# IC 卡模块模块使用说明 V1.0

## 功能描述

**522 系列模块支持对 M1 卡、S50 卡、S70 卡系列卡进行读、写、钱包操作、加密等操作；可以对 NTAG21X 系列卡片进行读、写操作。针对所有满足 14443A 协议的卡片都可以读取序列号。采用 DC5V 供电。模块采用 UART(TTL)口、485 口、232 口、USB 口与上位机通信。

## **522 系列模块默认功能

**522 系列模块默认功能：默认串口波特率：9600、8、N、1；当有限卡片靠近后，蜂鸣器“滴”的响一声，同时模块上的指示灯亮起，并通过串口发送卡片序列号相关的指令。当卡片离开后。模块上的指示灯熄灭。

## **522 系列模块功能特点

1. 支持通过命令修改串口波特率，掉电保存，只需设置一次。
2. 默认串口设置：9600、8、N、1。
3. 检测 IC 卡靠近后：支持主动输出卡片序列号，可通过命令配置关闭，掉电保存，只需设置一次。**默认：检测到卡片序列号后主动输出。**
4. 检测到 IC 卡靠近后：当卡片离开的时候，输出固定的命令表示卡片离开。只有在主动输出模式下有效。**默认：关闭，需通过命令配置打开，掉电保存。只需配置一次。**
5. 每个模块上面都有指示灯，用于指示模块当前的工作的状态。a、当模块正常供电后，模块上的指示灯会闪烁一下；b、当模块的串口接收到数据后，会闪烁一下；c、当有效卡片靠近模块后，模块上的指示灯会常亮。当卡片离开后，指示灯熄灭。
6. 模块支持通过命令设置地址，地址范围从 0x00-0xFE。掉电保存，只需设置一次，默认 0x00。
7. 模块支持通过命令查询模块当前地址是多少。

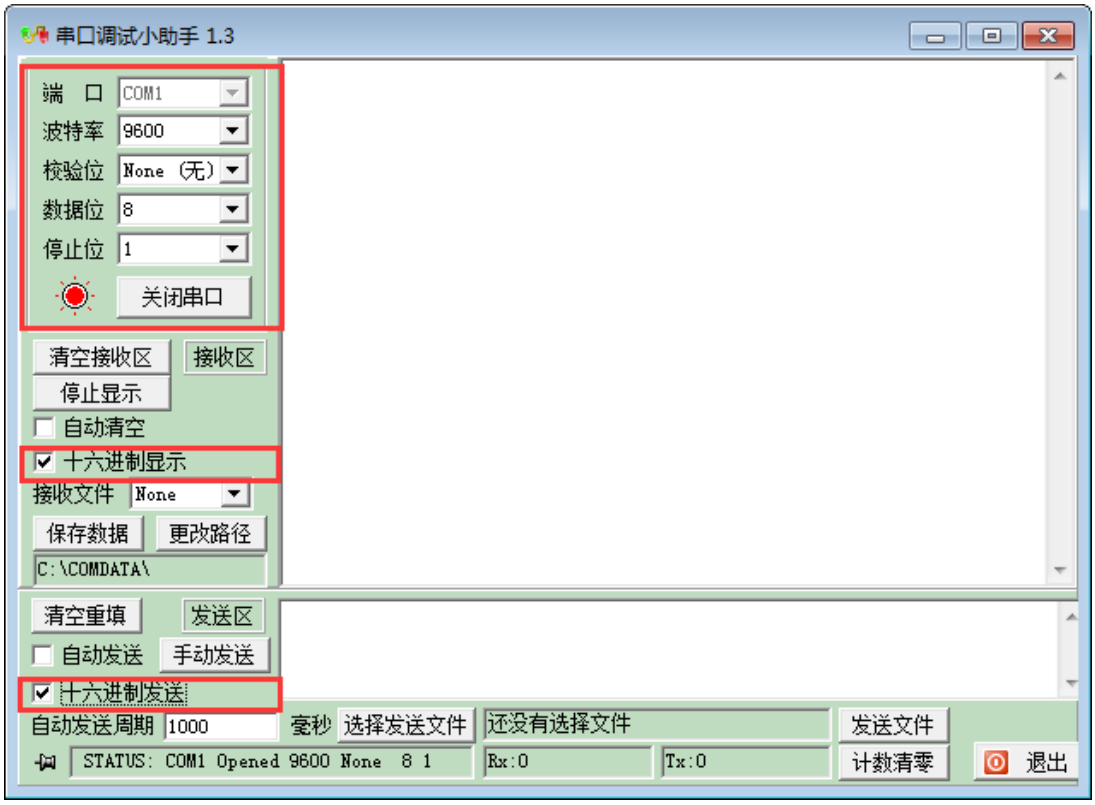
8. 如果模块上面有蜂鸣器的话。可以通过命令控制蜂鸣器“滴”的响一声。
9. 刷卡蜂鸣器提醒，支持通过命令设置进行关闭。默认：打开，掉电保存，只需设置一次。
10. 停止模块工作，用于降低模块的功耗，此时模块功耗约 5V/1.5mA；关闭模块发送 13.56MHZ 的能量波，有利于过 EMC 检测。
11. 模块支持命令寻卡、并实时反馈是否有卡片存在的状态。
12. 模块支持 UART(TTL)口、485 口、232 口、USB 口、韦根 26、韦根 34。在出货的时候只能选择其中的一种出货。不同型号的模块接口有所差异。

# 引脚定义

模块的引脚定义见实物背面或者淘宝的宝贝详情页面。

# 串口设置

**如下图所示：波特率：9600；校验位：None；数据位：8；停止位：1；十六进制显示。**



# 串口通信的指令协议说明

**数据通信以一帧为单位进行，格式如下：**

**数据通信帧结构**

| 起始符<br>STX | 地址<br>ADDR | 命令<br>CMD | 数据长度<br>Length | 数据<br>DATA | 校验和<br>BCC | 帧结束符<br>ETX |
|---|---|---|---|---|---|---|
| 1byte | 1byte | 1byte | 1byte | N bytes | 1byte | 1byte |

## 简要概括，每帧数据如下：

第 1 字节 STX：起始符，0x20；

第 2 字节 ADDR：地址，默认：0x00；

第 3 字节 CMD：命令—上位机发送给 IC 卡模块；

第 4 字节 Length：此帧有效数据的长度。从紧接着的第 1 个字节开始，到倒数第 3 个字节结束，为有效字节。

第 5 字节 DATA　到　倒数第 3 字节：　**有效数据**。

倒数第 2 字节 BCC：校验和；

倒数第 1 字节 ETX：结束符, 0x03；

## 数据帧中各字段说明下表

**数据帧各字段说明**

| 字段 | 长度 | 说明 | 补充 |
|---|---|---|---|
| STX | 1 | STX=0x20，数据帧的起始符。**每一帧数据都是以STX开始** | |
| ADDR | 1 | 地址，默认值：00 | |
| Cmd | 1 | **上位机** 发送给 **IC卡模块**：命令Command | |
| Length | 1 | 该帧所带数据信息长度。**从紧接着的第1个字节开始，到倒数第3个字节结束，为有效字节。** | |
| DATA | Length | 数据信息, 长度等于Length | |
| BCC | 1 | 校验和。从地址（ADDR）开始到数据（DATA）的最后一字节异或，**然后再取反**。 | |
| ETX | 1 | ETX=0x03，是一个帧的结束标志。**每帧数据的结束**。 | |

# 功能配置指令 0x2C 说明

配置的相关指令：

20 00 2C 04 14 14 19 14 DA 03

| 序号 | 第 1 字节 | 第 2 字节 | 第 3 字节 | 第 4 字节 | 第 5 字节 | 第 6 字节 | 第 7 字节 | 第 8 字节 | 第 9 字节 | 第 10 字节 |
|---|---|---|---|---|---|---|---|---|---|---|
| 值 | 0x20 | 0x00 | 0x2C | 0x04 | 0x14 | 0x14 | 0x19 | 0x14 | 0xDA | 0x03 |
| 功能 | 起始符 | 地址 | 功能设定指令 | 数据长度 | 刷卡主动输出控制 | 卡片离开输出指令控制 | 波特率设定 | 蜂鸣器打开或关闭 | 校验值 | 结束符 |

1. **关闭刷卡主动输出**：配置成 0x14，则关闭刷卡主动输出，其他任意值刷卡都会主动输出。
2. **打开刷卡离开指令**：配置成 0x14，则卡片离开的时候，会输出一条卡片离开的指令。
3. **波特率设置**：配置成 0x--，“--”取波特率的高 2 位。需要配置成 9600，则配置值 0x96；配置成 115200，则配置值 0x11。支持可设定的波特率有：9600、14400、19200、28800、38400、57600、115200。注意当为 485 接口的时候，最高波特率只能达到 28800。
4. **关闭蜂鸣器提示音**：配置成 0x14，则关闭蜂鸣器提示音，其他任意值则都有蜂鸣器提示音。

# 修改模块地址指令 0x2B 说明

修改地址的指令：20 00 2B 01 01 D4 03

| 序号 | 第 1 字节 | 第 2 字节 | 第 3 字节 | 第 4 字节 | 第 5 字节 | 第 6 字节 | 第 7 字节 |
|---|---|---|---|---|---|---|---|
| 值 | 0x20 | 0x00 | 0x2B | 0x01 | 0x01 | 0xD4 | 0x03 |
| 功能 | 起始符 | 原地址 | 修改地址 | 数据长度 | 新地址 | 校验值 | 结束符 |

该指令执行成功后，模块的地址从 0x00 变成了新地址 0x01。指令（20 00 2B 01 01 D4 03）执行成功后，上位机会收到携带新地址的反馈指令：20 01 2B 00 D5 03

# 模块地址查询指令 0x2D 说明

修改地址的指令：20 00 2D 00 D2 03

| 序号 | 第 1 字节 | 第 2 字节 | 第 3 字节 | 第 4 字节 | 第 5 字节 | 第 6 字节 |
|---|---|---|---|---|---|---|
| 值 | 0x20 | 0x00 | 0x2D | 0x00 | 0xD2 | 0x03 |
| 功能 | 起始符 | 原地址 | 修改地址 | 数据长度 | 校验值 | 结束符 |

指令（20 00 2D 00 D2 03）执行成功后，上位机会收到携带新地址的反馈指令：20 01 2D 00 D3 03

其中，01 表示模块的地址为 01。

**特别强调：上位机发送给模块的所有指令，只有修改模块地址指令 0x2B 和 模块地址查询指令 0x2D 不受模块本身地址指令的约束以外，其他任何一条指令都受模块地址的约束，只有指令中的地址和模块本身的地址一样。模块才会执行该条指令。当不需要用到地址的情况，指令的地址字节默认为 0x00 即可，因为模块本身默认的地址为 0x00。**

## 蜂鸣器响一声指令 0x30 说明

修改地址的指令：20 00 30 00 CF 03

| 序号 | 第 1 字节 | 第 2 字节 | 第 3 字节 | 第 4 字节 | 第 5 字节 | 第 6 字节 |
|---|---|---|---|---|---|---|
| 值 | 0x20 | 0x00 | 0x30 | 0x00 | 0xCF | 0x03 |
| 功能 | 起始符 | 原地址 | 修改地址 | 数据长度 | 校验值 | 结束符 |

指令（20 00 30 00 CF 03）执行成功后，上位机会收到携带新地址的反馈指令：20 00 30 00 CF 03 同时蜂鸣器会“滴”的响一声。

## 关闭模块功能指令 0x3A 说明

修改地址的指令：20 00 3A 00 C5 03

| 序号 | 第 1 字节 | 第 2 字节 | 第 3 字节 | 第 4 字节 | 第 5 字节 | 第 6 字节 |
|---|---|---|---|---|---|---|
| 值 | 0x20 | 0x00 | 0x3A | 0x00 | 0xC5 | 0x03 |
| 功能 | 起始符 | 原地址 | 修改地址 | 数据长度 | 校验值 | 结束符 |

指令（20 00 3A 00 C5 03）执行成功后，上位机会收到携带新地址的反馈指令：20 00 3A 00 C5 03 然后，模块就停止工作，此时模块的功耗约 1.5mA,刷任何卡都无作用，刷卡也不会有任何反应。需要上位机发送其他任何满足协议要求的指令即可激活模块。比如，发送寻卡指令：20 00 27 00 D8 03，即可激活模块。

## 寻卡指令 0x27 说明

修改地址的指令：20 00 27 00 D8 03

| 序号 | 第 1 字节 | 第 2 字节 | 第 3 字节 | 第 4 字节 | 第 5 字节 | 第 6 字节 |
|---|---|---|---|---|---|---|
| 值 | 0x20 | 0x00 | 0x27 | 0x00 | 0xD8 | 0x03 |
| 功能 | 起始符 | 原地址 | 修改地址 | 数据长度 | 校验值 | 结束符 |

上位机发送：20 00 27 00 D8 03

情况 1：若无卡片存在，则上位机收到无卡片的指令：20 00 27 01 02 DB 03

情况 2：若有卡片存在，则上位机收到卡片相关指令：20 00 00 08 04 00 00 00 A6 40 FE E4 0E 03。指令中每个字节的含义见后文。

# 常见问题

**问题 1：此模块读写 IC 卡的具体读写以及对 IC 卡的加密是怎么样操作的？**

**第 1 步**：刷卡。模块上的指示灯会亮，并且通过串口主动发送卡片序列号给上位机，此时上位机就会接收到卡片序列号的相关指令。指令：20 00 00 08 04 00 00 00 A6 40 FE E4 0F 03。

**20**：起始符

**00**：地址

**01**：命令字节，模块主动输出卡片序列号时，该字节为 0x00；其他指令为命令字

**08**：表示后面 8 个字节为有效数据位

**04 00**：表示卡片属性为 S50 卡

**00 00**：此 2 个字节无实际意义。

A6 40 FE E4 ：表示卡片序列号。**刷不同卡片，此 4 个字节会变。**

0F：校验和。**从地址（ADDR）开始到数据（DATA）的最后一字节异或，然后再取反 得到。**

**03**：帧结束符。

**第 2 步**：上位机就可以直接通过读指令、或者写指令、或者加密指令对 IC 卡进行读、或者写、或者加密操作了。

**读块指令举例**：读第 2 块数据，

**上位机发送指令：** 20 00 22 08 00 FF FF FF FF FF FF 02 D7 03

其中，紫色的 22 表示：此条命令为 22 号指令。22 号指令为读块指令；

其中，红色的 08 表示：紧接着后面有效数据有 1 个字节；

其中，橙色的 00 表示：表示采用密码 A 的方式校验卡片的密码，若需要采用密码 B 的方式校验卡片的密码，则此字节改为 0x01 即可。**说明：IC 卡一共包含 16 个扇区；每个扇区包含 4 个块，每个扇区的第 4 号块为密码块，而密码块中又包含密码 A 和 密码 B，密码 A 和密码 B 分别包含 6 个字节；所有扇区的密码块 默认的密码都为：0xFF 0xFF 0xFF 0xFF 0xFF 0xFF**

其中，淡绿色的 FF FF FF FF FF FF 表示：此条读块指令采用的密码；**注意：这个密码必须和需要读取的 IC 卡所在块对应的这个块所在扇区的密码 A 或者密码 B 保持一样，否则就会读卡识别。**

其中，绿色的 02 表示：需要读取卡片的 2 号块数据；

其中，蓝色的 D7 为 ECC 校验码，是 00 22 08 00 FF FF FF FF FF FF 02 首先异或，然后再取反得到的。**异或运算有小工具可以用，见我们的资料中的《按位异或工具》文件夹下。**

- **读块成功**，则上位机收到第 2 块的数据，如下：

20 00 22 11 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 CC 03

其中，粉色的 22 表示：该指令是读指令 22 号指令的返回指令。

其中，红色的 11 表示：紧接着后面有效数据有 17 个字节；

其中，青色的 00 表示：此读卡指令执行成功；

其中，绿色的 CC 表示：ECC 校验码；是 00 22 11 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 首先异或，然后再取反得到的。

- **读块失败，若是校验密码失败上位机收到指令：** 20 00 22 01 01 DD 03

其中，红色的 22 表示：该指令是读指令 22 号指令的返回指令。

其中，绿色的 01 表示：紧接着后面有效数据有 1 个字节；

其中，蓝色的 01 表示：次读卡指令执行失败，原因—密码校验失败。

**所有的读写操作过程中，只要密码校验失败都会反馈这条指令给上位机。**

- **读块失败，若是卡片防碰撞失败上位机收到指令：** 20 00 22 01 02 DE 03

其中，红色的 22 表示：该指令是读指令 22 号指令的返回指令。

其中，绿色的 01 表示：紧接着后面有效数据有 1 个字节；

其中，蓝色的 02 表示：次读卡指令执行失败，原因—密码防碰撞失败。

- **读块失败，若是卡片选择失败上位机收到指令：** 20 00 22 01 03 DF 03

其中，红色的 22 表示：该指令是读指令 22 号指令的返回指令。

其中，蓝色的 01 表示：后面有效字节长度 1 字节。

其中，绿色的 03 表示：次读卡指令执行失败，原因是卡片选择失败。

- **读块失败，若是块读取失败 上位机收到指令：** 20 00 22 01 04 D8 03

**写块指令举例：** 在第 2 块写入：00 11 22 33 44 55 66 77 88 99 aa bb cc dd ee ff 数据。

**上位机发送指令：20 00 23 18 00 FF FF FF FF FF FF 02 00 11 22 33 44 55 66 77 88 99 aa bb cc dd ee ff C6 03**

**20 00 80 0C 00 FF FF FF FF FF FF 02 00 00 00 00 71 03**

其中，粉色的 23 表示：此条命令为 23 号指令。23 号指令为写块指令；

其中，红色的 18 表示：紧接着后面有效数据有 24 个字节；

其中，青色的 00 表示：表示采用密码 A 的方式校验卡片的密码；

其中，紫色的 **FF FF FF FF FF FF** 表示：此条写块指令采用的密码；**注意：这个密码必须和需要读取的 IC 卡所在块对应的这个块所在扇区的密码 A 或者密码 B 保持一样，否则就会读卡识别。**

其中，绿色的 02 表示：**需要把后面的 16 个字节写到卡片的 2 号数据块**；

其中，00 11 22 33 44 55 66 77 88 99 aa bb cc dd ee ff 表示：**要写入到 IC 中的数据**

其中，蓝色的 C6 为 ECC 校验码，是 **00 23 18 00 FF FF FF FF FF FF 02 00 11 22 33 44 55 66 77 88 99 aa bb cc dd ee ff** 首先异或，然后再取反得到的。

- **写块成功**，则上位机收到指令： 20 00 23 01 00 DD 03

其中，红色的 23 表示：该指令是读指令 23 号指令的返回指令。

其中，蓝色的 01 表示：后面有效字节 1 字节。

其中，绿色的 00 表示：写指令执行成功。

- **写块失败，若是校验密码失败上位机收到指令：**20 00 23 01 01 DC 03
- **写块失败，若是卡片防碰撞失败上位机收到指令：**20 00 23 01 02 DF 03
- **写块失败，若是卡片选择失败上位机收到指令：**20 00 23 01 03 DE 03
- **写块失败，若是块写入失败 上位机收到指令：** 20 00 23 01 04 D9 03

## 修改卡片某个扇区的密码举例：

需要将卡片的第 0 扇区的密码 A 从 FF FF FF FF FF FF 改为 11 22 33 44 55 66。

**上位机发送指令：**20 00 26 0E 00 **FF FF FF FF FF FF** 11 22 33 44 55 66 00 A0 03

其中，粉色的 26 表示：此条命令为 23 号指令。23 号指令为写块指令；

其中，红色的 0E 表示：紧接着后面有效数据有 15 个字节；

其中，青色的 00 表示：表示采用密码 A 的方式校验卡片的密码，**同时也表示需要对密码 A 进行修改。**

其中，紫色的 **FF FF FF FF FF FF** 表示：此条修改指令采用的密码；**注意：这个密码必须和需要读取的 IC 卡所在块对应的这个块所在扇区的密码 A 或者密码 B 保持一样，否则就会读卡识别。**

其中，11 22 33 44 55 66 表示：**要最终写入到 IC 卡中的密码；**

其中，绿色的 00 表示：**需要修改扇区 0 的密码；**

- **修改密码成功**，则上位机收到指令：20 00 26 01 00 D8 03

其中，红色的 26 表示：该指令是读指令 23 号指令的返回指令。

其中，蓝色的 01 表示：后面有效字节 1 字节。

其中，绿色的 00 表示：写指令执行成功。

- 修改密码失败，若是校验密码失败上位机收到指令：20 00 26 01 01 D9 03
- 修改密码失败，若是卡片防碰撞失败上位机收到指令：20 00 26 01 02 D9 03
- 修改密码失败，若是未检测到卡片上位机收到指令：20 00 26 01 03 DB 03
- 修改密码失败，若是 写入块失败上位机收到指令：20 00 26 01 04 DC 03

**问题 2：如何计算所读的块对应卡片的第扇区？**

**回答：**比如，S50 的 IC 卡，此卡一共有 16 个扇区，这 16 个扇区又分为了 64 个块，每个扇区就包含了 4 个块，每 1 块又包含 16 个字节，因此 S50 卡的存储空间为 64×16=1024 字节（1KB）。**每个扇区的第 4 块是密码块，密码块只能写，不能读。所以在修改卡片每个扇区的密码的时候一定要记住密码**。举例：第 16 号块处于哪个扇区呢！ 16÷4 = 4 余 0；则 16 号块处于第 4 扇区的 0 号块。

**问题 3：如何计算任意扇区对应的密码块？**

**回答：**举例，计算第 4 扇区对应的密码块：4×4+3=19；则第 19 块为第 4 扇区的密码块。

读扇区指令

原理与读块和写块一样，就不再举例了！！！

# 指令协议

## 1.0 读块—ReadBlock

### 上位机写入：

20 00 22 08 00 FF FF FF FF FF FF 02 D7 03　　//读第 2 块数据，命令 22

### 上位机收到指令：

**有卡：**20 00 22 11 00 00 11 22 33 44 55 66 77 88 99 AA BB CC DD EE FF CC 03　//有卡在天线附近，上位机收到指令。

**卡片密码校验错误：20 00 22 01 01 DD 03**

**卡片防碰撞失败：20 00 22 01 02 DE 03**

**卡片选择失败：20 00 22 01 03 DF 03**

**块读取失败：　　20 00 22 01 04 D8 03**

## 1.1 读扇区

## 上位机写入：

20 00 24 08 00 FF FF FF FF FF FF 00 D3 03

//读第 0 扇区数据，命令 24，突出字节表示第 0 扇区

## 上位机收到指令：

**有卡：**20 00 24 31 00 A6 B7 E1 62 92 08 04 00 01 AC 69 1A 42 8F 45 1D 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 11 22 33 44 55 66 77 88 99 AA BB CC DD EE FF AD 03

**有卡但是密码校验错误：20 00 24 01 01 DB 03**

**卡片防碰撞失败：20 00 24 01 02 DF 03**

**卡片选择失败：20 00 24 01 03 D9 03**

**扇区读取失败：20 00 24 01 04 DE 03**

## 1.2　写块—WriteBlock

## 上位机写入：

20 00 23 18 00 FF FF FF FF FF FF 02 00 11 22 33 44 55 66 77 88 99 aa bb cc dd ee ff C6 03

//表示在 IC 卡的第 2 块写入 00 11 22 33 44 55 66 77 88 99 aa bb cc dd ee ff　数据。

20 00 00 23 18 00 FF FF FF FF FF FF 04 00 11 22 33 44 55 66 77 88 99 aa bb cc dd ee ff C0 03

## 上位机收到数据：

**有卡并写入成功：20 00 23 01 00 DD 03**

**有卡但是密码校验错误：20 00 23 01 01 DC 03**

**卡片防碰撞失败：20 00 23 01 02 DF 03**

**卡片选择失败：20 00 23 01 03 DE 03**

**块写入失败：　　20 00 23 01 04 D9 03**

**其他扇区写入指令：**

20 00 23 18 00 FF FF FF FF FF FF 04 00 11 22 33 44 55 66 77 88 99 aa bb cc dd ee ff C0 03

## 1.4 修改密钥

### 上位机写入：

20 00 26 0E 00 FF FF FF FF FF FF 11 22 33 44 55 66 00 A0 03

// 将第 0 扇区的密码 A 修改成 11 22 33 44 55 66

### 上位机收到数据：

**有卡并修改成功**：20 00 26 01 00 D8 03

**有卡但是密码校验错误：20 00 26 01 01 D9 03**

**卡片防碰撞失败：20 00 26 01 02 DA 03**

**卡片选择失败：20 00 26 01 03 DB 03**

**块写入失败： 20 00 26 01 04 DC 03**