



## 涂鸦 BLE 通用串口协议

设备接入 > MCU 开发接入 > BLE 单点通用方案 > 软件开发

文档版本: 20200727

[查看在线版本](#)

## 目录

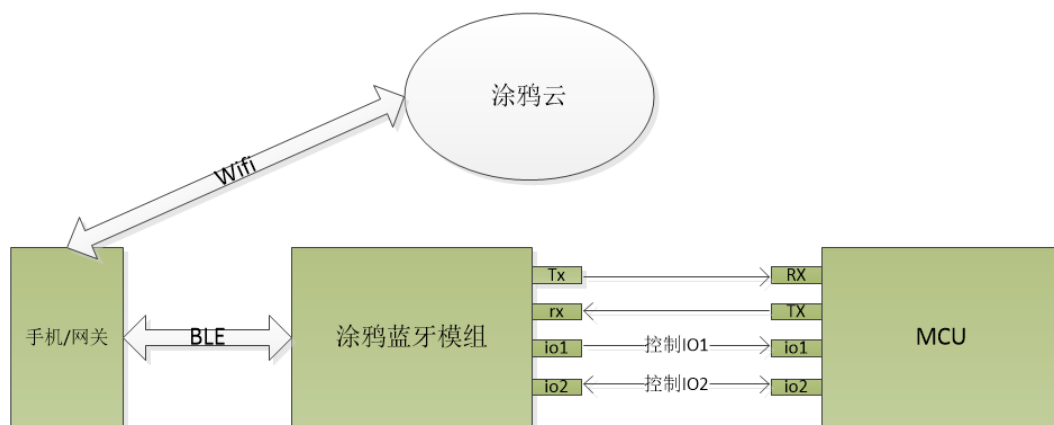
<b>1 概述</b>	<b>1</b>
1.1 文档说明	1
1.2 串口通讯约定	1
1.3 蓝牙参数说明	1
1.4 名称解释	2
1.5 帧数据包结构	3
1.6 Dp 格式说明	3
1.7 通用固件品类划分	4
<b>2 通用对接协议</b>	<b>6</b>
2.1 心跳包 (CMD-0x00)	6
2.2 获取 MCU 信息 (CMD-0x01)	7
2.3 请求模块工作模式 (CMD-0x02)	9
2.4 发送模块工作状态 (CMD-0x03)	10
2.5 重置模块 (CMD-0x04)	11
2.6 命令下发 (CMD-0x06)	13
2.7 状态上报 (CMD-0x07)	14
2.8 状态查询 (CMD-0x08)	16
2.9 模块解绑 (CMD-0x09)	17
2.10 记录型数据上报 (CMD-0xE0)	19
2.11 获取实时时间 (CMD-0xE1)	22
<b>3 MCU-OTA 部分接口</b>	<b>25</b>
3.1 查询 MCU 版本号 (CMD-0xE8)	25
3.2 MCU 主动发送当前版本号 (CMD-0xE9)	26
3.3 MCU-OTA 流程图	30
3.4 MCU-OTA 升级请求 (CMD-0xEA)	31
3.5 MCU-OTA 升级文件信息 (CMD-0xE8)	32
3.6 MCU-OTA 升级文件偏移请求 (CMD-0xEC)	34
3.7 MCU-OTA 升级数据 (CMD-0xED)	36
3.8 MCU-OTA 升级结束 (CMD-0xEE)	37

<b>4</b>	<b>产测相关接口</b>	<b>40</b>
4.1	RF 射频测试 (CMD-0x0E)	40
<b>5</b>	<b>低功耗功能附加协议</b>	<b>42</b>
5.1	各品类固件低功耗工作说明	42
5.2	使能低功耗功能 (CMD-0xE5)	45
5.3	修改低功耗模式下的广播间隔 (CMD-0xE2)	46
5.4	关闭系统计时器 (CMD-0xE4)	48
5.5	主动断开蓝牙连接 (CMD-0xE7)	50
5.6	模块唤醒管脚配置 (CMD-0xE3)	51
5.7	MCU 低功耗唤醒配置 (CMD-0xB0)	53
<b>6</b>	<b>门锁类通用固件附加协议</b>	<b>56</b>
6.1	动态密码 (CMD-0xE6)	56
6.2	请求上线 (CMD-0xA5)	58
6.3	离线密码 (CMD-0xA2)	59
6.4	蓝牙广播使能 (CMD-0xA3)	61
6.5	恢复出厂设置通知 (CMD-0xA1)	63
6.6	MCU 查询模块版本号 (CMD-0xA0)	64
6.7	门锁业务功能配置 (CMD-0xA6)	66
<b>7</b>	<b>健康类通用固件附加协议</b>	<b>68</b>
7.1	带标志位 DP 上报 (CMD-0xA4)	68

## 1 概述

### 1.1 文档说明

本文档主要为涂鸦 BLE 透传方案中串口协议描述。适用于如下架构的通讯方案：



### 1.2 串口通讯约定

名词	说明
波特率 (bps)	9600
数据位	8
奇偶校验	无
停止位	1
数据流控	无

### 1.3 蓝牙参数说明

- 门锁类通用固件

名词	说明
广播间隔	非低功耗模式下 100ms, 不可设置; 低功耗模式下默认 1000ms, MCU 可设置 0~2000ms(0 表示关闭)
连接参数	模块绑定已连接状态 (min_conn,max_conn,latency,timeout):(180ms,200ms,过程, (min_conn,max_conn,latency,timeout):(20ms,25ms,0
• 健康类通用固件	

名词	说明
广播间隔	非低功耗模式下 100ms, 不可设置; 低功耗模式下默认 1000ms, MCU 可设置 0~2000ms(0 表示关闭)
连接参数	模块绑定已连接状态 (min_conn,max_conn,latency,timeout):(180ms,200ms,过程, (min_conn,max_conn,latency,timeout):(20ms,25ms,0

## 1.4 名称解释

名词	说明
DP 点	一个 dp 点指的就是“一个功能点”或者“一条/一对指令码”，dp-data point。
PID	product id, 产品 id, 描述一类产品功能 (dp 点) 的集合。在涂鸦 IoT 平台创建的每一个产品都会产生一个唯一的产品编号，关联了产品具体的功能点、APP 控制面板、出货信息等所有跟这个产品相关的信息。

## 1.5 帧数据包结构

序号	长度 (byte)	字段	说明
0	2	帧头	0x55
1			0xAA
2	1	版本号	协议升级扩展用
3	1	命令字 CMD	具体帧类型
4	2	数据长度 Len	Len 高 8 位
5			Len 低 8 位
6~6+Len-1	Len	数据	
6+Len	1	CRC8	从帧头开始按字节求和得出的结果对 256 求余

说明：所有大于 1 个字节的数据均采用大端模式传输。

## 1.6 Dp 格式说明

字段	长度 (byte)	说明
dp_id	1	dp 点的指令码
dp_type	1	dp 点的数据类型
dp_data_len	2	dp 点的数据长度
dp_data_value	dp_data_len	dp 点的数据（具体参考 dp 规范）

Dp\_type 的取值范围及含义（云端定义）：

dp_type	取值	长度 (byte)	说明
raw	0x00	1~255	原始类型,HEX 数组
bool	0x01	1	布尔值
value	0x02	4	值类型 (int)
string	0x03	0~255	字符串 (可能为空)
enum	0x04	1	枚举型

## 1.7 通用固件品类划分

说明:

- 为了扩展蓝牙通用固件的功能,使通用固件具备某一品类的特性,对通用串口协议进行了扩展。目前,整个协议文档大致分为**通用对接协议**、**低功耗功能附加协议**、**门锁类通用固件附加协议**和**健康类通用固件附加协议**。
- 所有通用固件都支持通用对接协议,低功耗功能附加协议部分支持。而门锁类通用固件附加协议和健康类通用固件附加协议仅对应品类的通用固件支持。
- 各通用对接品类支持模块一览表:

通用对接品类	芯片/模组
门锁类	TYBN1、BK3431Q
健康类	BK3432、TYBT3L
其他类	TYBT3L、TYBT4L 等 telink 模组

- 有的模组会有多个品类的通用固件,
- 各芯片/模组最新固件协议接口详细支持情况,如下图:



# 1 概述

2 帧命令枚举

各芯片/模组最新固件协议接口支持情况								
接口名称 (单击传送门)	命令字CMD	TYEN1 (门机类)	BK3431Q (门机类)	BK3432 (道闸类)	ts825x (道闸类)	ts825x (其他)	ts826x (其他)	说明
通用对接接口	心跳检测	0x00	支持	支持	支持	支持	支持	
低功耗附加接口	查询产品信息	0x01	支持	支持	支持	支持	支持	
门机类附加接口	查询mcu 设定模块的工作模式	0x02	支持	支持	支持	支持	支持	
健康类附加接口	上报模块工作状态	0x03	支持	支持	支持	支持	支持	
产测附加接口	重置模块	0x04	支持	支持	支持	支持	支持	
米通用接口	命令下发	0x06	支持	支持	支持	支持	支持	
	状态上报	0x07	支持	支持	支持	支持	支持	
	状态查询	0x08	支持	支持	支持	支持	支持	
	门控参数上报 (离线唤醒)	0x09	支持	支持	不支持	支持	支持	
	门控实时时间	0x0E	支持	支持	支持	支持	支持	
	查询MCU版本号	0xE8	支持	支持	不支持	支持	支持	
	MCU主动发送版本号	0xE9	支持	支持	不支持	支持	支持	
	OTA升级请求	0xEA	支持	支持	不支持	支持	支持	
	OTA升级文件信息	0xEB	支持	支持	不支持	支持	支持	
	OTA升级文件清除	0xEC	支持	支持	不支持	支持	支持	
	OTA升级数据	0xED	支持	支持	不支持	支持	支持	
	OTA升级结束	0xEE	支持	支持	不支持	支持	支持	
	地址系统时间功能	0xE4	6.0+支持	3.0+支持	2.0+支持	支持	支持	
	低功耗功能	0xE5	不支持	不支持	2.0+支持	支持	支持	
	蓝牙唤醒功能	0xE7	支持	支持	支持	支持	支持	主要用于设备主动断开和手机等主机设备的连接
	低功耗模式广播唤醒	0xE2	支持	支持	不支持	支持	支持	主要用于控制低功耗模式下的功耗
	模块低功耗功耗策略配置	0xE3	不支持	不支持	2.0+支持	不支持	不支持	用于MCU配置低功耗策略模块的管脚
	设备密码	0xE6	支持	支持	不支持	不支持	不支持	
	MCU发送模块版本号	0xA0	支持	支持	不支持	不支持	不支持	
	恢复出厂设置通知	0xA1	支持	支持	支持	支持	不支持	APP点击恢复出厂设置后模块会向MCU发一个通知
	离线密码	0xA2	6.0+支持	2.0+支持	不支持	不支持	不支持	门机离线密码功能时使
	蓝牙广播功能	0xA3	6.0+支持	2.0+支持	不支持	不支持	不支持	可以用于广播控制配网的时机
	蓝牙上线	0xA5	6.0+支持	2.0+支持	不支持	支持	不支持	网关设备连接需求接口，主动上报需求接口
	门机业务功能配置	0xA6	待支持	待支持	不支持	不支持	不支持	配置一些门机业务的开关，默认是关闭的
	附加命令OP上报	0xA4	不支持	不支持	支持	支持	不支持	
	门机测试	0x0E	支持	支持	支持	支持	支持	产测接口，可以用于接口对模块做rsu测试
	重置模块连接状态	0xA0A	不支持	3.3+支持	不支持	支持	支持	

说明：（1）由于不同芯片/模组通用接口主要用途不一样，在协议接口上的支持情况不同。



## 2 通用对接协议

### 2.1 心跳包 (CMD-0x00)

说明：

- 模组上电后，以 3s 的间隔定期发送心跳。收到 MCU 的心跳包回应后，模组会认为 MCU 正常工作。在 MCU 首次（上电或重启）回复心跳包后，模组会向 MCU 查询产品信息。
- MCU 侧也可依据此心跳定期检测模块是否正常工作。若模块无心跳下发，则 MCU 可通过模块提供的硬件复位引脚复位模块。
- 模块在获取 MCU 信息之后，在低功耗模式下无心跳，正常功耗模式下以 10s 的间隔定期发送心跳。[特殊的：Telink模块在低功耗下无心跳，在获得MCU信息（PID）后也不再发送心跳包，因此也无法检测MCU是否发生重启。](#)

模块发送：

序号	长度 (byte)	字段	说明
0	2	帧头	0x55
1			0xAA
2	1	版本号	0x00
3	1	命令字 CMD	0x00
4	2	数据长度	0x00
5			0x00
6	1	CRC8	从帧头开始按字节求和得出的结果对 256 求余

MCU 返回：

序号	长度 (byte)	字段	说明
0	2	帧头	0x55
1			0xAA

序号	长度 (byte)	字段	说明
2	1	版本号	0x00
3	1	命令字 CMD	0x00
4	2	数据长度	0x00
5			0x01
6	1	State	见下表
7	1	CRC8	从帧头开始按字节求和得出的结果对 256 求余

State 返回值说明：

0x00：仅 MCU 上电后第一次收到模块心跳包后的返回值，模块端也可依据这一点判断工作过程中 MCU 是否重启。

0x01：除 MCU 重启后第一次返回 0x00 外，其余均返回此值。

## 2.2 获取 MCU 信息 (CMD-0x01)

说明：

- product key：固定为 8 字节，由涂鸦云开发者平台生成，用于云端记录产品相关信息。
- 产品信息由 product key 和 MCU 软件版本构成。
- MCU 软件版本号格式定义：采用点分十进制形式，“x.x.x” ( $0 \leq x \leq 99$ )，同时支持“x.x”及“x”形式，模块会自动扩展成“0.x.x”或“0.0.x”格式处理。

模块发送：

序号	长度 (byte)	字段	说明
0	2	帧头	0x55
1			0xAA

序号	长度 (byte)	字段	说明
2	1	版本号	0x00
3	1	命令字 CMD	0x01
4	2	数据长度	0x00
5			0x00
6	1	CRC8	从帧头开始按字节求和得出的结果对 256 求余

MCU 返回:

序号	长度 (byte)	字段	说明
0	2	帧头	0x55
1			0xAA
2	1	版本号	0x00
3	1	命令字 CMD	0x01
4	2	数据长度	0x00
5			0x0d
6~18	0x0d	Data	见下表
19	1	CRC8	从帧头开始按字节求和得出的结果对 256 求余

Data 格式:

1~8 9~13

PID 保留字段

例: 55 AA 00 01 00 0D 66 74 62 38 78 32 78 30 31 2E 30 2E 30 C0 (pid=ftb8x2x0,mcu ver=1.0.0) PID 为 8 位字符串, 如 “ftb8x2x0”。保留字段: 此字段原填充的是 MCU 软件版本号, 但模组目前不对该字段做解析, 字段保留。MCU 版本号通过 CMD E8\E9 上报。

## 2.3 请求模块工作模式 (CMD-0x02)

说明:

- 模块工作模式主要针对如何指示模块的工作状态以及如何重置模块而言, 主要分两种情况:
  - MCU 与模块配合处理, 即模块通过串口通知 MCU 模块当前的工作状态, 然后 MCU 提供显示支持; MCU 检测出模块的重置需求, 通过串口通知模块重置模块。
  - 模块自处理: 模块的工作状态通过模块的 GPIO 引脚驱动 LED 状态显示; 模块重置通过检测 GPIO 输入需求处理。(模块自处理重置为: 模块检测 GPIO 输入低电平持续 5s 以上触发模块重置。指示灯与按钮所使用的 GPIO 管脚由以下命令配置。)
- 目前仅支持 MCU 与模块配合处理模式。

模块发送:

序号	长度 (byte)	字段	说明
0	2	帧头	0x55
1			0xAA
2	1	版本号	0x00
3	1	命令字 CMD	0x02
4	2	数据长度	0x00
5			0x00
6	1	CRC8	从帧头开始按字节求和得出的结果对 256 求余

例: 55 aa 00 02 00 00 01

MCU 回复:

序号	长度 (byte)	字段	说明
0	2	帧头	0x55
1			0xAA
2	1	版本号	0x00
3	1	命令字 CMD	0x02
4	2	数据长度	0x00
5			0x00
6	1	CRC8	从帧头开始按字节求和得出的结果对 256 求余

例：55 AA 00 02 00 00 01

## 2.4 发送模块工作状态 (CMD-0x03)

说明：

- 模块工作状态：0x00-未绑定；0x01-绑定未连接；0x02-绑定已连接。~“模块自处理”工作模式相应的 LED 显示分别为：1-> 间隔闪烁 250ms；2-> 指示灯长灭；3-> 指示灯长亮。~
- 当模块收到 MCU 请求模块工作模式回复 CMD 0x02 后，则会向 MCU 下发模块工作状态。
- 当模块检测到模块状态发生变化，则主动下发模块状态至 MCU。
- 如设置模块工作模式为“模块自处理”，则 MCU 无需实现该协议。

模块发送：

序号	长度 (byte)	字段	说明
0	2	帧头	0x55
1			0xAA
2	1	版本号	0x00

序号	长度 (byte)	字段	说明
3	1	命令字 CMD	0x03
4	2	数据长度	0x00
5			0x01
6	1	State	见下表
7	1	CRC8	从帧头开始按字节求和得出的结果对 256 求余

State	工作状态说明	健康类/共享类通用固件注意
0x00	未绑定	健康类/共享类产品对“绑定”这个概念进行了模糊处理,
0x01	绑定未连接	未绑定和绑定未连接在健康类/共享类都认为是可配网状态
0x02	绑定已连接	绑定已连接在健康类/共享类认为是已配网已连接状态

## 2.5 重置模块 (CMD-0x04)

说明:

- 断开模块蓝牙连接, 解除蓝牙绑定关系, 清除模块离线缓存信息, 清除虚拟 ID, 重启。
- 由于之前Telink平台存在许多客户使用该接口作为解绑接口来使用, 为了不影响这部分客户的功能, Telnik平台重置后不会清除虚拟id。

MCU 发送:

序号	长度 (byte)	字段	说明
0	2	帧头	0x55
1			0xAA
2	1	版本号	0x00
3	1	命令字 CMD	0x04
4	2	数据长度	0x00
5			0x00
6	1	CRC8	从帧头开始按字节求和得出的结果对 256 求余

例：55 aa 00 04 00 00 03

模块回复：

序号	长度 (byte)	字段	说明
0	2	帧头	0x55
1			0xAA
2	1	版本号	0x00
3	1	命令字 CMD	0x04
4	2	数据长度	0x00
5			0x00
6	1	CRC8	从帧头开始按字节求和得出的结果对 256 求余

例：55 AA 00 04 00 00 03

## 2.6 命令下发 (CMD-0x06)

说明：

- datapoint 参考概述中 **dp 格式说明部分**。
- “命令下发” 可含多个 datapoint“命令数据单元”。
- “命令下发” 为异步处理协议，对应于 MCU 的 datapoint“状态上报”。

模块发送：

序号	长度 (byte)	字段	说明
0	2	帧头	0x55
1			0xAA
2	1	版本号	0x00
3	1	命令字 CMD	0x06
4	2	数据长度 Len	Len 高 8 位
5			Len 低 8 位
6~6+Len-1	Len	datapoint	见下表
6+Len	1	CRC8	从帧头开始按字节求和得出的结果对 256 求余

datapoint 格式：

datapoint 1

datapoint N

1

2

3~4

5~

n

n+1



n+1~n+2

n+3~

dp\_id

dp\_type

dp\_len

dp\_data

dp\_id

dp\_type

dp\_len

dp\_data

例：55 aa 00 06 00 05 03 01 00 01 01 10

MCU 返回：无

## 2.7 状态上报 (CMD-0x07)

说明：

- datapoint 参考概述中 **dp 格式说明部分**。
- “状态上报”可含多个 datapoint“命令数据单元”。
- “状态上报”为异步处理协议，“状态上报”触发机制有三类：
  1. MCU 收到“命令下发处理帧”时，正确执行相应 datapoint 命令，再通过“状态上报”帧将变化后的 datapoint 状态发送至模块；
  2. MCU 主动检测到 datapoint 有变化，将变化后的 datapoint 状态发送至模块；
  3. MCU 收到状态查询帧时，将所有的 datapoint 状态发送至模块。

MCU 发送：

序号	长度 (byte)	字段	说明
0	2	帧头	0x55
1			0xAA
2	1	版本号	0x00

序号	长度 (byte)	字段	说明
3	1	命令字 CMD	0x07
4	2	数据长度 Len	Len 高 8 位
5			Len 低 8 位
6~6+Len-1	Len	datapoint	见下表
6+Len	1	CRC8	从帧头开始按字节求和得出的结果对 256 求余

datapoint 格式:

datapoint 1

datapoint N

1

2

3~4

5~

n

n+1

n+1~n+2

n+3~

dp\_id

dp\_type

dp\_len

dp\_data

dp\_id

dp\_type

dp\_len

dp\_data

例：55 aa 00 06 00 05 03 01 00 01 01 10

模块返回：

序号	长度 (byte)	字段	说明
0	2	帧头	0x55
1			0xAA
2	1	版本号	0x00
3	1	命令字 CMD	0x07
4	2	数据长度	0x00
5			0x01
6	1	State	见下表
7	1	CRC8	从帧头开始按字节求和得出的结果对 256 求余

State 返回值说明：

0x00：成功

0x01：失败

## 2.8 状态查询 (CMD-0x08)

说明：

- “状态查询”为异步处理协议，主要用于模块查询 MCU 所有的“obj”类型的 datapoint 状态，当 MCU 收到此帧时，通过 CMD 0x07 状态上报帧上报 datapoint 状态。
- “状态查询”发送时机主要有两种：
  - 模块绑定已连接状态下，检测到 MCU 发生重启（通过心跳回复判断），查询发送；（备注：TelinK通用固件不支持检测MCU重启）。

2. 模块蓝牙离线再上线（由绑定未连接状态变化成绑定已连接状态）的情况，查询发送。

模块发送：

序号	长度 (byte)	字段	说明
0	2	帧头	0x55
1			0xAA
2	1	版本号	0x00
3	1	命令字 CMD	0x08
4	2	数据长度	0x00
5			0x00
6	1	CRC8	从帧头开始按字节求和得出的结果对 256 求余

例：55 aa 00 08 00 00 07

MCU 返回：无

## 2.9 模块解绑 (CMD-0x09)

说明：

- 仅解除和手机的绑定关系，并且断开蓝牙连接，不会清除数据和虚拟 ID。
- 备注：健康类（共享类）通用固件“绑定”概念被模糊处理了，故不支持模块解绑接口。

MCU 发送：

序号	长度 (byte)	字段	说明
0	2	帧头	0x55
1			0xAA
2	1	版本号	0x00

序号	长度 (byte)	字段	说明
3	1	命令字 CMD	0x09
4	2	数据长度	0x00
5			0x00
6	1	CRC8	从帧头开始按字节求和得出的结果对 256 求余

模块返回:

序号	长度 (byte)	字段	说明
0	2	帧头	0x55
1			0xAA
2	1	版本号	0x00
3	1	命令字 CMD	0x09
4	2	数据长度	0x00
5			0x01
6	1	State	见下表
7	1	CRC8	从帧头开始按字节求和得出的结果对 256 求余

State 返回值说明:

0x00: 成功

0x01: 失败

## 2.10 记录型数据上报 (CMD-0xE0)

说明：

- 该接口主要用于重要数据的上报，如果上报时模块处于离线状态，模块会将数据存储在模块 flash 中，待模块上线再上报至 APP；如果模块在线时，会在最后一条数据上报成功（连续上报的最后一条）后，释放缓存的数据至 app。
- 模块可存储最多存储 N 条 DP 数据，记录将循环覆盖存储：（详情查看功能解析部分）

- nrf52832/BK3431q 最多可存储 80 条，每条数据最长 200 字节。
- nrf52832/BK3431q 最多可存储 80 条，每条数据最长 200 字节。
- bk3432 最多存储 32 条，每条数据最长 32 字节。

- 蓝牙模块内部时钟精度有限，24 小时误差小于 1 分钟，但每次重连会重新校准时钟，如果对精度要求高的用户建议使用 MCU 自带时间上报。> 注意：无论设备是在线还是离线状态，记录型数据【强烈建议】使用该接口上报。

MCU 发送：

序号	长度 (byte)	字段	说明
0	2	帧头	0x55
1			0xAA
2	1	版本号	0x00
3	1	命令字 CMD	0xE0
4	2	数据长度 Len	Len 高 8 位
5			Len 低 8 位
6~6+Len-1	Len	Data	见下表
6+Len	1	CRC8	从帧头开始按字节求和得出的结果对 256 求余

Data 格式：

Report format

unix\_time\_string(optional)

datapoint 1

datapoint n

1

2~x

x

x+1

x+2~x+3

x+4~

n

n+1

n+1~n+2

n+3~

TYPE

unix\_time\_string(13byte)

dp\_id

dp\_type

dp\_len

dp\_data

dp\_id

dp\_type

dp\_len

dp\_data

说明:

TYPE	说明
0x01	格式 1-蓝牙模块自带时间上报
0x02	格式 2-只上报原始数据，时间为实际上报时候的实时时间
0x03	格式 3-MCU 自带时间上报

unix\_time\_string: 仅 TYPE 等于 0x02 时需要填, 其他格式不用填。

例:

- 格式 1-蓝牙模块自带时间上报: 55 AA 00 E0 00 17 01 66 02 00 04 00 00 00 01 67 03 00 05 72 77 72 77 77 68 04 00 01 00 89
- 格式 2-只上报原始数据, 时间为实际上报时候的实时时间: 55 AA 00 E0 00 1B 02 66 02 00 04 00 00 00 01 67 03 00 09 72 77 72 77 77 61 66 61 66 68 04 00 01 00 20
- 格式 3-MCU 自带时间上报: 55 AA 00 E0 00 28 03 31 35 38 39 31 36 38 33 32 37 30 30 30 66 02 00 04 00 00 00 01 67 03 00 09 72 77 72 77 77 61 66 61 66 68 04 00 01 00 D0

模块返回:

序号	长度 (byte)	字段	说明
0	2	帧头	0x55
1			0xAA
2	1	版本号	0x00
3	1	命令字 CMD	0xE0
4	2	数据长度	0x00
5			0x01
6	1	State	见下表
7	1	CRC8	从帧头开始按字节求和得出的结果对 256 求余

State 返回值说明:

0x00: 存储成功

其他: 存储失败



## 2.11 获取实时时间 (CMD-0xE1)

说明:

- 年月日格式时间请求建议使用格式 0x02。
- 设备上线后会主动同步一次云端时间给 MCU。

MCU 返回:

序号	长度 (byte)	字段	说明
0	2	帧头	0x55
1			0xAA
2	1	版本号	0x00
3	1	命令字 CMD	0xE1
4	2	数据长度	0x00
5			0x01
6	1	Time_Type	见下表
7	1	CRC8	从帧头开始按字节求和得出的结果对 256 求余

Time\_type 说明:

Time_Type	说明
0x00	格式 0-获取 7 字节时间时间类型 +2 字节时区信息
0x01	格式 1-获取 13 字节 ms 级 unix 时间 +2 字节时区信息
0x02	格式 2-获取 7 字节时间时间类型 +2 字节时区信息

备注：格式0获取自定义时间存在不同平台兼容性问题，后面版本会废除，年月日时间格式建议使用0x02格式。Telink通用固件已经不再支持格式0，请求格式0时间则会返回格式2时间。

模块返回：

序号	长度 (byte)	字段	说明
0	2	帧头	0x55
1			0xAA
2	1	版本号	0x00
3	1	命令字 CMD	0xE1
4	2	数据长度 Len	Len 高 8 位
5			Len 低 8 位
6~6+Len-1	Len	Time_Data	见下表
6+Len	1	CRC8	从帧头开始按字节求和得出的结果对 256 求余

• Time\_Data 格式 0：

结果码	时间格式	年	月	日	时	分	秒	星期	时区
1	2	3	4	5	6	7	8	9	10~11
Result	Time_Type	year	month	day	hour	min	sec	week	time_zone

• Time\_Data 格式 1：

结果码	时间格式	ms 级 unix 时间	时区
1	2	3~15	16~17
Result	Time_Type	unix_time_string	time_zone

- Time\_Data 格式 2:

结果码	时间格式	年	月	日	时	分	秒	星期	时区
1	2	3	4	5	6	7	8	9	10~11
Result	Time_Type	year	month	day	hour	min	sec	week	time_zone

Result 为 0x00 表示成功，其他表示失败。

例:

- Time\_Data 格式 0: > MCU-55 AA 00 E1 00 01 00 E1 > 模块-55 AA 00 E1 00 0B 00 00 01 0C 1E 0F 34 1F 01 03 20 9C //2019 年 12 月 30 日 15 点 52 分 31 秒星期一东八区
- Time\_Data 格式 1: > MCU-55 AA 00 E1 00 01 01 E2 > 模块-55 AA 00 E1 00 11 00 01 31 35 37 37 36 39 32 33 39 35 30 30 30 03 20 BB// 时间戳 1577692395000 东八区
- Time\_Data 格式 2: > MCU-55 AA 00 E1 00 01 02 E3 > 模块-55 AA 00 E1 00 0B 00 02 13 0C 1E 10 09 29 01 03 20 90 //2019 年 12 月 30 日 16 点 09 分 35 秒星期一东八区

## 3 MCU-OTA 部分接口

### 3.1 查询 MCU 版本号 (CMD-0xE8)

说明:

模块需要在每次发送获取 MCU 信息时, 同时发送查询 mcu 版本号指令。

模块发送:

序号	长度 (byte)	字段	说明
0	2	帧头	0x55
1			0xAA
2	1	版本号	0x00
3	1	命令字 CMD	0xE8
4	2	数据长度	0x00
5			0x00
6	1	CRC8	从帧头开始按字节求和得出的结果对 256 求余

MCU 返回:

序号	长度 (byte)	字段	说明
0	2	帧头	0x55
1			0xAA
2	1	版本号	0x00
3	1	命令字 CMD	0xE8
4	2	数据长度	0x00
5			0x06

序号	长度 (byte)	字段	说明
6~11	6	DATA	见下表
12	1	CRC8	从帧头开始按字节求和得出的结果对 256 求余

DATA 格式:

Mcu 当前固件版本号

Mcu 当前硬件版本号

1

2

3

4

5

6

Soft\_Ver

Hard\_ver

版本号, 例如 0x01 00 02 代表版本为 V1.0.2。

硬件版本号: PCBA 版本号。

### 3.2 MCU 主动发送当前版本号 (CMD-0xE9)

说明:

- 为了确保模块及时获取到 MCU 版本信息, MCU 在每次启动时 (一般在串口初始化后) 需要主动发送一次当前版本号到模块, 如果没有收到模块的响应, 需要再次发送。

MCU 返回:

序号	长度 (byte)	字段	说明
0	2	帧头	0x55
1			0xAA
2	1	版本号	0x00
3	1	命令字 CMD	0xE9
4	2	数据长度	0x00
5			0x06
6~11	6	DATA	见下表
12	1	CRC8	从帧头开始按字节求和得出的结果对 256 求余

DATA 格式:

Mcu 当前固件版本号

Mcu 当前硬件版本号

1

2

3

4

5

6

Soft\_Ver

Hard\_ver

版本号, 例如 0x01 00 02 代表版本为 V1.0.2。

硬件版本号: PCBA 版本号

模块返回:

序号	长度 (byte)	字段	说明
0	2	帧头	0x55
1			0xAA
2	1	版本号	0x00
3	1	命令字 CMD	0xE9
4	2	数据长度	0x00
5			0x01
6	1	State	见下表
7	1	CRC8	从帧头开始按字节求和得出的结果对 256 求余

State 返回值说明：

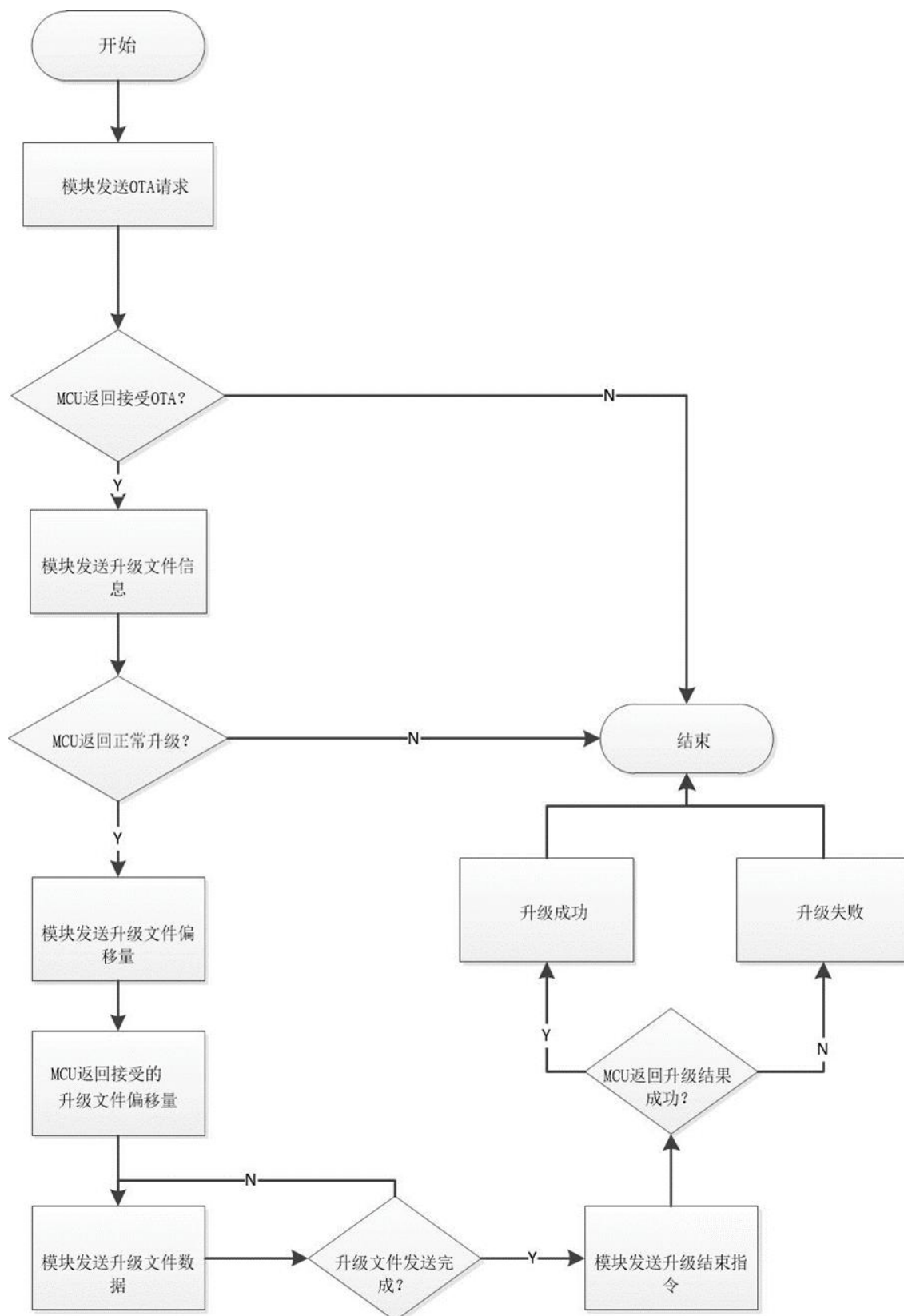
0x00：成功

其他：失败





## 3.3 MCU-OTA 流程图



### 3.4 MCU-OTA 升级请求 (CMD-0xEA)

模块发送:

序号	长度 (byte)	字段	说明
0	2	帧头	0x55
1			0xAA
2	1	版本号	0x00
3	1	命令字 CMD	0xEA
4	2	数据长度	0x00
5			0x02
6~7	2	最大单包数据长度	见下表
8	1	CRC8	从帧头开始按字节求和得出的结果对 256 求余

说明: 最大单包数据长度 Len1-设备允许的单包数据最大长度, 单位字节。

例: 55 AA 00 EA 00 02 00 C8 B3

MCU 回复:

序号	长度 (byte)	字段	说明
0	2	帧头	0x55
1			0xAA
2	1	版本号	0x00
3	1	命令字 CMD	0xEA
4	2	数据长度	0x00
5			0x06
6~11	6	Data	见下表

序号	长度 (byte)	字段	说明
12	1	CRC8	从帧头开始按字节求和得出的结果对 256 求余

Data 格式:

1

2

3

4

5

6

Flag

Mcu 当前固件版本号 version

可接受最大数据长度 len2

Flag: 0x00-允许升级, 0x01-拒绝升级。

Version: 当前固件版本号, 例如 0x01 00 02 代表版本为 V1.0.2。

Len1: 模块限定最大单包数据长度。

Len2: MCU 可接受最大包长度, 如果 len1 < len2, 升级以 len1 为准, 反之以 len2 为准。

例: 55 AA 00 EA 00 06 00 01 00 00 00 C8 B8

### 3.5 MCU-OTA 升级文件信息 (CMD-0xE8)

模块发送:

序号	长度 (byte)	字段	说明
0	2	帧头	0x55
1			0xAA

序号	长度 (byte)	字段	说明
2	1	版本号	0x00
3	1	命令字 CMD	0xEB
4	2	数据长度	0x00
5			0x23
6~40	35	Data	见下表
41	1	CRC8	从帧头开始按字节求和得出的结果对 256 求余

Data 格式:

8 字节	3 字节	16 字节	4 字节	4 字节
产品 PID	文件版本	文件 MD5	文件长度	CRC32

PID: MCU 的 PID。文件版本: 例如, 0x010002 代表版本为 V1.0.2。文件 MD5: 升级固件的 md5 值。文件长度: 升级固件的总长度, 单位字节。CRC32: 升级固件的 CRC32。

MCU 回复:

序号	长度 (byte)	字段	说明
0	2	帧头	0x55
1			0xAA
2	1	版本号	0x00
3	1	命令字 CMD	0xEB
4	2	数据长度	0x00
5			0x19
6~30	25	Data	见下表

序号	长度 (byte)	字段	说明
31	1	CRC8	从帧头开始按字节求和得出的结果对 256 求余

Data 格式:

1 字节	4 字节	4 字节	16 字节
STATE	已储存文件长度	已储存文件 CRC32	已储存文件 MD5 (目前不使用)

STATE: 0x00-正常升级。0x01-产品 PID 不一致。0x02-文件版本低于或者等于当前版本。0x03-文件大小超过范围其他-保留。

说明: 为了支持断点续传, 这里会返回设备端已经储存的文件信息, APP 在收到后, 首先根据设备返回的已储存文件长度计算新文件对应长度的 CRC32, 然后和设备返回的 CRC32 对比, 如果两者都吻合, 那么下面的文件起始传输请求中将起始传输偏移量改为该长度值, 否则文件起始传输偏移量改为 0, 表示从头开始传输。

注意: 每次断点续传都会完全按照 MCU OTA 流程的顺序, 从 OTA 升级请求开始, 所以 MCU 端如果有维护升级状态的话, 需要在收到模块工作状态为非绑定已连接的其他状态的时候要重置升级状态, 以确保可以开始下一个升级流程。

### 3.6 MCU-OTA 升级文件偏移请求 (CMD-0xEC)

模块发送:

序号	长度 (byte)	字段	说明
0	2	帧头	0x55
1			0xAA
2	1	版本号	0x00
3	1	命令字 CMD	0xEC

序号	长度 (byte)	字段	说明
4	2	数据长度	0x00
5			0x04
6~9	4	OFFSET	见下表
10	1	CRC8	从帧头开始按字节求和得出的结果对 256 求余

说明：offset-文件起始传输偏移量，四字节。

例：55 AA 00 EA 00 02 00 C8 B3

MCU 回复：

序号	长度 (byte)	字段	说明
0	2	帧头	0x55
1			0xAA
2	1	版本号	0x00
3	1	命令字 CMD	0xEC
4	2	数据长度	0x00
5			0x04
6~9	4	OFFSET	见下表
10	1	CRC8	从帧头开始按字节求和得出的结果对 256 求余

offset：MCU 要求的起始传输文件偏移量

说明：实际文件传输的偏移地址应该以 mcu 端要求的为准，且 mcu 端要求的地址会小于等于 APP 端给出的偏移。

### 3.7 MCU-OTA 升级数据 (CMD-0xED)

模块发送:

序号	长度 (byte)	字段	说明
0	2	帧头	0x55
1			0xAA
2	1	版本号	0x00
3	1	命令字 CMD	0xED
4	2	数据长度 Len	Len 高 8 位
5			Len 低 8 位
6~6+Len-1	Len	Data	见下表
6+Len	1	CRC8	从帧头开始按字节求和得出的结果对 256 求余

Data 格式:

2 字节	2 字节	2 字节	n 字节
包号	当前包数据长度 n	当前包数据 CRC16	当前包数据

注: 包号从 0 开始, 当前包数据长度不能大于 OTA 升级请求指令制定的最大包长度。

MCU 回复:

序号	长度 (byte)	字段	说明
0	2	帧头	0x55
1			0xAA
2	1	版本号	0x00

序号	长度 (byte)	字段	说明
3	1	命令字 CMD	0xED
4	2	数据长度	0x00
5			0x01
6	1	State	见下表
7	1	CRC8	从帧头开始按字节求和得出的结果对 256 求余

说明:

State	说明
0x00	成功
0x01	包号异常
0x02	长度不一致
0x03	CRC 校验失败
0x04	其他

### 3.8 MCU-OTA 升级结束 (CMD-0xEE)

模块发送:

序号	长度 (byte)	字段	说明
0	2	帧头	0x55
1			0xAA
2	1	版本号	0x00
3	1	命令字 CMD	0xEE



序号	长度 (byte)	字段	说明
4	2	数据长度	0x00
5			0x00
6	1	CRC8	从帧头开始按字节求和得出的结果对256 求余

MCU 回复:

序号	长度 (byte)	字段	说明
0	2	帧头	0x55
1			0xAA
2	1	版本号	0x00
3	1	命令字 CMD	0xEE
4	2	数据长度	0x00
5			0x01
6	1	State	见下表
7	1	CRC8	从帧头开始按字节求和得出的结果对256 求余

说明:

State	说明
0x00	成功
0x01	数据总长度错误
0x02	长度不一致



State	说明
0x03	其他

## 4 产测相关接口

### 4.1 RF 射频测试 (CMD-0x0E)

说明：

- 为了检测出厂后蓝牙模块的射频是否正常工作，需要测试模块的 RSSI 信号强度。
- 测试工具：蓝牙信标（涂鸦提供），作用：发射名称为 ty\_mdev 的广播信号。
- 测试步骤：首先将信标放在距离模块较近（0.5 米左右）的地方。然后通过串口发送该 rf 射频测试指令，模块会搜索蓝牙信标并返回信号强度值，一般信号强度大于-70db 认为模块射频工作正常。

注意：

- 一些特殊芯片/模块，目前只有BK3431Q,BK3432，这类模块不支持扫描信标的方式，测试 RSSI需要使用以下工具：
- 测试工具：蓝牙 dongle （涂鸦提供），作用：连接被测设备并返回 rssi。
- 测试步骤：首先将 dongle 放在距离模块较近（0.5 米左右）的地方。然后通过串口向模块发送该 rf 射频测试指令，dongle 会连接模块并返回信号强度值，一般信号强度大于-70db 认为模块射频工作正常。
- 模块需要保持非低功耗模式，且模块处于非绑定状态。

MCU 发送：

序号	长度 (byte)	字段	说明
0	2	帧头	0x55
1			0xAA
2	1	版本号	0x00
3	1	命令字 CMD	0x0E
4	2	数据长度	0x00
5			0x00
6	1	CRC8	从帧头开始按字节求和得出的结果对 256 求余

模块回复：

序号	长度 (byte)	字段	说明
0	2	帧头	0x55
1			0xAA
2	1	版本号	0x00
3	1	命令字 CMD	0x0E
4	2	数据长度 Len	Len 高 8 位
5			Len 低 8 位
6~6+Len-1	Len	Data	见下表
6+Len	1	CRC8	从帧头开始按字节求和得出的结果对 256 求余

Data 格式：

Data	说明
{"ret":true,"rssi":"-55"}	信号强度为-55db
{"ret":false}	没有搜索到该信号

## 5 低功耗功能附加协议

### 5.1 各品类固件低功耗工作说明

不同品类的通用固件在低功耗工作设计上有一些差别，下面将分别描述：

#### 1. 门锁类低功耗工作说明-TYBN1/BK3431Q

- 模块在获得 MCU 信息后，低功耗状态将不再发送心跳包，非低功耗下心跳包正常。
- 模块在获得 MCU 信息后，低功耗状态将不再发送心跳包，非低功耗下心跳包正常。
- 工作模式分为低功耗模式和非低功耗模式。
- 非低功耗模式蓝牙广播间隔固定为 100ms，模块串口可上行可下行。
- 低功耗模式蓝牙广播间隔为 MCU 设置的参数（如果是 0 则关闭广播，默认 1s），该模式下模块串口下行正常工作，上行禁用（不接收 MCU 串口数据）。
- 模块的低功耗工作状态由模块低功耗控制管脚 SCL 的电平决定，MCU 可以通过 SCL 输出不同电平控制模块的功耗状态，具体参考下表：

平台说明	模块低功耗控制管脚 SCL	低功耗对应的 SCL 电平	非低功耗对应的 SCL 电平
NORDIC	IO11	高	低
BK	P03	低	高

建议在唤醒模块后延时 20ms 再使用串口。

- 模块唤醒外部 MCU 的引脚为 SDL，当模块需要发送数据给外部 MCU 时，模块会改变 SDL 的电平 200ms，然后再发送数据，发送完成后恢复默认电平。

平台说明	模块唤醒 MCU 管脚 SDL	发数据时 SDL 电平	空闲时 SDL 电平
NORDIC	IO14	低	高
BK	P10	高	低

- 不支持使能低功耗接口，无需使能，直接由模块低功耗控制管脚 SCL 的电平决定。

- 不支持关闭系统计时功能。

注意：SCL 各平台默认上下拉情况可能存在差异，MCU 端与 SCL 对接引脚不要使用悬空状态。

## 2. 健康类低功耗工作说明-BK3432/BT3L

- 模块在获得 MCU 信息后, 低功耗状态将停止心跳包, 非低功耗下心跳包周期为 10s。注意：Telink 平台只有非低功耗下才有心跳。
- 模块将在每次连接事件后自动获取 APP 时间以校准蓝牙模块内部时间, 该模块内部 RTC 精度取决于晶振的质量, 对时间精度高的用户务必测量模块内部 RTC 的精度或外挂高精度 RTC, 测试程序可通过 FAE/产品经理找研发要。
- 工作模式分为低功耗模式和非低功耗模式。
- 非低功耗模式蓝牙广播间隔固定为 100ms, 模块串口可上行可下行。
- 低功耗模式蓝牙广播关闭, 可以维持蓝牙连接, 该模式下模块串口下行正常工作, 上行禁用 (不接收 MCU 串口数据)。
- 模块的低功耗工作状态由模块低功耗控制管脚 SCL 的电平决定, MCU 可以通过 SCL 输出不同电平控制模块的功耗状态, 具体参考下表:

平台说明	模块低功耗控制管脚 SCL	低功耗对应的 SCL 电平	非低功耗对应的 SCL 电平
BK3432	P03 (可配置)	低	高
BT3L	TL_B5	低	高

建议在唤醒模块后延时 20ms 再使用串口。

- 默认关闭低功耗, 需要使能低功耗后才能进入低功耗模式。
- 可选择关闭低功耗下系统计时以降低功耗, 默认关闭。
- BK3432 可依据心跳回应自动识别 MCU 使用的是哪一个串口, 识别一次后永久记忆。需要更换串口必须重新烧录授权模块固件。

注意：SCL 各平台默认上下拉情况可能存在差异，MCU 端与 SCL 对接引脚不要使用悬空状态。

## 3. 其他类低功耗工作说明-Telink平台

- 将模块低功耗管脚拉低后，模块串口不再接受数据，但是蓝牙通信和串口下发仍然正常工作。管脚拉高后，模块串口接受正常使用。
- 将模块低功耗管脚拉低后，模块串口不再接受数据，但是蓝牙通信和串口下发仍然正常工作。管脚拉高后，模块串口接受正常使用。
- 当模块绑定处于绑定已连接状态，将拉高连接状态指示管脚通知 MCU，断开连接后将自动拉低连接状态指示管脚。
- 当模块从低功耗模式下唤醒时，需要延时 10ms，模块串口才能接受到 MCU 数据。当模块处于深度睡眠模式，唤醒模块后，将重启模块，此时需要延时 600ms，串口才能接受数据。

模组说明	模块低功耗控制管脚 SCL	低功耗对应的 SCL 电平	非低功耗对应的 SCL 电平
BT3L	模组丝印 TL_B5 管脚	低	高

- 每次连接后模块将自动获取 APP 时间以校准蓝牙模块内部时间，泰凌微模块没有使用外部 rtc，时钟精度不是很高，24 小时低于 1 分钟，对时钟精度要求高的可以外接。
- 当供电电压低于正常工作电压时，芯片内部 flash 操作将有出错的风险，造成固件或者用户数据被异常修改。有两种方法可以避免：

1. 当 MCU 检测到电池电压过低时，切断模块工作电源
  2. 当 MCU 检测到电池电压过低时，可以关闭广播和系统计时，让芯片处于深度睡眠模式，从而不会工作。泰凌微模块最低工作电压为 1.8V，MCU 可以设置在 2.0V(要略高于 1.8V) 关闭模块。
- 模块唤醒外部 MCU 的引脚为 SDL，当模块需要发送数据给外部 MCU 时，模块会改变 SDL 的电平 10ms，然后再发送数据，发送完成后恢复默认电平。

模组说明	模块唤醒 MCU 管脚 SDL	发数据时 SDL 电平	空闲时 SDL 电平
BT3L	模组丝印 TL_D2 管脚	高	低

## 5.2 使能低功耗功能 (CMD-0xE5)

说明：

- 门锁类通用固件暂不支持（TYBN1 通用固件和 BK3431Q 通用固件）
- 模块出厂时为非低功耗模块，需要通过该指令使能低功耗功能。然后才能通过拉低低功耗使能管脚，使模块进入低功耗状态。该设置将永久储存。

MCU 发送：

序号	长度 (byte)	字段	说明
0	2	帧头	0x55
1			0xAA
2	1	版本号	0x00
3	1	命令字 CMD	0xE5
4	2	数据长度	0x00
5			0x01
6	1	Data	见下表
7	1	CRC8	从帧头开始按字节求和得出的结果对 256 求余

Data 格式：

Data	说明
0x00	关闭低功耗功能
0x01	打开低功耗功能

模块恢复：



序号	长度 (byte)	字段	说明
0	2	帧头	0x55
1			0xAA
2	1	版本号	0x00
3	1	命令字 CMD	0xE5
4	2	数据长度	0x00
5			0x01
6	1	State	见下表
7	1	CRC8	从帧头开始按字节求和得出的结果对 256 求余

State 返回值说明:

0x00: 设置成功

其他: 设置失败

### 5.3 修改低功耗模式下的广播间隔 (CMD-0xE2)

说明:

- BK3432 健康类通用固件暂不支持
- 为降低休眠时的功耗, 可以通过该指令修改广播间隔, 广播参数将永久保存。当设置为 0 时, 将关闭广播。该设置将永久储存。
- 低功耗下广播间隔默认1s, 广播间隔越大连接所需要的时间越长, 甚至某些性能差手机可能很难连接上, 不建议客户修改更大的广播间隔值。

MCU 发送:

序号	长度 (byte)	字段	说明
0	2	帧头	0x55
1			0xAA
2	1	版本号	0x00
3	1	命令字 CMD	0xE2
4	2	数据长度	0x00
5			0x01
6	1	Adv_interval	见下表
7	1	CRC8	从帧头开始按字节求和得出的结果对 256 求余

Adv\_interval: 可设置数值范围为 0 到 20, 单位为 100ms, 即实际广播间隔范围为 100ms 到 2 秒, 当设置数值为 0 时将关闭广播

例: 55 aa 00 E2 00 01 00 E2(设置低功耗模式下关闭广播) 55 aa 00 E2 00 01 06 E8 (设置低功耗下广播间隔为 600ms)

模块恢复:

序号	长度 (byte)	字段	说明
0	2	帧头	0x55
1			0xAA
2	1	版本号	0x00
3	1	命令字 CMD	0xE2
4	2	数据长度	0x00
5			0x01
6	1	State	见下表

序号	长度 (byte)	字段	说明
7	1	CRC8	从帧头开始按字节求和得出的结果对 256 求余

State 返回值说明:

0x00: 设置成功

其他: 设置失败

#### 5.4 关闭系统计时器 (CMD-0xE4)

说明:

- 为降 Telink 芯片低休眠时的功耗, 可以通过该指令关闭蓝牙模块内部计时功能, 如果 MCU 不需要时间功能, 可以关闭改功能, 当计时功能和广播功能都关闭后, 然后拉低 SDA, 模块将进入深度睡眠, 功耗降低至 3ua, 唤醒后, 模块重启, 重新运行。该设置将永久储存。
- BK3431Q 和 TYBN1 中, 由于单纯计时功耗比较低, 主要耗电的是存 flash 操作, 这里只是关闭了 flash 存储操作。打开后, 时钟可周期性 (1min) 存 flash, 可解决重启后模块 RTC 时钟时间重置的问题。(默认为关闭)

MCU 发送:

序号	长度 (byte)	字段	说明
0	2	帧头	0x55
1			0xAA
2	1	版本号	0x00
3	1	命令字 CMD	0xE4
4	2	数据长度	0x00
5			0x01

序号	长度 (byte)	字段	说明
6	1	Data	见下表
7	1	CRC8	从帧头开始按字节求和得出的结果对 256 求余

Data 格式:

Data	说明
0x00	关闭系统计时器
0x01	打开系统计时器

模块恢复:

序号	长度 (byte)	字段	说明
0	2	帧头	0x55
1			0xAA
2	1	版本号	0x00
3	1	命令字 CMD	0xE4
4	2	数据长度	0x00
5			0x01
6	1	State	见下表
7	1	CRC8	从帧头开始按字节求和得出的结果对 256 求余

State 返回值说明:

0x00: 设置成功

其他: 设置失败

## 5.5 主动断开蓝牙连接 (CMD-0xE7)

说明:

- 为降低休眠时的功耗, MCU 在不需要蓝牙连接的时候, 可以先断开模块蓝牙连接, 再控制模块进入低功耗, 以达到模块最低功耗状态。该接口主要功能为断开蓝牙连接。

MCU 发送:

序号	长度 (byte)	字段	说明
0	2	帧头	0x55
1			0xAA
2	1	版本号	0x00
3	1	命令字 CMD	0xE7
4	2	数据长度	0x00
5			0x00
6	1	CRC8	从帧头开始按字节求和得出的结果对 256 求余

模块回复:

序号	长度 (byte)	字段	说明
0	2	帧头	0x55
1			0xAA

序号	长度 (byte)	字段	说明
2	1	版本号	0x00
3	1	命令字 CMD	0xE7
4	2	数据长度	0x00
5			0x01
6	1	State	见下表
7	1	CRC8	从帧头开始按字节求和得出的结果对 256 求余

State 返回值说明：

0x00：设置成功

其他：设置失败

## 5.6 模块唤醒管脚配置 (CMD-0xE3)

说明：

- 适用模块：目前仅适用于 BK3432 通用固件
- 主要用于芯片对接客户自定义模块低功耗唤醒管脚。如果客户需要使用非默认管脚外的管脚进行唤醒模块，最好在 MCU 初始化 UART 后立即通过该指令对模块低功耗唤醒管脚进行配置。
- [设置永久存储](#)。 > 注意：由于模块进入低功耗后串口不可上行，所以 MCU 需要在模块上电 1s 内（模块上电 1s 内不会进入低功耗）进行设置或者在开低功耗使能之前设置（模块默认是关低功耗使能的）。

MCU 发送：

序号	长度 (byte)	字段	说明
0	2	帧头	0x55

序号	长度 (byte)	字段	说明
1			0xAA
2	1	版本号	0x00
3	1	命令字 CMD	0xE3
4	2	数据长度	0x00
5			0x06
6~11	6	数据内容 CFG	见下表
12	1	CRC8	从帧头开始按字节求和得出的结果对 256 求余

数据内容 CFG 格式:

4 字节	1 字节	1 字节
PIN_NUM	保留	保留

说明: PIN\_NUM 大端传输, 保留字段不解析, 填 0xff/0x00 即可。如果对 PIN\_NUM 不清楚可直接找 FAE 确认配置指令。

例子:

1. 设置 BK3432 P03 为模块低功耗唤醒管脚 (P03 对应 PIN\_NUM 为 0x03) 55 AA 00 E3 00 06 00 00 00 03 00 00 EB
2. 设置 BK3432 P11 为模块低功耗唤醒管脚 (P11 对应 PIN\_NUM 为 0x11) 55 AA 00 E3 00 06 00 00 00 11 00 00 F9 > 说明: BK3432 目前有 P02、P03、P04、P05、P10、P11、P12、P13、P34、P14、P35、P32、P31 可配置。BK 的 Pxx 对应 PIN\_NUM 为 0xxx。

模块回复:

序号	长度 (byte)	字段	说明
0	2	帧头	0x55
1			0xAA
2	1	版本号	0x00
3	1	命令字 CMD	0xE3
4	2	数据长度	0x00
5			0x01
6	1	State	见下表
7	1	CRC8	从帧头开始按字节求和得出的结果对 256 求余

State 返回值说明：

0x00：设置成功

其他：设置失败

## 5.7 MCU 低功耗唤醒配置 (CMD-0xB0)

说明：

- 适用模块：目前仅 BK3431Q 通用固件 3.3 版本以上支持。
- 考虑到原定唤醒时间 200ms 过长，开放该值由 mcu 设置，用于 mcu 配置自身从低功耗唤醒所需要的时间 t，默认 200ms。模块向mcu发送串口数据将会先拉高或拉低 t 时间左右的mcu唤醒管脚。
- MCU修改后需测试唤醒时间是否能正常唤醒mcu,如果不能需则调大。如果对于该延迟时间不是特别在意，建议不设置，使用默认值。
- 调用时机：建议MCU在收到CMD 0x02 (55 aa 00 02 00 00 01)后，调用该接口设置mcu低功耗唤醒配置。（该设置非永久存储，模块上电/重启后默认200ms）

MCU 发送：



序号	长度 (byte)	字段	说明
0	2	帧头	0x55
1			0xAA
2	1	版本号	0x00
3	1	命令字 CMD	0xB0
4	2	数据长度	0x00
5			0x01
6	1	interval	见说明
7	1	CRC8	从帧头开始按字节求和得出的结果对 256 求余

说明：interval: 单位 (10ms)，取值范围 1~20. 即目前设定最小支持 10ms，最大支持 200ms。

例：55 aa 00 E2 00 01 00 E2(设置低功耗模式下关闭广播) 55 aa 00 E2 00 01 06 E8 (设置低功耗下广播间隔为 600ms)

模块回复：

序号	长度 (byte)	字段	说明
0	2	帧头	0x55
1			0xAA
2	1	版本号	0x00
3	1	命令字 CMD	0xB0
4	2	数据长度	0x00
5			0x01
6	1	State	见下表

序号	长度 (byte)	字段	说明
7	1	CRC8	从帧头开始按字节求和得出的结果对 256 求余

State 返回值说明：

0x00：设置成功

其他：设置失败

## 6 门锁类通用固件附加协议

该章节协议为门锁类通用固件附加的协议，其他品类通用固件不支持该协议。目前门锁类通用固件有 BK3431Q 通用固件，TYBN1 通用固件。

### 6.1 动态密码 (CMD-0xE6)

说明：

- 模块计算动态密码基于时间，必须确保云端和设备时间同步，计算的动态密码才一致，否则将导致密码错误。（设备与 APP 建立连接会自动同步时间）
- 管理员密码入参暂不支持，当前管理员密码长度填 0 即可

MCU 发送：

序号	长度 (byte)	字段	说明
0	2	帧头	0x55
1			0xAA
2	1	版本号	0x00
3	1	命令字 CMD	0xE6
4	2	数据长度 Len	Len 高 8 位
5			Len 低 8 位
6~6+Len-1	Len	Data	见下表
6+Len	1	CRC8	从帧头开始按字节求和得出的结果对 256 求余

Data 格式：

8 字节	1 字节	N 字节	N 字节	.....
password	管理员密码长度	第 1 组管理员 密码	第 2 组管理员 密码	.....

password: 用户输入的密码数据 Data[0]~Data[7] 数据内容范围为 '0'~'9' 数据传输使用 ASCII 码

管理员密码入参暂不支持, 当前管理员密码长度填 0 即可

例: MCU 发送不带管理员密码的数据包

55 aa 00 E6 00 09 30 31 32 33 34 35 36 37 00 8a

模块回复:

序号	长度 (byte)	字段	说明
0	2	帧头	0x55
1			0xAA
2	1	版本号	0x00
3	1	命令字 CMD	0xE6
4	2	数据长度	0x00
5			0x01
6	1	State	见下表
7	1	CRC8	从帧头开始按字节求和得出的结果对 256 求余

State 返回值说明:

0x00: 密码核对通过

0x01: 密码核对失败

例：55 AA 00 E6 00 01 01 E7(密码核对失败) 55 AA 00 E6 00 01 00 E6 (密码核对通过)

## 6.2 请求上线 (CMD-0xA5)

说明：

- 该接口主要用于网关按需连接，MCU 调用该接口后，蓝牙模块会启动 30s 高频广播，类似一个“举手”的过程，蓝牙主机扫描带标志的模块广播后，会主动连接模块。模块上线后，MCU 即可正常上报 DP。
- 通常用法：记录型数据都调用 0xE0 上报，如果 MCU 检测到模块为绑定未连接状态，则调用该接口请求上线，模块上线后会自动释放通过 0xE0 上报的数据。
- 实时数据不符合主动上报一般使用场景，但 MCU 端如果想实时数据也上报，有两种方法：
  - 调用该接口后，等待模块工作状态变为绑定已连接（模块上线会下发工作状态）
  - 通过 0xE0 的 0x02 格式上报实时数据，模块上线后会将数据释放给 APP（不建议使用）

MCU 发送：

序号	长度 (byte)	字段	说明
0	2	帧头	0x55
1			0xAA
2	1	版本号	0x00
3	1	命令字 CMD	0xA5
4	2	数据长度	0x00
5			0x00
6	1	CRC8	从帧头开始按字节求和得出的结果对 256 求余

模块回复：

序号	长度 (byte)	字段	说明
0	2	帧头	0x55

序号	长度 (byte)	字段	说明
1			0xAA
2	1	版本号	0x00
3	1	命令字 CMD	0xA5
4	2	数据长度	0x00
5			0x01
6	1	State	见下表
7	1	CRC8	从帧头开始按字节求和得出的结果对 256 求余

State 返回值说明：

0x00：成功

0x01：失败

### 6.3 离线密码 (CMD-0xA2)

说明：

- 设备长时间不联网也可使用的动态密码。
- 模块内部时钟精度不是很高，24 小时低于 1min，模块在每次上线时候会同步一次云端时间，模块内部时钟不支持掉电工作，即掉电会重置。如果MCU有外接时钟，强烈建议时钟源选择0x00-MCU上传格林时间。（使用模块内部时钟可找研发要测试程序测量时钟误差）

MCU 发送：

序号	长度 (byte)	字段	说明
0	2	帧头	0x55

序号	长度 (byte)	字段	说明
1			0xAA
2	1	版本号	0x00
3	1	命令字 CMD	0xA2
4	2	数据长度 Len	Len 高 8 位
5			Len 低 8 位
6~6+Len-1	Len	Data	见下表
6+Len	1	CRC8	从帧头开始按字节求和得出的结果对 256 求余

Data 格式:

1 字节	1 字节	1 字节	1 字节	1 字节	1 字节	1 字节	1 字节	N 字节
TimeSou	2000+Y	Mon	Day	Hour	Min	Sec	Code_le	Code

TimeSource: 0x00 时间来源于 MCU 上传的 year/mon/day/hort/min/sec 字段; 0x01 使用模块内部时间, year/mon/day/hort/min/sec 不解析, 填 0x00 即可 [MCU上传时间说明](#): MCU传的时间应是格林时间的年月日格式, \*\*即0时区的年月日时间\*\*。如北京时间2020年6月20日12时00分00秒, 格林时间填0x14 0x06 0x14 0x04 0x00 0x00 Code\_len: 密码长度 Code: 密码 (区别于动态密码中密码传ascii码 '1' \~ '9' 的格式, 离线密码直接传数字, 1即0x01……9即0x09, 可参考下面示例)

模块回复:

序号	长度 (byte)	字段	说明
0	2	帧头	0x55
1			0xAA
2	1	版本号	0x00

序号	长度 (byte)	字段	说明
3	1	命令字 CMD	0xA2
4	2	数据长度 Len	Len 高 8 位
5			Len 低 8 位
6~6+Len-1	Len	Data	见下表
6+Len	1	CRC8	从帧头开始按字节求和得出的结果对 256 求余

Data 格式:

1 字节	1 字节	1 字节	N 字节
Result	Type	Decode_len	Decode

Result:0x00-正确; 其他-错误 (后续数据无意义) Type:0x00-验证成功 0x01 清空单条成功 0x02-清空所有成功 Code\_len: 加密后的数据长度 code: 加密后的清空码/开锁密码

Type 和 code 用于 MCU DP 上报使用,参照门锁 dp 协议离线密码功能解析,dpid:65,66,67

例如: 使用模块内部时间 + 密码 (2279084005) MCU- 55 AA 00 A2 00 12 01 00 00 00 00 00 00 0A 02 02 07 09 00 08 04 00 00 05 E3 模块-55 AA 00 A2 00 13 00 00 10 F3 50 3C 8F FF 03 F5 E9 0D 54 99 2A 62 A1 DE 42 F9

#### 6.4 蓝牙广播使能 (CMD-0xA3)

说明:

1. 模块非低功耗固定 100ms 间隔的广播, 低功耗默认 1000ms 间隔 (MCU 可设置 0~2000, 0 代表广播) 的广播。APP 扫描到广播即可配网。一些用户希望配网的时机完全由 MCU 控制, 可调用该接口来实现。
2. 广播使能状态模块会记录在 flash 中, 即希望配网时间由 MCU 控制的用户, 需要在串口初始化后调用该接口调整为 MCU 希望的默认使能状态。MCU 应该在需要配网的时候打开使能, 不需要配网的时候关闭使能。



3. 模块默认是使能广播状态，通过该接口关闭模块广播使能，模块不管是低功耗还是非低功耗都不会有广播。
4. 如果关闭广播使能之前模块处于广播状态，关闭后模块会立即停止广播。
5. 打开广播使能后模块会立即启动广播，具体参照（1）。

区别：与修改低功耗下广播间隔来控制广播的区别主要在于，该接口可控制非低功耗下的广播，而修改低功耗下广播间隔只能作用于低功耗状态。所以控制配网时机需要使用使能广播接口。

MCU 发送:

序号	长度 (byte)	字段	说明
0	2	帧头	0x55
1			0xAA
2	1	版本号	0x00
3	1	命令字 CMD	0xA3
4	2	数据长度	0x00
5			0x01
6	1	Data	见下表
7	1	CRC8	从帧头开始按字节求和得出的结果对 256 求余

Data 格式:

Data	说明
------	----

0x00	关闭广播使能
------	--------

0x01	打开广播使能
------	--------

模块回复:

序号	长度 (byte)	字段	说明
0	2	帧头	0x55
1			0xAA
2	1	版本号	0x00
3	1	命令字 CMD	0xA3
4	2	数据长度	0x00
5			0x01
6	1	State	见下表
7	1	CRC8	从帧头开始按字节求和得出的结果对 256 求余

State 返回值说明:

0x00: 设置成功

其他: 设置失败

### 6.5 恢复出厂设置通知 (CMD-0xA1)

说明:

- 当 APP 向模块发送恢复出厂设置命令时, 模块会向 MCU 发出恢复出厂设置通知, MCU 可以根据该指令做恢复出厂设置功能。

模块发送:

序号	长度 (byte)	字段	说明
0	2	帧头	0x55
1			0xAA

序号	长度 (byte)	字段	说明
2	1	版本号	0x00
3	1	命令字 CMD	0xA1
4	2	数据长度	0x00
5			0x00
6	1	CRC8	从帧头开始按字节求和得出的结果对 256 求余

MCU 返回:

无

## 6.6 MCU 查询模块版本号 (CMD-0xA0)

说明:

- MCU 如果需要获得模块的版本信息, 可通过该接口查询。如果 MCU 不需要模块的版本信息, 可以不实现该协议。

MCU 发送:

序号	长度 (byte)	字段	说明
0	2	帧头	0x55
1			0xAA
2	1	版本号	0x00
3	1	命令字 CMD	0xA0
4	2	数据长度	0x00
5			0x00

序号	长度 (byte)	字段	说明
6	1	CRC8	从帧头开始按字节求和得出的结果对 256 求余

模块回复:

序号	长度 (byte)	字段	说明
0	2	帧头	0x55
1			0xAA
2	1	版本号	0x00
3	1	命令字 CMD	0xA0
4	2	数据长度	0x00
5			0x06
6~11	6	DATA	见下表
12	1	CRC8	从帧头开始按字节求和得出的结果对 256 求余

DATA 格式:

模块当前固件版本号

模块当前硬件版本号

1

2

3

4

5

6

Soft\_Ver

Hard\_ver

版本号，例如 0x01 00 02 代表版本为 V1.0.2。

硬件版本号：PCBA 版本号

## 6.7 门锁业务功能配置 (CMD-0xA6)

说明：

- 适用模块：TYBN1,BK3431Q（暂无版本支持）
- 一些门锁功能需要模块封装处理 dp 部分字段，为了不影响不使用这些功能的客户，将对这部分功能设置开关，且默认关闭。（该设置永久存储）
- 目前需要通过该接口配置的功能有：

1. 门锁配件功能。

MCU 发送：

序号	长度 (byte)	字段	说明
0	2	帧头	0x55
1			0xAA
2	1	版本号	0x00
3	1	命令字 CMD	0xA6
4	2	数据长度	0x00
5			0x04
6~9	4	DATA	见下表
10	1	CRC8	从帧头开始按字节求和得出的结果对 256 求余

CFG 格式：

配置项 0	配置项 1	配置项 2	配置项 3
1	2	3	4
FLAG	保留 (0x00)	保留 (0x00)	保留 (0x00)

FLAG 说明: bit0: 门锁配件功能使能 (0 关/1 开, 默认关闭) bit1: 保留 bit2: 保留 bit3: 保留 bit4: 保留 bit5: 保留 bit6: 保留 bit7: 保留

示例: 55 AA 00 A6 00 04 01 00 00 00 AA(打开门锁配件功能) 55 AA 00 A6 00 04 00 00 00 00 A9(关闭门锁配件功能)

模块回复:

序号	长度 (byte)	字段	说明
0	2	帧头	0x55
1			0xAA
2	1	版本号	0x00
3	1	命令字 CMD	0xA6
4	2	数据长度	0x00
5			0x01
6	1	State	见下表
7	1	CRC8	从帧头开始按字节求和得出的结果对 256 求余

State 返回值说明:

0x00: 设置成功

其他: 设置失败

## 7 健康类通用固件附加协议

该章节协议仅适用于健康类通用固件。

### 7.1 带标志位 DP 上报 (CMD-0xA4)

说明：

- 适用固件：BK3432 共享协议通用固件、TYBT3L 共享协议通用固件。
- 可根据不同标志选择是否上报面板或云端。一般用于动态数据、实时数据。

MCU 发送：

序号	长度 (byte)	字段	说明
0	2	帧头	0x55
1			0xAA
2	1	版本号	0x00
3	1	命令字 CMD	0xA4
4	2	数据长度 Len	Len 高 8 位
5			Len 低 8 位
6~6+Len-1	Len	Data	见下表
6+Len	1	CRC8	从帧头开始按字节求和得出的结果对 256 求余

Data 格式：

2 字节	1 字节	1 字节	【可选】13 字节	m 字节
序号 SN	Flag	Time_flag	Time_date	datapoint

序号 SN(2)：两字节，高字节在前。Flag (1)：0x00 - 同时上报云端和面板；0x01 - 上报云

端，不上报面板；0x02 - 上报面板，不上报云端；0x03 - 都不上报。Flag (1)：0x00 - 同时上报云端和面板；0x01 - 上报云端，不上报面板；0x02 - 上报面板，不上报云端；0x03 - 都不上报。Time\_date：仅 Time\_flag 等于 0x01 时需要填写，该字段为 13 位 unix 时间字符串。DP 数据封装 (m)：datapoint 参考概述中 dp 格式说明部分。例：55 aa 00 A4 00 16 00 01 01 00 66 02 00 04 00 00 00 01 28

模块回复：

序号	长度 (byte)	字段	说明
0	2	帧头	0x55
1			0xAA
2	1	版本号	0x00
3	1	命令字 CMD	0xA4
4	2	数据长度	0x00
5			0x04
6~9	4	Data	见下表
10	1	CRC8	从帧头开始按字节求和得出的结果对 256 求余

Data 格式：

2 字节	1 字节	1 字节
序号 SN	Flag	State

序号 SN(2)：取自上报 SN Flag (1)：取自上报 flag State(1):0x00 成功其他失败

[回到顶部 ↑](#)