



MIL1005 双模蓝牙透传模块 技术规格书

BEACOOOL

©2018～2019

Revision History

Version	Date	Author	Description
V1.0	2018-4-25	Luo Jing	Initial version
V1.1	2019-07-02	Nick Kong	Add NVRAM
V1.2	2019-11-26	Jeamson Yu	Adjust the default baud rate to 9600 and the package format

PCB Version:

2015-130

2015-134

2016-110

目录	
1 产品概述.....	4
2 应用领域.....	4
3 硬件尺寸图.....	5
4 Pin 脚定义	6
5 电气特性.....	7
6 功耗	7
7 射频特性.....	8
8 应用框图.....	9
9 UART 默认设置	9
10 HCI 协议.....	10
10.1 包格式.....	12
10.2 CMD 命令.....	13
10.3 EVENT 事件.....	27
11 BLE Attribute List.....	33

1 产品概述

MIL1005是支持蓝牙4.2标准协议的模组，同时支持BT3.0模式（BR/EDR）以及BLE模式，该模块基于蓝牙芯片供应商BEACOOOL公司的单芯片，遵循BT4.2蓝牙规范。

- 支持标准BT3.0 + EDR;
- 支持标准BLE协议;
- 支持SPP协议;
- 支持UART, I2C接口;
- 支持低功耗模式;
- 支持蓝牙 Class2模式;
- 支持11路GPIO复用;
- 工业级设计;
- 数据加密;
- 内置PCB天线;
- 输入电压:不采用内部HVLDO输入1.8V ~ 3.6V;
采用内部HVLDO输入3.1V ~ 5.5V

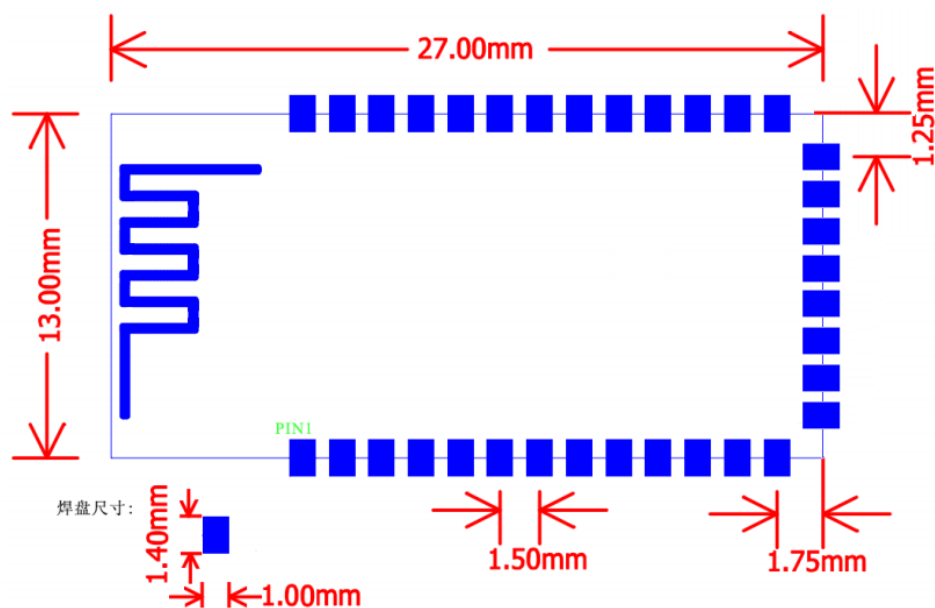
2 应用领域

MIL1005支持蓝牙SPP标准协议，可与所有版本安卓手机收发数据，同时其又支持最新蓝牙标准BLE（BT4.2），可与支持BLE的iOS设备配对连接，不需要MFI认证及加密芯片，不需要额外开发包及授权费用，iOS设备不需要越狱，支持后台程序常驻运行。

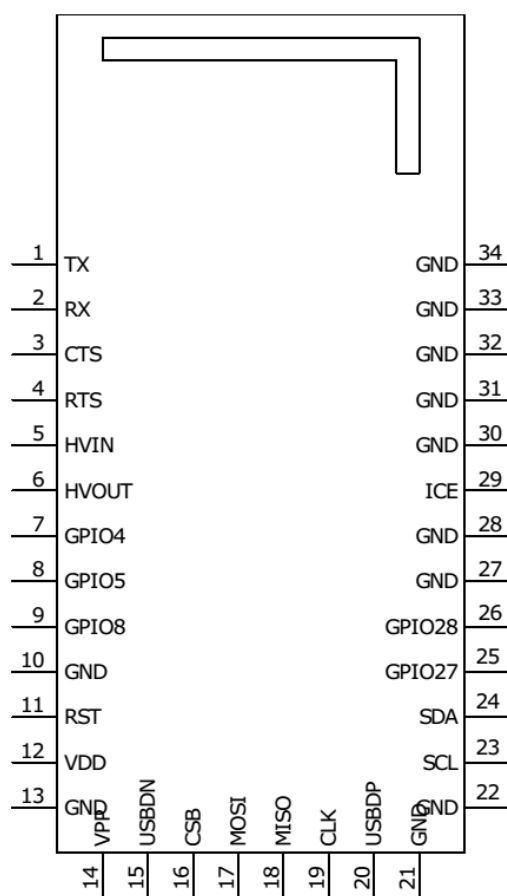
- ◆ 手机周边设备;
- ◆ 计算机周边设备;
- ◆ 医疗设备无线数据传输;
- ◆ 车载仪器无线数据传输;
- ◆ 无线遥控器;
- ◆ 无线遥控飞机;
- ◆ 无线游戏手柄;



3 硬件尺寸图



图一 硬件尺寸



图二 Pin 脚定义

4 Pin 脚定义

PIN	NAME	I/O	FUNCTION
1	TX	O	UART 数据输出
2	RX	I	UART 数据输入
3	CTS	I	UART 流控 Clear To Send (默认无流控)
4	RTS	O	UART 流控: Request To Send (默认无流控)
5	HVIN	Power In	HVLDO 输入, 3~5.5V, 4.7uF bypass cap
6	HVOUT	Power Out	HVLDO 输出, 2.85V. Bypass cap need here, 1uF
7	GPIO4	/	未启用
8	GPIO5	/	未启用
9	GPIO8	O	中断输出。 模块从 UART 发数据前通过此引脚发送中断给 MCU。
10	GND	/	GND
11	/RST		复位引脚, 低电平有效。
12	VDD	Power In	模块电源输入, 1.8~3.6V。
13	GND	/	GND
14	VPP	/	OTP 供电 6.5V。(2016-110 Only)
15	USBDN	I/O	USB 数据信号。
16	CSB	I/O	SPI 片选信号。
17	MOSI	I/O	SPI 数据信号, 主输出从输入。
18	MISO	I/O	SPI 数据信号, 主输出从输出。
19	CLK	I/O	SPI 时钟信号
20	USBDP	I/O	USB 数据信号。
21-22	GND	/	GND
23	SCL	I/O	I2C 时钟信号。
24	SDA	I/O	I2C 数据信号。
25	GPIO27	I	唤醒信号。 工作状态下: 0: UART 无动作时保持低电平(此时模块 UART 掉电不工作); 1: MCU 通过 UART 发送数据时保持高电平(提前 5ms 以上); Sleep 状态下: 0: 进入 Sleep 状态时保持低电平。(参考 10.2.20) 1: 高电平将模块从 Sleep 休眠模式唤醒。
26	GPIO28	/	未启用。
27-28	GND	/	GND
29	ICE	/	ICE 调试口
30-32	GND	/	GND
33	RF	RF	天线接口 (2016-110 无此 Pin)
34	GND	/	GND (2016-110 无此 Pin)

5 电气特性

Rating	Min	Typ	Max	Unit
VDD	1.8	/	3.6	V
VIO	VDD -0.3	VDD	VDD +0.3	V
HVIN	3.1	4.2	5.5	V
HVOUT	2.75	2.85	2.95	V
Work temperature	-20	/	+85	°C
Storage temperature	-40	/	+140	°C

6 功耗

W/O DC-DC	Parameter	Average Current	Unit
Sleep	/	620	nA
Sniff	500ms interval	21.99	uA
Discoverable	ADV interval: 640ms Scan interval: 1280ms Scan window: 11.25ms	138.66	uA

With DC-DC	Parameter	Average Current	Unit
Sleep	/	620	nA
Sniff	Sniff Interval:500ms	17.92	uA
Discoverable	ADV interval: 640ms Scan interval: 1280ms Scan window: 11.25ms	89.5	uA

7 射频特性

Rating	Value	Unit
Basic Rate 发射功率	8	dBm
Basic Rate 灵敏度	-90	dBm
BLE 发射功率	8	dBm
BLE 灵敏度	-93	dBm

8 应用框图



图三 模块应用框图

9 UART 默认设置

波特率：9600

数据位：8

停止位：1

校验位：无

流控： 无

10 使用 YC1021 输出 12M 时钟驱动 MCU 注意事项

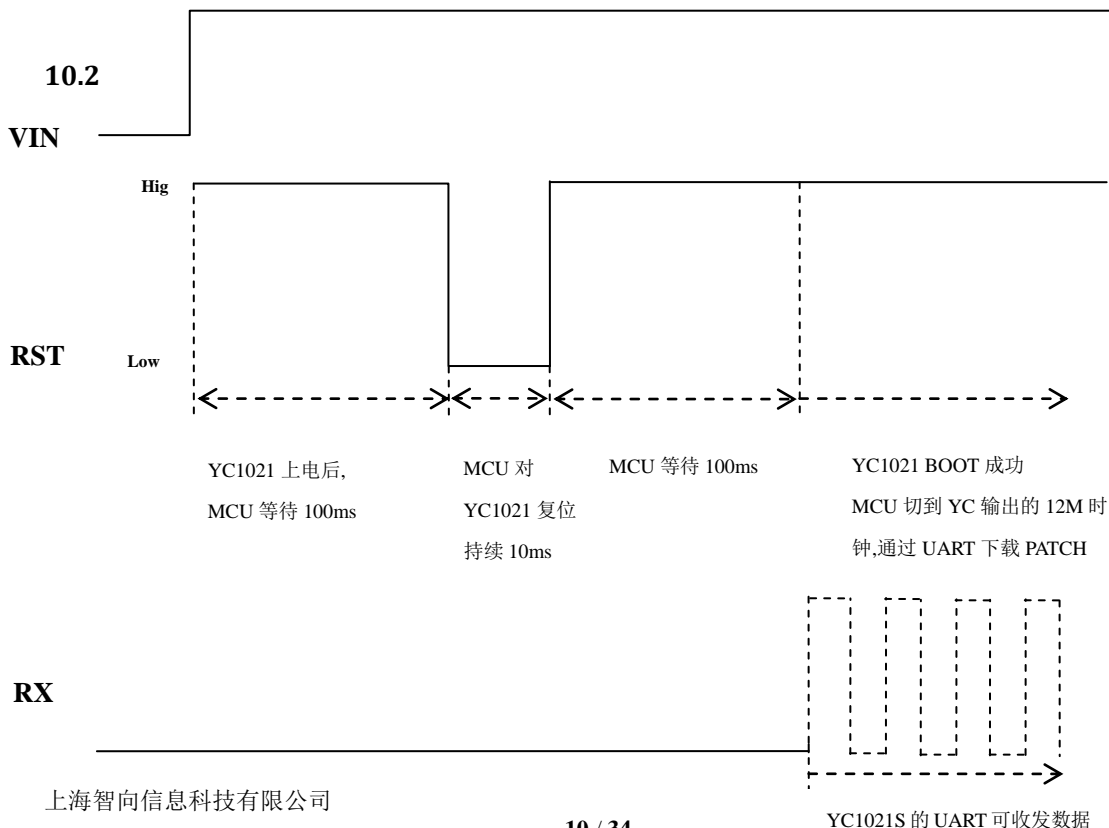
10.1 使用 YC1021 输出 12M 时钟驱动 MCU

当使用 YC1021 输出 12M 时钟驱动 MCU 时，MCU 的工作时序如下表所示：MCU 等待 YC1021 完成 BOOT，复位 YC1021，再等 YC1021 完成 BOOT，切换到 12M 时钟，通过串口下载 PATCH。

需要注意以下几点：

- YC1021 的 BOOT 时间为几十 ms，当 YC1021 的 GPIO5 正常输出 12M 方波，表示已经完成 BOOT。比较安全的等待时间约为 100ms。
- YC1021 的复位信号为低电平，复位时间约为 10ms。
- MCU 在不使用外部 12MHz 时钟前需先切回内部 RC 时钟，包括下面情况：复位 YC1021，使 YC1021 下电，使 YC1021 进入睡眠模式，使 YC1021 进入低功耗模式等。

	使用 MCU 内部 RC 时钟作为工作时钟				切换工作时钟	使用外部 12M 时钟作为工作时钟
MCU 工作 时序	YC1021 上电	等待	复位 YC1021	等待	主控 MCU 切换到外部 12M 输出作为工作时钟	UART 下载 Patch (HCI Boot)
时间 (ms)		100	10	100		



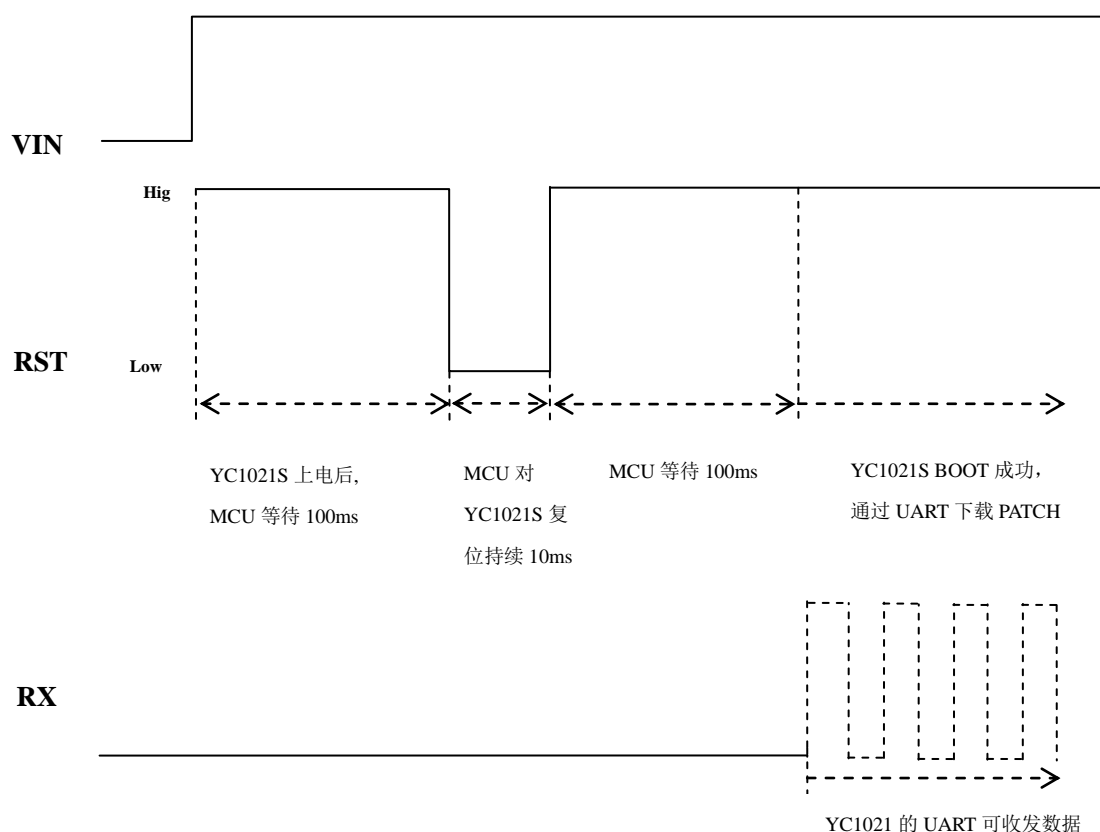
不使用 YC1021 输出 12M 时钟驱动 MCU

当 MCU 不使用 YC1021 的 12M 输出作为时钟时，MCU 的工作时序如下表所示：MCU 等待 YC1021 完成 BOOT，复位 YC1021，再等 YC1021 完成 BOOT，通过串口下载 PATCH。

需要注意以下几点：

- YC1021 的 BOOT 时间为几十 ms，比较安全的等待时间约为 100ms。
- YC1021 的复位信号为低电平，持续时间约为 10ms。

	YC1021 上电及复位				BOOT 完成，下载 PATCH
MCU 工作 时序	YC1021 上电	等待	复位 YC1021	等待	UART 下载 Patch (HCI Boot)
时间 (ms)		100	10	100	



11 HCI 协议

MIL1005 的 UART 通信协称为 HCI 协议，格式类似于蓝牙标准 HCI 协议。

- MCU 发送给模块的包称为 CMD（命令），MCU 通过发送 CMD 来完成配置蓝牙、控制蓝牙连接、发送数据等操作。
- 模块发送给 MCU 的包称为 EVENT（事件），模块通过发送 EVENT 来完成通知蓝牙状态变化、上报数据等操作。
- 模块接收到每个 CMD 后都会回复一个与之对应的 EVENT 作为回应（通常为 HCI_EVENT_CMD_COMPLETE）。此机制应作为软件流控机制处理。即，MCU 发送 CMD 后应等待一个与之对应的 EVENT，收到此 EVENT 后再发送新的 CMD。
- 模块上电/复位初始化完成后会发送 HCI_EVENT_I_AM_READY 来通知 MCU 自己已经准备好可以开始工作。MCU 需要收到此 EVENT 后方可发送第一个 CMD。
- HCI 包为小端传输，即低字节先传输。
- MCU 通过 UART 发送数据前，必须保证“LPM 控制”脚拉高并保持 5ms 以上。发送完毕后方可拉低。

11.1 包格式

Byte0~2	Byte3	Byte4	Byte5	Byte6~ Byte(length+5)	Byte(length+6)
Head	Packet Type	Opcode	Length	Payload	Check Sum
固定起始 包头	包类型	操作码	内容长度	内容	校验和

HCI 包结构如上表所示，

- Head: 固定起始包头，与 Packet Type 对应，CMD 为“0x43 0x4D 0x44”，Event 为“0x45 0x56 0x54”；
- Packet Type: 包类型，0x01 表示 CMD，0x02 表示 Event；
- Opcode: 操作码，指示不同 CMD 和 Event 指令。具体含义参见 10.1~10.2；
- Length: 内容长度；
- Payload: 包内容；
- Check Sum: Byte3~Byte(length+5)的校验和

11.2 CMD 命令

CMD 是 MCU 发送给蓝牙模块的指令，用于配置蓝牙模块、控制蓝牙连接和发送数据等。模块接收到每个 CMD 后都会回复一个与之对应的 EVENT 作为回应（通常为 HCI_EVENT_CMD_RESPONSE）。此机制应作为软件流控机制处理。即，MCU 发送 CMD 后应等待一个与之对应的 EVENT，收到此 EVENT 后再发送新的 CMD。

所有 CMD 汇总如下：

CMD 命令名称	Opcode 操作码	描述
HCI_CMD_SET_BT_ADDR	0x00	设置 BT3.0 地址
HCI_CMD_SET_BLE_ADDR	0x01	设置 BLE 地址
HCI_CMD_SET_VISIBILITY	0x02	设置可发现和广播
HCI_CMD_SET_BT_NAME	0x03	设置 BT3.0 名称
HCI_CMD_SET_BLE_NAME	0x04	设置 BLE 名称
HCI_CMD_SEND_SPP_DATA	0x05	发送 BT3.0 (SPP) 数据
HCI_CMD_SEND_BLE_DATA	0x09	发送 BLE 数据
HCI_CMD_STATUS_REQUEST	0x0B	请求蓝牙状态
HCI_CMD_SET_PAIRING_MODE	0x0C	设置配对模式
HCI_CMD_SET_PINCODE	0x0D	设置配对码
HCI_CMD_SET_UART_FLOW	0x0E	设置 UART 流控
HCI_CMD_SET_UART_BAUD	0x0F	设置 UART 波特率
HCI_CMD_VERSION_REQUEST	0x10	查询模块固件版本
HCI_CMD_BT_DISCONNECT	0x11	断开 BT3.0 连接
HCI_CMD_BLE_DISCONNECT	0x12	断开 BLE 连接
HCI_CMD_SET_NVRAM	0x26	下发 NV 数据
HCI_CMD_ENTER_SLEEP_MODE	0x27	进入睡眠模式
HCI_CMD_CONFIRM_GKEY	0x28	Numeric Comparison 配对方式中对密钥的比较
HCI_CMD_SET_CREDIT_GIVEN	*0x29	设置 Spp 流控
HCI_CMD_SET_ADV_DATA	0x2A	设置 ADV 数据
HCI_CMD_POWER_REQ	0x2B	查询模块电源电压
HCI_CMD_POWER_SET	0x2C	读取电源电压功能开关
HCI_CMD_PASSKEY_ENTRY	*0x30	输入 Passkey
HCI_CMD_SET_GPIO	*0x31	初始化 gpio
HCI_CMD_READ_GPIO	*0x32	读取 gpio 状态
HCI_CMD_LE_SET_PAIRING	*0x33	设置配对模式
HCI_CMD_LE_SET_ADV_DATA	*0x34	设置 adv 数据
HCI_CMD_LE_SET_SCAN_DATA	*0x35	设置 scan 数据
HCI_CMD_LE_SEND_CONN_UPDATE_REQ	*0x36	更新连接参数
HCI_CMD_LE_SET_ADV_PARM	*0x37	设置广播参数

HCI_CMD_LE_START_PAIRING	*0x38	开始配对
HCI_CMD_SET_WAKE_GPIO	*0x40	设置唤醒 IO
HCI_CMD_SET_TX_POWER	*0x42	设置发射功率
HCI_CMD_LE_CONFIRM_GKEY	*0x48	Ble Numeric Comparison 配对方式中对密钥的比较
HCI_CMD_REJECT_JUSTWORK	*0x49	拒绝 justwork 配对方式 (pci 认证时候使用)
HCI_CMD_RESET_CHIP_REQ	*0x51	复位芯片
HCI_CMD_LE_SET_FIXED_PASSKEY	*0x61	设置固定的 passkey
HCI_TEST_CMD_CLOSE_LPM	*0xFF	关闭 LPM

11.2.1 HCI_CMD_SET_BT_ADDR

HCI_CMD_SET_BT_ADDR 用于设置 BT3.0 设备地址，操作码 0x00。

模块收到此命令后会回复 HCI_EVENT_CMD_COMPLETE，回复内容长度为 0x00。

命令格式如下：

描述	位置	取值
CMD	Byte0	0x01
Opcode	Byte1	0x00
Length	Byte2	0x06
Payload	Byte3~Byte8	BT3.0 地址（小端格式）

11.2.2 HCI_CMD_SET_BLE_ADDR

HCI_CMD_SET_BLE_ADDR 用于设置 BLE 设备地址，操作码 0x01。模块收到此命令后会回复 HCI_EVENT_CMD_COMPLETE，回复内容长度为 0x00。

命令格式如下：

描述	位置	取值
CMD	Byte0	0x01
Opcode	Byte1	0x01
Length	Byte2	0x06
Payload	Byte3~Byte8	BLE 设备地址（小端格式）

11.2.3 HCI_CMD_SET_VISIBILITY

HCI_CMD_SET_VISIBILITY 用于设置蓝牙的可发现和广播状态，操作码 0x02。Payload 中 Bit0 表示 BT3.0 可发现（可以被搜索），Bit1 表示 BT3.0 可连接（可以被连接），没有特殊需求时这两位开关应设为同样值，即取为 00B 或 11B。Bit2 表示 BLE 可发现，BLE 在可

发现状态下可以被搜索和连接，同时会发送 ADV 广播包。

模块收到此命令后会回复 HCI_EVENT_CMD_COMPLETE，回复内容长度为 0x00。

命令格式如下：

描述	位置	取值
CMD	Byte0	0x01
Opcode	Byte1	0x02
Length	Byte2	0x01
Payload	Byte3	Bit0:BT3.0 可发现; Bit1:BT3.0 可连接; Bit2:BLE 可发现 (ADV 广播);

11.2.4 HCI_CMD_SET_BT_NAME

HCI_CMD_SET_BT_NAME 用于设置 BT3.0 的蓝牙设备名称，操作码为 0x03。命令长度根据蓝牙设备名称长度而定，最大长度为 32byte。蓝牙设备名称是以 ASCII 编码的字符串。

模块收到此命令后会回复 HCI_EVENT_CMD_COMPLETE，回复内容长度为 0x00。

命令格式如下：

描述	位置	取值
CMD	Byte0	0x01
Opcode	Byte1	0x03
Length	Byte2	0x01~0x20
Payload	Byte3 ~Byte (Length+3)	蓝牙设备名称

11.2.5 HCI_CMD_SET_BLE_NAME

HCI_CMD_SET_BLE_NAME 用于设置 BLE 的蓝牙设备名称，操作码为 0x04。命令长度根据蓝牙设备名称长度而定，最大长度为 24byte。蓝牙设备名称是以 ASCII 编码的字符串。

模块收到此命令后会回复 HCI_EVENT_CMD_COMPLETE，回复内容长度为 0x00。

命令格式如下：

描述	位置	取值
CMD	Byte0	0x01
Opcode	Byte1	0x04
Length	Byte2	0x01~0x18
Payload	Byte3 ~Byte (Length+3)	蓝牙设备名称

11.2.6 HCI_CMD_SEND_SPP_DATA

HCI_CMD_SEND_SPP_DATA 用于发送 BT3.0 数据（SPP 协议），操作码为 0x05。每个 SPP 数据包的长度小于等于 127 时可以达到最佳的数据吞吐率。

模块收到此命令后会回复 HCI_EVENT_CMD_COMPLETE，回复内容长度为 0x00。

命令格式如下：

描述	位置	取值
CMD	Byte0	0x01
Opcode	Byte1	0x05
Length	Byte2	0x01~0xFF（推荐小于 127）
Payload	Byte3 ~Byte（Length+3）	BT3.0 数据（SPP 协议）

11.2.7 HCI_CMD_SEND_BLE_DATA

HCI_CMD_SEND_BLE_DATA 用于发送 BLE 数据（GATT 协议），操作码为 0x09。

模块收到此命令后会回复 HCI_EVENT_CMD_COMPLETE，回复内容长度为 0x00。

命令格式如下：

描述	位置	取值
CMD	Byte0	0x01
Opcode	Byte1	0x09
Length	Byte2	0x01~0xFF
Payload	Byte3~Byte4	Attribute Handle，默认 0x2A 0x00
	Byte5 ~Byte（Length+3）	BLE 数据（GATT 协议）

11.2.8 HCI_CMD_STATUS_REQUEST

HCI_CMD_STATUS_REQUEST 用于请求蓝牙状态，操作码为 0x0B。

模块收到此命令后会回复 HCI_EVENT_STATUS_RESPONSE，回复内容请参考 10.3.11。

命令格式如下：

描述	位置	取值
CMD	Byte0	0x01
Opcode	Byte1	0x0B
Length	Byte2	0x00

11.2.9 HCI_CMD_SET_PAIRING_MODE

HCI_CMD_SET_PAIRING_MODE 用于设置 BT3.0 的配对方式，操作码为 0x0C。模块

默认配对模式为 0x01 Just Work (SSP)。

模块收到此命令后会回复 HCI_EVENT_CMD_COMPLETE，回复内容长度为 0x00。

命令格式如下：

描述	位置	取值
CMD	Byte0	0x01
Opcode	Byte1	0x0C
Length	Byte2	0x01
Payload	Byte3	0x00:pincode 0x01:just work 0x02: passkey 0x03: confirm

11.2.10 HCI_CMD_SET_PINCODE

HCI_CMD_SET_PINCODE 用于设置 BT3.0 的配对 PIN 码，操作码为 0x0D。模块默认配对 PIN 码为 0x30 0x30 0x30 0x30

模块收到此命令后会回复 HCI_EVENT_CMD_COMPLETE，回复内容长度为 0x00。

命令格式如下：

描述	位置	取值
CMD	Byte0	0x01
Opcode	Byte1	0x0D
Length	Byte2	0x01~0x10
Payload	Byte3~Byte(Length-3)	Pincode

11.2.11 HCI_CMD_SET_UART_FLOW

HCI_CMD_SET_UART_FLOW 用于设置 UART 流控，操作码为 0x0E。0x00 为关闭 UART 流控，0x01 为开启 UART 流控。

模块收到此命令后会回复 HCI_EVENT_CMD_COMPLETE，回复内容长度为 0x00。

命令格式如下：

描述	位置	取值
CMD	Byte0	0x01
Opcode	Byte1	0x0E
Length	Byte2	0x01
Payload	Byte3	0x00:关闭 UART 流控 0x01:开启 UART 流控

11.2.12 HCI_CMD_SET_UART_BAUD

HCI_CMD_SET_UART_BAUD 用于设置 UART 波特率，操作码为 0x0F。UART 波特率默认为 115200，最大 1Mbps。设置波特率时将波特率数字用 ASCII 编码字符串输入。例如：设置 921600 波特率，完整的包为“01 0F 06 39 32 31 36 30 30”。

模块收到此命令后会回复 HCI_EVENT_CMD_COMPLETE，回复内容长度为 0x00。此回复将基于新波特率发送。

命令格式如下：

描述	位置	取值
CMD	Byte0	0x01
Opcode	Byte1	0x0F
Length	Byte2	0x01~0x07
Payload	Byte3	波特率（ASCII 编码字符串）

11.2.13 HCI_CMD_VERSION_REQUEST

HCI_CMD_VERSION_REQUEST 用于查询模块固件版本，操作码为 0x10。

模块收到此命令后会回复 HCI_EVENT_CMD_COMPLETE，回复内容长度为 0x02，回复内容为固件版本号：1~65535。

命令格式如下：

描述	位置	取值
CMD	Byte0	0x01
Opcode	Byte1	0x10
Length	Byte2	0x00

11.2.14 HCI_CMD_BT_DISCONNECT

HCI_CMD_BT_DISCONNECT 用于断开 BT3.0（SPP 协议）连接，操作码为 0x11。

模块收到此命令后会回复 HCI_EVENT_CMD_COMPLETE，回复内容长度为 0x00。

命令格式如下：

描述	位置	取值
CMD	Byte0	0x01
Opcode	Byte1	0x11
Length	Byte2	0x00

11.2.15 HCI_CMD_BLE_DISCONNECT

HCI_CMD_BT_DISCONNECT 用于断开 BLE 连接，操作码为 0x12。

模块收到此命令后会回复 HCI_EVENT_CMD_COMPLETE，回复内容长度为 0x00。

命令格式如下：

描述	位置	取值
CMD	Byte0	0x01
Opcode	Byte1	0x12
Length	Byte2	0x00

11.2.16 HCI_CMD_SET_COD

HCI_CMD_SET_COD 用于设置 BT3.0 COD(Class of Device)，操作码为 0x15。模块 COD 默认为 0x040424，无特殊需求不用设置此值。

模块收到此命令后会回复 HCI_EVENT_CMD_COMPLETE，回复内容长度为 0x00。
命令格式如下：

描述	位置	取值
CMD	Byte0	0x01
Opcode	Byte1	0x15
Length	Byte2	0x03
Payload	Byte3~Byte5	Class of Device

11.2.17 HCI_CMD_SET_NVRAM

HCI_CMD_SET_NVRAM 用于设置 NVRAM 数据，操作码为 0x26。如果您使用的是 EEPROM 或 FLASH 版本模块，无需使用此指令。模块需要在掉电情况下保存数据，在没有 EEPROM 和 FLASH 的情况下模块无法保存这些数据。此时 MCU 应为模块开辟一块非易失存储器（如 FLASH）帮助模块保存数据，这段存储器称为 NVRAM。模块在需要保存数据时发送 HCI_EVENT_NVRAM_CHANGED 将数据发至 MCU，MCU 则在模块上电后使用 HCI_CMD_SET_NVRAM 命令将数据发送给模块。MCU 不用关心模块存储数据的内容。

模块收到此命令后会回复 HCI_EVENT_CMD_COMPLETE，回复内容长度为 0x00。
命令格式如下：

描述	位置	取值
CMD	Byte0	0x01
Opcode	Byte1	0x26
Length	Byte2	0xAA
Payload	Byte3~Byte172	NV 数据(170Byte)

NVRAM 格式说明

描述	位置	取值		
CMD	Byte0	设备编号		
Opcode	Byte1	0x35	0x36	0x37
Length	Byte2~ Byte17	Master address (不足不 0)	IRK	8byte:Ediv 8byte:IRK
Payload	Byte18~Byte33	Long Term Key(LTK)	Long Term Key(LTK)	Long Term Key(LTK)

*设备编号表示连接的先后顺序，最新配对连接或配对后再连接的设备，设备编号为 00，其他设备编号依次是 01 02 03

11.2.18 HCI_CMD_ENTER_SLEEP_MODE

HCI_CMD_ENTER_SLEEP_MODE 用于使模块进入睡眠模式，操作码为 0x27。进入睡眠模式后模块相当于下电状态。

注意：务必在发送此命令最后一个字节（Length）之前，将 PIN25（GPIO27）设为低电平。

模块收到此命令后会立刻进入睡眠模式，**无任何回复**。

命令格式如下：

描述	位置	取值
CMD	Byte0	0x01
Opcode	Byte1	0x27
Length	Byte2	0x00

11.2.19 HCI_CMD_SET_CREDIT_GIVEN

HCI_CMD_SET_CREDIT_GIVEN 用于设置 spp 流控，操作码为 0x29。

描述	位置	取值
CMD	Byte0	0x01
Opcode	Byte1	0x29
Length	Byte2	0x01
Payload	Byte3	流控的增加值

11.2.20 HCI_CMD_SET_ADV_DATA

HCI_CMD_SET_ADV_DATA 用于设置 BLE ADV DATA。当 ADV Data 长度大于 31 字节时，模块会将超出部分（按照 ADV Data 格式）放置在 Scan Resp Data 中。

模块收到此命令后会回复 HCI_EVENT_CMD_COMPLETE，回复内容长度为 0x00。

命令格式如下：

描述	位置	取值
----	----	----

CMD	Byte0	0x01
Opcode	Byte1	0x2A
Length	Byte2	0x01~0x3E
Payload	Byte3~ Byte(Length-3)	ADV Data

11.2.21 HCI_CMD_POWER_REQ

HCI_CMD_POWER_REQ 用于查询模块电源电压，操作码为 0x2b。

模块收到此命令后会回复 HCI_EVENT_CMD_COMPLETE，回复内容长度为 0x02，回复内容为 2 个的 byte 的电压值。2 个 byte 为定点数，第一个 byte 为电压值的整数部分，第二个 byte 为电压值的小数部分，2 个 byte 都为十六进制。例 03 22 位 3.34V。

命令格式如下：

描述	位置	取值
CMD	Byte0	0x01
Opcode	Byte1	0x2B
Length	Byte2	0x00

11.2.22 HCI_CMD_POWER_SET

HCI_CMD_POWER_SET 用于设置模块读取电源电压功能开关，操作码为 0x2c。

模块收到此命令后会回复 HCI_EVENT_CMD_COMPLETE，回复内容长度为 0x00。

命令格式如下：

描述	位置	取值
CMD	Byte0	0x01
Opcode	Byte1	0x2C
Length	Byte2	0x01
Payload	Byte3	0x00:关闭电压检测 0x01:开启电压检测

11.2.23 HCI_CMD_CONFIRM_GKEY

HCI_CMD_CONFIRM_GKEY 用于 Numeric Comparison 配对方式中对密钥的比较，收到 HCI_EVENT_GKEY 事件后返回。

模块收到此命令后会回复 HCI_EVENT_CMD_COMPLETE，回复内容长度为 0x00。

命令格式如下：

描述	位置	取值
CMD	Byte0	0x01
Opcode	Byte1	0x28
Length	Byte2	0x01
Payload	Byte3	0x00:密钥匹配 0x01:密钥不匹配

11.2.24 HCI_CMD_PASSKEY_ENTRY

HCI_CMD_PASSKEY_ENTRY 用于输入 passkey，操作码为 0x30。

描述	位置	取值
CMD	Byte0	0x01
Opcode	Byte1	0x30
Length	Byte2	0x04
Payload	Byte3~Byte6	Passkey Data

11.2.25 HCI_CMD_SET_GPIO

HCI_CMD_SET_GPIO 用于设置 GPIO，但并不是每个 GPIO 都可设，要根据实际电路图。模块收到此命令后会回复 HCI_EVENT_CMD_COMPLETE，内容长度为 0x00。操作码为 0x31。

描述	位置	取值
CMD	Byte0	0x01
Opcode	Byte1	0x31
Length	Byte2	0x03
Payload	Byte3	Byte3 表示输出\输入， 00 为输入，01 为输出； Byte4 表示 GPIO 号； Byte5，如果是输出的话， 00 代表输出低电平，01 表示输出高电平， 如果是输入的话， 01 表示下拉， 00 表示上拉；

11.2.26 HCI_CMD_READ_GPIO

HCI_CMD_READ_GPIO 用于读取 GPIO 设置。

模块收到此命令后会回复 HCI_EVENT_CMD_COMPLETE， 回复内容长度为 0x02，后接高低电平指示， 01 00 表示高电平， 00 00 表示低电平。
命令格式如下：

描述	位置	取值
CMD	Byte0	0x01
Opcode	Byte1	0x32
Length	Byte2	0x01
Payload	Byte3	Byte3: 表示 GPIO 号；

11.2.27 HCI_CMD_LE_SET_PAIRING

HCI_CMD_LE_SET_PAIRING 设置 BLE 配对模式，模式说明如下表。
模块收到此命令后会回复 HCI_EVENT_CMD_COMPLETE，回复内容长度为 0x00。
命令格式如下：

描述	位置	取值
CMD	Byte0	0x01
Opcode	Byte1	0x33
Length	Byte2	0x01
Payload	Byte3	0x00 LE_PAIRING_NONE: 不加密 0x01 LE_PAIRING_JUSTWORK: 加密，用户不需要操作，NO MITM。 0x02 LE_PAIRING_PASSKEY: 需要手机输入验证码并确认，支持 MITM。 0x03 LE_PAIRING_NUMERIC_COMPARE: 手机和设备显示确认码，用户确认是否相同。 默认：0x00 不加密

加密相关返回的 EVENT：

1. LE_PAIRING_JUSTWORK: 配对成功返回 HCI_EVENT_NVRAM_REP，包含配对信息。
2. LE_PAIRING_PASSKEY: 先返回 HCI_EVENT_LE_TK，包含输入 passkey 信息，配对成功后返回 HCI_EVENT_NVRAM_REP，包含配对信息。
3. LE_PAIRING_NUMERIC_COMPARE BLE 4.2 加密，为数字比较方式，手机和设备显示确认码，用户确认是否相同。

11.2.28 HCI_CMD_LE_SET_ADV_DATA

HCI_CMD_LE_SET_ADV_DATA 用于设置 BLE ADV DATA。ADV Data 长度为 31。
ADV Data 可能包含 BLE 名字，HCI_CMD_SET_BLE_NAME 会自动更新 ADV Data，所以 ADV Data 要在设置 BLE 名字之后设置。
模块收到此命令后会回复 HCI_EVENT_CMD_COMPLETE，回复内容长度为 0x00。
命令格式如下：

描述	位置	取值
CMD	Byte0	0x01
Opcode	Byte1	0x34
Length	Byte2	0x1f
Payload	Byte3~Byte(Length-3)	Adv data 数据

11.2.29 HCI_CMD_LE_SET_SCAN_DATA

HCI_CMD_LE_SET_SCAN_DATA 用于设置 Scan Data，Scan Data 长度为 31。

Scan Data 可能包含 BLE 名字，HCI_CMD_SET_BLE_NAME 会自动更新 Scan Data，所以 Scan Data 要在设置 BLE 名字之后设置。

模块收到此命令后会回复 HCI_EVENT_CMD_COMPLETE，回复内容长度为 0x00。

命令格式如下：

描述	位置	取值
CMD	Byte0	0x01
Opcode	Byte1	0x35
Length	Byte2	Length< 0x20
Payload	Byte3~Byte (Length-3)	scan data 数据

11.2.30 HCI_CMD_LE_SEND_CONN_UPDATE_REQ

HCI_CMD_LE_SEND_CONN_UPDATE_REQ 用于设置 CONNECTION PARAMETER UPDATE REQUEST 数据并发送。

模块收到此命令后会回复 HCI_EVENT_CMD_COMPLETE，回复内容长度为 0x00。

命令格式如下：

描述	位置	取值
CMD	Byte0	0x01
Opcode	Byte1	0x36
Length	Byte2	0x08
Payload	Byte3~Byte4	interval min: (最小单位 1.25ms)
	Byte5~Byte6	Le interval max (最小单位 1.25ms)
	Byte7~Byte8	Slave latency (最大忽略 30 个包)
	Byte9~Byte10	Timeout (最小单位 10ms)

11.2.31 HCI_CMD_LE_SET_ADV_PARM

HCI_CMD_LE_SET_ADV_PARM 用于设置 ADVR 的间隔和持续的时间，操作码为 0x37。

模块收到此命令后会回复 HCI_EVENT_CMD_COMPLETE，回复内容长度为 0x00。

命令格式如下：

描述	位置	取值
CMD	Byte0	0x01
Opcode	Byte1	0x37
Length	Byte2	0x04
Payload	Byte3~Byte4	Adv 间隔 (时间单位 0.625ms)

	Byte5~Byte6	Adv 持续时间（时间单位 100ms）
--	-------------	----------------------

11.2.32 HCI_CMD_LE_START_PAIRING

HCI_CMD_LE_START_PAIRING 用于开始配对，操作码为 0x38。

模块收到此命令后会回复 HCI_EVENT_CMD_COMPLETE，回复内容长度为 0x00。

命令格式如下：

描述	位置	取值
CMD	Byte0	0x01
Opcode	Byte1	0x38
Length	Byte2	0x00

11.2.33 HCI_CMD_SET_WAKE_GPIO

HCI_CMD_SET_WAKE_GPIO 用于在发送 UART 数据前唤醒上位机的 GPIO 设置。

模块收到此命令后会回复 HCI_EVENT_CMD_COMPLETE，回复内容长度为 0x00。

命令格式如下：

描述	位置	取值
CMD	Byte0	0x01
Opcode	Byte1	0x40
Length	Byte2	0x05
Payload	Byte3	Bit[0:6]: GPIO 编号 Bit7: 1: 输出高唤醒; 0: 输出低唤醒
	Byte4~Byte7	IO 唤醒后延时指定时间后发送数据，单位 us

11.2.34 HCI_CMD_SET_TX_POWER

HCI_CMD_SET_TX_POWER 用于设置发射功率，操作码为 0x42。

描述	位置	取值
CMD	Byte0	0x01
Opcode	Byte1	0x42
Length	Byte2	0x01
Payload	Byte4	发射功率

11.2.35 HCI_CMD_LE_CONFIRM_GKEY

HCI_CMD_CONFIRM_GKEY 用于 Numeric Comparison 配对方式中对密钥的比较，收到 HCI_EVENT_GKEY 事件后返回。

模块收到此命令后会回复 HCI_EVENT_CMD_COMPLETE，回复内容长度为 0x00。命令格式如下：

描述	位置	取值
CMD	Byte0	0x01
Opcode	Byte1	0x48
Length	Byte2	0x01
Payload	Byte4	0x00:密钥匹配 0x01:密钥不匹配

11.2.36 HCI_CMD_REJECT_JUSTWORK

HCI_CMD_REJECT_JUSTWORK 用于设置拒绝 justwork 配对方式（用于 pci 认证），操作码为 0x49。

描述	位置	取值
CMD	Byte0	0x01
Opcode	Byte1	0x49
Length	Byte2	0x01
Payload	Byte4	0x00: 关闭拒绝 justwork 0x01: 打开拒绝 justwork

11.2.37 HCI_CMD_RESET_CHIP_REQ

HCI_CMD_RESET_CHIP_REQ 用于复位芯片，操作码为 0x51。

描述	位置	取值
CMD	Byte0	0x01
Opcode	Byte1	0x51
Length	Byte2	0x00

11.2.38 HCI_CMD_LE_SET_FIXED_PASSKEY

HCI_CMD_LE_SET_FIXED_PASSKEY 用于设置 passkey，操作码为 0x61。

描述	位置	取值
CMD	Byte0	0x01

Opcode	Byte1	0x61
Length	Byte2	0x05
Payload	Byte3	0x00: 随机 passkey 0x01: 自定义 passkey
	Byte4~Byte7	Passkey

11.2.39 HCI_TEST_CMD_CLOSE_LPM

HCI_TEST_CMD_CLOSE_LPM 用于关闭 LPM，操作码为 0xff。

描述	位置	取值
CMD	Byte0	0x01
Opcode	Byte1	0xff
Length	Byte2	0x00

11.3 EVENT 事件

模块发送给 MCU 的包称为 EVENT（事件），模块通过发送 EVENT 来完成通知蓝牙状态变化、上报数据等操作。

所有 EVENT 汇总如下：

EVENT 事件名称	Opcode 操作码	描述
HCI_EVENT_SPP_CONN_REP	0x00	BT3.0 连接建立
HCI_EVENT_LE_CONN_REP	0x02	BLE 连接建立
HCI_EVENT_SPP_DIS_REP	0x03	BT3.0 连接断开
HCI_EVENT_LE_DIS_REP	0x05	BLE 连接断开
HCI_EVENT_CMD_RES	0x06	命令已完成
HCI_EVENT_SPP_DATA_REP	0x07	接收到 BT3.0 数据（SPP）
HCI_EVENT_LE_DATA_REP	0x08	接收到 BLE 数据
HCI_EVENT_STANDBY_REP	0x09	模块准备好
HCI_EVENT_STATUS_RES	0x0A	状态回复
HCI_EVENT_NVRAM_REP	0x0D	上传 NVRAM 数据
HCI_EVENT_INVALID_PACKET	0x0F	HCI 包格式错误
HCI_EVENT_GKEY	0x0E	发送 Numeric Comparison 配对方式中产生的密钥
HCI_EVENT_GET_PASSKEY	0x10	发送 passkey 的值到 MCU
HCI_EVENT_LE_TK	0x11	BLE PASSKEY 配对方式中

		通知 MCU 返回密钥
HCI_EVENT_LE_PAIRING_STATE	0x14	通知 MCU Ble 的配对状态
HCI_EVENT_LE_ENCRYPTION_STATE	0x15	通知 MCU 当前加密状态
HCI_EVENT_LE_GKEY	0x1d	发送 Ble Numeric Comparison 配对方式中产生的密钥

11.3.1 HCI_EVENT_SPP_CONN_REP

HCI_EVENT_SPP_CONN_REP 表示 BT3.0 连接建立。操作码为 0x00。

事件格式如下：

描述	位置	取值
EVENT	Byte0	0x02
Opcode	Byte1	0x00
Length	Byte2	0x00

11.3.2 HCI_EVENT_LE_CONN_REP

HCI_EVENT_LE_CONN_REP 表示 BLE 连接已经建立。操作码为 0x02。

事件格式如下：

描述	位置	取值
EVENT	Byte0	0x02
Opcode	Byte1	0x02
Length	Byte2	0x00

11.3.3 HCI_EVENT_SPP_DIS_REP

HCI_EVENT_SPP_DIS_REP 表示 BT3.0 连接已经断开。操作码为 0x03。

事件格式如下：

描述	位置	取值
EVENT	Byte0	0x02
Opcode	Byte1	0x03
Length	Byte2	0x00

11.3.4 HCI_EVENT_LE_DIS_REP

HCI_EVENT_LE_DIS_REP 表示 BLE 连接已经断开。操作码为 0x05。

事件格式如下：

描述	位置	取值
EVENT	Byte0	0x02
Opcode	Byte1	0x05
Length	Byte2	0x00

11.3.5 HCI_EVENT_CMD_RES

模块完成每一条命令后都会回复事件 HCI_EVENT_CMD_RES，操作码为 0x06。此事件的 Byte3 是命令操作码，用来指示完成了什么命令；Byte4 是命令完成状态，用来指示命令是否成功完成；从 Byte5 开始是长度可变的回复内容，回复内容格式参见对应的命令描述。事件格式如下，

描述	位置	取值
EVENT	Byte0	0x02
Opcode	Byte1	0x06
Length	Byte2	Response Content length + 2
Payload	Byte3	完成命令操作码
Payload	Byte4	命令完成状态： 0x00 成功 0x01 失败
	Byte5~Byte (Length + 3)	回复内容，因命令不同而有差异。

11.3.6 HCI_EVENT_SPP_DATA_REP

HCI_EVENT_SPP_DATA_REP 模块接收到 BT3.0 数据（SPP 协议）后会通过此事件发送给 MCU，操作码 0x07。

事件格式如下，

描述	位置	取值
EVENT	Byte0	0x02
Opcode	Byte1	0x07
Length	Byte2	0x01~0xFF
Payload	Byte3~Byte (Length+3)	BT3.0 数据（SPP 协议）

11.3.7 HCI_EVENT_LE_DATA_REP

模块接收到 BLE 数据（GATT 协议）后会通过此事件发送给 MCU，操作码 0x08。
事件格式如下，

描述	位置	取值
EVENT	Byte0	0x02
Opcode	Byte1	0x08
Length	Byte2	0x01~0xFF
Payload	Byte3~Byte4	Attribute Handle
	Byte5~Byte (Length+3)	BLE 数据

11.3.8 HCI_EVENT_STANDBY_REP

模块上电/复位初始化完成后会发送 HCI_EVENT_I_AM_READY 来通知 MCU 自己已经准备好可以开始工作。MCU 需要收到此 EVENT 后方可发送第一个 CMD。
事件格式如下，

描述	位置	取值
EVENT	Byte0	0x02
Opcode	Byte1	0x09
Length	Byte2	0x00

HCI_EVENT_STATUS_RES

HCI_EVENT_STATUS_RES 用于回复 HCI_CMD_STAUS_REQUEST。操作码为 0x0A。
事件格式如下，

描述	位置	取值
EVENT	Byte0	0x02
Opcode	Byte1	0x0A
Length	Byte2	0x01
Payload	Byte3	模块状态： bit0:3.0 可发现； bit1:3.0 可连接； bit2: 4.2 可发现（广播 ADV）； bit4:BT3.0（SPP 协议）已连接； bit5:BLE 已连接；

11.3.9 HCI_EVENT_NVRAM_REP

模块需要将 NVRAM 数据保存至 MCU 时会发送 HCI_EVENT_NVRAM_REP 事件给 MCU。操作码 0x0D。关于 NVRAM 的作用和工作原理，请参考 HCI_CMD_SET_NVRAM。
事件格式如下，

描述	位置	取值
EVENT	Byte0	0x02
Opcode	Byte1	0x0D
Length	Byte2	0x78
Payload	Byte3~Byte123	NVRAM 数据

11.3.10 HCI_EVENT_INVALID_PACKET

模块收到无法处理的指令时会发送 HCI_EVENT_UART_EXCEPTION。通常由主机发送 HCI 包格式错误引起，发出此 EVENT 后模块会主动 ASSERT，此时需将模块复位或重新上电。

事件格式如下，

描述	位置	取值
EVENT	Byte0	0x02
Opcode	Byte1	0x0F
Length	Byte2	0x00

11.3.11 HCI_EVENT_GKEY

在 Numeric Comparison 配对方式中会产生密钥，需要和配对另一方比较，MCU 比较后需要返回 HCI_EVENT_GKEY。操作码 0x0E。

事件格式如下，

描述	位置	取值
EVENT	Byte0	0x02
Opcode	Byte1	0x0E
Length	Byte2	0x04
Payload	Byte3~ Byte7	4 个字节 16 进制的密钥

11.3.12 HCI_EVENT_LE_TK

在 BLE PASSKEY 配对方式中，需要对 TK 值进行校验，在手机上输入对应的 TK 值进行配对。

事件格式如下，

描述	位置	取值
EVENT	Byte0	0x02
Opcode	Byte1	0x11
Length	Byte2	0x04
Payload	Byte3~Byte6	TK 数据

11.3.13 HCI_EVENT_LE_PAIRING_STATE

在蓝牙发起配对的时候，模块会向 MCU 发送事件 HCI_EVENT_LE_PAIRING_STATE。具体格式如下，

描述	位置	取值
EVENT	Byte0	0x02
Opcode	Byte1	0x14
Length	Byte2	0x02
Payload	Byte3~Byte4	0x0001: BT pairing success 0x0101: BT pairing fail 0x0080: BLE pairing success 0x0180: BLE pairing fail

11.3.14 HCI_EVENT_LE_ENCRYPTION_STATE

在收到加密指令之后，模块会向 MCU 发送加密状态的事件 HCI_EVENT_LE_ENCRYPTION_STATE。

具体格式如下，

描述	位置	取值
EVENT	Byte0	0x02
Opcode	Byte1	0x15
Length	Byte2	0x01
Payload	Byte3	0x00: 停止加密 0x01: 开始加密

11.3.15 HCI_EVENT_LE_GKEY

在 BLE Numeric Comparison 配对方式中会产生密钥，需要和配对另一方比较，MCU 比较后需要返回 HCI_EVENT_LE_GKEY。操作码 0x0E。

事件格式如下，

描述	位置	取值
EVENT	Byte0	0x02
Opcode	Byte1	0x1d
Length	Byte2	0x04
Payload	Byte3~Byte6	4 个字节 16 进制的密钥

12 BLE Attribute List

自定义 Service:

Server	UUID	Handle
UUID_BEACOOOL_MAJOR_SERVICE	0x49535343-FE7D4-AE58-FA99-FAFD205E455	0x28

自定义发送 Characteristic:

Characteristic	UUID	Property	Handle
UUID_CHARACTERISTIC_UPLOAD	0x49535343-1E4D-4BD9-BA61-23C647249616	Notify	0x2A
UUID_CHARACTERISTIC_BIDIR2	0x49535343-ACA3-481C-91EC-D85E28A60318	Notify&Write	0x31

自定义接受 Characteristic:

Characteristic	UUID	Property	Handle
UUID_CHARACTERISTIC_REV1	0x49535343-8841-43F4-A8D4-ECBE34729BB3	Write	0x2D
UUID_CHARACTERISTIC_REV2	0x49535343-6DAA-4D02-ABF6-19569ACA69FE	Write Without Resp	0x2F