**纯打击反制枪网口固件升级协议说明**

|  |  |  |  |
| --- | --- | --- | --- |
| 拟制 | 陈安东 | 日期 | 2023年08月01日 |
| 修正 |  | 日期 |  |
| 审批 |  | 日期 |  |

**变更记录**

|  |  |  |  |
| --- | --- | --- | --- |
| **版本** | **说明** | **拟制人** | **日期** |
| V1.0 | 初稿 | 陈安东 | 2023-08-01 |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

# 1概述

## 1.1 前言

本文档说明纯打击反制枪通过网口(CH9121串口转网口)升级固件的详细信息，用于上位机开发人员在开发及调测时参考，以下产品名称均简称为反制枪。

## 1.2 适用范围

本文档适用于反制枪通过网口更新固件的应用场景。

# 2总体说明

## 2.1 Alink协议格式

ALINK协议基于MAVLINK协议实现，其格式如表 1所示。

表 1 ALink协议格式

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **字节** | **定义** | **内容** | **数值范围** | **说明** |
| 0 | magic | 帧头 | 0xFD | 表示开始一个新的包 |
| 1 | len\_l | 有效数据  长度低8位 | 0~255 | 表示有效数据的长度的低8位 |
| 2 | len\_h | 有效数据  长度高8位 | 0~255 | 表示有效数据的长度的高8位 |
| 3 | Seq | 帧序号 | 0~255 | 每个设备计数自己的发送序列，允许检测丢包。 |
| 4 | destid | 目标ID | 0~255 | 接收者的设备ID（纯打击反制枪为0x04，PC为0x1C） |
| 5 | sourceid | 源ID | 0~255 | 发送者的设备ID（雷达为0x03，PC为0x1C） |
| 6 | msgid | 消息ID | 0~255 | 消息ID用于识别该帧的含义，详见后文描述 |
| 7 | ans | 应答 | 0/非0 | 0表示 |
| 8 | checksum | 包头校验值 | 0~255 | 计算校验值校验从字节0至字节7(和校验) |
| 9至（N+8） | payload | 有效数据 | （0~65014）字节 | 有效传送的数据 |
| N+8+1至N+8+2 | crc | 整帧数据校验（2个字节） | 计算校验值不包含帧头，校验从字节1至字节N+8，注：校验包括1个扩展字节，默认的CRC的扩展字节为0x00。 | |

MAVLINK是一个专为微型飞行器制定的开源通信协议。由于MAVLINK具有轻量、易扩展等特点，非常适合用于无人机系统的数据通信中。MAVLINK是遵循LGPL许可的开源项目，因此可以被用来作为闭源和开源应用程序中的一个库，免版权费。

MAVLINK通信协议的帧头（magic）表示一个新的数据包开始标志，该标志可用于串行通信中进行数据同步。

MAVLINK通信协议的有效数据长度高8位（len\_h）和低8位(len\_l)组合起来表示该MAVLINK帧要传送的数据字节数，其组合后大小范围是0~65014。当有效数据长度为0时，表示该MAVLINK帧为一个命令帧，此时MAVLINK帧总字节数为11，当有效数据长度为N时（0<N<65014），表示该MAVLINK帧为一个数据帧，此时MAVLINK帧总字节数为11+N。

MAVLINK通信协议的帧序号高8位（seq\_h）和低8位(seq\_l)用于区分MAVLINK帧的次序，每个设备递增计数自己的发送序列，允许检测是否丢包，并实现重传。包序号由发送者递增，接收者应答时保持原包序号不变（即应答的包序号为接收到的包序号）。

MAVLINK通信协议发送者的设备ID（sourceid）和接收者的设备ID（destid），根据系统的实际业务需求对其进行重新定义，每个MAVLINK帧包含了发送者和接收者的身份信息，**当一个设备接收到一个MAVLINK帧，判断接收者的设备ID为自己的设备ID，则进行处理和应答；如果接收者的设备ID不是自己的设备ID，则根据路由表对该帧进行转发。**

MAVLINK通信协议的消息ID（msgid）用于识别该MAVLINK帧的含义，接收设备根据消息ID做出相应的处理和应答。

MAVLINK通信协议的包头校验值是从字节0至字节7的checksum(和)校验。

MAVLINK通信协议的有效数据（payload）为MAVLINK帧要传送的数据，一帧最大能传送65014字节的数据。

MAVLINK通信协议的数据校验值是从字节1至字节N+8的CRC16校验，这里规定CRC16校验的初始值为0xFFFF，多项式为0x1021。MAVLINK使能扩展CRC，（宏MAVLINK\_CRC\_EXTRA的值为1），并且规定除飞控特殊MSGID外，CRC的扩展字节为0x00。

## 2.2 交互流程

上位机先与反制枪建立连接，然后查询反制枪版本号版本无误后通过TCP向反制枪发送升级镜像文件，升级镜像头部文件格式如下：

typedef struct   
{  
 uint32\_t headerLen;  //头的长度  
 uint32\_t headerVersion;  //头的版本信息

uint32\_t firmwareAOffset;       //固件A在当前文件的偏移量

uint32\_t firmwareALength; //固件A长度

uint32\_t firwwareACrc; //固件A crc信息

uint32\_t firmwareBOffset;       //固件B在当前文件的偏移量

uint32\_t firmwareBLength; //固件B长度

uint32\_t firwwareBCrc; //固件Bcrc信息  
uint32\_t corpInfoLen ;  //公司信息长度  
char pCorpInfo[32];  //公司信息  
uint32\_t devNamelen；     //产品名字长度  
char pDevName[32];   //ACUR101  
uint32\_t fwVersionLen;  //版本信息长度  
char pFwVersion[64]; //固件版本信息

uint8\_t reserve[92] //预留  
uint32\_t headerCrc; //头的crc信息

}ImageHead\_t;

头部信息中填充固件长度和偏移量，公司和产品名称，以及版本信息和头部crc校验值，长度256bytes。

数据包按1K有效数据大小发送固件数据。

系统默认从A区启动，启动标志设置在flash中，执行升级动作时系统升级对区，升级完成之后更新启动标志，下次系统由对区启动。

升级失败需要回退到当前版本(数据擦除之前)。

上位机与反制枪的典型交互流程如图 1所示。

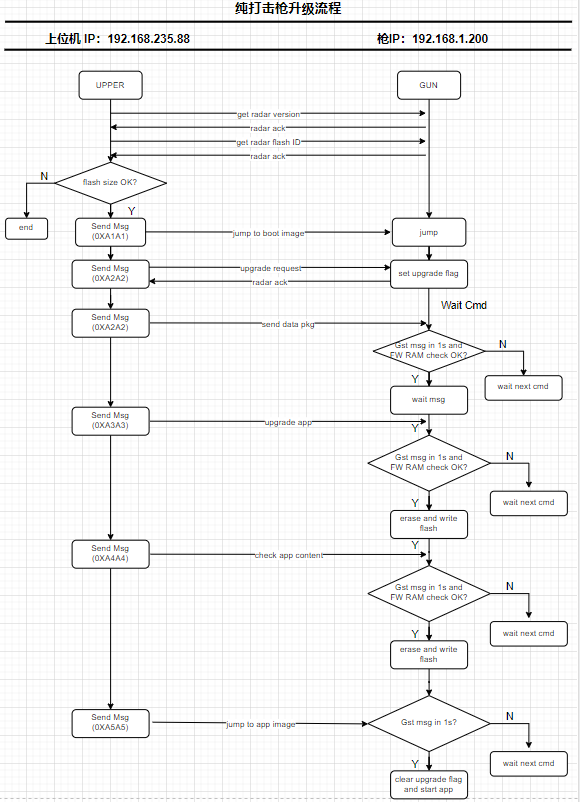


图 1 典型交互流程

# 3升级指令

**表3.5.6 反制枪升级指令ID（ -> 反制枪）**

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **消息ID** | **宏定义** | **说明** |
| 1 | 0xAB | ID\_GET\_VERSIONS | 获取版本信息 |
| 2 | 0xA1 | ID\_RESET | 系统复位 |
| 3 | 0xA7 | ID\_REQUEST\_UPGRADE | 请求固件升级 |
| 4 | 0xA8 | ID\_DOWNLOAD\_IMAGE | 下载固件数据 |
| 5 | 0xAC | ID\_CHECK\_IMAGE | 校验固件数据 |
| 6 | 0xA9 | ID\_WRITE\_IMAGE | 写入固件数据 |
| 7 | 0xA6 | ID\_GET\_WRITE\_STATUS | 获取固件写入状态 |
| 8 | 0xAD | ID\_GOTO\_APP | 运行APP固件 |
| 9 | 0xAE | ID\_GET\_TIMEOUT\_RETRYTIMES | 获取超时时间 |

## 3.1获取版本信息(0xAB)

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 1. 消息ID | 0xAB | | | |
| 消息描述 | 获取版本信息 | | | |
| 方向 | 🡪 反制枪 | | | |
| 发送频率 | 用户触发 | | | |
| 参数payload | 字节 | Name | Type | Description |
|  |  |  |  |
| 参数长度 | 0 | | | |
| 应答 | 有 | | | |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 消息ID | 0xAB | | | |
| 消息描述 | 获取版本信息 应答 | | | |
| 方向 | 反制枪 🡪 | | | |
| 发送频率 | 用户触发 | | | |
| 参数payload | 字节 | Name | Type | Description |
| 4 | runVersion | uint32\_t | 当前运行版  0:boot  1:app |
| 64 | appVersion | uint8\_t | 软件版本号，见版本定义 |
| 32 | bootVersion | uint8\_t | Bootloader版本号，见版本定义 |
| 32 | hwVersion | uint8\_t | 硬件版本号，见版本定义 |
| 32 | protocolVersion | uint8\_t | 协议版本号，见版本定义 |
| 参数长度 | 164 | | | |
| 应答 |  | | | |

## 3.2系统复位(0xA1)

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 1. 消息ID | 0xA1 | | | |
| 消息描述 | 系统复位 | | | |
| 方向 | 🡪 反制枪 | | | |
| 发送频率 | 用户触发 | | | |
| 参数payload | 字节 | Name | Type | Description |
| 2 | resetCode | uint16\_t | 确认码0x55AA |
| 2 | type | uint16\_t | 0x0000：无动作  0x0001：软件复位重启  0x0002：复位进入bootloader  0x0003：复位进入日志模式  0x0004：复位进入升级模式 |
| 参数长度 | 4 | | | |
| 应答 | 无 | | | |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 消息ID | 0xA1 | | | |
| 消息描述 | 系统复位 应答 | | | |
| 方向 | 反制枪 🡪 | | | |
| 发送频率 | 用户触发 | | | |
| 参数payload | 字节 | Name | Type | Description |
| 1 | status | uint8\_t | 成功：无回复  1：请求失败  10：状态错误  其他错误 |
| 参数长度 | 1 | | | |
| 应答 |  | | | |

## 3.3请求固件升级(0xA7)

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 消息ID | 0xA7 | | | |
| 消息描述 | 请求固件升级 | | | |
| 方向 | 🡪 反制枪 | | | |
| 发送频率 | 用户触发 | | | |
| 参数payload | 字节 | Name | Type | Description |
| 4 | headerLen | uint32\_t | 头的长度 |
| 4 | headerVersion | uint32\_t | 头的版本信息 |
| 4 | firmwareOffset | uint32\_t | 固件在当前文件的偏移量 |
| 4 | firmwareLength | uint32\_t | 固件长度 |
| 4 | firmwareCrc | uint32\_t | 固件crc信息(使用crc32计算) |
| 4 | corpInfoLen | uint32\_t | 公司信息长度 |
| 32 | corpInfo | uint8\_t | 公司信息 |
| 4 | devNameLen | uint32\_t | 产品名字长度 |
| 32 | devName | uint8\_t | 产品名称 |
| 4 | fwVersionLen | uint32\_t | 版本信息长度 |
| 64 | fwVersion | uint8\_t | 固件版本信息 |
| 92 | reserve | uint8\_t | 预留 |
| 4 | headCrc | uint32\_t | 头的crc信息 |
| 参数长度 | 256 | | | |
| 应答 | 有 | | | |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 消息ID | 0xA7 | | | |
| 消息描述 | 请求固件升级 应答 | | | |
| 方向 | 反制枪 🡪 | | | |
| 发送频率 | 用户触发 | | | |
| 参数payload | 字节 | Name | Type | Description |
| 1 | status | uint8\_t | 0：成功  1：请求失败  10：状态错误  其他错误 |
| 参数长度 | 1 | | | |
| 应答 |  | | | |

## 3.4下载固件数据(0xA8)

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 消息ID | 0xA8 | | | |
| 消息描述 | 下载固件数据 | | | |
| 方向 | 🡪 反制枪 | | | |
| 发送频率 | 用户触发 | | | |
| 参数payload | 字节 | Name | Type | Description |
| 4 | imageOffset | uint32\_t | 数据偏移位置 |
| 4 | imageLength | uint32\_t | 数据长度 |
| n | imageData | uint8\_t | 升级数据流，最大4096字节 |
| 参数长度 | 8+n | | | |
| 应答 | 有 | | | |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 消息ID | 0xA8 | | | |
| 消息描述 | 下载固件数据 应答 | | | |
| 方向 | 反制枪 🡪 | | | |
| 发送频率 | 用户触发 | | | |
| 参数payload | 字节 | Name | Type | Description |
| 1 | status | uint8\_t | 0：成功  1：下载出错  10：状态错误  其他错误 |
| 参数长度 | 1 | | | |
| 应答 |  | | | |

## 3.5校验固件数据(0xAC)

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 消息ID | 0xAC | | | |
| 消息描述 | 校验固件数据 | | | |
| 方向 | 🡪 反制枪 | | | |
| 发送频率 | 用户触发 | | | |
| 参数payload | 字节 | Name | Type | Description |
|  |  |  |  |
| 参数长度 | 0 | | | |
| 应答 | 有 | | | |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 消息ID | 0xAC | | | |
| 消息描述 | 校验固件数据 应答 | | | |
| 方向 | 反制枪 🡪 | | | |
| 发送频率 | 用户触发 | | | |
| 参数payload | 字节 | Name | Type | Description |
| 1 | status | uint8\_t | 0：成功  1：校验错误  10：状态错误  其他错误 |
| 参数长度 | 1 | | | |
| 应答 |  | | | |

## 3.6写入固件数据(0xA9)

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 消息ID | 0xA9 | | | |
| 消息描述 | 写入固件数据 | | | |
| 方向 | 🡪 反制枪 | | | |
| 发送频率 | 用户触发 | | | |
| 参数payload | 字节 | Name | Type | Description |
|  |  |  |  |
| 参数长度 | 0 | | | |
| 应答 | 有 | | | |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 消息ID | 0xA9 | | | |
| 消息描述 | 写入固件数据 应答 | | | |
| 方向 | 反制枪 🡪 | | | |
| 发送频率 | 用户触发 | | | |
| 参数payload | 字节 | Name | Type | Description |
| 1 | status | uint8\_t | 0：开始写入数据  1：启动写入失败  10：不在升级状态  其它：失败 |
| 参数长度 | 1 | | | |
| 应答 |  | | | |

## 3.7获取固件写入状态(0xA6)

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 消息ID | 0xA6 | | | |
| 消息描述 | 获取固件写入状态 | | | |
| 方向 | 🡪 反制枪 | | | |
| 发送频率 | 用户触发 | | | |
| 参数payload | 字节 | Name | Type | Description |
|  |  |  |  |
| 参数长度 | 0 | | | |
| 应答 | 有 | | | |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 消息ID | 0xA6 | | | |
| 消息描述 | 获取固件写入状态 应答 | | | |
| 方向 | 反制枪 🡪 | | | |
| 发送频率 | 用户触发 | | | |
| 参数payload | 字节 | Name | Type | Description |
| 1 | status | uint8\_t | 0：读取成功，写入中  1：写入失败  2：写入成功  10：不在写入状态  其它：失败 |
| 2 | permil | uint16\_t | 写入运行千分比 |
| 参数长度 | 3 | | | |
| 应答 |  | | | |

## 3.8运行APP固件(0xAD)

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 1. 消息ID | 0xAD | | | |
| 消息描述 | 运行APP固件 | | | |
| 方向 | 🡪 反制枪 | | | |
| 发送频率 | 用户触发 | | | |
| 参数payload | 字节 | Name | Type | Description |
|  |  |  |  |
| 参数长度 | 0 | | | |
| 应答 | 有 | | | |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 消息ID | 0xAD | | | |
| 消息描述 | 运行APP固件 应答 | | | |
| 方向 | 反制枪 🡪 | | | |
| 发送频率 | 用户触发 | | | |
| 参数payload | 字节 | Name | Type | Description |
| 1 | status | uint8\_t | 0：成功  1：运行失败  10：不在可运行状态  其它：失败 |
| 参数长度 | 1 | | | |
| 应答 |  | | | |

## 3.9获取超时时间(0xAE)

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 1. 消息ID | 0xAE | | | |
| 消息描述 | 获取超时时间和重试次数 | | | |
| 方向 | 🡪 反制枪 | | | |
| 发送频率 | 用户触发 | | | |
| 参数payload | 字节 | Name | Type | Description |
|  |  |  |  |
| 参数长度 | 0 | | | |
| 应答 | 有 | | | |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 消息ID | 0xAE | | | |
| 消息描述 | 获取超时时间和重试次数 应答 | | | |
| 方向 | 反制枪 🡪 | | | |
| 发送频率 | 用户触发 | | | |
| 参数payload | 字节 | Name | Type | Description |
| 2 | imagePkgLenMax | uint16\_t | 下载固件数据包最大字节数 |
| 2 | cmdTimeoutMs | uint16\_t | 指令超时时间 |
| 2 | chechTimeoutS | uint16\_t | 校验超时时间 |
| 2 | writeTimeoutS | uint16\_t | 写入超时时间 |
| 参数长度 | 8 | | | |
| 应答 |  | | | |

# 4附录A 参考资料

1、《基于ZYNQ 7EV芯片的反无产品固件升级方案》V1