IAP 升级 V2.0 及底板程序设计方案

版本号	修改内容	修改人	修改时间
V1.0	新建	张浩	2023-06-28

目 录

1 概述

1.1 背景

为适配新版系统，需要升级升级软件。特起草本方案。

2 IAP 升级工具 2.0 制作概要

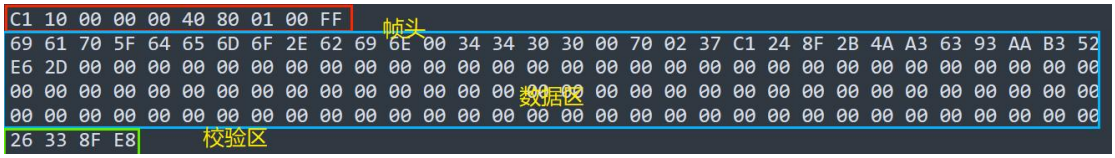
2.1 起始帧设计

起始帧由设备地址(1 字节)、功能码(1 字节)、起始地址高低位(2 字节)、数据大小高低位(2 字节)、数据区总字节(1 字节)、ymodem 帧头标识码(1 字节)、数据包数高位(1 字节)、数据包数低位(1 字节)，帧头共计 10 字节。

数据区共计 128 字节(bin 文件切分所得)。

数据区 crc 校验高位(1 字节)、数据区 crc 校验低位(1 字节)、帧头加数据区 modbus 校验高位(1 字节)、帧头加数据区 modbus 校验低位(1 字节)，共计 4 字节。

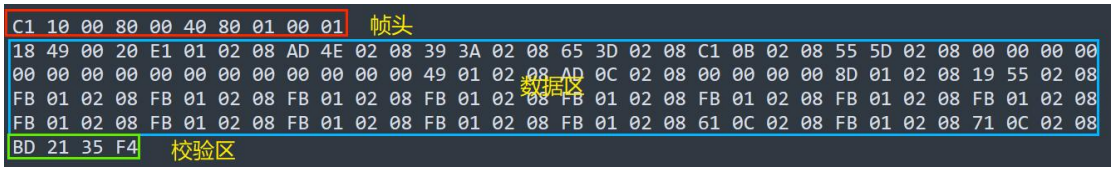
起始地址起始帧初始化为 0x0000，代表 ModBus 起始帧，数据包格式 0x00FF 为 Ymodem 起始帧格式。具体如下图所示：



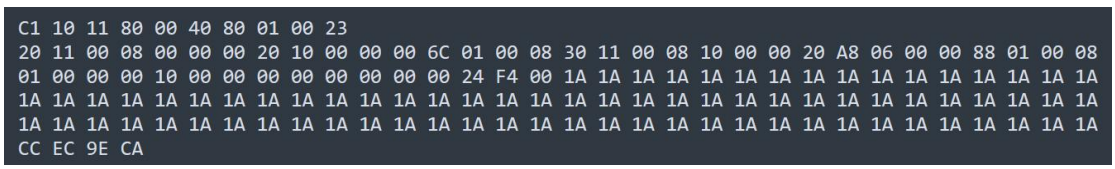
其中数据区包括：升级文件名称 ASCII 码，升级文件大小 ASCII 码，升级文件 MD5 校验码。不足 128 字节使用以 0x00 填充。

2.2 数据帧设计

数据帧帧头组成与起始帧一样，起始地址为数据包数做 128 偏移。数据包数 0001 为第一个包。Ymodem 头帧(SOH：0x01)代表数据区的 128 字节为从升级文件的开头切分的 128 字节。尾部的校验区与起始帧相同。具体如下图所示：

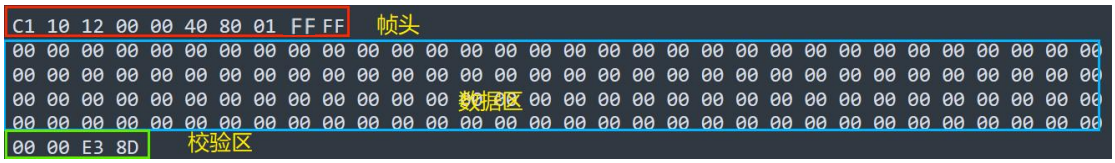


数据帧最后一帧若不满 128 字节其余使用 0x1A 进行填充。如下图所示：



2.3 结束帧设计

结束帧帧头组成与起始帧一样，第 8 个字节为 SOH 帧(0x01)为传输 128 字节。起始地址为传输的所有包数加 1 后的地址偏移量。数据包数 0xFFFF 为 Ymodem 协议结束帧规格。数据区的 128 字节全为 00，代表结束帧。尾部的校验区与起始帧相同。具体如下图所示：



3 底板程序修改概要

3.1 升级指示帧接收设计（握手帧）

计划发送：

C1 03 50 00 00 0C CH CL

含义：从 5000 寄存器开始读取 13 个寄存器共 26 个字节（Flash 已固化的版本号、升级刻度值、MD5 校验）；

如果回复：

C1 03 1A 23 07 07 00 12 34 56 78 90 12 FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF CH CL（无写入状态回复）

将返回的尾部 16 字节与待升级文件的 MD5 码作比较。

如果比对不通过。则说明该设备底板未进行升级操作或者板中系统版本与升级版本不符。系统版本发生改变则开始发送**起始帧**。执行覆盖写入操作。

如果比对通过，则说明写入的版本与升级版本一致，软件拿到返回字节的升级刻度值（已写入包号 2 字节+最后写入末地址 4 字节）后，对 bin 文件切分。根据刻度值找到发生断点的数据包，进行数据续传操作。

3.1.1 底板需做功能

若软件升级的系统版本跟底板系统版本不一致后。

接收起始帧后，对起始帧的数据信息向特定的 Flash 缓存区进行写入固化。

固化完成后回复：C1 10 00 00 00 40 80 CH CL（起始地址与发送格式相同，进行相同字段回复）

若系统版本未发生改变，则根据返回字节的升级刻度信息写入缓存区 Flash 地址。供升级软件重新切分和断点续传。

3.2 处理接收到的数据帧设计

3.2.1 底板接收区设计

如果接收到的功能码为 0x03，则为查询帧（包括基础信息量查询、断点刻度查询）；

如果接收到的功能码为 0x10，则为升级数据帧（包括起始帧、数据帧、结束

帧）；

3.2.2 基础功能帧

常规的基础功能，包括 GPIO 口的查询等。收到 8 字节后。例如：C1 03 00 01 00 01 CH CL。运行基础功能进行常规回复。

3.2.3 升级指示帧（握手操作）

功能码为 0x03。例如：C1 03 00 06 00 08 CH CL。意为**握手信息查询**，执行相关操作（**具体见 3.1**）。

3.2.4 升级数据帧

收到功能码为 0x10 后，底板判定为起始帧、数据帧、结束帧。

起始帧、数据帧、结束帧三帧的区别为，起始地址为 0x0000 为起始帧。起始地址是包数的 128 倍为数据帧。包数为 0xFFFF 的为结束帧标识。

例如：上方数据帧设计所示。将数据区的数据共计 128 字节在升级指示帧所设置的 Flash 地址开始擦除并写入。写入完成后**更新当前写入包数和最新的末写入地址**，供后期断点续传使用。当接收到结束帧时停止写入。

接收完毕后，根据起始帧存储的数据大小，由起始 Flash 地址加上大小，将所得的整个区域做 MD5 校验，与起始帧存储至 Flash 的 16 字节 MD5 数据作比较。

若校对正确则说明数据完整性正常。

若错误则回复：C1 90 CH CL，说明数据传输受到干扰，数据不能支持继续升级，需从新执行升级操作。

3.2.5 升级信息和刻度值信息写入规范

设计在接收数据帧时，将接收到的每帧有效数据（128 字节），按照顺序放入缓存区暂存。待接收长度达到 2048 字节后（STM32F103RET6 每页擦写大小为 2K），将 2048 字节按照定义的数据缓存地址，进行写入。一组规格为（2048 字节，共计 2K）写入完成后，将刻度值信息起始包号更新至 0x10（意为 16 个有效数据包已写入），缓存地址在起始地址的基础上向后偏移 2K 字节，以此类推。

4 超时及包校验处理机制

4.1 底板超时处理机制

升级过程中，当底板不再响应“卡死”。软件发送某个数据包时，持续长时间没有得到答复。则判定底板出现由于不确定因素导致无法正常运行相应功能，升级软件执行当前包重传操作，如果一个等待时间周期内仍未得到答复，则重新开始起始握手链接操作。若握手失败，判定升级失败，等待底板重新上电后再次进行升级操作。若握手成功，则从底板给到的刻度信息执行断点续传。以实现双方设备健康升级。

4.2 刻度混乱处理机制

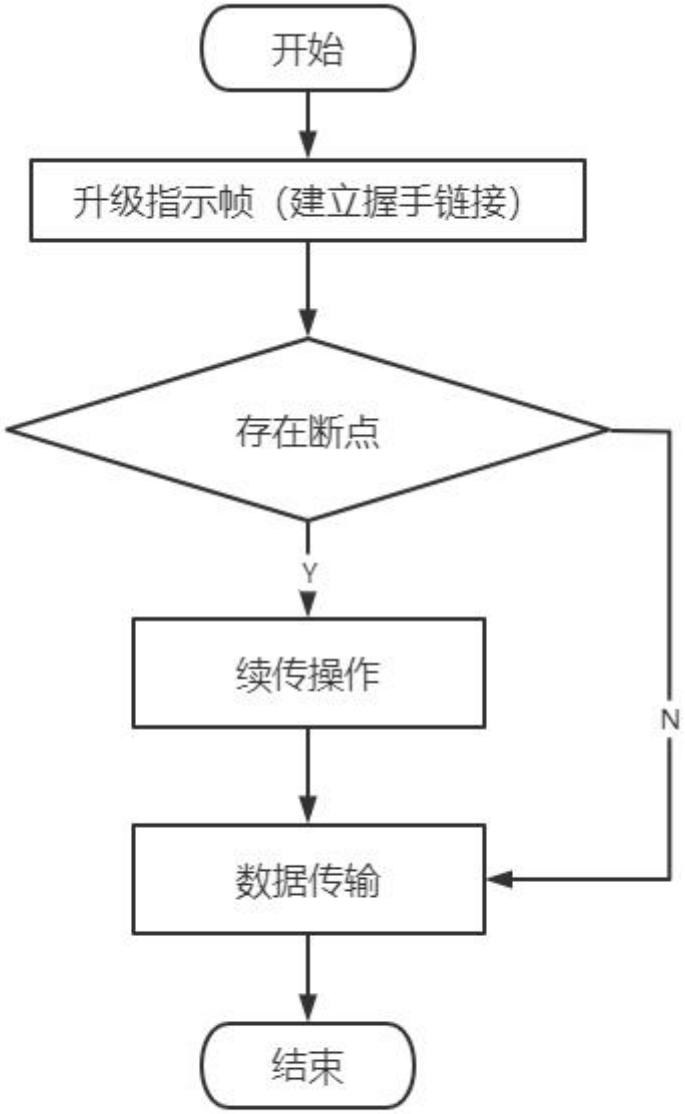
当升级过程中，双方某一方掉电后，升级活动提前结束。待双方恢复正常后，再次握手后执行断点续传。在此过程中，软件发送的数据包与底板存储的刻度信息出现不一致时，底板判定出现刻度混乱，执行刻度混乱处理机制。

底板检测不一致后发送异常回复，软件得到异常回复后，重新进行握手操作，以获取最新的真实包数和写入地址后进行续传操作。

以此机制规避 MD5 校验失败的几率。

5 整体流程图

5.1 IAP 升级概览图

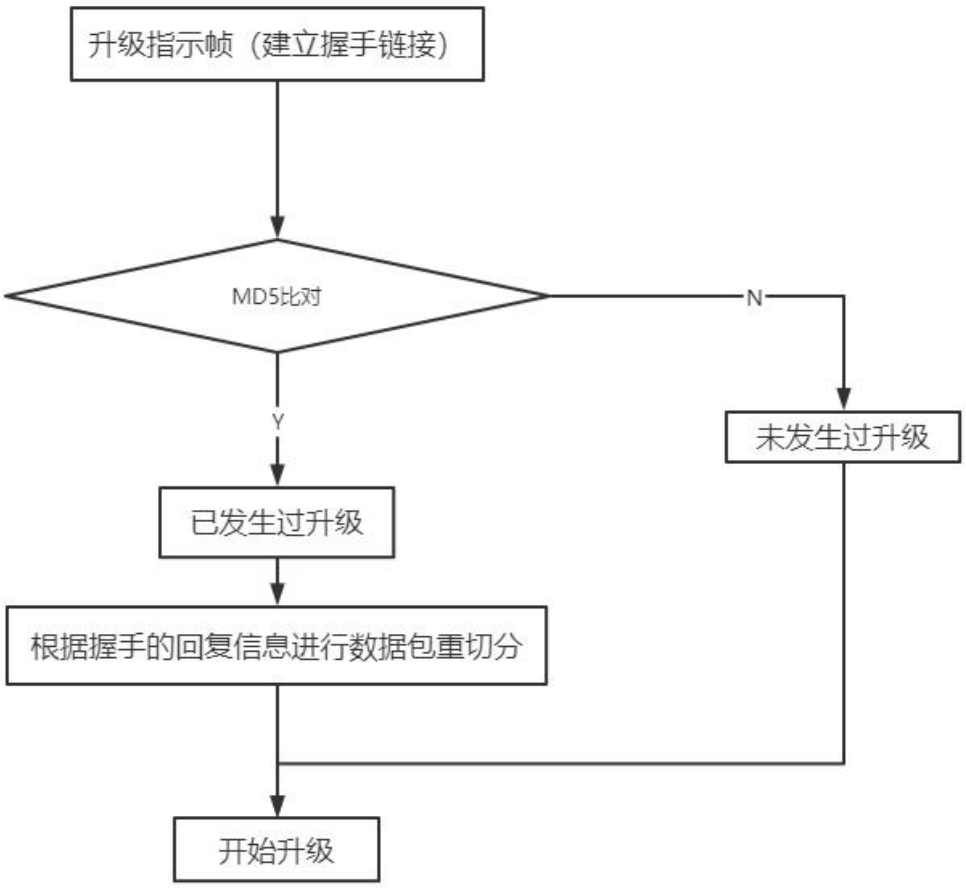


IAP升级工具V2.0
流程概览图

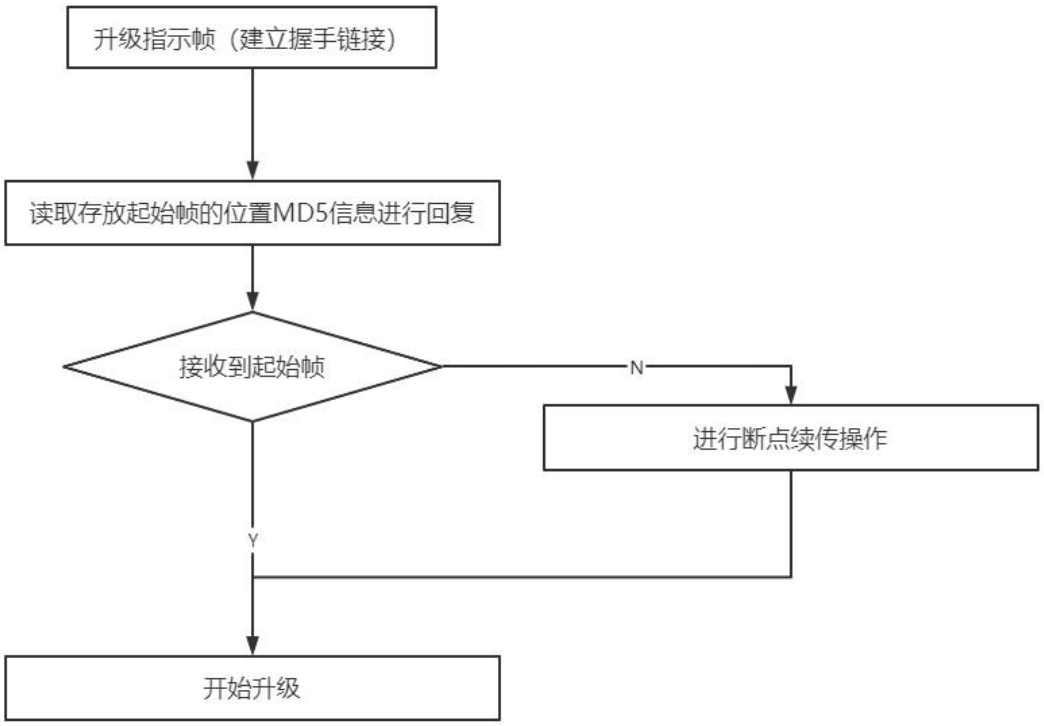
5.2 升级指示帧流程图

升级时首先 IAP 升级软件 V2.0 首先会发送升级指示帧（进行握手链接）。读取底板存储起始帧位置的 MD5 校验码返回给软件做比对。比对完成，若为默认值则判定为未进行过升级执行升级操作。

若收到 MD5 校验码后不是默认值则判定已发生过升级操作，随后发送断点问询得到断电刻度值后，软件对数据包的第一包的发送做调整。升级指示帧流程图如下图所示。



IAP升级工具V2.0
升级指示帧流程图

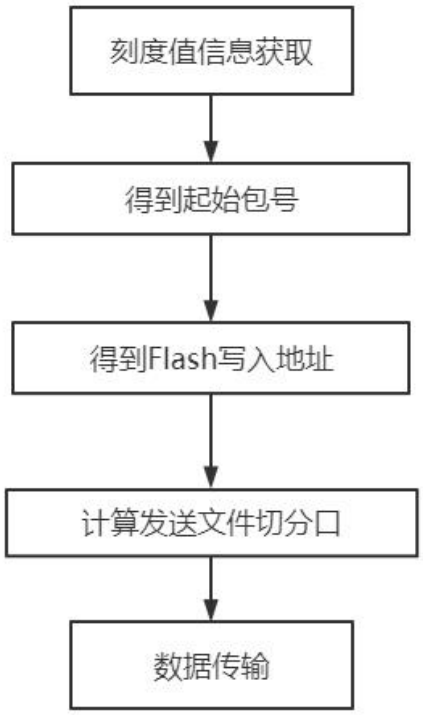


iocollect
升级指示帧流程图

5.3 断点续传流程图

升级软件在握手时检测发生断点后，问询特定地址 Flash 以得到刻度值。软件得到刻度值的回复后对升级文件做相应处理。

软件进行数据包的重新切分并从断点处进行发送，并执行续传操作。断点续传流程图如下所示。



IAP升级工具V2.0
断点续传流程图

5.4 载荷数据帧传输流程图

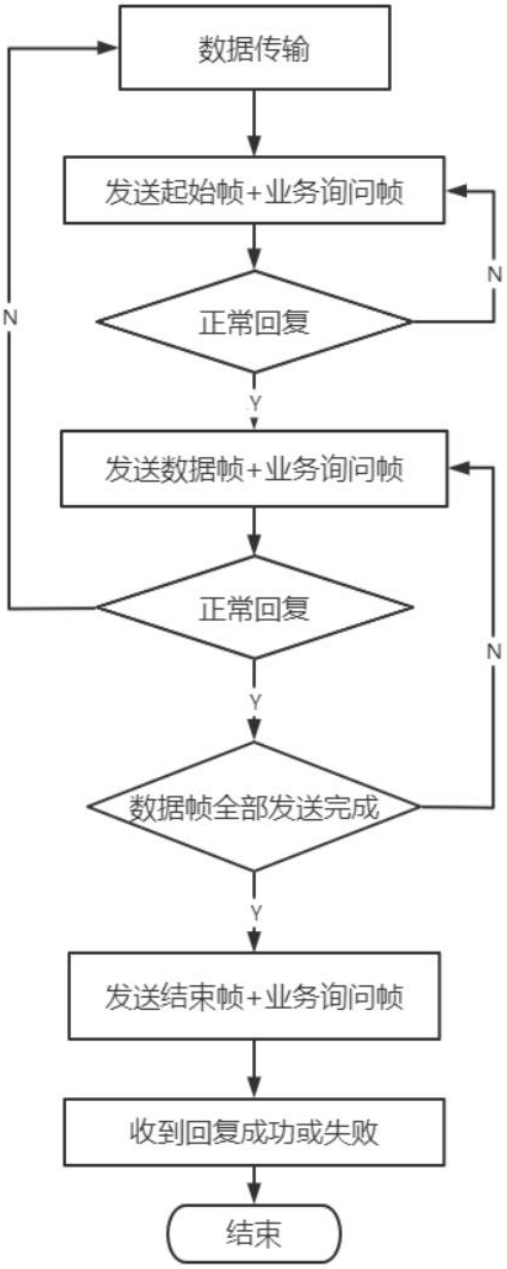
IAP 升级工具 V2.0 进行数据传输时，首先发送起始帧+业务闻讯帧，若收到从机的正常回复则继续发送数据帧，若接收到错误回复则重新执行数据传输操作。

传输数据帧（bin 文件内容），将整个升级文件切分成 128 字节等分的数据载荷并封装成 modbus 协议进行传输。数据帧全部发送完成后，发送结束帧，完成升级操作。

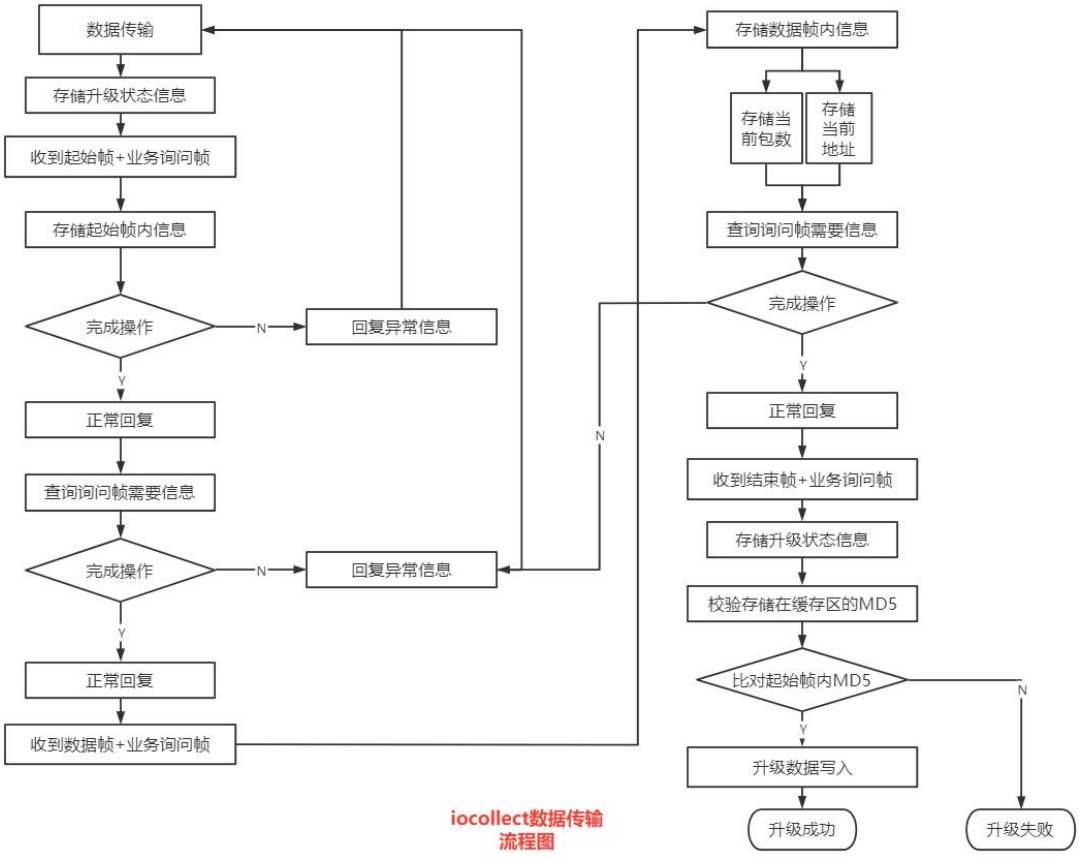
从机在执行数据传输操作时首先读取起始帧的数据信息并存储，包括文件名、文件大小、文件 MD5 校验码。然后将特定位置写入“正在升级”定义字段。做完操作后进行回复，若没有执行完成则回复错误信息。查询询问帧的信息，查询到后进行标准回复。

收到数据帧后将数据区的数据存储到预设的 Flash 地址上进行保存。进行擦除和写入 Flash 的操作。写入完成后，存储当前已写入包数和下一次应该写入的 Flash 地址。再次查询询问帧的信息，查询到后进行标准回复。

收到结束帧后更新升级状态信息为“正常启动”定义字段。将数据开始写入的地址到最后一个字节写入的数据做 MD5 校验。并将校验值与起始帧保存的 MD5 校验码作比较。若比对正确则信息完整性正常，升级信息保存成功。若不正确则信息完整性异常，升级信息写入失败。



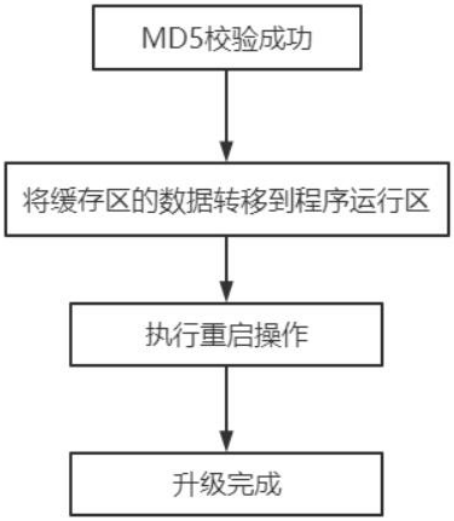
IAP升级工具V2.0
数据传输流程图



iocollect数据传输流程图

5.5 底板升级数据转移流程图

数据校验完成后，将缓存区的数据根据存储的起始地址和包大小来计算整个升级数据的大小将升级数据分批次转移至程序运行的 Flash 区域，转移完成后执行重启操作。升级成功。



底板升级数据转移流程图

升级完成后（已确认 MD5 校验完成），进行结束帧的回复。至此升级结束。