

# 基于无线 IAP 的工业嵌入式系统升级技术应用

彭亮,沈安文,张宁,周立峰

(华中科技大学控制科学与工程系,湖北武汉 430074)

**摘要:**文中研究了工业嵌入式系统的固件程序及应用程序升级技术。基于 IAP 的远程升级技术解决了有线升级和停机升级限制,具备更大的灵活性。以 LPC2368 为例,设计了一款基于无线微波传输的 IAP 升级方案,进行了合理的 Flash 区间分配,并将通信协议引入代码传输进程,提高了抗误码能力,设计了基于断点续传的防死机升级方案,解决了传输中断引起的传输效率及代码安全问题。对升级方案的软件部分进行了全面介绍。实践表明:该方案可靠、高效,在工业控制领域具有广阔的应用前景。

**关键词:**远程升级;IAP;抗误码;断点续升级;ARM

**中图分类号:**TP311 **文献标识码:**A **文章编号:**1002-1841(2013)12-0036-03

## Application of Industrial Embedded System Upgrade Technology Based on Wireless IAP

PENG Liang, SHEN An-wen, ZHANG Ning, ZHOU Li-feng

(Department of Control Science and Engineering, Huazhong University of Science & Technology, Wuhan 430074, China)

**Abstract:** A remote on-line upgrading technology based on IAP (in application program) of firmware program and the application for industry embedded systems was presented. It eliminated the limits of wired-upgrading or down-upgrading, and thus became more flexible. Taking LPC2368 as an example, a kind of project using wireless microwave updating method was designed, with the flash memory space allocated effectively, and error-resisting capacity highly based on Modbus. What's more, breakpoint renewal updating technology which improved the efficiency and enhanced the reliability in data transmission was creatively designed. After that, the update software was introduced in detail. Practice shows that the proposed method is reliable and efficient, and has a broad application prospect in the industrial control field.

**Key words:** remote on-line upgrade; IAP; error-resisting; breakpoint renewal upgrade; ARM

### 0 引言

随着电子技术的发展,以 DSP、ARM 为代表的嵌入式设备广泛应用于现代制造业。与传统 PC 机相比,嵌入式设备使用更灵活,安装更方便,便于裁剪和升级<sup>[1]</sup>。目前,大量的嵌入式设备(例如监控设备<sup>[2]</sup>、通信设备<sup>[3]</sup>、仪表设备)等,大量应用于制造业现场。这些设备往往安装分散,且数量较多,影响设备固件及应用程序升级。

基于嵌入式系统开发的设备可以采用更新 Flash 存储区的数据来实现对自身的软件版本升级<sup>[2]</sup>。IAP(In Application Program)方式是在运行程序的控制下,对 Flash 中某段程序空间进行读取、擦除和写入操作。相比于 JTAG (Joint Test Action Group)和 ISP (In System Program)方式,IAP 更新方式不需要中断设备软件的正常运行,可以读/写 Flash 中其他程序空间代码,甚至可以控制对某段/页的读写操作,为数据存储和固件升级提供更大的灵活性。文中以 LPC2368 芯片为例,采用 IAP 方式实现设备的远程无线升级。

### 1 Boot 简介及 IAP 概述

LPC2300 系列处理器在出厂时,由厂家在片内固化了一段

Boot 代码,控制芯片复位后的初始化操作,并提供对 Flash 编程的方法。Boot 程序可以对芯片进行擦除、编程。在应用编程(IAP)是用户的应用代码对片内 Flash 存储器进行擦除/编程的方法。Boot 装载程序提供了 IAP 编程接口,可以实现对片内 Flash 存储器的编程<sup>[4]</sup>。

通过 IAP 实现对 ARM 芯片片内 Flash 或者片外 Flash 的读取/擦除/编程操作,可以为嵌入式系统提供更广泛的应用,一方面可以方便地实现非易失性数据的存储,将工业设备的运行状态和运行参数写入 Flash 中,便于外部系统或者片内系统的调用;另一方面可以通过 Flash 代码区域的合理分配和 IAP 在线修改运行代码,实现设备运行程序的动态更新及切换。

IAP 不同于 ISP,除了不需要在升级过程中停机以外,IAP 实现 ARM 片内 RAM 的数据到 Flash 空间的数据的相互访问,所以与片外的接口不仅局限于 UART0,还可以方便地通过 SPI、I<sup>2</sup>C 或者以太网进行数据传输<sup>[5]</sup>。设计中,采用无线通讯方式,利用串行接口,实现远程升级。

### 2 无线 IAP 的具体实现

通过应用编程方式实现设备运行程序的更新需要上位机与 ARM 嵌入式系统协调配合,结构图如图 1 所示。上位机负责将要升级的程序进行编译,形成 HEX 文件,之后按照一定的帧格式进行组包,再通过无线传输媒介将数据帧发送到接收

设备;接收设备,即 ARM 嵌入式系统,通过无线接收装置,接收无线信号,对数据帧进行校验,之后存储到片内 RAM 区内进行缓存,完成数据接收以后,启动 IAP,对非当前运行的程序空间进行擦除和编程,实现程序升级。可以采用的无线媒介包括无线电微波信号、GPRS 信号及无线 Ethernet 信号等。

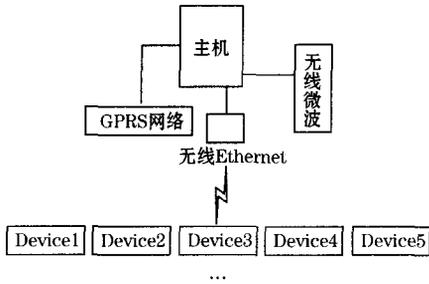


图 1 无线 IAP 升级系统结构

2.1 硬件平台

ARM 分布式设备实现无线 IAP,首先需要 1 套完整的硬件配置,包括 ARM 最小系统,以及无线信号接收外围电路。设计中采用 ZF02P 无线模块(433M ISM 频段内,8 个信道)作为接收电路,硬件结构如图 2 所示。

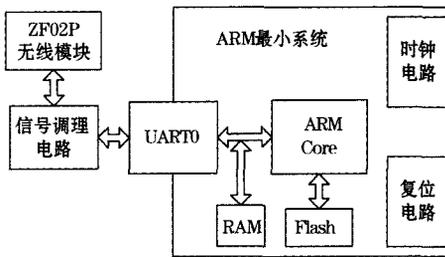


图 2 嵌入式系统 IAP 硬件结构

ZF02P 无线模块接收上位机发送的数据帧,通过串口及处理程序对数据帧进行解析之后,将要更新升级的代码缓存到指定的 RAM 空间。

2.2 IAP 函数的调用方法

IAP 程序是 Thumb 代码,位于地址 0x7FFF FFF0。在 ARM 系统中实现状态转换的指令是“BX Addr”<sup>[6]</sup>,目标地址 Addr 的最低位(bit0)仅来确定最终状态,实际的“目的地址 = Addr & 0xFFFF FFFE”。在调用 IAP 函数时,不仅要实现跳转而且还要完成状态转换,具体 C 代码如下所示。

```
#define IAP_LOCATION 0x7FFFFFF1 // IAP 程序入口
typedef void (* IAP) (unsigned int [], unsigned int []);
// 定义函数类型指针
.....
IAP iap_entry;
unsigned long command[5]; // IAP 命令表
unsigned long result[2]; // IAP 返回值
iap_entry = (IAP) IAP_LOCATION; // 设置函数指针
iap_entry (command, result); // 调用 IAP
```

2.3 分配 FLASH 区间

LPC2368 有 512K 的 Flash 区间,其中 Boot 代码占据 Flash 顶部的 8 KB 空间,余下的 504 KB 可以由用户自己设定存储内容<sup>[6]</sup>。为便于进行读写和擦除操作,Flash 按照大小分为不同

的扇区,表 1 为 LPC2368 的 Flash 扇区配置情况。

表 1 LPC2368 扇区配置

扇区号	扇区大小
0 - 7	4 KB
8 - 21	32 KB
22 - 27	4 KB

在设计中,为了实现系统升级,对 ARM 的片内 512 KB 大小的 Flash 重新分区,如图 3 所示。

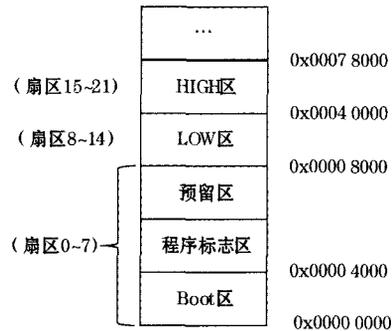


图 3 Flash 区间分配表

Boot 区又叫固件区,存放系统 BootLoader,可以完成代码升级。Boot 区的首地址是 0x0000 0000。

LOW 区及 HIGH 区为程序存储区,可以选择 32 K 倍数大小的空间,设计中选择 224 KB(32 KB × 7)。如果当前运行程序存储在 LOW 区,那么可升级程序存储区为 HIGH 区,如果当前运行程序存储在 HIGH 区,那么可升级程序存储区为 LOW 区。

程序标志区标记当前程序运行区,存储用户程序区的首地址以及升级程序的升级进度。程序标志区的首地址为 0x0000 4000。有用信息仅仅使用该存储区的前 8 个字节。

前 4 个字节为运行标志区,用来保存当前用户代码区的首地址。如果运行标志区为 0x0000 8000,那么说明当前正在运行 LOW 区的代码程序;如果运行标志区为 0x0004 0000,那么说明当前正在运行 HIGH 区的代码程序;如果运行标志区为其他,那么说明当前正在运行固件区的代码程序。

后 4 个字节为升级状态区,用来保存当前升级程序的升级进度。如果前 2 个字节为 0xAA,说明当前升级已经完成;如果前 2 个字节为 0x55,说明当前升级正在进行中,且后 2 个字节表示正在升级拷贝的程序块序号,范围为 0 ~ 1791(设置 Flash 一次升级容量为 256 字节,则 224 KB 对应 1 792 个升级程序块)。

2.4 通讯协议及抗误码设计

系统采用表 2 的数据帧格式作为通讯协议进行通讯。一帧消息由帧头(0xAA)开始,以帧尾(0xFF)结束,其中包括设备号、操作码、升级块编号、数据长度、升级块数据、CRC 校验码等有效信息。

操作码对应每个数据帧的功能,其中 0x04 表示升级数据帧,0x05 表示升级请求帧,0x08 表示升级信息帧,0x10 表示升级完成帧,0x11 表示主动复位帧。通过对操作码的识别可以完

表2 通讯协议帧格式说明

定义	Start	S_ID	O_Ins	B_Num
含义	帧头	设备号	操作码	升级块编号
长度(字节)	1	1	1	1
定义	B_Len	B_Dat	CRC	Stop
含义	数据长度	升级块数据	CRC 校验码	帧尾
长度(字节)	2	0-256	2	1

成不同的主从交互任务。

主从设备之间传输的是要运行的代码,所以小到一个字节的传输错误也会引起非常严重的运行问题。为了保证所编程到 Flash 中的数据正确无误,设计中采用循环冗余码校验(CRC)、应答机制及延时重传机制。采用 CRC16 方式对数据帧进行校验,保证从机设备侧数据帧的误码可靠检测,丢弃误码数据帧,不进行 Flash 编程。主机未检测到从机应答信息,延时 1 s 后重新发送该数据帧,累计 4 次未收到应答,则执行报错机制。

## 2.5 断点续升级防死机设计

在升级的过程中,难免会遇到设备突然断电或者干扰强烈连续误码等引起的升级中断问题。发生此类问题后,由于新版本程序未能全部编程到 Flash 区,所以新版本程序无法运行;另外,由于中断以前,设备已经记录了该次的升级任务,所以约定按照新版本程序进行启动,这样就导致用户程序运行到一半产生问题或者根本无法启动,造成死机。

为避免上面的问题发生,系统采用断点续升级处理方式,包括以下内容:

(1) 在接收到升级请求后,不对运行标志区进行更新,而是在升级任务完成以后修改运行标志区,这样有效避免升级失败时仍运行新版本程序指令。

(2) 在运行标志区以外,设立升级标志区,记录当前的升级状态和当前升级的程序块。

(3) 当发生升级中断以后,设备复位上电,首先查询程序标志区信息,发现升级未完成,且运行标志区仍然为老版本程序首地址,设备会直接跳转到升级程序,并且将当前正在升级的程序块序号发送给主机,主机接收到该信息,将该程序块数据帧重新发送给从机设备,并且继续下去直至升级完成。

(4) 升级完成后,由从机修改程序标志区相关信息,并复位执行新版本程序。这样有效防止升级中断带来的死机问题,并且节省中断引起的时间浪费问题。

## 2.6 整体升级流程

软件流程图如图 4 所示。系统复位以后首先进行串口及数据缓冲区初始化,之后读取程序标记区内的升级标记区数据,判断升级是否已经完成,如果升级状态数据为 0xAA (表明升级完成),则直接跳转到运行标记区所标示的 HIGH 区或者 LOW 区,运行程序代码;如果升级状态数据为 0x55 (表明升级为完成),则直接跳转到代码升级区。

设备在执行用户代码的时,不断检测串口接收到的数据,一旦接收到升级请求,直接保存现场,并且跳转到代码升级区。

运行到代码升级区时,首先读取程序标记区内信息,并按照一定的帧格式将该信息发送给上位机。上位机接收到升级请求之后,根据升级标记区的升级状态信息,选择合适的程序数据进行组包和发送。设备接收到升级数据帧,将数据缓存到 RAM 指定区域,然后进行 CRC 校验,通过校验则将缓存区数据

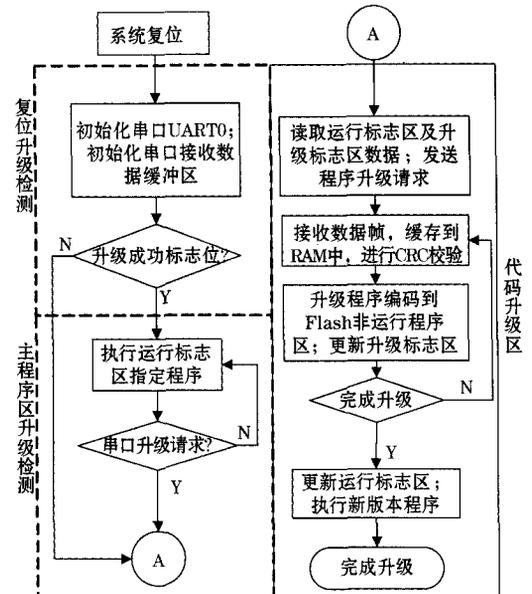


图4 升级整体程序流程图

通过 IAP 函数编程到 Flash 指定地址,并且更新升级标志区内的升级块号数据。当设备接收到升级完成帧以后,更新升级标志区内的升级块号数据为 0,并且将升级状态更新为 0xAA,之后将运行标志区数据更新为新程序地址,最后转到新程序地址区,执行新版本程序,完成升级。

## 3 试验验证

采用该设计方案对现有的水质监测设备进行固件程序升级。新版本程序大小为 196 KB,通过上位机服务器,对 LPC2368 进行运行状态升级,串口传输速度为 9 600 bit/s,连续 10 次升级均成功,平均升级时间为 312 s。在每次升级过程中,人为制造断电事故,重新上电进行续升级均获得成功。在发生一次中断续传事件情况下,除去中断重启时间,平均升级时间为 314 s。试验证明,该方案可以可靠、快速实现远程升级,并且具有中断续升级功能。

## 4 结束语

文中系统地提出了无线 IAP 远程升级技术方案,并以 LPC2368 为例进行具体实现讲解,重点介绍了抗误码设计和断点续传技术以及升级的整体流程和软件方案。通过升级实验,验证了系统的可行性及可靠性,具有很好的应用价值和参考价值。基于该方案的设计,可以考虑采用其他的无线接口进行优化(例如 GPRS),提高数据传输率和传输距离。

## 参考文献:

- [1] 邢涛,刘大成. 嵌入式技术推动工业工程发展的战略思考. 工业工程, 2008, 11(1): 7-10.
- [2] 郑旭东,张培仁,高修峰. 嵌入式网络视频监控系统. 仪表技术与传感器, 2006(8): 24-26.
- [3] 苑玮琦,林峻楠. 嵌入式以太网接口的研究与实现. 仪表技术与传感器, 2008(11): 59-61.
- [4] NXP Semiconductor. LPC2000 secondary boot loader for code update using IAP[M/OL]. [2011-03-15]. <http://www.nxp.com>.
- [5] 张雄杰,张俊奎,潘仕彬,等. 单片机的远程 IAP/ISP 系统设计. 单片机与嵌入式系统应用, 2007(6): 68-70.
- [6] NXP Semiconductor. NXP Semiconductor Rev. 03. 2009.

作者简介:彭亮(1988—),硕士,主要研究领域为水质智能检测技术。

E-mail: plxgl@163.com