协议是一种发送并等待的协议,即发送方发送一个数据包以后,都要等待接收方的确认。将文件分块的大小定位 1 024 字节,传输请求由上位机发起,每

个传输帧由帧头、数据段、帧尾组成,帧格式如图1所示。上位机软件将数据以每次1024字节加上包头、包号、包号补码、末尾加上CRC校验字段,打包成帧格式传送^[1-2]。



图1 Ymodem 协议分块传输帧结构

Ymodem 协议流程如图2所示。

3 在应用编程(IAP)的实现

3.1 技术原理

对于STM32来说,因为它的中断向量表位于程序存储器的最低地址区,为了使第1部分代码能够正确地响应中断,通常会安排第1部分代码处于Flash的开始区域,而第2部分代码紧随其后,STM32中断向量分布如图3所示^[3-5]。

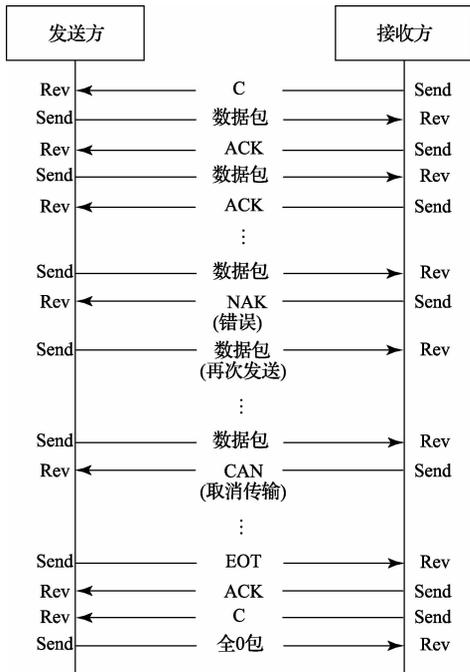


图2 Ymodem 协议通信流程

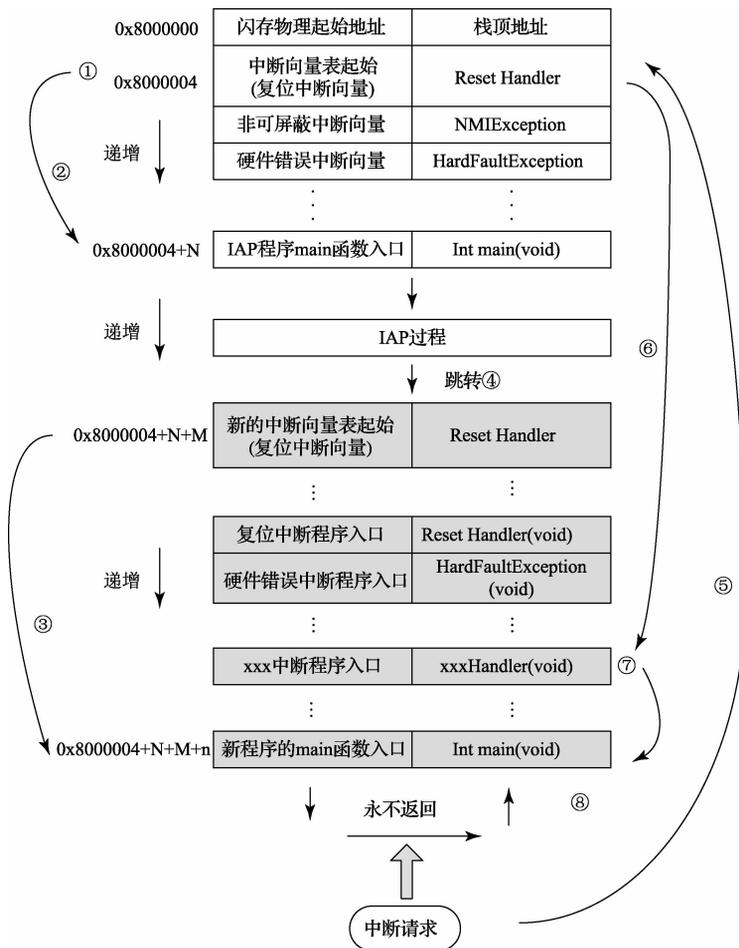


图3 STM32 中断向量分布

STM32 的 IAP 技术原理:

1) STM32 复位后,从地址为 0x8000004 处取出复位中断向量的地址,并跳转执行复位中断服务程序,随后跳转至 IAP 程序的 main 函数,如图 3 中标号①、②所示。

2) 执行完 IAP 后(APP 程序如图 3 中以灰色底纹方格表示,地址始于 0x8000004+N+M)跳转至新写入程序的复位向量表,取出新程序的复位中断向量的地址,并跳转执行新程序的复位中断服务程序,随后跳转至新程序的

main 函数,其过程如图 3 的标号③所示。新程序的 main 函数具有永不返回的特性,即一旦进入 APP 程序,便不会再运行 IAP 的任何代码^[6-7]。

3.2 IAP 关键技术实现

IAP 功能实现流程如图 4 所示。根据 Ymodem 协议,数据固定以每帧 1 024 字节传输,接收端对每帧都会进行 CRC 校验,以确保数据接收的准确性,数据准确无误才会写入指定的 flash 区域。关键技术实现如下。

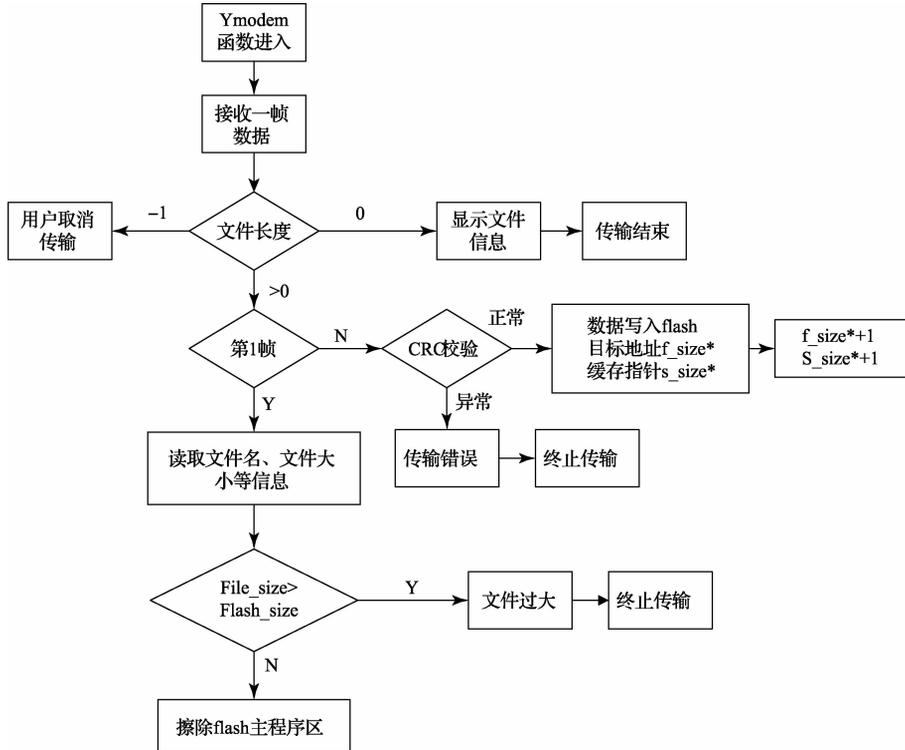


图 4 IAP 功能流程

3.2.1 程序起始位置和中断向量表设置^[8-9]

设置程序起始位置的方法是(keil uvision4 集成开发环境)在工程的“Option for Target...”界面中的“Target”页里将“IROM”的“Start”列改为“程序起始位置”。

IAP 中断向量表设置如下:

```
void NVIC_SetVectorTable(u32 NVIC_VectTab, u32 Offset);
```

```
void NVIC_SetVectorTable(0x8000000, 0x00); // 偏移量 0x00
```

APP 中断向量表设置如下:

```
void NVIC_SetVectorTable(u32 NVIC_VectTab, u32 Offset);
```

```
void NVIC_SetVectorTable(0x8000000, 0x8000); // 偏移量 0x8000
```

3.2.2 APP 程序区 flash 擦除^[10-11]

内置 flash 有 1 MB 的存储空间,分为 12 个扇区,前两个扇区(32K)预留给 IAP 程序,其余的 10 个扇区分配给 APP 程序,因此每次更新 APP 程序之前,都要先擦除分配给 APP 程序 flash 空间。

```
# define FLASH_Sector_2 ((uint16_t)0x0010) //< 第 3 扇区目标地址
```

```
:
```

```
: //< 第 i 扇区目标地址
```

```
:
```

```
# define FLASH_Sector_11 ((uint16_t)0x0058) //< 第 12 扇区目标地址
```

```
# define VoltageRange_3 ((uint8_t)0x02) //< CPU 电压工作模式: 2.7~3.6V
```

```
# FLASH_EraseSector(FLASH_Sector_2, Voltage-
```

```
Range_3); //擦除第3扇区
:
: //擦除第i扇区
:
```

```
FLASH_EraseSector (FLASH_Sector_11,
VoltageRange_3); //擦除第12扇区
```

3.2.3 APP程序写入flash^[12]

IAP程序把接收到的APP程序写入到flash指定的位置,完成代码的更新。

```
memcpy (buf_ptr, packet_data + PACKET_
HEADER, packet_length); //把数据拷贝到缓存地址
指针
```

```
RamSource = (uint32_t)buf; //赋值要写入数据地
址指针
```

```
for (j = 0; (j < packet_length) &&
(FlashDestination < ApplicationAddress + size); j +=
4)
```

```
{ //每次写入4个字节数据
FLASH_ProgramWord(FlashDestination, *(uint32_
t*)RamSource);
```

```
if (*(uint32_t*)FlashDestination != *(uint32_t
*)RamSource)
```

```
{ //验证失败,错误退出
return -2; //返回错误代码
}
```

```
FlashDestination += 4;
RamSource += 4;
}
```

3.2.4 IAP跳转到APP程序^[13-15]

#define ApplicationAddress 0x8008000 //定义IAP入口地址,第3扇区开始

```
JumpAddress = *( _ _ IO uint32 _ t * )
(ApplicationAddress + 4); //赋值 APP 程序地址
```

```
_ set _ MSP ( * ( _ _ IO uint32 _ t * )
ApplicationAddress); // 初始化 APP 程序堆栈指针
```

```
Jump_To_Application (); // 设置完成,跳转至 APP
程序
```

4 实际应用^[16-18]

按照APP更新操作流程图指引,见图5,即使是没有任何开发经验的人员也可轻易实现采集器APP代码的更新。

上位机和采集器(使用STM32F207芯片)用标准RS232串口线连接,在上位机上打开WINDOWS系统自带的超级终端软件,波特率设置为9600、8、无、1、无,在空白处点击右键选择“发送文件...”,浏览查找bin格式升级文件,选择Ymodem协议,点击“发送”按钮,开始发送文件。

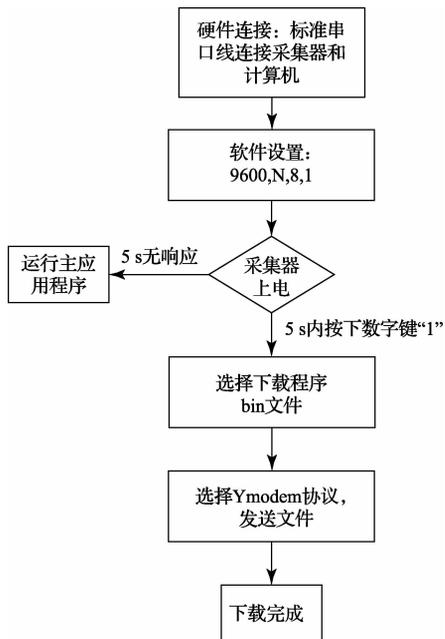


图5 APP更新操作流程

图6为正在更新APP,图7为更新APP成功界面。



图6 正在更新APP

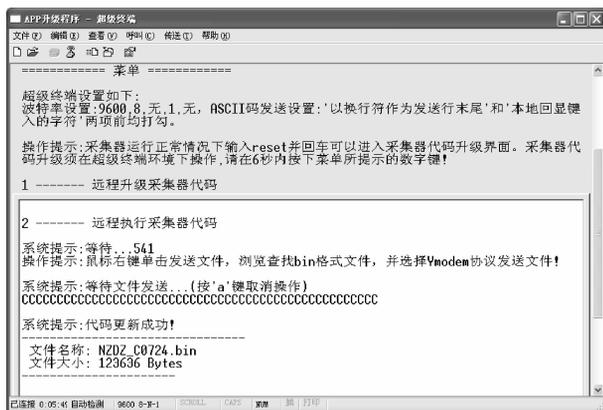


图7 更新APP成功

5 结 论

如果 IAP 程序被破坏,采集器必须返厂拆开机器才能重新烧写程序,这是很麻烦并且非常耗费时间和金钱的。针对这样的需求,STM32 在对 Flash 区域实行读保护的同时,自动地对 Flash 区的前 4 页设置为写保护,这样可以有效地保证 IAP 程序(第一部分代码)区域不会被意外地破坏。

该文开发的基于 STM32 在应用编程(IAP)能够在不改变观测场现有通信方式的情况下,在值班房轻松实现采集器代码的更新,它相对传统的程序升级方式具有较大的优势,能有效节约时间,降低人力成本,提高系统的可扩展性和可维护性,具有良好的应用价值和推广价值。

参考文献

- [1] 吴兆芝. ARM 平台多进程微内核嵌入式操作系统 Ymodem 下载功能设计与实现[J]. 南京晓庄学院学报, 2013(3):79-83,89.
- [2] 戈润栋,马旭东. CAN 总线分布式系统程序的以太网在线更新[J]. 工业控制计算机, 2013, 26(11): 19-20,24.
- [3] 李兴鹤,蔡亮,宋吉波,等. STM32 用户基于 IAP 的程序更新技术[J]. 单片机与嵌入式系统应用, 2012, 12(1):74-75.
- [4] 刘岩俊. 基于 DSP 的嵌入式温度测量系统设计与实现[J]. 国外电子测量技术, 2014, 33(1):78-81.
- [5] 冷雪,周九飞,付金宝,等. 基于 DSP 的生化分析仪温控系统设计[J]. 电子测量与仪器学报, 2011, 25(4): 360-365.
- [6] 彭刚,春志强. 基于 ARM Cortex-M3 的 STM32 系列嵌入式微控制器应用实践[M]. 北京:电子工业出版社, 2011:320-325.
- [7] 左堃. 基于 ARM Cortex-M3 的 Bootloader 技术[J]. 武昌理工学院学报, 2011, 6(3):94-97.
- [8] 孙立新. 基于 Bootloader 的嵌入式软件通用更新机制[J]. 电视技术, 2011, 35(15):89-90,113.
- [9] 吕雪芹,敖振浪,陈冰怀. 基于 VK3234 的共享中断编

程关键技术[J]. 电子测量技术, 2014, 37(4):87-91.

- [10] STM32F2x7 In-Application Programming(IAP) over Ethernet. STMicroelectronics, 2011(5).
- [11] 孙伟,郭宝亮,陈龙. 便携式水听器测试仪的研究与实现[J]. 仪器仪表学报, 2011, 32(2):375-380.
- [12] 李兴鹤,蔡亮,宋吉波,等. STM32 用户基于 IAP 的程序更新技术[J]. 单片机与嵌入式系统应用, 2012, 12(1):74-75.
- [13] 朱传宏,沈严,颜云松,等. 基于 Cortex-M3 的引导程序分析与设计[J]. 计算机与数字工程, 2012, 40(10): 58-59,109.
- [14] 阙凡博. 基于 stm32 的程序远程升级设计[J]. 仪器仪表用户, 2013, 20(5):90-92.
- [15] DAI ZH C, XIANG Y. Design of remote upgrade of equipment monitoring system software [C]. Information Technology and Computer Science (ITCS), 2010 Second International Conference on. IEEE, 2010:462-465.
- [16] 陈峰峰,胡毅,许艳. STM32F10x 在应用中编程的实现方法[J]. 单片机与嵌入式系统应用, 2009(9):25-27,31.
- [17] 徐洋,马跃. STM32F103 系列微控制器在应用编程技术研究[J]. 单片机与嵌入式系统应用, 2013, 13(8): 35-37,40.
- [18] 高金涛,张宏鹏. 可远程升级的 GPS/GPRS 车载终端设计 [J]. 电子设计工程, 2011, 19(21): 155-158.

作者简介

雷卫延,工学硕士,工程师。主要研究方向为信息处理、嵌入式系统应用、上位机系统应用等。

E-mail:leiweiyan@163.com

敖振浪,学士,正研级高工。主要研究方向为气象装备研发、嵌入式系统设计、复杂算法设计等。

周钦强,工学硕士,高级工程师。主要研究方向为数据处理、嵌入式系统应用、上位机系统应用等。