



# 高频读写器 开发手册 V2.1



手册内容主要包括：

- 读写器指令描述
- 主机与读写器之间数据传输格式
- 告警信息

如本开发手册中所提供的信息有不明确之处或与实际情况不符之处，请联系我们。联系方式：

- 广东思谷智能技术有限公司
- 电话：+86-769-26627955
- 传真：+86-769-26621889

## 文档标志说明

### 注意标志



当文档出现“注意标志”时表明该处为使用过程中需要注意之处。若使用过程中不遵守或未注意该处信息，将可能直接或间接导致读写器无法正常工作。请务必阅读标记有注意标记的内容。

---

# 1 目录

1. 序言 .....	4
2 读写器与主机之间的数据传输.....	5
2.1 主机与读写器之间的指令格式 .....	5
2.1.1 主机到读写器的指令格式.....	6
2.1.2 读写器到主机的指令格式.....	6
2.2 CRC 计算方式.....	7
3 读、写命令详解 .....	7
3.1 目录请求 ( 读 UID ) .....	8
3.2 读数据 .....	9
3.2.1 按字节读(推荐) .....	9
3.2.2 读多块.....	10
3.3 写数据 .....	12
3.3.1 按字节写(推荐) .....	12
3.3.2 写多块.....	13
3.4 擦除标签(复用按字节写功能).....	14
4 系统设置相关命令说明 .....	15
4.1 设置用户配置 .....	16
4.2 设置网络配置 .....	17
4.3 设置拓展用户配置 .....	18
4.4 GPIO 控制.....	20
4.4.1 GPO 控制.....	20
4.4.2 GPI 触发信息.....	21
5 告警信息列表 .....	22
6 应用举例.....	23
6.1 静态读写 .....	23
6.2 字节填充.....	26

# 1. 序言

本手册叙述的是，广东思谷智能技术有限公司（以下简称思谷）基于ISO 15693标准的高频RFID读写器(以下简称读写器)和主机(上位机，工控机、服务器、PLC)之间的通讯协议，包括标签的操作，读写器的配置与控制。

通讯方式兼容RS232/RS485、TCP/IP。命令的响应将通过命令发送端口返回，自动返回的数据将通过配置通讯端口返回。

## 两种工作模式

自动读取模式，亦可接受指令，且指令驱动优先级高。可通过设置使读写器工作模式为自动扫描或者纯指令交互式，如表格1.1所示：

表格1.1 工作模式简介

工作模式	描述
自动读取模式	在标签进入读写器的读写范围时，读写器自动读取用户指定的数据（标签UID、块数据或字节数据），并根据配置信息确定是否上传到主机到主机。此工作模式可同时接收并处理交互模式的指令。
指令交互模式	读写器不进行任何自动读取的操作，当主机发送指令到读写器时，读写器根据指令工作。

若在项目应用时需要标签进行读写操作，建议在写入的时候加上校验，并且在写入之后回读进行确认。

不同的型号，读写器与主机之间的通讯方式可以是RS232、RS485或者TCP/IP。若采用RS232或者RS485的通讯方式，通讯端口配置如表格1.2所示：

表格1.2 串口通讯端口配置

波特率	115200（默认值，可使用DEMO进行修改）
校验位	N
数据位	8

停止位	1
-----	---

使用TCP/IP的通讯方式时，通讯端口配置如表格1.3所示：

表格1.3 TCP/IP通讯端口配置

读写器IP地址	192.168.1.10（默认值，可使用DEMO进行修改）
本地端口号	3001

## 2 读写器与主机之间的数据传输

所有的数据传输都必须遵从严格的通讯格式，基本通讯格式描述如下：

### 2.1 主机与读写器之间的指令格式

主机与读写器之间的通讯遵循以下协议：

Header	Len	Cmd	Data	Crc-16
--------	-----	-----	------	--------

字段	长度	说明
Header	1 byte	帧头。固定值 0xFF
Len	1 byte	包长度。含 Len, Cmd, Data 字段
Cmd	1 byte	命令码。
Data	N bytes	用户数据。
Crc	2 bytes	CRC 校验。含 Header，Len，Cmd，Data 字段的 CRC 校验

其中 Data 格式定义如下：

CtrlFlg	CtrlFlg 参数	命令参数（读写需要的地址长度等参数）
---------	------------	--------------------

字段	长度	说明				
CtrlFlg	2 bytes	Bit15 IsResp	Bit 14:3 Reserve to 0	Bit2: Padding	Bit1: Reserve to 0	Bit0: ReaderID
[status]	1 byte	Bit15:IsResp 置位，此字段出现；此帧为响应帧； Bit15:IsResp 复位，此字段不出现；此帧为请求帧；				
[ReaderID]	1 byte	Bit0:ReaderID 置位，此字段出现，此时只有读写器 ID 与 ReaderID 一致，读写器才响应； Bit0:ReaderID 复位，此字段不出现；				
[TotalRespLen]	1 byte	Bit2: Padding 置位，此字段出现，此时若响应包长度不足 TotalRespLen 字节，将自动填充为 TotalRespLen 字节的长度，使用 0x00 在正常帧后				

		面填充；若响应帧长度超过 TotalRespLen，传输实际帧长度的数据； Bit2: Padding 复位，此字段不出现，响应包不进行任何填充处理；
Para	M bytes	根据各个功能来定义

注：数据传输采用大端字节序，即先传输高位字节，再传输低位字节。如 0x1234，先传输 0x12，再传输 0x34。

### 2.1.1 主机到读写器的指令格式

字段	长度	说明				
Header	1 byte	帧头。固定值 0xFF				
Len	1 byte	包长度。含 Len，Cmd，Status，Data 字段				
Cmd	1 byte	命令码。				
CtrlFlg	2 bytes	Bit15 IsResp	Bit 14:3 Reserve to 0	Bit2: Padding	Bit1: Reserve to 0	Bit0: ReaderID
[ReaderID]	1 byte	Bit0:ReaderID 置位，此字段出现，此时只有读写器 ID 与 ReaderID 一致，读写器才响应； Bit0:ReaderID 复位，此字段不出现；				
[TotalRespLen]	1byte	Bit2: Padding 置位，此字段出现，此时若响应包长度不足 TotalRespLen 字节，将自动填充为 TotalRespLen 字节的长度，使用 0x00 在正常帧后面填充；若响应帧长度超过 TotalRespLen，传输实际帧长度的数据； Bit2: Padding 复位，此字段不出现，响应包不进行任何填充处理；				
Para	M bytes	根据各个功能来定义				
Crc	2 bytes	CRC 校验。				

### 2.1.2 读写器到主机的指令格式

字段	长度	说明				
Header	1 byte	帧头。固定值 0xFF				
Len	1 byte	包长度。含 Len，Cmd，Status，Data 字段				
Cmd	1 byte	命令码。				
CtrlFlg	2 bytes	Bit15 IsResp	Bit 14:3 Reserve to 0	Bit2: Padding	Bit1: Reserve to 0	Bit0: ReaderID
Status	1 byte	命令执行状态				
[ReaderID]	1 byte	与请求帧一致				
[TotalRespLen]	1 byte	与请求帧一致				
Para	M bytes	根据各个功能来定义				

Crc	2 byte	CRC 校验。
Padding	M bytes	填充

## 2.2 CRC 计算方式

CRC采用CRC16算法，初始值为0xFFFF，计算示例如下：

```
const unsigned short wCRCTalbeAbs[] = {
    0x0000, 0xCC01, 0xD801, 0x1400,
    0xF001, 0x3C00, 0x2800, 0xE401,
    0xA001, 0x6C00, 0x7800, 0xB401,
    0x5000, 0x9C01, 0x8801, 0x4400,
};

unsigned short CRC16 (unsigned char* pchMsg, unsigned int wDataLen)
{
    unsigned short wCRC = 0xFFFF;
    unsigned int l = 0;
    unsigned char chChar = 0;
    for (i = 0; i < wDataLen; i++)
    {
        chChar = *pchMsg++;
        wCRC = wCRCTalbeAbs[(chChar ^ wCRC) & 15] ^ (wCRC >> 4);
        wCRC = wCRCTalbeAbs[((chChar >> 4) ^ wCRC) & 15] ^ (wCRC >> 4);
    }
    return wCRC;
}
```

读取UID数据码

FF 05 01 00 01 01    计算后的CRC：B8 19

# 3 读、写命令详解

思谷高频读写器通过访问不同的命令码（即 Cmd），从而实现执行不同的命令，并返回相应的数据，思谷高频读写器支持对标签进行读写操作的命令码如表 3.1 所示：

表 3.1 思谷高频读写器命令码

命令类型	命令码	功能	说明
	0x01	读取标签 UID	
	0x11	按字节读取标签内存	
	0x23	读多个数据块的数据	

RFID 命令	0x12	按字节写标签内存	
	0x24	写多个数据块的数据	
	0x2B	获取标签系统信息	
	0x2C	获取标签块安全状态	
	0x11	按字节读取标签内存	
	0x12	按字节写标签内存	
	0x10	检测标签在位信号	

### 3.1 目录请求（读 UID）

命令编码：**0x01**

功能说明：读取天线场范围内标签的UID，不支持多标签读取。

主机到读写器指令包格式如下：

字段	长度	说明				
Header	1 byte	0xFF				
Len	1 byte	包长度。含 Len,Cmd,Data 字段				
Cmd	1 byte	0x01				
CtrlFlg	2 bytes	Bit15 IsResp	Bit 14:3 Reserve to 0	Bit2: Padding	Bit1: Reserve to 0	Bit0: ReaderID
[ReaderID]	1 byte	CtrlFlg Bit0:ReaderID 置位，此字段出现，此时只有读写器 ID 与 ReaderID 一致，读写器才响应； CtrlFlg Bit0:ReaderID 复位，此字段不出现；				
[TotalRespLen]	1 byte	CtrlFlg Bit2: Padding 置位，此字段出现，此时若响应包长度不足 TotalRespLen 字节，将自动填充为 TotalRespLen 字节的长度，使用 0x00 在正常帧后面填充；若响应帧长度超过 TotalRespLen，传输实际帧长度的数据； CtrlFlg Bit2: Padding 复位，此字段不出现，响应包不进行任何填充处理；				
Crc	2 bytes	CRC 校验。				
Header   Len   Cmd   CtrlFlg   ReaderID   Crc-h   Crc-l						
例如请求帧：   FF   05   01   0001   00   78   D8						

命令执行完成，读写器响应数据格式如下：

字段	长度	说明
Header	1 byte	0xFF
Len	1 byte	包长度
Cmd	1 byte	0x01



CtrlFlg	2 bytes	除最高位置位，其他与请求帧一致	
Status	1 byte	成功，0x00	失败，非 0x00
[ReaderID]	1 byte	与请求帧一致	
[TotalRespLen]	1 byte	与请求帧一致	
[Uid]	8 bytes	读取的 UID	此字段不出现
Crc	2 bytes	CRC 校验。	
[Padding]	N bytes	与 TotalRespLen 字段是否出现，以及 TotalRespLen 的值有关	
Header   Len   Cmd   CtrlFlg   status   ReaderID   UID   Crc-h   Crc-l			
例如响应帧：FF   0E   01   8001   00(成功)   00   (797FBB39500104E0) 7D 79			
FF   06   01   8001   80(失败)   00   69 30			

## 3.2 读数据

**电子标签内存按照块地址划分，每个块有固定的字节大小（4 字节或者 8 字节）**

读数据方式	描述
字节读	按字节操作，数据长度大于（小于）块大小的整数倍
多块读	对多个块访问，获取数据长度为块大小*块数量（4*cnt 或 8*cnt）

用户根据自己的内存数据划分选择合适的读取方式，字节读写是最简单最方便快捷的方式。

可配置数据**读取校验**，具体配置见 4.1 用户配置。

### 3.2.1 按字节读(推荐)

命令编码：**0x11**

功能：按照字节读取标签内存，需要配置字节的起始地址和字节数量。

主机到读写器指令包格式如下：

字段	长度	说明				
Header	1 byte	0xFF				
Len	1 byte	包长度。含 Len, Cmd, Data 字段				
Cmd	1 byte	0x11				
CtrlFlg	2 bytes	Bit15 IsResp	Bit 14:3 Reserve to 0	Bit2: Padding	Bit1: Reserve to 0	Bit0: ReaderID
[ReaderID]	1 byte	CtrlFlg Bit0:ReaderID 置位，此字段出现，此时只有读写器 ID 与 ReaderID 一致，读写器才响应； CtrlFlg Bit0:ReaderID 复位，此字段不出现；				
[TotalRespLen]	1 byte	CtrlFlg Bit2: Padding 置位，此字段出现，此时若响应包长度不足 TotalRespLen 字节，将自动填充为 TotalRespLen 字节的长度，使用				

		0x00 在正常帧后面填充；若响应帧长度超过 TotalRespLen，传输实际帧长度的数据； CtrlFlg Bit2: Padding 复位，此字段不出现，响应包不进行任何填充处理；
StartAddress	2 bytes	起始地址
BytesNum	1 byte	读取的字节数量
Crc	2 bytes	CRC 校验。
读地址 01 长度为 8 的请求数据：		
Header	Len	Cmd CtrlFlg ReaderID StartAddress BytesNum Crc-h Crc-l
FF	08	11 0001 00 0001 08 35 72

命令执行完成后，读写器返回指令包格式如下：

字段	长度	说明
Header	1 byte	0xFF
Len	1 byte	包长度
Cmd	1 byte	0x11
CtrlFlg	2 bytes	除最高位置位，其他与请求帧一致
Status	1 byte	成功，0x00
[ReaderID]	1 byte	与请求帧一致
[TotalRespLen]	1 byte	与请求帧一致
Bytes Data	M bytes	读取到的字节信息
Crc	2 bytes	CRC 校验。
[Padding]	N bytes	与 TotalRespLen 字段是否出现，以及 TotalRespLen 的值有关
读地址 01 长度为 8 的响应数据：		
Header	Len	Cmd CtrlFlg status ReaderID BytesData Crc-h Crc-l
FF	0E	11 8001 00 00 (AA AA AA AA AA AA AA AA) 9A B5
FF	06	11 8001 80(失败)00 AA F1

3.2.2 读多块

命令编码：**0x23**

功能说明：读取标签指定块的数据内容，可对多块进行读取，最大支持 8 块。读取的块数越小，操作越稳定，花费的时间也越短。在进行标签内存读取时，根据是否进行读取校验，重复读取来进行校验。

主机到读写器指令包格式如下：

字段	长度	说明
Header	1 byte	0xFF
Len	1 byte	包长度。含 Len,Cmd,Data 字段

Cmd	1 byte	0x23						
CtrlFlg	2 bytes	Bit15 IsResp	Bit 14:3 Reserve to 0	Bit2: Padding	Bit1: Reserve to 0	Bit0: ReaderID		
[ReaderID]	1 byte	CtrlFlg Bit0:ReaderID 置位，此字段出现，此时只有读写器 ID 与 ReaderID 一致，读写器才响应； CtrlFlg Bit0:ReaderID 复位，此字段不出现；						
[TotalRespLen]	1byte	CtrlFlg Bit2: Padding 置位，此字段出现，此时若响应包长度不足 TotalRespLen 字节，将自动填充为 TotalRespLen 字节的长度，使用 0x00 在正常帧后面填充；若响应帧长度超过 TotalRespLen，传输实际帧长度的数据； CtrlFlg Bit2: Padding 复位，此字段不出现，响应包不进行任何填充处理；						
StartBlk	1 byte	起始块						
BlkCnt	1 byte	块数量						
Crc	2 bytes	CRC 校验						
读 0~3 块数据请求数据：								
Header	Len	Cmd	CtrlFlg	ReaderID	StartBlk	BlkCnt	Crc-h	Crc-l
FF	07	23	0001	00	00	04	A3	7E

命令执行完成，读写器响应数据格式如下：

字段	长度	说明						
Header	1 byte	0xFF						
Len	1 byte	包长度						
Cmd	1 byte	0x23						
CtrlFlg	2 bytes	除最高位置位，其他与请求帧一致						
Status	1 byte	成功，0x00	失败，非 0x00					
[ReaderID]	1 byte	与请求帧一致						
[Antenna]	1 byte	与请求帧一致						
[TotalRespLen]	1 byte	与请求帧一致						
[Datas]	N bytes	读取的数据	此字段不出现					
Crc	2 bytes	CRC 校验。						
[Padding]	N bytes	与 TotalRespLen 字段是否出现，以及 TotalRespLen 的值有关						
读 0~3 块数据响应数据：								
Header	Len	Cmd	CtrlFlg	status	ReaderID	BytesData	Crc-h	Crc-l
FF	16	23	8001	00	00	(AAAAAAAAA0A1A2A3AAAAAAAAAAAAAAAA)	46	D6
FF	06	23	8001	80(失败)	00		6E	C8

注：读取的数据长度与标签的内存结构有关：( BlkCnt\*块大小 ) 即为读取的数据长度

### 3.3 写数据

写数据方式	描述
字节写	按字节写入，数据长度大于（小于）块大小的整数倍
多块写	对多个块写入，操作数据长度为块大小*块数量（4*cnt 或 8*cnt）

用户根据自己的内存数据划分选择合适的读取方式，字节读写是最简单最方便快捷的方式。

可配置数据**写校验**（写入后读出校验），具体配置见 4.1 用户配置。

#### 3.3.1 按字节写(推荐)

命令编码：**0x12**

功能：按字节的形式写标签内存。

主机到读写器指令包格式如下：

字段	长度	说明							
Header	1 byte	0xFF							
Len	1 byte	包长度。含 Len, Cmd, Data 字段							
Cmd	1 byte	0x12							
CtrlFlg	2 bytes	Bit15 IsResp	Bit 14:3 Reserve to 0	Bit2: Padding	Bit1: Reserve to 0	Bit0: ReaderID			
[ReaderID]	1 byte	CtrlFlg Bit0:ReaderID 置位，此字段出现，此时只有读写器 ID 与 ReaderID 一致，读写器才响应； CtrlFlg Bit0:ReaderID 复位，此字段不出现；							
[TotalRespLen]	1 byte	CtrlFlg Bit2: Padding 置位，此字段出现，此时若响应包长度不足 TotalRespLen 字节，将自动填充为 TotalRespLen 字节的长度，使用 0x00 在正常帧后面填充；若响应帧长度超过 TotalRespLen，传输实际帧长度的数据； CtrlFlg Bit2: Padding 复位，此字段不出现，响应包不进行任何填充处理；							
Start Address	2 bytes	起始地址							
BytesCnt	1 byte	写入的字节数量							
Datas	M bytes	待写入的数据							
Crc	2 bytes	CRC 校验。							
从 0 写 10 个字节请求数据:									
Header	Len	Cmd	CtrlFlg	ReaderID	StartAddress	ByteCnt	Datas	Crc-h	Crc-l
FF	12	12	0001	00	0000	0A	(00010203040506070809)	66	ED

命令执行完成后，读写器返回的指令包格式如下：

字段	长度	说明
Header	1 byte	0xFF
Len	1 byte	包长度
Cmd	1 byte	0x12
CtrlFlg	2 bytes	除最高位置位，其他与请求帧一致
Status	1 byte	成功，0x00
[ReaderID]	1 byte	与请求帧一致
[TotalRespLen]	1 byte	与请求帧一致
Crc	2 bytes	CRC 校验。
[Padding]	N bytes	与 TotalRespLen 字段是否出现，以及 TotalRespLen 的值有关

从 0 写 10 个字节响应数据：

Header	Len	Cmd	CtrlFlg	status	ReaderID	Crc-h	Crc-l
FF	06	12	8001	00(成功)	00	6A	D4
FF	06	12	8001	80(失败)	00	AA	B5

### 3.3.2 写多块

命令编码：**0x24**

功能说明：将数据内容写入标签的指定块。将数据写入标签后，将再读取出来进行校验。

主机到读写器请求格式如下：

字段	长度	说明
Header	1 byte	0xFF
Len	1 byte	包长度。含 Len,Cmd,Data 字段
Cmd	1 byte	0x24
CtrlFlg	2 bytes	<div>Bit15</div> <div>IsResp</div> <div>Bit 14:3</div> <div>Reserve to 0</div> <div>Bit2:</div> <div>Padding</div> <div>Bit1:</div> <div>Reserve to 0</div> <div>Bit0:</div> <div>ReaderID</div>
[ReaderID]	1 byte	CtrlFlg Bit0:ReaderID 置位，此字段出现，此时只有读写器 ID 与 ReaderID 一致，读写器才响应； CtrlFlg Bit0:ReaderID 复位，此字段不出现；
[TotalRespLen]	1 byte	CtrlFlg Bit2: Padding 置位，此字段出现，此时若响应包长度不足 TotalRespLen 字节，将自动填充为 TotalRespLen 字节的长度，使用 0x00 在正常帧后面填充；若响应帧长度超过 TotalRespLen，传输实际帧长度的数据； CtrlFlg Bit2: Padding 复位，此字段不出现，响应包不进行任何填充处理；
StartBlk	1 byte	起始块
BlkCnt	1 byte	块数量

Datas	N bytes	需要写入到标签里面的数据							
Crc	2 bytes	CRC 校验。							
从块 0 写入 2 个块数据请求数据：									
Header	Len	Cmd	CtrlFlg	ReaderID	StartBlk	BlkCnt	Data	Crc-h	Crc-l
FF	0F	24	0001	00	00	02	(00010203 04050607)	B2	36

命令执行完成，读写器返回响应数据格式如下：

字段	长度	说明					
Header	1 byte	0xFF					
Len	1 byte	包长度					
Cmd	1 byte	0x24					
CtrlFlg	2 bytes	除最高位置位，其他与请求帧一致					
Status	1 byte	成功，0x00	失败，非 0x00				
[ReaderID]	1 byte	与请求帧一致					
[Antenna]	1 byte	与请求帧一致					
[TotalRespLen]	1 byte	与请求帧一致					
Crc	2 bytes	CRC 校验。					
[Padding]	N bytes	与 TotalRespLen 字段是否出现，以及 TotalRespLen 的值有关					
从块 0 写入 2 个块数据响应数据：							
Header	Len	Cmd	CtrlFlg	status	ReaderID	Crc-h	Crc-l
FF	06	24	8001	00 (成功)	00	6E	1C
FF	06	24	8001	80 (失败)	00	AE	7D

### 3.4 擦除标签(复用按字节写功能)

命令编码：**0x12**

功能说明：将一片标签内存写为指定值

主机到读写器请求数据格式如下：

字段	长度	说明				
Header	1 byte	0xFF				
Len	1 byte	0B				
Cmd	1 byte	0x12				
CtrlFlg	2 byte	Bit15 IsResp	Bit 14:3 Reserve to 0	Bit2: Padding	Bit1: Reserve to 0	Bit0: ReaderID
[ReaderID]	1 byte	CtrlFlg Bit0:ReaderID 置位，此字段出现，此时只有读写器 ID 与 ReaderID 一致，读写器才响应； CtrlFlg Bit0:ReaderID 复位，此字段不出现；				
[TotalRespLen]	1byte	CtrlFlg Bit2: Padding 置位，此字段出现，此时若响应包长度不足				

		TotalRespLen 字节，将自动填充为 TotalRespLen 字节的长度，使用 0x00 在正常帧后面填充；若响应帧长度超过 TotalRespLen，传输实际帧长度的数据；  CtrlFlg Bit2: Padding 复位，此字段不出现，响应包不进行任何填充处理；									
StartADDR	2byte	Bit15: 擦除标签内存功能 (固定 1)				Bit 14:0 地址					
Cnt1	1byte	固定值 03									
Cnt2	1byte	擦除数量									
Data	1byte	写入的数据									
Data check	1byte	Data 字段与 0xFF 的异或值，用于确认使用擦除标签内存功能									
Crc	2 byte	CRC 校验。									
从地址 1 开始的 10 个长度值擦除为 AA 值：											
Header	Len	Cmd	CtrlFlg	ReaderID	StartAddr	Cnt1	Cnt2	Data	DataCheck	Crc-h	Crc-l
FF	0B	12	0001	01	8001	03	0A	AA	55	B9	DB

命令执行完成，读写器返回指令包格式如下：

字段	长度	说明					
Header	1 byte	0xFF					
Len	1 byte	包长度					
Cmd	1 byte	0x12					
CtrlFlg	2 byte	除最高位置位，其他与请求帧一致					
Status	1 byte	成功，0x00	失败，非 0x00				
[ReaderID]	1 byte	与请求帧一致					
[TotalRespLen]	1byte	与请求帧一致					
Crc	2 byte	CRC 校验。					
[Padding]	Nbytes	与 TotalRespLen 字段是否出现，以及 TotalRespLen 的值有关					
擦除成功响应数据：							
Header	Len	Cmd	CtrlFlg	status	ReaderID	Crc-h	Crc-l
FF	06	12	8001	00	01	AA	15

4 系统设置相关命令说明

系统设置相关的命令如表 4.1 所示：

表 4.1 系统设置相关命令

CmdCode	功能	CmdCode	功能
0xA0	设置拓展配置	0x04	设置波特率
0xAE	获取用户配置	0x16	保存用户配置
0xB1	设置网络配置	0x1A	清除配置
0xB0	获取网络配置	0x1C	设置用户配置

0xAC	复位 MCU	0x1E	获取软件版本
0xA1	获取拓展配置	0xAA	GPI 触发提醒
0xA9	GPO 控制		

### 4.1 设置用户配置

命令编码：**0x1C**

功能说明：设置读写器的用户配置，掉电可保存。

主机到读写器请求数据格式如下：

字段	长度	说明				
Header	1 byte	0xFF				
Len	1 byte	包长度。含 Len, Cmd, Data 字段				
Cmd	1 byte	0x1C				
CtrlFlg	2 bytes	Bit15 IsResp	Bit 14:3 Reserve to 0	Bit2: Padding	Bit1: Reserve to 0	Bit0: ReaderID
[ReaderID]	1 byte	CtrlFlg Bit0:ReaderID 置位，此字段出现，此时只有读写器 ID 与 ReaderID 一致，读写器才响应； CtrlFlg Bit0:ReaderID 复位，此字段不出现；				
[TotalRespLen]	1 byte	CtrlFlg Bit2: Padding 置位，此字段出现，此时若响应包长度不足 TotalRespLen 字节，将自动填充为 TotalRespLen 字节的长度，使用 0x00 在正常帧后面填充；若响应帧长度超过 TotalRespLen，传输实际帧长度的数据； CtrlFlg Bit2: Padding 复位，此字段不出现，响应包不进行任何填充处理；				
WorkMode	1 byte					
Reader_ID	1 byte					
RFChipPower	1 byte					
Check	1 byte					
CommPort	1 byte					
EnabledAnt	1 byte					
AvailableTime	1 byte					
Crc	2 bytes	CRC 校验。				

命令执行完成，读写器返回指令包格式如下：

字段	长度	说明
Header	1 byte	0xFF
Len	1 byte	包长度



Cmd	1 byte	0x1C	
CtrlFlg	2 bytes	除最高位置位，其他与请求帧一致	
Status	1 byte	成功，0x00	失败，非 0x00
[ReaderID]	1 byte	与请求帧一致	
[TotalRespLen ]	1 byte	与请求帧一致	
Crc	2 bytes	CRC 校验。	
[Padding]	N bytes	与 TotalRespLen 字段是否出现，以及 TotalRespLen 的值有关	

配置项详解：

配置项		默认值	其它可配置值	备注
WorkMode	工作模式	交互模式 ( 0x00 )	自动寻卡模式 ( 0x01 )	自动寻卡时，亦可接受串口指令
Reader_ID	读写器 ID	0x00	0x01-0xFF (DP:0x01-0x7E)	用于 485 总线下的设备识别号
RFChipPower	功率	全功率 ( 0x01 )	半功率 ( 0x00 )	选择全功率
Check	数据校验	通讯校验 ( 0x01 )	Bit0:通讯校验 ( 强制开启 ) Bit1:读校验 0x03 Bit2:写校验 0x05 读写校验 0x07	读校验：内部执行两次读取比较 写校验：写入后读出比较
CommPort	通讯接口	RS232 (0x00)	RS485(0x01) TCP(0x02)	底层自集成，无需特别设置
EnabledAnt	RFU	( 0x01 )	RFU	RFU
AvailableTime	RFU	( 0x00 )	RFU	RFU

**注：**为保存用户配置参数，在执行设置用户配置时，系统将自动关闭部分功能。请在接收到设置用户配置命令的响应后，再执行其他的命令操作，正常情况下响应时间在 150 毫秒以内。

## 4.2 设置网络配置

命令编码：**0xB1**

功能说明：设置读写器的网络配置，掉电可保存。只有支持网口的读写器才支持此命令。

主机到读写器请求数据格式如下：

字段	长度	说明
Header	1 byte	0xFF
Len	1 byte	包长度。含 Len,Cmd,Data 字段

Cmd	1 byte	0xB1				
CtrlFlg	2 bytes	Bit15 IsResp	Bit 14:3 Reserve to 0	Bit2: Padding	Bit1: Reserve to 0	Bit0: ReaderID
[ReaderID]	1 byte	CtrlFlg Bit0:ReaderID 置位，此字段出现，此时只有读写器 ID 与 ReaderID 一致，读写器才响应； CtrlFlg Bit0:ReaderID 复位，此字段不出现；				
[TotalRespLen]	1 byte	CtrlFlg Bit2: Padding 置位，此字段出现，此时若响应包长度不足 TotalRespLen 字节，将自动填充为 TotalRespLen 字节的长度，使用 0x00 在正常帧后面填充；若响应帧长度超过 TotalRespLen，传输实际帧长度的数据； CtrlFlg Bit2: Padding 复位，此字段不出现，响应包不进行任何填充处理；				
Ip	4 bytes	Ip 地址				
Mask	4 bytes	子网掩码				
gateway	4 bytes	网关				
Crc	2 bytes	CRC 校验。				

命令执行完成，读写器返回请求数据格式如下：

字段	长度	说明	
Header	1 byte	0xFF	
Len	1 byte	包长度	
Cmd	1 byte	0xB1	
CtrlFlg	2 bytes	除最高位置位，其他与请求帧一致	
Status	1 byte	成功，0x00	失败，非 0x00
[ReaderID]	1 byte	与请求帧一致	
[TotalRespLen ]	1 byte	与请求帧一致	
Crc	2 bytes	CRC 校验。	
[Padding]	N bytes	与 TotalRespLen 字段是否出现，以及 TotalRespLen 的值有关	

## 4.3 设置拓展用户配置

命令编码：**0xA0**

功能说明：设置读写器的扩展用户配置，掉电不保存。主要包括自动读卡的配置信息。

主机到读写器指令包格式如下：

字段	长度	说明
Header	1 byte	0xFF
Len	1 byte	包长度。含 Len,Cmd,Data 字段

Cmd	1 byte	0xA0				
CtrlFlg	2 bytes	Bit15 IsResp	Bit 14:3 Reserve to 0	Bit2: Padding	Bit1: Reserve to 0	Bit0: ReaderID
[ReaderID]	1 byte	CtrlFlg Bit0:ReaderID 置位，此字段出现，此时只有读写器 ID 与 ReaderID 一致，读写器才响应； CtrlFlg Bit0:ReaderID 复位，此字段不出现；				
[TotalRespLen]	1 byte	CtrlFlg Bit2: Padding 置位，此字段出现，此时若响应包长度不足 TotalRespLen 字节，将自动填充为 TotalRespLen 字节的长度，使用 0x00 在正常帧后面填充；若响应帧长度超过 TotalRespLen，传输实际帧长度的数据； CtrlFlg Bit2: Padding 复位，此字段不出现，响应包不进行任何填充处理；				
SubCmd	1 byte	子命令 0x00:读取 UID，0x01:按块读取，0x03：按字节读取				
GpoAutoCtrl	2 bytes	Gpo 自动控制				
CachePara	2 bytes	缓存参数				
ReadPara	4 bytes	读取参数				
Crc	2 bytes	CRC 校验。				

GpoAutoCtrl的定义如下：

地址	定义	说明
Bit 15	Enable	使能位
Bit14:13	GPO	需要自动控制的 GPO 端口 00：GPO1      01：GPO2 10：GPO3      11：GPO4
Bit12	DstStat	GPO 控制的目标状态：0：断开，1：连接
Bit11:0	Timeout	超时时间，单位 10ms

CachePara用来定义当前读取功能的缓存参数，具体定义如下：

子命令	地址	定义	说明
0x00(读取 UID)	Bit 15	Enable	使能位
0x01(按块读取)	Bit14:12	RESERVE	预留
0x3(按字节读取)	Bit11:0	Timeout	超时时间，单位 10ms

ReadPara用来定义当前读取功能的块参数/字节参数，具体定义如下：

子命令	地址	定义	说明
0x01(按块读取)	Byte 1	Enable	使能读取 UID
0x3(按字节读取)	Byte2和Byte3	Start Address	起始块号/地址
	Byte4	Cnt	块/字节数量

命令执行完成，读写器返回响应数据格式如下：

字段	长度	说明	
Header	1 byte	0xFF	
Len	1 byte	包长度	
Cmd	1 byte	0xA0	
CtrlFlg	2 bytes	除最高位置位，其他与请求帧一致	
Status	1 byte	成功，0x00	失败，非 0x00
[ReaderID]	1 byte	与请求帧一致	
[TotalRespLen ]	1 byte	与请求帧一致	
Crc	2 bytes	CRC 校验。	
[Padding]	N bytes	与 TotalRespLen 字段是否出现，以及 TotalRespLen 的值有关	

4.4 GPIO 控制

4.4.1 GPO 控制

命令编码：**0xA9**

功能说明：控制GPO的通/断状态。

主机到读写器请求数据格式如下：

字段	长度	说明
Header	1 byte	0xFF
Len	1 byte	包长度。含 Len,Cmd,Data 字段
Cmd	1 byte	0xA9
CtrlFlg	2 bytes	<div> <div>Bit15:</div> <div>IsResp</div> <div>(固定 0)</div> </div> <div> <div>Bit 14:5</div> <div>Reserve</div> </div> <div> <div>Bit4:</div> <div>ReadUid</div> <div>(取值 0)</div> </div> <div> <div>Bit3:</div> <div>AddrMode</div> <div>(取值 0)</div> </div> <div> <div>Bit2:</div> <div>Padding</div> </div> <div> <div>Bit1:</div> <div>Reserve</div> </div> <div> <div>Bit0:</div> <div>ReaderID</div> </div>
[ReaderID]	1 byte	CtrlFlg Bit0:ReaderID 置位，此字段出现，此时只有读写器 ID 与 ReaderID 一致，读写器才响应； CtrlFlg Bit0:ReaderID 复位，此字段不出现；
[TotalRespLen]	1 byte	CtrlFlg Bit2: Padding 置位，此字段出现，此时若响应包长度不足 TotalRespLen 字节，将自动填充为 TotalRespLen 字节的长度，使用 0x00 在正常帧后面填充；若响应帧长度超过 TotalRespLen，传输实际帧长度的数据； CtrlFlg Bit2: Padding 复位，此字段不出现，响应包不进行任何填充处理；
GPO	1 byte	GPO 端口 (GPO1 0X01) (GPO2 0X02) (GPO3 0X03) (GPO4 0X04)

IsConnect	1 byte	输出状态 01 表示输出高 00 表示输出低
Crc	2 bytes	CRC 校验。
GPO 输出高请求数据：		
Header	Len	Cmd CtrlFlg ReaderID GPO IsConnect Crc-h Crc-l
FF	07	A9 0001 00 01 01 5A A0

命令执行完成，读写器返回指令包格式如下：

字段	长度	说明
Header	1 byte	0xFF
Len	1 byte	包长度
Cmd	1 byte	0xA9
CtrlFlg	2 bytes	除最高位置位，其他与请求帧一致
Status	1 byte	成功，0x00
[ReaderID]	1 byte	与请求帧一致
[TotalRespLen ]	1 byte	与请求帧一致
Crc	2 bytes	CRC 校验。
[Padding]	N bytes	与 TotalRespLen 字段是否出现，以及 TotalRespLen 的值有关
GPO 输出高响应数据：		
Header	Len	Cmd CtrlFlg status ReaderID Crc-h Crc-l
FF	06	A9 8001 00 00 71 30

注：读写器所支持的GPO数量参见所选设备的用户手册；设置CONNECT为0x01时，表示控制GPOX-和GPOX+导通，设置为0x00时则表示断开。

4.4.2 GPI 触发信息

命令编码：**0xA4**

功能说明：当有GPI触发时，提醒主机。

主机到读写器指令包格式如下：

字段	长度	说明
Header	1 byte	0xFF
Len	1 byte	包长度。含 Len,Cmd,Data 字段
Cmd	1 byte	0xA9
CtrlFlg	2 bytes	<div> <div>Bit15: IsResp (固定 0)</div> <div>Bit 14:5 Reserve</div> <div>Bit4: ReadUid (取值 0)</div> <div>Bit3: AddrMode (取值 0)</div> <div>Bit2: Padding</div> <div>Bit1: Reserve</div> <div>Bit0: ReaderID</div> </div>
[ReaderID]	1 byte	CtrlFlg Bit0:ReaderID 置位，此字段出现，此时只有读写器 ID 与 ReaderID 一致，读写器才响应；

		CtrlFlg Bit0:ReaderID 复位，此字段不出现；				
[TotalRespLen]	1 byte	CtrlFlg Bit2: Padding 置位，此字段出现，此时若响应包长度不足 TotalRespLen 字节，将自动填充为 TotalRespLen 字节的长度，使用 0x00 在正常帧后面填充；若响应帧长度超过 TotalRespLen，传输实际帧长度的数据；  CtrlFlg Bit2: Padding 复位，此字段不出现，响应包不进行任何填充处理；				
Crc	2 bytes	CRC 校验。				
Header	Len	Cmd	CtrlFlg	ReaderID	Crc-h	Crc-l
FF	05	A4	0001	00	B4	FA

命令执行完成，读写器返回指令包格式如下：

字段	长度	说明
Header	1 byte	0xFF
Len	1 byte	包长度
Cmd	1 byte	0xA9
CtrlFlg	2 bytes	除最高位置位，其他与请求帧一致
Status	1 byte	成功，0x00
[ReaderID]	1 byte	与请求帧一致
[TotalRespLen ]	1 byte	与请求帧一致
GPI Count	1 byte	输入的点数
GPI Status	1byte	值
Crc	2 bytes	CRC 校验。
[Padding]	N bytes	与 TotalRespLen 字段是否出现，以及 TotalRespLen 的值有关
Header	Len	Cmd
FF	08	A4
CtrlFlg	status	ReaderID
8001	00	00
GPI Count	GPI Status	Crc-h
04	03	Crc-l
	A9	CB

注：读写器所支持的GPI数量参见所选设备的用户手册。

## 5 告警信息列表

指令执行结果的成功与否，可依据返回指令的“状态”位判定。若“状态”不为0x00，则指令执行失败。按照“状态”的不同，可分为以下几种情况：

状态码	含义	备注
0x00	指令执行成功	
0x80	指令执行失败	一般出现的原因是无标签处于可读区域,或者标签读取失败

0x82	参数错误	请检查读写起始地址，读写长度是否配置正确
0x83	读写器发生未知错误	
0x90	无标签在可读区域	此错误码将在指令即时有效的情况下，无标签在可读区域时返回
0x91	射频数据传输错误	数据传输时发生格式错误，可能原因射频受到干扰，标签处理临界区域，或者有多个标签在可读区域
0x92	写数据地址错误	标签没有请求的数据地址
0x93	写数据块被锁	所请求的数据地址被锁，不可再执行写操作
0x94	写数据块失败	所请求的数据地址编程失败，可能是此标签已达到规写次数
0x95	读取标签失败，读取一半标签离开	标签移动过快或标签所在的区域读写器工作不稳定，读写器无法完成全部的读取数据操作
0x96	写标签失败，写标签一部分数据后标签离开	标签移动过快或标签所在的区域读写器工作不稳定，读写器无法完成全部的写数据操作
0x97	写写标签失败，写标签一部分后射频数据传输错误	读写器写了一部分数据后受到干扰导致数据传输异常
0x98	数据校验错误	仅在启用了读写校验时可能出现
0x99	标签型号解析错误	读取的标签型号暂不能兼容
0xA1	射频模块异常	射频模块有异常现象
0xB0	参数有误	读写指令的数据格式不对，或操作的数据大于限定的长度

## 6 应用举例

### 6.1 静态读写

#### 1、读写器配置

在静态读写的情况下，读写器不需要支持自动读卡的方式，可将自动读卡关闭。关闭自动读卡发送如下命令(未考虑设置读写器 ID)：FF 0C 1C 00 01 00 00 00 01 01 00 08 01 39 DB

请求帧和响应帧的解析数据如下表所示：

字段	说明
FF	帧头
0C	帧长度
1C	命令码
00 01	控制码
00	ReaderID 号
00	工作模式
00	新的 ReaderID 号
01	射频芯片功率
01	是否进行读/写校验
00	通讯端口号
08	使用的天线号，默认 08
01	空闲间隙，一般不用到，默认 01
39 D8	CRC 校验

若读写器采用的 RS485 进行组网，当 RS485 网络内存在多个读写器时，需要设置读写器的 ID。

关闭读写器自动读卡，且设置读写器 ID 为 0x01 的命令格式为：FF 0C 1C 00 01 00 00 01 01 00 08 01 E8 DA  
关闭读写器自动读卡，且设置读写器 ID 为 0x02 的命令格式为：FF 0C 1C 00 01 00 00 02 01 01 00 08 01 DB DA

2、读标签内存

以控制读写器0x01读取标签地址0开始的4个字节为例，发送的命令格式为：FF 08 11 00 01

01 00 00 04 5C 72。若标签存储的数据为0x00010203，读取成功时，读写器的响应数据为：

FF 0A 11 80 01 00 01 00 01 02 03 42 E0.请求帧和响应帧的解析数据如下表所示：

请求帧		响应帧	
字段	说明	字段	说明
FF	帧头	FF	帧头
08	帧长度	0A	帧长度
11	字节读	11	字节读
00 01	控制码	80 01	控制码
01	ReaderID	00	执行状态，00 表示



			成功
00 00	起始地址	01	ReaderID 号
04	读取字节数量	00 01 02 03	数据
5C 72	CRC 校验	42 E0	CRC 校验

以控制读写器0x02读取标签地址8开始的4个字节为例，发送的命令格式为：**FF 08 11 00 01**

**02 00 08 04 D8 75**。若标签存储的数据为0x0809AAA，则读取成功时，读写器的响应数据

为：**FF 0A 11 80 01 00 02 08 09 AA AA 5E 98**

### 3、写标签内存

以控制读写器0x01写标签地址4开始的4个字节为例，写的数据为41424344，发送的命令格

式为：**FF 0C 12 00 01 01 00 04 04 41 42 43 44 4E A1**。若执行成功，读写器响应数据为：**FF 06**

**12 80 01 00 01 AA 15**

请求帧和响应帧的解析数据如下表所示：

请求帧		响应帧	
字段	说明	字段	说明
FF	帧头	FF	帧头
0C	帧长度	06	帧长度
12	字节写	12	命令码
00 01	控制码	80 01	控制码
01	ReaderID	00	执行状态，00 表示成功
0004	起始地址	01	ReaderID 号
04	写入数据长度	AA 15	CRC 校验
41 42 43 44	数据		
4E A1	CRC 校验		

以控制读写器0x02写标签地址2开始的4个字节为例，写的数据为10111213，发送的命令格

式为：**FF 0C 12 00 01 02 00 02 04 10 11 12 13 BE 7D**。若执行成功，读写器响应数据为：**FF**

**06 12 80 01 00 02 AB 55**

## 6.2 字节填充

在使用部分 PLC(如，欧姆龙 CP1H)作为上位机进行控制时，只能使用固定长度或者固定的结束符作为一帧数据结束判断标志。在此种情况下，需要使用字节填充功能才能很好的对读写器进行集成。使用此功能需要在请求帧的 CtrlFlg 字段进行标记，标记位置为 Bit 2(padding)。举例：

读取 UID，读取成功时，返回 18 字节数据。

读取 91 字节，读取成功时，返回 100 字节。

如 PLC 无法使用间隔时间作为帧结束标志，可开启填充功能。此时需要把读取 UID 和读取 91 字节都开启填充功能，填充值设置为 100 字节。开启后两个命令的执行的返回帧都是 100 字节，成功和失败帧都是 100 字节。将读取 UID 设置填充到 100 字节的命令如下表所示：

请求帧		响应帧	
字段	说明	字段	说明
FF	帧头	FF	帧头
06	帧长度	0F	有效帧长度
01	字节读	01	字节读
00 05	控制码，使能 Padding	80 05	控制码
00	ReaderID	00	执行状态，00 表示 成功
64	TotalRespLen	00	ReadeID 号
43 38	CRC 校验	64	TotalRespLen
		E8 47 BB 39 50 01 04 E0	UID
		A6 65	CRC 校验
		82 个填充字节 0	

注：返回帧中，CRC 只计算有效数据，填充字节不包含在内。