M6e 模组系列指令集

————深圳铨顺宏科技有限公司

修改日期	修改内容	修订人
2016.6.3	增加常用指令集	茹健
2016.6.6	增加快速与模块建立通讯	茹健
2016.6.13	增加参数保存/清除	茹健
2017.4.5	增加温度传感器标签读取	茹健

修订版

目　　录

重要事项

A.发送指令的 length 不包括 SOH,Length,opcode,CRC，共 5 个字节

B.接收指令的 length 不包括 SOH,Length,opcode,status,CRC，共 7 个字节

C.校验码计算是从 Length 开始至 CRC 之前的数据

一. Boot Loader 命令

1.1 获取版本号（03H）

发送：FF 00 03 1D 0C

接收格式:

字段	字节	描述
SOH	1	头部（0xFF）
Length	1	请参考重要事项
Opcode	1	操作码
Status	2	状态位
Bootloader ver	4	Bootloader 版本号
Hardware Ver	4	硬件版本号
Firmware Date	4	软件编译日期
Firmware Version	4	软件版本号
Supported Protocols	4	支持协议（可不管）
CRC	2	检验码

注 1：状态位为 00 00 表示指令执行成功，其它为错误;相应错误码请参考硬件手册；

注 2：后面所有指令返回的状态位描述与注 1 一致，不在赘述；

注 3：校验码的计算方式请参考文档最后面；

从硬件版本号区分模块：

Hardware Ver[0]	模块
0x18	M6e
0x19	M6e-PRC
0x20	M6e-Mirco
0x30	M6e-NANO

示例：

Send：FF 00 03 1D 0C

Response:FF 14 03 00 00 10 11 16 00 18 00 00 01 20 16 01
04 01 19 00 0D 00 00 00 10 6C 67

1.2 获取当前正在运行的程序（0CH）

发送:FF 00 0C 1D 03

接收格式：

字段	字节	描述
SOH	1	头部（0xFF）
Length	1	除了基本数据外的长度

Opcode	1	操作码
Status	2	状态位
Program	1	当前正在运行程序
CRC	2	校验码

注：若 program & 0x1 == 1,则需要执行启动应用程序指令。

示例：

Send：FF 00 0C 1D 03

Response: FF 01 0C 00 00 32 63 63

1.3 启动应用程序(04H)

发送：FF 00 04 1D 0B

接收不需要判断，但不能不去接收；

1.4 波特率设置(06H)

发送格式：

字段	字节	描述
SOH	1	同上
Length	1	同上
Opcode	1	0x06
Bundrate	4	波特率
CRC	2	校验码

接收格式：

字段	字节	描述
SOH	1	同上
Length	1	同上
Opcode	1	0x06
Status	2	状态位
CRC	2	校验码

模块支持波特率为：9600,19200,38400,57600,115200(默认),230400,460800,921600

示例：

Send：FF 04 06 00 01 C2 00 A4 60

Response:FF 00 06 00 00 E4 06

二．参数获取

2.1 天线获取(61H)

发送格式：

字段	字节	描述
SOH	1	同上
Length	1	同上
Opcode	1	0x61
Option	0x02	返回天线搜索顺序由设置多天线搜索指定的配置（91H 指令）
	0x03	返回所有 TX 天线及其相关的功率，由 91H（option :0x03）指令设置
	0x04	返回所有 TX 天线和相关的功率及其停留时间，由 91H（option :0x03）指令设置
	0x05	返回所有“有效”逻辑天线端口和连接状态。
CRC	2	校验码

接收格式（option = 0x05）：

字段	字节	描述
SOH	1	同上
Length	1	同上
Opcode	1	0x61
Status	2	状态位
Option	1	0x05
Logical	1	逻辑天线端口
Connection status	0x00	天线未连接
	0x01	天线已连接
CRC	1	校验码

注：蓝色部分为重复。

示例：

Send：FF 01 61 05 BD B8

Response:FF 09 61 00 00 05 01 01 02 00 03 00 04 00 5C F4

接收格式（option=0x03）：

字段	字节	描述
SOH	1	同上
Length	1	同上
Opcode	1	0x61
Status	2	状态位

Option	1	0x03
Antenna	1	天线端口号
Read power	2	读取功率
Write power	2	写入功率
CRC	2	校验码

注：蓝色部分可重复。

2.2 获取读取功率（62H）

发送格式：

字段	字节	描述
SOH	1	同上
Length	1	同上
Opcode	1	0x62
Option	0x00	返回当前的功率
	0x01	返回当前的功率，模块支持的最大读功率，模块支持的最小功率
CRC	2	校验码

接收格式：

字段	字节	描述
SOH	1	同上
Length	1	同上
Opcode	1	0x62
Status	2	状态位
Option	1	与发送指令里面一致
Current power	2	当前读取功率
Max power	2	模块支持最大功率（仅 option 为 0x01）
Min power	2	模块支持最小功率（仅 option 为 0x01）
CRC	2	校验码

注：在此文档中功率单位都为 cendi-dBm,如 30dBm = 3000 cendi-dBm;

示例：

Send：FF 01 62 01 BE BC

Response：FF 07 62 00 00 01 0B B8 0B B8 01 F4 7F 77

2.3 获取模块协议（63H）

发送指令：FF 00 63 1D 6C

接收格式：

字段	字节	描述
SOH	1	同上

Length	1	同上
Opcode	1	0x63
Status	2	状态位
Current protocol	2	当前支持协议
CRC	2	校验位

协议：

协议名字	Value
ISO180006B	0x0003
ISO180006C(GEN2)	0x0005
IPX64	0x0007
IPX256	0x0008
ATA	0x001D

注：默认模块只支持 ISO180006C(GEN2)；若需要支持其它协议，需要烧录 License;

示例：

Send：FF 00 63 1D 6C

Response：FF 02 63 00 00 00 00 21 43

2.4 获取写功率(64H)

发送格式：

字段	字节	描述
SOH	1	同上
Length	1	同上
Opcode	1	0x64
Option	0x00	返回当前写功率
	0x01	返回当前的功率,模块支持的最大写功率,模块支持的最小功率
CRC	2	校验码

接收格式：

字段	字节	描述
SOH	1	同上
Length	1	同上
Opcode	1	0x64
Status	2	状态位
Option	1	与发送指令一致
Current power	2	当前模块写功率
Max power	2	模块支持最大的写功率（仅 option 为 0x01）
Min power	2	模块支持最小的写功率（仅 option 为 0x01）
CRC	2	校验码

示例：

Send：FF 01 64 01 B8 BC

Response：FF 07 64 00 00 01 0B B8 0B B8 01 F4 FF BC

2.5 获取跳频列表(65H)

发送指令：FF 00 65 1D 6A

接收格式：

字段	字节	描述
SOH	1	同上
Length	1	同上
Opcode	1	0x65
Status	2	状态位
Frequency	4	频点
CRC	2	校验位

注：蓝色部分可重复。

示例：

Send：FF 00 65 1D 6A

Response：FF 0C 65 00 00 00 0D C3 70 00 0D F6 38 00 0E 26 12 60 B2

2.6 获取 GPIO 状态(66H)

发送指令：FF 01 66 01 BA BC

接收格式：

字段	字节	描述
SOH	1	同上
Length	1	同上
Opcode	1	0x66
Status	2	状态位
Option	1	0x01
Id	1	GPIO 引脚 ID
Output	1	引脚方向 0x01:表示输出 0x00:表示输入
High	1	高低电平
CRC	2	状态位

注：蓝色部分可重复。

示例：

Send：FF 01 66 01 BA BC

Response：FF 0D 66 00 00 01 01 00 01 02 00 01 03 00 01 04 00 01 BA F5

2.7 获取模块当前频段国家(67H)

发送指令：FF 00 67 1D 68

接收格式：

字段	字节	描述
SOH	1	同上
Length	1	同上
Opcode	1	0x67
Status	2	状态位
Region	1	当前频段国家
CRC	2	校验码

示例：

Send：FF 00 67 1D 68

Response：FF 01 67 00 00 00 B4 81

2.8 获取当前电源模式(68H)

发送指令：FF 00 68 1D 67

接收格式：

字段	字节	描述
SOH	1	同上
Length	1	同上
Opcode	1	0x68
Status	1	状态位
Power mode	1	功耗模式
CRC	1	校验位

Power mode:

模式	value
MINSAVE	1
SLEEP	4
FULL	0

注：每种模式下的功耗请参考对应模块的硬件手册。

示例：

Send：FF 00 68 1D 67

Response：FF 01 68 00 00 00 A4 BF

2.9 获取模块配置(6AH)

发送格式：

字段	字节	描述
SOH	1	同上
Length	1	同上
Opcode	1	0x6A
Option	1	0x01

Key	1	请参考 configuration 表格
CRC	1	校验码

接收格式：

字段	字节	描述
SOH	1	同上
Length	1	同上
Opcode	1	操作码
Status	1	操作码
Option	1	0x01
Key	1	与发送指令一致
Value	1	Key 值对应的状态
CRC	2	校验位

Configuration:

Key	value	描述
0x0	0	任何天线读到的数据，只要 EPC 一致，都将覆盖前面的数据
	1	不同的天线，同一 EPC，只覆盖相同天线读到的数据
0x01	0	为读写器提供高的灵敏度
	1	为了降低功耗而降低灵敏度
0x02	0	最大读取 EPC 96 bit
	1	最大读取 EPC 496 bit
0x06	0	缓存中的数据，以第一次读取的时间戳为准
	1	缓存中的数据，以最大的 RSSI 值为准
0x0B	0	不同的协议覆盖以前的记录
	1	不同的协议创建新的记录
0x0C	0	连续读取时，不使能每个标签只返回一次
	1	连续读取时，使能每个标签只返回一次
0x1E	0	取消 GPI 触发读卡
	1	使能 GPI 触发读卡

示例：

Send：FF 02 6A 01 08 2E 46

Response：FF 03 6A 00 00 01 08 01 36 45

2.10 获取可用的协议（70H）

发送指令：FF 00 70 1D 7F

接收格式：

字段	字节	描述
SOH	1	同上
Length	1	同上
Opcode	1	0x70
Status	2	状态位
Protocol	2	当前支持协议
CRC	2	校验位

注:蓝色部分可重复。

示例：

Send：FF 00 70 1D 7F

Response：FF 02 70 00 00 00 05 3B 75

2.11 获取当前模块支持的频段国家（71H）

发送指令：FF 00 71 1D 7E

接收格式：

字段	字节	描述
SOH	1	同上
Length	1	同上
Opcode	1	0x71
Status	2	状态位
Region	1	国家频段
CRC	2	校验位

注：蓝色部分可重复。

Region:

国家	频段	Value	模块
North America(NA)	902~928MHz	1	M6e/Mirco
European Union(EU)	865.1~867.9MHz	2	
Korea(KR)	910 • 914MHz	3	
India(IN)	865~867MHz	4	M6e/Mirco/NANO
Japan(JP)	A.916.8~923.4MHz B.916.8~920.8MHz	5	A:NANO B:Mirco/M6e-PRC
People's Republic of China(PRC)	920~925MHz	6	M6e/Mirco/NANO
European Union 2(EU2)	869~869.85MHz	7	
European Union 3(EU3)	865.6~867.6MHz	8	M6e/Mirco/NANO

Korea 2(KR2)	917~923.5MHz	9	M6e/Mirco/NANO
People's Republic of China(PRC2)	840.125~844.875MHz	10	M6e-PRC
Australia(AU)	920~926MHz	11	M6e/Mirco/NANO
New Zealand(NZ)	922~927.5MHz	12	M6e/Mirco/NANO
Reduced FCC region(NA2)	917.4~927.2MHz	13	Mirco/NANO
5MHZ FCC band(NA3)	917.5~922.5MHz	14	Mirco/NANO
OPEN	M6e and Mirco: 865~869MH 920~925MHz M6e-PRC:840~845MHz 920~925MHz NANO:859~873MHz 915~930MHz	0XFF	

示例：

Send：FF 00 71 1D 7E

Response：FF 08 71 00 00 01 04 06 08 09 0B 0C FF CB D8

2.12 获取当前温度（72H）

发送指令：FF 00 72 1D 7D

接收格式：

字段	字节	描述
SOH	1	同上
Length	1	同上
Opcode	1	0x72
Status	2	状态位
Temperature	1	当前温度
CRC	2	校验位

示例：

Send：FF 00 72 1D 7D

Response:FF 01 72 00 00 1D 48 1A

三．参数设置

3.1 天线设置（91H）

3.1.1 单天线设置

发送格式：

字段	字节	描述
SOH	1	同上
Length	1	同上
Opcode	1	0x91
TX ANT	1	发射端口
RX ANT	1	接收端口
CRC	2	校验码

接收格式：

字段	字节	描述
SOH	1	同上
Length	1	同上
Opcode	1	0x91
Status	2	状态位
CRC	2	校验码

注：发射端口与接收端口必须一致；常用于写标签；

示例：

Send：FF 02 91 01 01 70 3B

Response：FF 00 91 00 00 17 58

3.1.2 多天线设置

发送格式：

字段	字节	描述
SOH	1	同上
Length	1	同上
Opcode	1	0x91
Option	1	0x02
TX ANT	1	发射端口

RX ANT	1	接收端口
CRC	2	校验码

注：发射端口与接收端口必须一致；当设置多天线时，蓝色字段可重复；

示例：

Send：FF 03 91 02 01 01 42 C5

Response：FF 00 91 00 00 17 58

3.1.3 设置天线功率和停留时间

发送格式：

字段	字节	描述
SOH	1	同上
Length	1	同上
Opcode	1	0x91
option	0x03	设置天线和功率
	0x04	设置天线，功率，停留时间
TX ANT	1	发射端口
Read power	2	读功率
Write power	2	写功率
Settling Time	2	天线停留时间，仅 option=0x04 时存在
CRC	2	校验码

注：当设置多天线时，蓝色部分了重复；

示例：

Send：FF 15 91 03 01 0B B8 00 00 02 0B B8 00 00 03 0B B8 00 00 04 0B B8 00 00 95 EF

Response：FF 00 91 00 00 17 58

3.2 设置读功率（92H）

发送格式：

字段	字节	描述
SOH	1	同上
Length	1	同上
Opcode	1	0x92
Read power	2	读取功率
CRC	2	校验码

接收格式：

字段	字节	描述
SOH	1	同上
Length	1	同上
Opcode	1	0x92
Status	2	状态位
CRC	2	校验码

示例：

Send：FF 02 92 0B B8 4A E1

Response：FF 00 92 00 00 27 3B

3.3 设置协议（93H）

发送格式：

字段	字节	描述
SOH	1	同上
Length	1	同上
Opcode	1	0x93
Protocol	2	标签协议
CRC	2	校验码

接收格式：

字段	字节	描述
SOH	1	同上
Length	1	同上
Opcode	1	0x93
Status	2	状态位
CRC	2	校验码

注：Protocol 字段请参考 2.3 指令中的协议表格；

示例：

Send：FF 02 93 00 05 51 7D

Response：FF 00 93 00 00 37 1A

3.4 设置写功率（94H）

发送格式：

字段	字节	描述
SOH	1	同上
Length	1	同上
Opcode	1	0x94
Write power	2	写功率
CRC	2	校验码

接收格式：

字段	字节	描述

SOH	1	同上
Length	1	同上
Opcode	1	0x94
Status	2	状态位
CRC	2	校验码

示例：

Send： FF 02 94 09 C4 28 5B

Response： FF 00 94 00 00 47 FD

3.5 设置跳频频点（95H）

发送格式：

字段	字节	描述
SOH	1	同上
Length	1	同上
Opcode	1	0x95
Frequency	4	频点
CRC	2	校验码

注：当设置为多个频点时，蓝色部分可重复；频点单位 KHz;

接收格式：

字段	字节	描述
SOH	1	同上
Length	1	同上
Opcode	1	0x95
Status	2	状态位
CRC	2	校验码

示例：

Send： FF 0C 95 00 0D C3 70 00 0D F6 38 00 0E 26 12 C1 8F

Response： FF 00 95 00 00 57 DC

3.6 设置 GPIO（96H）

发送格式：

字段	字节	描述
SOH	1	同上
Length	1	同上
Opcode	1	0x96
Option	1	0x01
Pin	1	GPIO 引脚
Direction	1	1:out 0:input

Value	1	Direction 为 out 时的初始值
CRC	2	校验码

接收格式：

字段	字节	描述
SOH	1	同上
Length	1	同上
Opcode	1	0x96
Status	2	状态位
Option	1	与发射指令一致
CRC	2	校验码

示例：

Send：FF　04 96 01 01 01 00 2C 68

Response：FF 00 96 00 00 67 BF

3.7 设置频段（97H）

发送格式：

字段	字节	描述
SOH	1	同上
Length	1	同上
Opcode	1	0x97
Region	1	国家
CRC	2	校验码

接收格式：

字段	字节	描述
SOH	1	同上
Length	1	同上
Opcode	1	0x97
Status	2	状态位
CRC	2	校验码

示例：

Send：FF　01　97　01　4B　BC

Response：FF　00　97　00　00　77　9E

3.8 设置电源模式（98H）

发送格式：

字段	字节	描述
SOH	1	同上
Length	1	同上
Opcode	1	0x98
Power mode	1	电源模式

CRC	2	校验码

接收格式：

字段	字节	描述
SOH	1	同上
Length	1	同上
Opcode	1	0x98
Status	2	状态位
CRC	2	校验码

注：电源模式请参考 2.8 指令中的 power mode 表格；

示例：

Send：FF 01 98 03 44 BE

Response：FF 00 98 00 00 86 71

3.9 设置读写器配置（9AH）

发送格式：

字段	字节	描述
SOH	1	同上
Length	1	同上
Opcode	1	0x9A
Option	1	0x01
Key	1	
Value	1	
CRC	2	校验码

注：key 和 value 字段请参考 2.9 指令中的 Configuration 表格；

示例：

Send：FF 03 9A 01 01 01 AE 5C

Response：FF 00 9A 00 00 A6 33

3.10 用户自定义参数(9DH)

发送格式：

字段	字节	描述
SOH	1	同上
Length	1	同上
Opcode	1	0x9D
UserConfig Operation	0x01	保存配置
	0x04	清除配置
Category	1	0x01
Type（默认都是 0x01）	0x00	模块默认的参数
	0x01	用户自定义的参数
CRC	2	校验码

保存配置：

Send：FF 03 9D 01 01 01 37 CB
Response：FF 02 9D 00 00 01 01 D8 11

清除操作：
Send：FF 03 9D 04 01 01 67 6E
Response：FF 02 9D 00 00 04 01 DD 11

四．GEN2 配置

4.1 GEN2 设置(9BH)

发送格式：

字段	字节	描述
SOH	1	同上
Length	1	同上
Opcode	1	0x9B
Protocol	1	0x05
Parameter	1	请参考 Parameter 表格
Value	1	请根据 Parameter 字段参考对应的表格
Stattoc Q	1	静态 Q 值，只有设置静态 Q 值时，此字段才存在
CRC	2	校验码

接收格式：

字段	字节	描述
SOH	1	同上
Length	1	同上
Opcode	1	0x9B
Status	2	状态位
CRC	2	校验码

4.2 GEN2 参数获取(6BH)

发送格式：

字段	字节	描述
SOH	1	同上
Length	1	同上
Opcode	1	0x6B
Protocol	1	协议

Parameter	1	请参考 Parameter 表格
CRC	2	校验码

接收格式：

字段	字节	描述
SOH	1	同上
Length	1	同上
Opcode	1	0x6B
Status	2	状态位
Protocol	1	协议
Parameter	1	与发射指令一致
Value		请根据 Parameter 参考对应的表格
Stattoc Q	1	静态 Q 值，只有获取 Q 值，并且 value 为 0x01 时，此字段才存在

Parameter：

Parameter	value
Seesion	0x00
Target	0x01
Tagencoding	0x02
BLF	0x10
Tari	0x11
Q	0x12

A.Session 参数对应 value:

Session	Value
S0	0x00
S1	0x01
S2	0x02
S3	0x03

示例：

Send：FF 03 9B 05 00 00 DC E8

Response：FF 00 9B 00 00 B6 12

B.Target 参数对应 value:

Target	Value
A	0x0100
B	0x0101
AB	0x0000
BA	0x0001

示例：

Send：FF 04 9B 05 01 01 00 A2 FD

Response：FF 00 9B 00 00 B6 12

C.Targencoding 参数对应 value:

Targencoding	Value
FM0	0x00
M2	0x01
M4	0x02
M8	0x03

示例：

Send：FF 03 9B 05 02 02 DE EA

Response：FF 00 9B 00 00 B6 12

D.BLF 参数对应 value:

BLF	Value
250Khz	0x00
320KHz	0x02
640KHz	0x04

示例：

Send：FF 03 9B 05 10 00 CC E8

Response：FF 00 9B 00 00 B6 12

E.Q 参数对应 value:

Q(动态或静态)	Value(十进制)	Static Q
动态	0x00	无
静态	0x01	0~15

示例：

Send：FF 03 9B 05 12 00 CE E8

Response：FF 00 9B 00 00 B6 12

F. Tari 参数对应 value：

Tari	Value
25 us	0x00
12.5 us	0x01
6.25 us	0x02

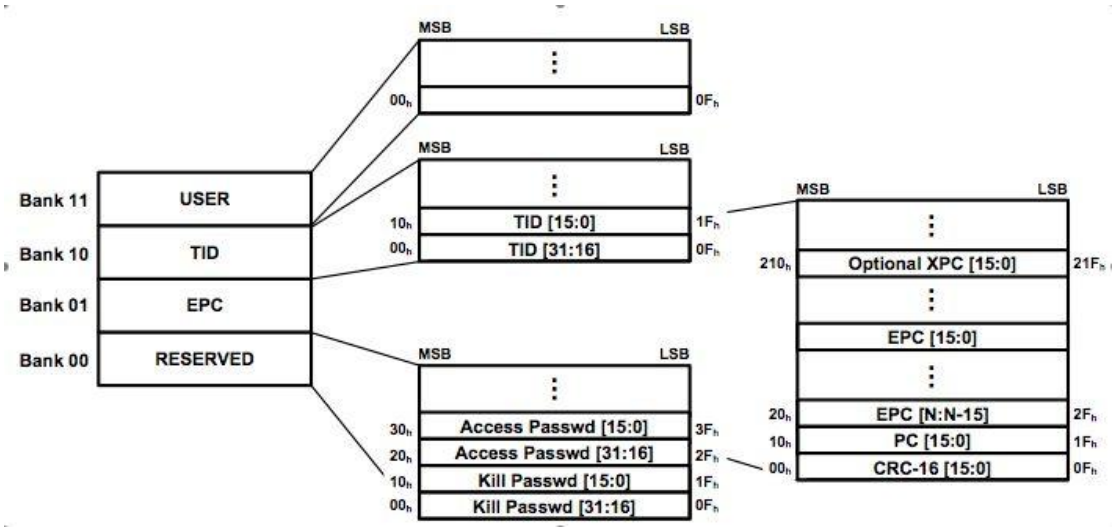
示例：

Send：FF 03 9B 05 11 00 CD E8

Response：FF 00 9B 00 00 B6 12

五.应用命令

5.1 GEN2 标签内存映射



5.2 选择标签

字段		值或字节（十六进制表示值，其它表示字节数）	描述
Select options	Select contents	0x00	不存在访问密码和选择条件
		0x01	指定完整 EPC 为选择条件，除了 Select Address 字段不存在，其它都存在
		0x02	以 TID 为选择条件，可以是 TID 中的某一部分数据
		0x03	以 USER 区数据为选择条件，可以是 USER

			中的某一部分数据
		0x04	以 EPC 中某一部分数据进行过滤
		0x05	只存在访问密码，不存在选择条件
	Select Invert	0x08	反转，排除根据上面选择条件而刷选出的标签;若不反转，则为 0；
	Extented select Data	0x20	允许选择的数据比 255 位多；若没有，则为 0；
选择条件			
Select Address		4	选择刷选数据的起始地址
Select Data Length		1(如果 Extented select Data 使能，则为 2 字节)	Select Data 数据长度，单位：bit
Select Data		M	选择刷选的数据，字节个数为 2 的倍数

注：select options = Select contents | Select Invert | Extented select Data.

5.3 单次读卡（规定时间读卡）（22H）

注 1：在执行 22 指令之前，必须要清除缓存（5.9 清除缓存（2AH））；

注 2：22 指令只需要解析标签个数和状态码，需要执行 29 指令获取标签数据（5.8 从模块缓存读取数据（29H））；

5.3.1 标签检索(读取 EPC)

发送格式：

字段	字节	描述
SOH	1	同上
Length	1	同上
Opcode	1	0x22
Option	1	0x00
Search flag	2	0x0013
Time out	2	读取时间
CRC	2	校验码

接收格式：

字段	字节	描述
SOH	1	同上
Length	1	同上
Opcode	1	0x22

Status	2	状态位
Option	1	与发送一致
Search flag	2	与发送一致
Cout	4	标签个数
CRC	2	校验码

示例：

Send：FF 05 22 00 00 13 01 F4 2B 19

Response:FF 07 22 00 00 00 00 13 00 00 00 01 8B 58

5.3.2 刷选标签（读取 EPC）

发送格式：

字段	字节	描述
SOH	1	同上
Length	1	同上
Opcode	1	0x22
Option	1	请参考 5.2 中的 select option
Search flag	2	0x0013
Time out	2	读取时间
Access password	4	若 option = 0x00,此字段省略
根据 option 字段，插入 5.2 中的选择条件		
CRC	2	校验码

注：返回格式与 5.3.1 一致；

示例：

Send：FF 10 22 04 00 13 01 F4 00 00 00 00 00 00 00 20
10 E2 00 C1 18

Response:FF 07 22 00 00 04 00 13 00 00 00 01 02 5E

5.3.3 多内存区域读取（同时读取 EPC 与其它内存区）

发送格式：

字段	字节	描述
SOH	1	同上
Length	1	同上
Opcode	1	0x22
Option	1	0x00
Search flag	2	0x0017
Time out	2	读取时间
Access password	4	若 option = 0x00,此字段不存在
根据 option 字段，插入 5.2 中的选择条件		
Embedded command count	1	嵌入命令个数，当前仅支持一个

Embedded command length	1	嵌入命令长度，从 Embedded Time out_2 至 Embedded Read length，单位：字节
Embedded Opcode	1	0x28
Embedded Time out_2	2	与 time out 一致
Option	1	0x00
Embedded Read bank	1	读取区域，请参考 Bank 表格
Embedded Read address	4	读取起始地址
Embedded Read length	1	读取数据长度(单位:字,1 字 = 2 字节)
CRC	2	校验码

注：返回格式请参考 5.3.1，其中只需要解析状态码和标签个数；

注：5.3.2 与 5.3.3 指令也可以结合，但会降低读取速度，不建议使用；

注：Embedded Read length 若为 0，在代表读取对应 bank 的全部数据，但有限制：USER 区仅限于 64 字节；在返回状态为 00 00, 的情况下，返回格式只需要解析出标签个数即可。

Bank:

Bank	Value
Reserved	0x00
EPC	0x01
TID	0x02
USER	0x03

示例 1(option = 0x0)：

Send：FF 11 22 00 00 17 01 F4 01 09 28 01 F4 00 02 00
00 00 00 00 0D 76

Response：FF 0D 22 00 00 00 00 17 00 00 00 05 01 28 00
0E 00 0E C7 FB

示例 2(option = 0x03)：

Sned ：FF 1B 22 03 00 17 00 64 00 00 00 00 00 00 00 0E
08 00 01 09 28 00 64 00 03 00 00 00 08 04 86 F5

Response：FF 15 22 00 00 03 00 17 00 00 00 01 01 28 00
02 00 00 B3 6B 8C 68 31 4C 59 00 F6 C5

注：示例 2 可以用于 RFMicron S3 芯片温度参数读取；

5.4 写 EPC（23H）

字段	字节	描述
SOH	1	同上
Length	1	同上

Opcode	1	0x23
Time out	2	超时时间
Select option	1	请参考 5.2 中的 select option
Access password	4	若 select option = 0x00, 则此字段忽略。
选择条件，请参考 5.2		
RFU	1	若 select option 字段为 0，则此字段才存在，且为 00
Tag EPC ID	M	最大支持 496 位(取决于 9AH 指令的设置)
CRC	2	校验码

接收格式：

字段	字节	描述
SOH	1	同上
Length	1	同上
Opcode	1	与发送指令一致
Status	2	状态位
CRC	2	校验码

示例：

Send：FF 10 23 03 E8 00 00 E2 00 30 35 10 03 01 08 17
20 65 CC BB 27

Response:FF 00 23 00 00 90 C1

5.5 写标签数据（24H）

发送格式：

字段	字节	描述
SOH	1	同上
Length	1	同上
Opcode	1	0x24
Time out	2	超时时间
Option	1	请参考 5.2 中的 select option
Write address	4	写入标签对应区域的起始地址，单位：字
Write Bank	1	指定要写入的标签区域,请参考 5.3.3 中的 bank 表格
Access password	4	访问密码,当 option = 0x00 时，此字段不存在
请参考 5.2 中的选择条件		
Write data	M	要写入的数据
CRC	2	校验码

接收格式：

字段	字节	描述

SOH	1	同上
Length	1	同上
Opcode	1	与发送指令一致
Status	2	状态位
CRC	2	校验码

示例：

EPC:E2 00 41 40 19 17 02 10 22 60 11 11

New USER:12 34

Send：FF 1B 24 03 E8 01 00 00 00 00 03 00 00 00 00 60 E2 00 41 40 19 17 02 10 22 60 11 11 12 34 58 64

5.6 lock 标签（25H）

发送格式：

字段	字节	描述
SOH	1	同上
Length	1	同上
Opcode	1	0x25
Timeout	2	超时时间
Option	1	请参考 5.2 中的 select option
accessPassword	4	密码必须存在
Mask	2	请参考ｍａｓｋ表格
Action	2	锁定时与ｍａｓｋ一致;若解锁时，则为 0
请参考 5.2 中的选择条件		
CRC	2	校验码

Mask:

功能	value
EPC 锁定或解锁	（1＜＜４）｜（１＜＜５）
ＴＩＤ锁定或解锁	（１＜＜２）｜（１＜＜３）
ＵＳＥＲ锁定或解锁	（１＜＜０）｜（１＜＜１）
ＡｃｃｅｓｓＰａｓｓｗｏｒｄ锁定或解锁	（１＜＜６）｜（１＜＜７）
Ｋｉｌｌ锁定与解锁	（１＜＜８）｜（１＜＜９）

Ａｃｔｉｏｎ:

功能	value
USER 区永久锁定	（１＜＜０）｜（１＜＜１）
USER 区锁定	１　＜＜　１
ＵＳＥＲ永不锁定	１　＜＜　０
ＴＩＤ永久锁定	（１＜＜２）｜（１＜＜３）

ＴＩＤ锁定	１　＜＜　３
ＴＩＤ永不锁定	１　＜＜　２
ＥＰＣ永久锁定	（1＜＜４）｜（１＜＜５）
ＥＰＣ锁定	１　＜＜　５
ＥＰＣ永不锁定	１　＜＜　４
访问密码永久锁定	（１＜＜６）｜（１＜＜７）
访问密码锁定	１　＜＜　７
访问密码永不锁定	１　＜＜　６
Ｋｉｌｌ永久锁定	（１＜＜８）｜（１＜＜９）
Ｋｉｌｌ锁定	１　＜＜　９
Ｋｉｌｌ永不锁定	１　＜＜　８

注：解锁时Ａｃｔｉｏｎ都为０；

接收判断状态位即可。

示例：

Send：**FF 10 25 03 E8 01 11 22 33 44 03 00 02 00 20 A0 00 00 07 C4 D9**

5.7 Kill 标签（26H）

发送格式：

字段	字节	描述
SOH	1	同上
Length	1	同上
Opcode	1	0x26
Time out	2	超时时间
Option	1	请参考 5.2 中的 select option
Kill password	4	访问密码，kill 标签必须有销毁密码
RFU	1	0x00,保留
请参考 5.2 中的选择条件		
CRC	2	校验码

注：返回数据只需判断状态位即可。

示例：

Send：**FF 13 26 03 E8 01 11 11 22 22 00 50 11 22 33 44 55 66 77 88 99 AA DD DB**

5.8 从模块缓存读取数据（29H）

发送格式：

字段	字节	描述
SOH	1	同上

Length	1	同上
Opcode	1	0x29
Metadata flags	2	元数据，请参考 Metadata flags 表格
Option	1	0x00
CRC	2	校验码

接收格式：

字段	字节	描述
SOH	1	同上
Length	1	同上
Opcode	1	0x29
Status	2	状态位
Metadata flags	2	与发送一致
option	1	0x00
Tag count	1	标签个数，此数据包包含的标签个数
Read count	1	标签读取次数
RSSI	1	信号强度
Antenna ID1	1	读取标签的天线端口
Frequency	3	读取标签的频点
Timestamp	4	读取标签时的相对时间
Phase	2	相位
Protocol	1	标签协议
Embedded data length	2	读取标签其它区域数据的长度
Embeddeb data	M	读取标签其它区域的数据
GPIO	1	读取标签时的 GPIO 状态
EPC length	2	读取的 EPC 长度（bits），从 PC 字段至 EPC CRC
PC	2	EPC 区域的 PC 值
EPC ID	M	EPC ID 号
EPC CRC	2	EPC 区的校验码
CRC	2	校验码

重要一：29 指令返回的数据包大小不会超过 255 字节，所以每次返回的标签个数有限；在 29 指令的返回里面有个字段是 tag count,此字段的含义是当前数据包里面包含的标签个数；tag count 字段要与 22H 指令的返回字段 count 比较，若 tag count 小于 count，则要继续执行 29 指令，知道 tag count 累加等于 count 为止。

重要二：蓝色部分是每个标签返回时的数据；29H 的返回可能不只一个标签，所以蓝色部分可重复；

重要三：从 read count 至 GPIO 参数都是可以通过 metadata flags 来控制返回。

Metadata flags:

Key	Value
NONE	0x0000
Read count	0x0001
RSSI	0x0002
Antenna ID	0x0004
Frequency	0x0008
Timestamp	0x0010
Phase	0x0020
Protocol	0x0040
Embedded Data	0x0080
GPIO Status	0x0100
All	0x01FF

示例：

Send：FF 03 29 01 FF 00 1B 03

Response：FF 26 29 00 00 01 FF 00 01 01 CF 11 0D ED 6E 00
00 01 F4 00 65 05 00 00 0F 00 80 30 00 E2 00 30
98 06 15 02 49 13 80 8A C6 70 95 F6 3C

5.9 清除缓存（2AH）

发送指令：FF 00 2A 1D 25

返回：FF 00 2A 00 00 01 E8

5.10 连续盘点

5.10.1 连续读卡（EPC）

发送格式：

字段	字节	**描述**
SOH	1	同上
Length	1	同上
Opcode1	1	0x2F
Time out	2	0x0000
Option1	1	0x01
Opcode2	1	0x22
Search flag	2	0x0000
protocol	1	标签协议 GEN2(0x05)/6B(0x03)
length	1	Option2 至 metadata flags 的长度
Opcode3	1	0x22
Option2	1	0x10
searchflag	2	0x001B,详细请参开 Search flags 表格

timeout	2	超时时间
Metadata flags	2	元数据，请参考 5.8 中的 Metadata flags 表格
CRC	2	校验码

接收格式 1：

字段	字节	描述
SOH	1	同上
Length	1	同上
Opcode	1	0x2F
Status	2	状态位
Option1	1	与发送指令一致
Opcode2	1	与发送指令一致
Search flag	2	0x0000
CRC	2	校验码

接收格式 2：

字段	字节	描述
SOH	1	同上
Length	1	同上
Opcode	1	0x22
Status	2	状态位
Option2	1	与发送指令一致
Search flags	2	与发送指令一致
Metadata flags	2	与发送指令一致
Tag count	1	标签个数
Read count	1	标签读取次数
RSSI	1	信号强度
Antenna ID	1	读取标签的天线端口
Frequency	3	读取标签的频点
Timestamp	4	读取标签时的相对时间
Phase	2	相位
Protocol	1	标签协议
Embedded data length	2	读取标签其它区域数据的长度
Embeddeb data	M	读取标签其它区域的数据
GPIO	1	读取标签时的 GPIO 状态
EPC length	2	读取的 EPC 长度（bits），从 PC 字段至 EPC CRC
PC	2	EPC 区域的 PC 值
EPC ID	M	EPC ID 号
EPC CRC	2	EPC 区的校验码

CRC	2	校验码

示例：

Send：FF 10 2F 00 00 01 22 00 00 05 07 22 10 00 1B
03 E8 01 FF DD 2B

Response1:FF 04 2F 00 00 01 22 00 00 6D C3

Response2：FF 28 22 00 00 10 00 1B 01 FF 01 01 D1 11
0E 17 E9 00 00 00 11 00 10 05 00 00 03 00
80 30 00 00 00 00 00 23 8A 00 00 00 00 46
F3 9E 11 C4 97

5.10.2 选择性盘点标签

发送格式：

字段	字节	**描述**
SOH	1	同上
Length	1	同上
Opcode1	1	0x2F
Time out	2	0x0000
Option1	1	0x01
Opcode2	1	0x22
Search flag	2	0x0000
Protocol	1	标签协议 GEN2(0x05)
Length	1	Option2 至 CRC 之前所有数据的长度
Opcode3	1	0x22
Option2	1	0x10 | select option(select option 请参考 5.2)
Search flag	2	0x001B,详细请参开 Search flags 表格
Time out	2	超时时间
Metadata flags	2	元数据，请参考 5.8 中的 Metadata flags 表格
请参考 5.2 中的选择条件		
CRC	2	校验码

注：接收格式与 5.10.1 的一致；

示例：

Send：FF 1B 2F 00 00 01 22 00 00 05 12 22 14 00 1B 03
E8 01 FF 00 00 00 00 00 00 00 20 10 E2 00 61 BD

5.10.3 盘点标签其它区域

发送格式：

字段	字节	**描述**

SOH	1	同上
Length	1	同上
Opcode1	1	0x2F
Time out	2	0x0000
Option1	1	0x01
Opcode2	1	0x22
Search flag	2	0x0000
protocol	1	标签协议 GEN2(0x05)
length	1	Option2 至 CRC 之前所有数据的字节个数
Opcode3	1	0x22
Option2	1	0x10
Search flag	2	0x001F,详细请参开 Search flags 表格
Time out	2	超时时间
Metadata flags	2	元数据，请参考 5.8 中的 Metadata flags 表格
Embedded command count	1	嵌入命令个数，当前仅支持一个
Embedded command length	1	嵌入命令长度，从 Embedded Time out_2 至 Embedded Read length，单位：字节
Embedded Opcode	1	0x28
Embedded Time out_2	2	与 time out 一致
Option	1	0x00
Embedded Read bank	1	读取区域，请参考 5.3.3 Bank 表格
Embedded Read address	4	读取起始地址
Embedded Read length	1	读取数据长度(单位：字，1 字 = 2 字节)
CRC	2	校验码

注：返回格式与 5.10.1 一致；

示例,读取 TID：

Send:FF 1C 2F 00 00 01 22 00 00 05 13 22 10 00 1F 03
E8 01 FF 01 09 28 03 E8 00 02 00 00 00 00 00 1B
2C

Response1: FF 04 2F 00 00 01 22 00 00 6D C3

Response2: FF 1E 22 00 00 10 00 1F 01 FF 01 01 AE 11
0E 16 72 00 00 00 20 00 97 05 00 00 0F 00 30
08 00 00 16 8C 0B 3C 06

5.11 停止读卡

Send： FF 03 2F 00 00 02 5E 86

Response：FF 01 2F 00 00 02 30 E6

Search flags:

Key	Value	描述
Antenna configured	0	天线配置
Atenna_1_THEN_2	1	从天线 1 开始轮询
Atenna_2_THEN_1	2	从天线 2 开始轮询
Configured list	3	配置链表
Embedded command	4	选择读取其它区域
Tag streaming	8	标签流
Large tag population support	16	支持大容量标签
Status report streaming	32	状态报告
Return on N tags	64	返回 N 个标签，用于单次读卡
Read fast search	128	快速读取标签
Stats report sreaming	256	统计报告
GPI trigger read	512	GPI 触发读卡

5.12 指定读取标签内存(单标签)

发送格式：

字段	字节	描述
SOH	1	头部，0xFF
Length	1	长度
Opcode	1	0x28
Timeout	2	超时时间
Option	1	功能选项
Read bank	1	指定读取内存区域
Read address	4	指定读取起始地址
Read length	1	指定读取长度，单位：字
Access password	4	访问密码
请参考 5.2 中的选择条件		
CRC	2	校验码

接收格式：

字段	字节	描述
SOH	1	头部，0xFF
Length	1	长度
Opcode	1	0x28
Status	2	状态码
Option	1	功能控制
Data	N	读取的数据
CRC	2	校验码

Send：FF 14 28 03 E8 03 00 00 00 00 00 02 00 00 00 00 00 00 00 20 10 12 34 D1 E7

Reponse： FF 05 28 00 00 03 11 11 22 22 10 BF

六. CRC 计算

CRC 计算方法：

```
static uint16_t crctable[] =
{
   0x0000, 0x1021, 0x2042, 0x3063,
   0x4084, 0x50a5, 0x60c6, 0x70e7,
   0x8108, 0x9129, 0xa14a, 0xb16b,
   0xc18c, 0xd1ad, 0xe1ce, 0xf1ef,
};

static uint16_t
tm_crc(uint8_t *u8Buf, uint8_t len)
{
   uint16_t crc;
   int i;

   crc = 0xffff;

   for (i = 0; i < len ; i++)
   {
      crc = ((crc << 4) | (u8Buf[i] >> 4))    ^ crctable[crc >> 12];
      crc = ((crc << 4) | (u8Buf[i] & 0xf)) ^ crctable[crc >> 12];
   }

   return crc;
}
```

七．快速与模块建立通讯

7.1 上电初始化

a. 获取当前运行程序：FF 00 0C 1D 03

b. 设置频段：FF 01 97 06 4B BB

c. 设置协议：FF 02 93 00 05 51 7D

d. 设置天线：FF 03 91 02 01 01 42 C5

7.2 单次读卡

a. 清楚缓存：FF 00 2A 1D 25

b. 检索标签：FF 05 22 00 00 13 01 F4 2B 19

C. 从模块缓存获取标签数据：FF 03 29 01 FF 00 1B 03

7.3 连续盘点

a. 关闭过滤器：FF 03 9A 01 0C 00 A3 5D

b. 开始读卡：FF 10 2F 00 00 01 22 00 00 05 07 22 10 00 1B 03 E8 01 FF DD 2B

C. 停止读卡：FF 03 2F 00 00 02 5E 86