# 1 前期开发

## 1.1相关设置

中断向量表 0~100

Boot 800~5000 将backup区数据备份到app

App 5000~20000 把上位机发送的hex数据写到backup区

Backup 20000~50000

CONFIG不用升级

Boot和app合并用IPE升级

## 1.2通讯方式

通讯方式UART/485

波特率115200

中断向量表地址固定

Boot程序不用中断

App开中断

# RS485数据帧格式

## 2.1帧格式

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **帧头** | **地址** | **通信命令** | **数据长度** | **数据包内容** | **校验资料** |
| 单字节 | 单字节 | 单字节 | 单字节 | 多字节 | 2字节 |
| 0x3A | 0x16 | 0xF0 | - | - | - |

说明：

* 帧头： 单字节， 内容为 0x3A， 为固定值。
* 地址： 单字节， 内容为 0x16， 为固定值。
* 通信命令： 单字节， Boot Loader命令为0xF0，更多信息参考BMS通信协议。
* 数据长度: 单字节， 内容为该通讯数据帧内数据缓冲区内的数据长度。 主机发送数据时， 如果不包含其他数据则统一设置为 1。
* 数据内容： 多字节， 内容为具体各个命令对应的数据字节， 字节数是不固定的， 数量由数据长度部分的数值确定。 主机发送数据时， 如无特别命令要求， 建议设置为 0。
* 校验资料： 两字节， 内容为通讯数据的累加校验和数据， 包括：地址、通信命令、数据长度、数据内容的累加和，低字节在前， 高字节在后。

帧尾： 两字节， 内容为结束标识 1（为固定值 0x0D） 和结束标识 2（为固定值 0x0A）

## 2.2发送新固件信息（0xF6）

此指令，上位机需获取本地固件的信息，发送给BMS，BMS依据此信息接收数据并判断数据是否准确和完整。

包括：固件版本、CRC32校验、固件大小、总帧数。

|  |  |  |  |
| --- | --- | --- | --- |
| 主机 | 数据包大小：17 | 命令 | 参数 |
| 0xF6 | 16字节 |
| BMS | 数据包大小：2 | 命令 | 参数 |
| 0xF6 | 1字节 |
| 说明 | 参数说明：   |  |  | | --- | --- | | 主机发送 | 新固件信息 | | BMS返回 | 应答：0x00(OK)，其它(Error)。 | | | |

固件信息：

|  |  |  |
| --- | --- | --- |
| **字节** | **名称** | **备注** |
| 1~2 | 保留 |  |
| 3~5 | 总字节数 | 低字节在前，高字节在后。 |
| 6~7 | 总帧数 | 低字节在前，高字节在后。 |
| 8~11 | CRC32校验码 | 低字节在前，高字节在后。  采用CRC32-MPEG2标准，详细信息如下： |
| 12~16 | 保留（5字节） |  |

## 2.3发送新固件数据（0xF7）

包括：当前帧号、帧数据。

|  |  |  |  |
| --- | --- | --- | --- |
| 主机 | 数据包大小：N+1 | 命令 | 参数 |
| 0xF7 | 多字节（N） |
| BMS | 数据包大小：2 | 命令 | 参数 |
| 0xF7 | 1字节 |
| 说明 | 参数说明：最后一帧数据的接收完成后，自动完成新固件的升级。   |  |  | | --- | --- | | 主机发送 | 新固件数据，见下表说明。 | | BMS返回 | 应答：0x00(OK)，其它(Error)。 | | | |

固件信息：

|  |  |  |
| --- | --- | --- |
| **字节** | **名称** | **备注** |
| 1~2 | 当前固件数据帧号。 | 范围：0~（总帧数-1）。 |
| 3~N | 固件数据 | 每帧最长数据为128字节。 |

# 3核心代码

## 3.1固件程序

文件

BSPFLASH.c

BSPUART.c

UartLoadApp.c

函数

UartRcvMsgDeal

变量

## 3.2上位机

函数

WriteflashCommandAPI

WriteflashDataAPI

\_readThread

ReadReceiveRS485Data

变量

gLoadingSection

updateStep

Cycletimer

Flash\_SectionNum

UserFileData.Data

UserFileData.SectionDataNum

## 3.3跳转语句

跳转到app

(\*((void(\*)(void))0x5000))();

跳转到boot

asm("reset");

# 4开发流程

## 4.1测试相关指令

|  |  |
| --- | --- |
| Boot区 | |
| 跳到5000 | 3A 16 F0 02 F5 00 |
|  |  |
| 查询20000 地址数据 | 3A 16 F0 02 F1 00 |
|  |  |
| 擦除5000地址数据 | 3A 16 F0 02 F0 00 |
|  |  |
| 查询5000 地址数据 | 3A 16 F0 02 F2 00 |
|  |  |
|  |  |
| 写数据到5000地址 | 3A 16 F0 02 F3 00 |
|  |  |
| 查询00~100地址数据 | 3A 16 F0 02 F8 00 |
|  |  |
| 中断表擦除 | 3A 16 F0 11 F6 00 00 F8 01 00 04 00 57 4D CE 63 00 00 00 00 00 |
|  |  |
| 中断向量表写 |  |
| app区 | |
| reset | 3A 16 F0 02 F2 00 |
|  |  |
| 查询20000 地址数据 | 3A 16 F0 02 F5 00 |
|  |  |

## 4.2操作步骤

|  |  |
| --- | --- |
| 步骤1 | 用IPE烧录 合并hex文件 |
| 步骤2 | 发跳转3A 16 F0 02 F3 00 到app |
| 步骤3 | 打开上位机加载烧录app程序hex文件 |
| 步骤4 | 烧录完成后，发复位指令3A 16 F0 02 F2 00 |
| 步骤5 | 打开上位机烧录向量表hex文件 |
| 步骤6 | 发跳转指令到app |

# 5后记

升级的文件和app文件大小不一样如何取

50000地址以后flash驱动不能正常使用，需要优化

App应用程序标识未添加

Boot里面把backup数据拷贝到app上位机还需实现（目前是用串口助手手动完成）

App升级hex文件大小未测试（主要是考虑flash转页擦除未经过测试）