Computer Science and Application 计算机科学与应用, 2017, 7(9), 886-893
Published Online September 2017 in Hans. http://www.hanspub.org/journal/csa
https://doi.org/10.12677/csa.2017.79101

Hans汉斯

Research of IAP Remote Upgrade Technology in Space Application System

Zheng Li, Xiaoyuan Liu, Yunxia Cao, Fan Yang

Shenyang Institute of Automation (SIA), Chinese Academy of Sciences, Shenyang Liaoning
Email: lizheng@sia.cn

Received: Sep. 1st, 2017; accepted: Sep. 15th, 2017; published: Sep. 22nd, 2017

Abstract

The working principle of In-Application Programming (IAP) is introduced first, and a new method of chip burning is designed that has changed the traditional way of the boot loader upgrade based on LPC2138 processor. As a result, remote program firmware upgrade can be realized through communication network. Meanwhile, the solution of software remote upgrade in the environment of space application is given, combined with the rapid development of space application in our country and the needs of remote software upgrade.

Keywords

ARM, IAP, Remote Upgrade, Space Application

IAP远程升级技术在空间应用初探

李　正，刘晓源，曹云侠，杨　帆

中国科学院沈阳自动化研究所，辽宁 沈阳
Email: lizheng@sia.cn

收稿日期：2017年9月1日；录用日期：2017年9月15日；发布日期：2017年9月22日

摘　要

介绍了在应用编程In-Application Programming (IAP) [1]的工作原理，以LPC2138处理器为工作平台，改变了传统的bootloader升级方式，设计了一种新型的芯片烧写方法，通过通信网络实现远程程序的固件升级，结合我国空间应用系统的快速发展和软件远程升级的需要，给出了空间应用系统环境下的软件远程升级解决方案。

文章引用: 李正, 刘晓源, 曹云侠, 杨帆. IAP 远程升级技术在空间应用初探[J]. 计算机科学与应用, 2017, 7(9): 886-893. DOI: 10.12677/csa.2017.79101

关键词

ARM，IAP，远程升级，空间应用

1. 引言

随着我国空间技术与航天建设发展，特别是近几年受空间站建立和深空探测等多项航天规划影响，越来越多的探测器、卫星载荷等空间飞行器在轨运行。期间，飞行器因功能需要升级、屏蔽故障模块或者因自身软件漏洞等原因，软件需要进行可靠的远程升级[2]。目前，空间应用系统由于受无人在轨运行、通信资源有限，升级可靠性要求高等因素影响，软件远程升级真正应用还不普及，但是已经在我国航天发展过程中提出了强烈的应用需求。

软件远程升级在地面应用系统目前已经有了很完善的应用，软件系统在线升级，传统的研究方向主要集中在软件系统本身[3]，升级方式也多种多样，如 Windows 操作系统等平台的软件升级可以通过更新动态链接库(DLL)或者静态库(LIB)即打补丁的方式进行升级。嵌入式系统升级的方式也有很多，主要有 ICP (In-Circuit Programming), ISP (In-System Programming)等方式。这些方式通过仿真器或者串行接口下载线进行连接下载程序，都需要额外的辅助设备[4] [5] [6]。在地面应用中资源丰富，可以额外增加辅助设备，但是在空间应用系统中，设备产品已经无人值守在轨运行，资源上也无法重新配置，即使预先设计考虑到这些升级方式，也要增加原系统额外的硬件资源，对于航天空间应用有一定的弊端。

IAP 可通过专门设计的固件程序来编程内部存储器，不需要硬件支持，所以 IAP 技术提高了嵌入式系统的可扩展性与可维护性[7]，能在不变的硬件平台上升级其软件版本，提供更多功能及增值服务，适合在轨飞行设备进行软件升级。本文以 ARM 为核心的 LPC2138 芯片[8]为平台，设计了基于 IAP 方式的远程程序升级系统，实现了一种在线软件升级方法和新的解决方案，为我国空间应用系统软件升级提供一种可行可借鉴的方案和初始研究。

2. IAP 概述

2.1. IAP 原理

LPC2138 芯片是基于实时仿真和嵌入式跟踪的 32/16 位 ARM7TDMI 微控制器，在网络控制、通信及工业电子等产品中有广泛的应用。它是带有 32 KB RAM 和 512 KB 高速 Flash 存储器的处理器，出厂时在片内固化了一段 Boot 程序。它可以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，且提供了 IAP 编程接口。该 Boot 程序在出厂时固化在 512KBFlash 的顶部 12 KB 范围内，当芯片上电以后，首先对 Boot 区执行一次重映射[7]，映射到片内存储器空间的最高处，即接近 0x80000000 的地方，称之为 Boot Block。Boot Block 的最低 64 字节为中断向量表，又被重新映射到芯片的最低地址 0x00000000 处，最低地址 0x00000000 开始的 64 字节则存储用户的有效中断向量。经过这样的地址重新映射后，IAP 代码的入口就位于 0x7FFFFFF0 处[8]，映射过程如图 1。

用户在应用 IAP 的过程中，可自行对 Flash 存储系统进行修改。由于 IAP 程序是 Thumb 代码，位于地址 0x7FFF FFF0，所以需要在 ADS 编译选项中，选中 ARM/Thumb Interworking 项。IAP 程序会使用

Figure 1. Boot program remapping after power up
图 1. Boot 程序上电后的重映射

片内 RAM 空间的顶部 32 个字节。因此在应用 IAP 时，用户程序应该避免使用这部分空间，在启动代码 Startup.s 文件中 InitStack 函数内调整堆栈空间位置，修改代码如下：

```
InitStack
MSR CPSR_c, #0xdf；设置系统模式堆栈
LDR SP, =StackUsr-32；//避免使用片内 RAM 的顶部 32 Byte
MOV PC, R0
```

2.2. IAP 命令格式

IAP 命令格式代码是调用 IAP 程序时用户指定的方法，IAP 程序会根据用户命令码执行相应的操作，并返回各种结果，如下表 1。

2.3. IAP 接口函数

根据 IAP 程序入口地址和 IAP 各种命令码，就可以用 C 语言实现 IAP 用户接口函数，方法如下。

1) 定义 IAP 用户函数指针

```
void (*IAP_Entry)(uint32 param_tab[], uint32 result_tab[]);
```

其中 param_tab 为用户输入缓冲区，result_tab 为程序返回结果缓冲区，IAP_Entry 为用户函数

2) 初始化 IAP 用户函数指针

```
IAP_Entry = (void(*)())IAP_ENTER_ADR;//其中 IAP_ENTER_ADR 为 IAP 程序入口地址
```

3) 调用 IAP 用户函数

```
(*IAP_Entry)(paramin, paramout);
```

其中 paramin 为用户输入 IAP 命令码缓冲区，paramout 为 IAP 程序执行后返回值缓冲区。通过对 paramin 传递不同的 IAP 命令可以实现不同的 IAP 程序调用，如版本号查询、扇区选择和编程等等。

2.4. IAP 编程步骤

使用 IAP 函数对片内 Flash 执行编程操作时，需要按步骤进行操作，在对某一个扇区进行擦除/编程操作之前，必须选择扇区，然后才能正常操作。流程为：确定命令参数- > 选择扇区- > 删除扇区- >

Table 1. IAP command table
表 1. IAP 命令格式表

IAP 命令	命令代码
准备编程扇区	50
将 RAM 内容复制到 Flash	51
擦除扇区	52
扇区查空	53
读器件 ID	54
读 boot 代码版本	55
比较	56

查空扇区-> 选择扇区-> 编程扇区-> 校验扇区。需要注意 IAP 程序在编程时只能写入规定大小的数据字节数，如字节数大小必须是：256、512、1024 或者 4096。

3. IAP 远程升级系统设计

3.1. 远程升级总体结构

为了给出 IAP 远程升级的通用性与普遍性，设计远程升级模式如下图 2 所示。具体的网络可以为 Internet 网络，也可以为星地通信网络。LPC2138 通过卫星与地面 IAP 升级服务器建立通信连接，要升级的程序在地面的 IAP 升级服务器上。当需要对在轨软件进行更新时，即可把要更新的程序发送到基于 LPC2138 的在轨载荷产品中，完成软件版本升级。通过该方式便于软件的维护、管理和更新发布，有效解决代码维护、测试等问题，延长软件生命周期，提高试验任务的正确性、可靠性。

3.2. 远程升级方式与 FLASH 扇区分布设计

LPC2138 有 500 KB 的 Flash 可用，分布在 26 个扇区中，不同的扇区其可存储的数据大小不同，在芯片复位时，程序从 0x00000000 处开始运行。针对这些特点，设计 Flash 存储分布格式如下图 3。本设计采用导出 IAP 用户程序，实行系统程序在线方式完成软件版本更新。首先，将编写的 IAP 程序通过 ADS 编译器中的“分散加载文件”实现代码定位，并将其定位到最后一个扇区。这样，当要 IAP 远程升级时，待升级的新程序可以覆盖正在运行的系统程序。这是一种很危险的行为，一旦在覆盖过程中出现地址冲突将造成无法悔改的错误，整个软件系统也就崩溃了。而在程序的覆盖过程中只用到了 IAP 程序，所以把用户的 IAP 程序与系统程序分离开来并定位到最后一个扇区，当待升级程序区程序覆盖系统运行程序区时就不会出现冲突，从而可完成在线更新的升级方式。

3.3. 远程通信协议设计与升级流程

空间应用系统应提供自动化的数据输送和分配系统，保障安全、可靠的数据交流、翻译、转换、在系统之间的数据和信息的路由选择、应用、数据存储[9]；IAP 升级服务程序在升级过程中必须保证升级程序数据传输的正确性，对每次发送的一帧数据都要进行校验以保证数据的正确性。同时，还要保证帧与帧之间的顺序必须正确。只有在完整的程序传输完毕后才能通过 IAP 对原程序进行覆盖更新，否则将会造成原程序的损坏，导致系统崩溃。设计帧格式如下表 2 和表 3。

发送帧类型有版本号请求、升级开始、数据注入、升级结束等指令。首先，地面运控中心通过通信网络向在轨载荷发送软件版本号请求，然后通过遥测参数识别在轨载荷软件返回的版本号，若与服务器的版本号不同，IAP 服务程序开始升级指令，IAP 服务器程序首先将要更新的程序读取，并按 1024 字节字段形成数据注入帧表。然后，逐帧将更新程序注入到在轨载荷软件中。每注入一帧数据后，通过遥测

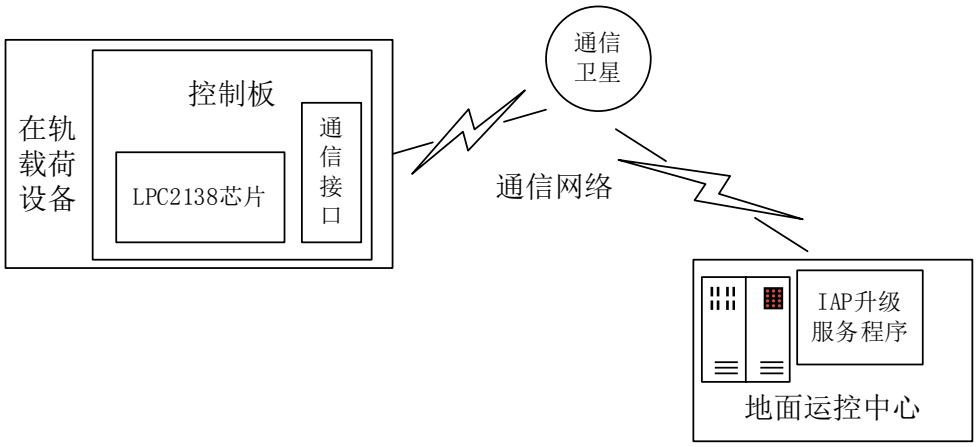

Figure 2. Remote upgrade structure of IAP
图 2. IAP 远程升级结构

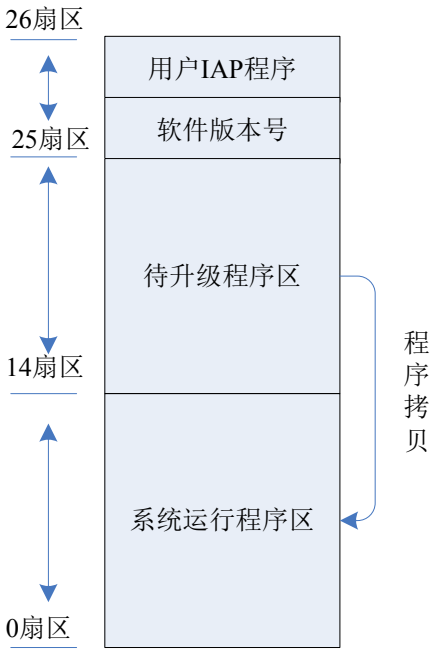

Figure 3. Flash sector distribution
图 3. Flash 扇区分配

Table 2. Data format of injection
表 2. 数据注入帧格式

帧头	发送帧类型	帧号	发送帧数据	CRC 校验
2 byte	1 byte	2 byte	1024 byte，不足补 FF	2 byte

Table 3. Data format of telemetry
表 3. 数据遥测帧格式

帧头	遥测帧类型	帧长度	应答帧数据	CRC 校验
2 byte	1 byte	2 byte	根据帧长度定	2 byte

参数确认注入是否成功，然后再进行下一帧注入。

遥测帧类型有版本号、校验错误、注入正确、升级成功等类型。应答帧数据中针对不同类型设置相应的参数值，如版本号类型，应答帧数据为版本号，校验错误和注入正确都要返回当前注入的帧号计数。地面在轨中心根据遥测结果决定是否继续注入。通过这种方式，确保了更新程序的顺序正确性。同时，为了保证数据的正确性采用CRC校验。在轨IAP客户程序将接收的正确注入数据存入到待升级程序区……直到完整的接收完全部程序，然后将软件版本号更新，最后，将待升级程序区的程序覆盖到系统运行程序区，完成远程升级过程。IAP 服务程序和客户程序基本流程如图 4，基于普遍性，本系统采用 Internet 网络进行了在线远程升级测试，效果良好。

4. 远程升级试验

在地面模拟在轨应用工作流程，进行远程升级试验演练，通过 Internet 网络进行广义测试升级试验。地面模式远程升级试验如图 5 所示。首先，利用单位已有的基于 LPC2138 的通信产品，写好应用程序

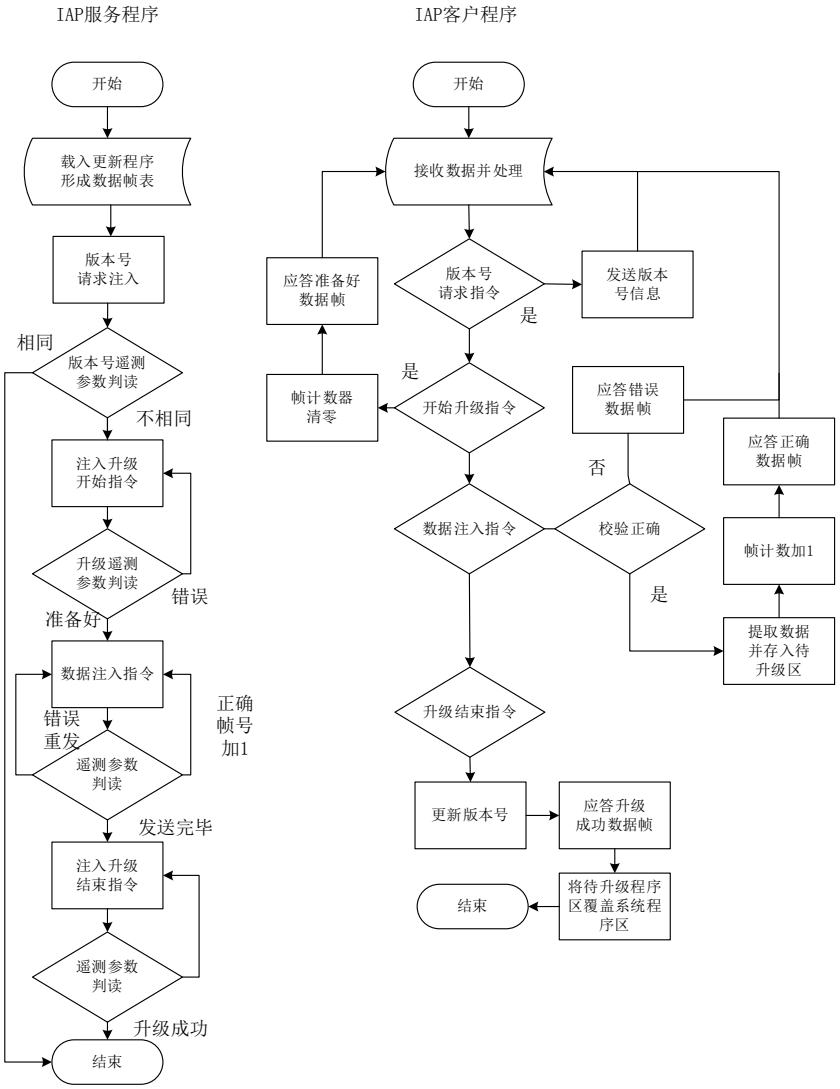

Figure 4. Basic flow chart of IAP remote upgrade
图 4. IAP 远程升级过程基本流程图

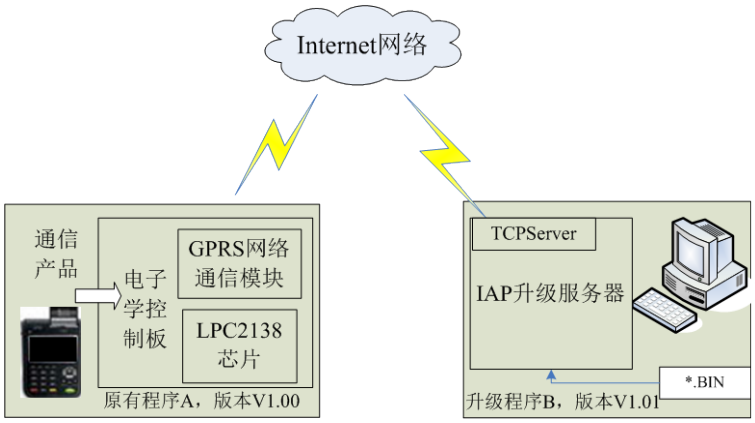

Figure 5. Experiment of remote upgrade by simulation
图 5. IAP 地面模拟远程升级试验

A，软件版本 V1.00，该软件已经内嵌 IAP 远程升级客户程序。在 IAP 远程升级服务器上，开发一个基于 Socket 的 TCP 网络服务器，内嵌 IAP 升级服务器程序。首先，运行 IAP 升级服务器，让通信产品输入 IAP 升级服务器的 IP 地址和端口号，通过 Socket 网络建立客户端与服务器端的网络连接。通信网络建立后，IAP 服务器程序向通信产品发送版本号请求，得知其软件版本号与自身要升级的版本号不同后，发起远程升级指令从而进入升级流程，升级完毕后，重新对通信产品加电，通信产品运行程序为应用程序 B，软件版本号为 V1.01。基于 Internet 的网络通信具有普遍意义，通过该地面模拟方式成功验了基于 IAP 的软件远程升级的正确性，星地软件远程升级过程与之相同，在通信链路上会有一定差别。

5. 结论

空间应用系统对芯片的等级要求较高，选择 IAP 升级方式对芯片的选型也有要求。本文提出的在线程序远程升级方式升级便利，有利于程序的版本管理，而且设计简单，升级稳定可靠，对同类或其它单片机的远程升级具有一定的借鉴作用。由于采用 IAP 方式，用户程序可对 Flash 存储系统进行修改，也给该芯片留有“后门”的余地，对软件的安全性也要有充分考虑。在远程升级时，要尽可能避免出测控区影响升级过程的情况。IAP 技术为软件系统在线远程升级提供了良好的解决方案，也为数据存储和固件的升级带来了极大的灵活性。相信，在未来航天软件技术发展过程中，IAP 远程升级平台必将为提高在轨有效载荷软件稳定运行和增值服务创造更大价值，必将得到更广泛的应用。

资助信息

实验柜系统，课题编号：Y4k3170301。

参考文献 (References)

[1] 周立功, 张华. 深入浅出 ARM7[M]. 北京航空航天大学出版社, 2005: 426-438.
[2] 王婷, 高玉娥, 董文博. 面向空间应用的嵌入式系统软件重构技术[J]. 测控技术, 2017, 36(2): 111-114.
[3] 焦诚, 李英. 卫星导航地面控制系统在线升级与验证方法[J]. 现代导航, 2016, 7(2): 94-98.
[4] 顾程华, 林宏飞, 徐文卿. 基于 IAP 的微控制器程序升级技术[J]. 工业控制计算机, 2017, 30(6): 13-14.
[5] 陈亮. 基于 STM32 处理器的存储器 IAP 编程技术[J]. 网络与信息工程, 2017(10): 77-78.
[6] 周振齐. 单片机 IAP 在应用软件升级的方法探究[J]. 数码世界, 2015(5): 20-23.
[7] 韩兆渊, 王晓东, 黄国勇. 基于 IAP 的北斗终端程序远程升级技术的研究[J]. 计算机与数字工程, 2017, 45(5):

844-848.

[8] LPC2131/2132/2138 User Manual. http://www.docin.com/p-88394452.html

[9] 廖苹. 国际空间站远程医疗概况与展望[J]. 载人航天信息, 2014(5): 13-19.