

MODBUS 读卡器说明书



一、产品简介：

本 Modbus 非接触卡读写器是基于自主软硬件技术开发的,同时支持 125Khz 的 id 卡和 13.56M 的 IC 卡的门禁读卡器。本产品采用低功耗,环保器件设计制造。本产品具有以下特色功能

- 支持 MODBUS_RTU 通讯协议
- 狙击 IC 复制卡,完美解决复制卡安全问题
- 支持 IC 卡, ID 卡, 二代证等
- 全环境设计, -30 度到 75 度可正常工作
- 金属表面直接安装

二、产品性能：

- 电源 DC6V-15VDC ($\pm 5\%$)
- 电流 静态 30 mA, 最大值小于 50mA
- 通讯 MODBUS_RTU (485)
- 支持协议 EM 低频卡传输协议, ISO14443A/B
- 支持 Gicard 安全门禁方案
- 状态提示 双色 LED / 1 个蜂鸣器
- 操作温度 -40°C to $+75^{\circ}\text{C}$

- 保存温度 -40° C to +80° C
- 湿度 0 ~ 100% 全防水
- 防护等级 IP65 (产品灌环氧树脂)
- 颜色 碳黑色
- 尺寸 86*86*9.5mm

三、接线定义:

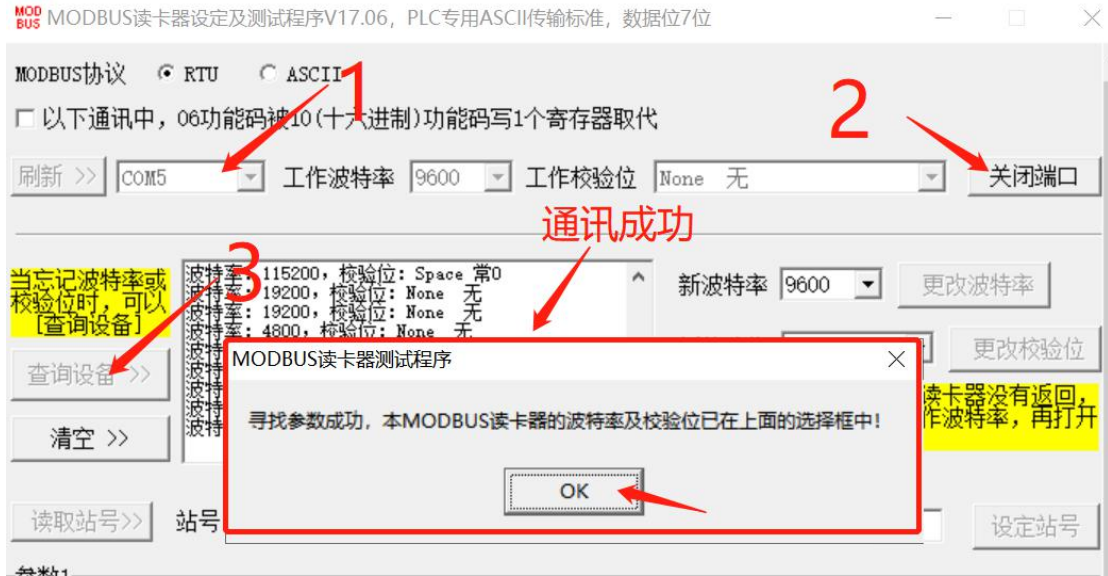
序号	接线端名称	颜色	说明	备注
1	VCC	红色	12V 直流电源	供电电流须大于 300 毫安
2	485+	棕色	485+ TXD(232)	
3	485-	蓝色	485- RXD(232)	
4	BUZ	黄色	蜂鸣器控制信号	低电平有效 (输入)
5	LED	橙色	LED 控制信号	低电平有效 (输入)
6	DATA0	绿色	继电器 1 输出	OC 输出, 电流小于 100ma
7	DATA1	白色	继电器 2 输出	OC 输出, 电流小于 100ma
8	GND	黑色	电源地	

四、MODBUS 相关参数:

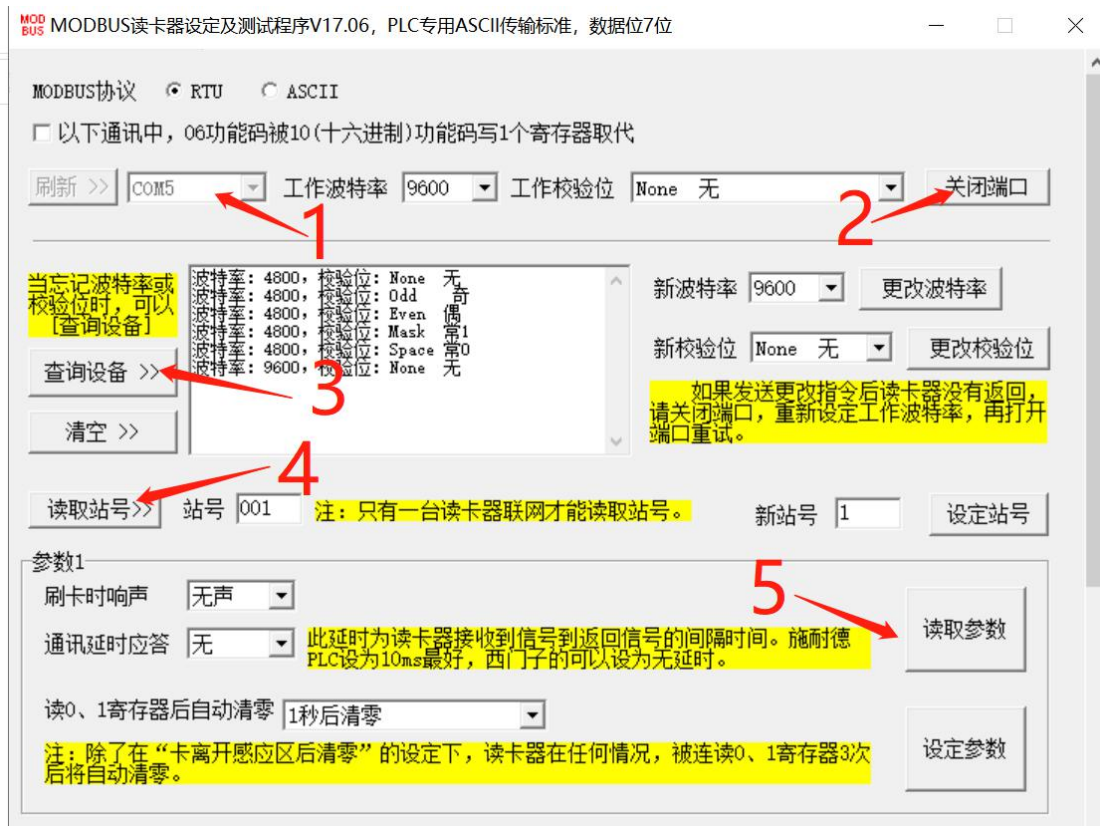
- 1、站号 1-254, 波特率 4800-57600, 数据位 8、7, 停止位 1、2, 校验位: None (无校验)、(Odd) 奇校验、(Even) 偶校验、Mask(常 1) Space(常 0)。
- 2、RTU 读卡器默认参数: 站号 2、波特率 19200、数据位 8, 停止位 1, 无校验。
- 3、MODBUS 读卡器通过 MODBUS-RTU 方式与 PLC 通信, MODBUS 读卡器为从站、PLC 为主站, 需要实现即时刷卡功能, 可用 PLC 设备每隔 0.2 秒读卡一次。

五、快速测试方法：

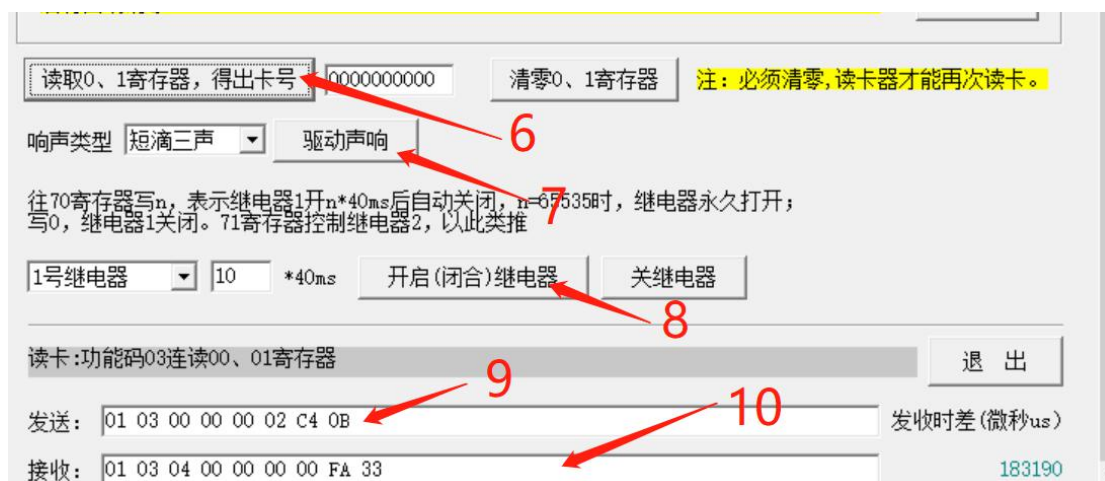
1、按图正确接线，读卡器通过 485 与电脑通讯，打开测试软件按下列流程进行：



成功查找到设备后弹出上图窗口，点击确定后进行“读取站号（4）”等操作，如下图：



点击下图“驱动声响（7）”，蜂鸣器会响起，说明软件与读卡器通讯成功；对着读卡器刷卡，然后点击“读取 0、1 寄存器得出卡号”按钮（如图标“6”处），右侧方框应显示刚才读取的卡号（此处显示的卡号是经过软件处理的 10 位卡号），同时“接收”方框会显示接收到的数据串（如图标“10”处，其中第 4-7 字节是读取到的真实卡号）；其他功能可自行测试。参见下图：



六、常用指令

（以下指令假设地址为 0x02，通讯协议格式见后续章节）：

```

00 03 00 02 00 01 24 1B //查找设备或读取站号（只有一个设备在线时
    才能操作成功）
02 06 00 02 00 02 A9 F8 //设置站号
02 03 00 03 00 01 74 39 //读取参数
02 03 00 00 00 02 C4 38 //读取卡号
02 06 00 03 80 31 D9 ED //设置参数
02 10 00 00 00 02 04 00 00 00 00 FC EB //清 0 读卡寄存器
02 06 00 04 00 01 09 F8 //驱动蜂鸣器响一声
02 06 00 46 00 19 A9 E6 //开启第一个继电器（定时关闭）
02 10 00 3C 00 02 04 25 80 55 AA 4A 61 //将波特率设成 9600
  
```

七、读卡器地址表（部分功能无效需定制）

地址表 (十进制)	说明	备注
0000-0001	存放 IC 卡 4 个字节卡号	断电不

		保存						
0002	读卡器站号（机号）	断电保存						
0003	设备参数设置：刷卡响声、通讯延时、自动清零等	断电保存						
0004	发送控制蜂鸣器声音：长响，短滴，响两声等	断电不保存						
0005~0059	暂无定义							
0060		断电保存						
0061	波特率设定操作确认码							
0062	校验位设定	断电保存						
0063	校验位设定操作确认码							
0064~0069	暂无定义							
0070	驱动继电器 1	断电不保存						
0071	驱动继电器 2	断电不保存						
...								
0078	设定读卡后发出继电器开关信号功能						断电保存（定制机型才具有此功能）要和 79 寄存器一起写才能设置成功	
		15-12 位	11 位	10-8 位	7-2 位	1 位		0 位
	写寄存器	无定义	为 0 时，再次刷卡，卡号寄存器需要清零才能驱动继电器，为 1 时不需要清零	为 0：继电器闭合 0.5 秒 为 1：继电器闭合 1 秒 为 2：继电器闭合 5 秒 为 7：卡在继电器闭合卡离开时断开	无定义	为 1 驱动继电器 为 0 不驱动		为 1 驱动继电器 1 为 0 不驱动
读寄存器	无定义							

0079	设定读卡后发出开关信号功能的确认码 需定制	要和 78 寄存器一起写
0080	<p>控制读卡器指示灯，用 06H 或 10H 写一个寄存器，用 03H 可读多个寄存器。</p> <p>其中寄存器的 16 个 bit 位，最高位 bit15 到 bit8 保留不用使用，bit7~bit4 这 4 个位控制绿灯的显示，bit3~bit0 控制红灯。4 个位组合代表的 0~15 个数值，分别对应不同的 LED 灯的开关模式，</p> <p>如往 0080 寄存器写值（十六进制）：</p> <p>0000 表示 关闭指示灯；</p> <p>0001 表示 打开红灯；</p> <p>0002 表示 红灯每秒闪一次；</p> <p>0010 表示 打开绿灯；</p> <p>0020 表示 绿灯每秒闪一次；</p> <p>0011 表示 红绿灯一起亮；</p> <p>0021 表示 绿灯闪红灯亮；</p> <p>0022 表示 红绿灯交替每秒闪一次</p> <p>0012 表示 绿灯亮红灯闪；</p> <p>FFFF（出厂默认值）表示 不控制指示灯，感应到卡指示灯自动变绿色。</p>	断电不保存（定制机型才具有此功能）

八、寄存器说明：

注：西门子 PLC 中的 40001 寄存器对应于本读写器的 0000 寄存器，以此类推（下面有关于寄存器的说明都是以本读写器的说明为准）。

1、0000 至 0001 共 2 个寄存器存放 IC 卡卡号（4 个字节）：可用 03H 功能码来读或连读，

2、0002：存放读卡器的站号（机号），可读可写，写可以更改站号，用 06H/10H 功能码，可用 03H 寄存器来读或连读。

3、0003：设备参数设置：刷卡时是否发响声，通讯延时应答，读 0000、0001 寄存器后自动清零等，用 06H/10H 功能码写，可用 03H 功能码来读一个或连读多个寄存器。如用功能 06H 写 1 表示刷卡发响声，写 0 表示刷卡不发出响声。其他设定请查看软件。

4、03 寄存器 16 个 bit 的数据格式说明：

bi	bi	bi	bi	bi	bi	bi	bi	bi	bi	bi	bi	bi	bi	bi	bi
t1	t1	t1	t1	t1	t1	t9	t8	t7	t6	t5	t4	t3	t2	t1	t0

5	4	3	2	1	0										
1	0	0	0	0	0	0	0	0/1	0/1	0/1	0/1	0/1	0/1	0/1	0/1
设定参数确认码								设定读卡后清零方式				设定帧间隔延时			刷卡响声

比如设定刷卡时响一声，帧间隔延时为 10ms，读卡后清零方式为卡离开感应区清零，写值 80 75（十六进制） 128 117（十进制）↑ 10000000 ↑ 01110101（二进制）到 0003 寄存器。

具体参数设置请参考测试软件。

5、0004：驱动读卡器响声，用 06H/10H 功能码，可用 03H 功能码来读或连读多个寄存器。

如写为 0 表示短滴一声，见下表

0	短滴一声
1	短滴两声
2	短滴三声
3	长鸣一声
4	长鸣两声
5	长鸣三声
6	一长一短
7	一长两短
8	一长三短
9	两长一短
10H	两长两短
11	两长三短
其他	短滴一声

6、0005-0059：暂无定义。

九、波特率更改说明

波特率出厂时默认为 9600、19200，波特率有 4800，9600，19200，38400 四档可设，在 0060 寄存器中写入波特率值，再在 0061 寄存器中写入 21930（十六进制为 055AA）。如需将波特率改为 9600，在 0060 寄存器写入 9600，接着在一秒中内在 0061 寄存器中写入 21930。

十、通讯校验位更改说明

校验位出厂是为 N(None), 也就是无校验, 共有 None 无、Odd 奇、Even 偶、Mask 常 1、Space 常 0 五种方式可设, 在 006H2 寄存器中写入 0~4 中的一个值(分别对应 None、Odd、Even、Mask、Space), 再在 006H3 寄存器中写入 21930 (十六进制为 055AA)。也可以采用连写 006H2、0006H3 两个寄存器, 也就是用功能码 10H (十六进制)。如需将校验为改为为 None, 在 006H2 寄存器写入 0, 接着在一秒中内在 006H2 寄存器中写入 21930。

十一、继电器控制

往 0070 寄存器写值 n, 表示继电器 1 开 n*40ms 后自动关闭, n=65535 时, 继电器永久打开, 写 0 时, 表示关闭继电器。

往 0071 寄存器写值 n, 表示继电器 2 开 n*40ms 后自动关闭, n=65535 时, 继电器永久打开, 写 0 时, 表示关闭继电器。

以此类推。

十二、报文说明

在数据报文层面, 寄存器起始地址都是从 0 开始。

如 RTU 通讯模式, 读取卡号寄存器 40001 和 40002, 发送报文如下:

02 03 00 00 00 02 C4 38

02 表示读卡器的站号 (机号);

03 是读取寄存器的功能码;

00 00 表示需要读取的寄存器的起始地址;

00 02 表示需要读取寄存器的个数;

C4 38 表示 CRC16 检验 (MODBUS 格式);

读卡器返回:

02 03 04 1C 04 2D BF D3 82

02 读卡器站号;

03 功能码；

04 寄存器返回的字节长度；

1C 04 2D BF 四个字节卡号，高位在前；

D3 82 CRC16 检验；

注意：这里的报文是帧数据格式，如果使用自由通讯可以按照此帧形式编程，如果使用的是 MODBUS 协议，请查看 PLC 或其他工控机设备的手册 MODBUS 通讯部分，PLC 使用 modbus 协议已经简化了通讯步骤，功能码在 plc 上一般是指令形式，比如：03H 信捷指令是 REGR, 06H 是 REGW, 10H 是 MRGW, 检验码并不需要自己编程算法发送，PLC 系统会自动发送。

十三、功能码的介绍及作用

1. 03H 功能码读取保持寄存器

读取从站（读卡器）保持寄存器（4X 类型）的二进制数据，不支持广播。发送报文要规定需要读取保持寄存器的起始地址，寄存器的数量，保持寄存器寻址起始地址为 000H，即寄存器 1-16 所对应的地址分别为 000H-0015H。

如需从站号为 2 的读卡器上读取卡号，因存卡号寄存器为 40001-40002，所以发送数据格式如下：

站号	功能码	起始地址	地址个数	检验码 CRC16
02H	03H	0000H	0002H	C438

响应 03H 功能码

响应信息中的寄存器数据为二进制数据，每个寄存器分别对应 2 个字节，第一个字节为高位数据，第二个字节为低位数据。

如读取卡号寄存器后，响应的数据格式如下：

站号	功能码	数据字节长度	起始地址	地址个数	检验码
02H	03H	0004H	9A0AH	E458H	8D13

2. 06H 功能码写单个寄存器

把一个值写到一个保存寄存器（4X 类型）中，广播时，写值到所有从站的相同寄存器中。

发送信息要规定写值的寄存器类型，寄存器寻址起始地址为 000H，寄存器 1 所对应的地址为 0000H。

如需驱动站号为 2 的读卡器发出长鸣一声，因驱动响声蜂鸣器寄存器为 40005，所以发送数据格式如下：

站号	功能码	起始地址	写入数据	检验码 (CRC16)
02H	06H	0004H	0004H	C9FB

正常响应 06H 功能码写值驱动发声是在寄存器值改变以后将接收到的数据传送回去：

站号	功能码	起始地址	写入数据	检验码 (CRC16)
02H	06H	0004H	0004H	C9FB

3. 功能码 10H 写多个寄存器

把数据按顺序写到各（4X）类型寄存器中，广播时，可把数据写到所有从站的相同类型的寄存器中。

如需清零站号为 2 的读卡器的卡号寄存器，因卡号寄存器为 40001-40002，所以发送数据格式如下：

站号	功能码	起始地址	地址个数	数据长度	数据内容	检验码
02H	10H	0000H	0002H	04H	0000H 0000H	FCEB

正常响应 10H 功能码写值清零卡号寄存器是在寄存器值改变以后将接收到的数据传送回去：

站号	功能码	起始地址	地址个数	检验码 (CRC16)
----	-----	------	------	----------------

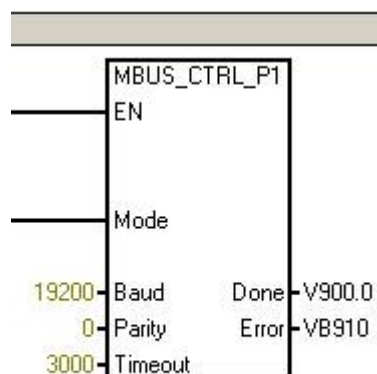
02H	10H	0000H	0002H	41FB
-----	-----	-------	-------	------

十四、RTU 通讯模式和 ASCII 通讯模式的区别

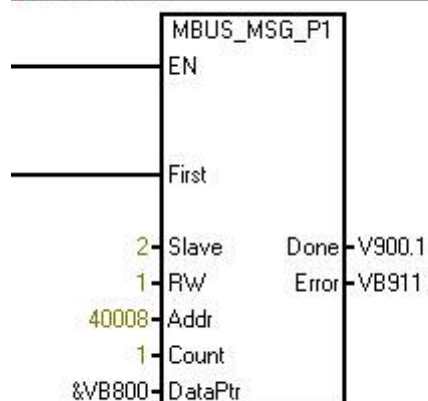
默认的串口通讯参数				
通讯模式	波特率	数据位	检验位	停止位
RTU 模式	19200	8	NONE	1
ASCII 模式	19200	7	NONE	2
通讯数据报文格式				
RTU 模式	<u>02 03 00 00 00 02 C4 38</u> 站号 功能码 寄存器地址 寄存器个数 CRC16 检验			
ASCII 模式	<u>3A 30 32 30 33 30 30 30 30 30 30 30 32 49 39 0D 0A</u> 起始字符 站号 功能码 寄存器地址 寄存器个数 LRC 检验 结束字符			
总结	RTU 直接字符串发送数据，效率高，没有起始和结束字符 CRC16 检验； ASCII 把 1 个字节字符拆成 2 个字节的 ASCII 码，数据多一倍，效率慢，有起止字符和结束字符 LRC 检验。			

附一：MODBUS 读卡器与不同厂家 PLC 的连接

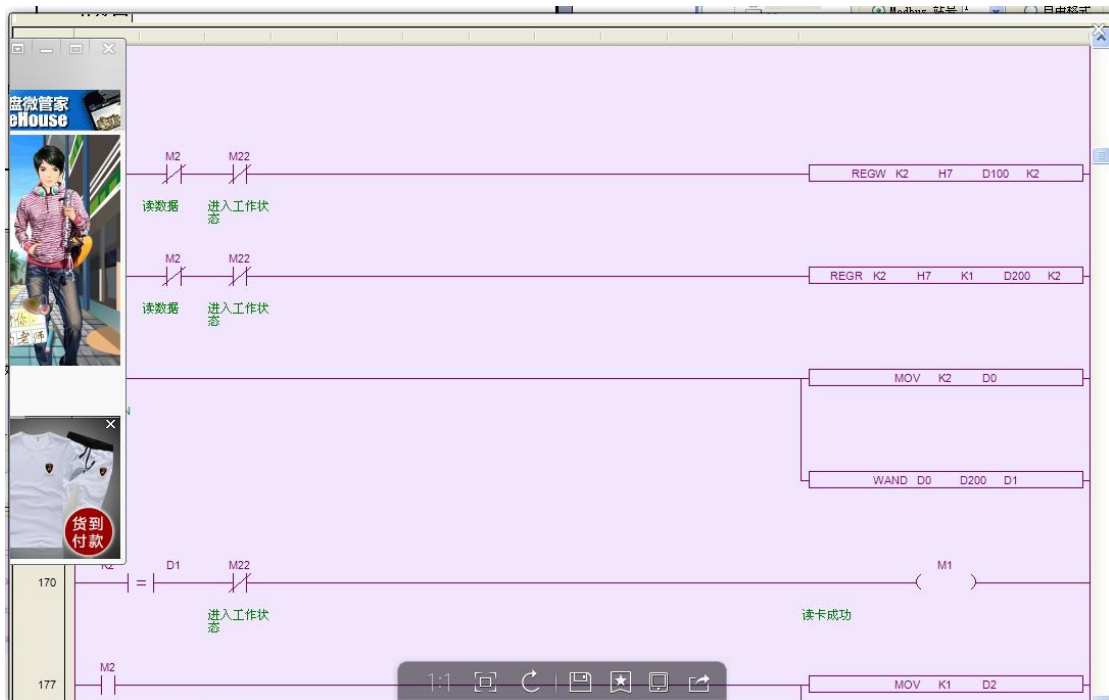
西门子 S7-200



存放读卡命令值：8



信捷的 PLC（一体机），型号 XP3-18R

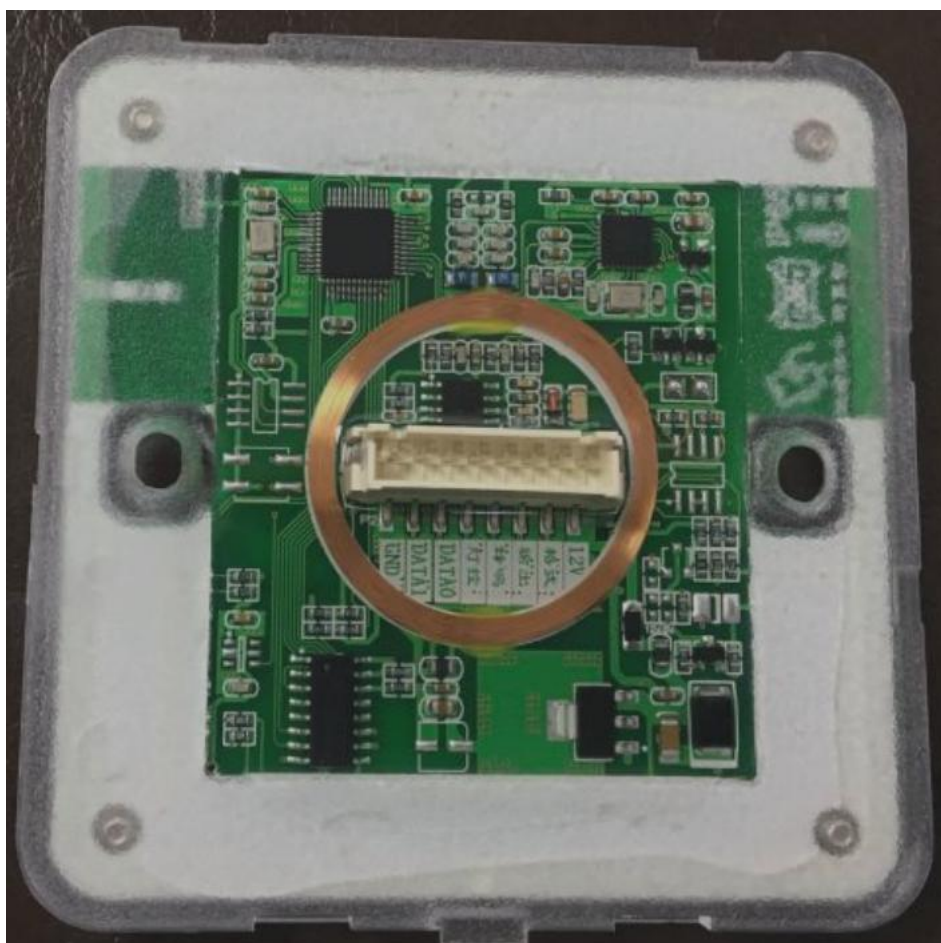


欧姆龙 CP1E N60
关键的数据格式书写

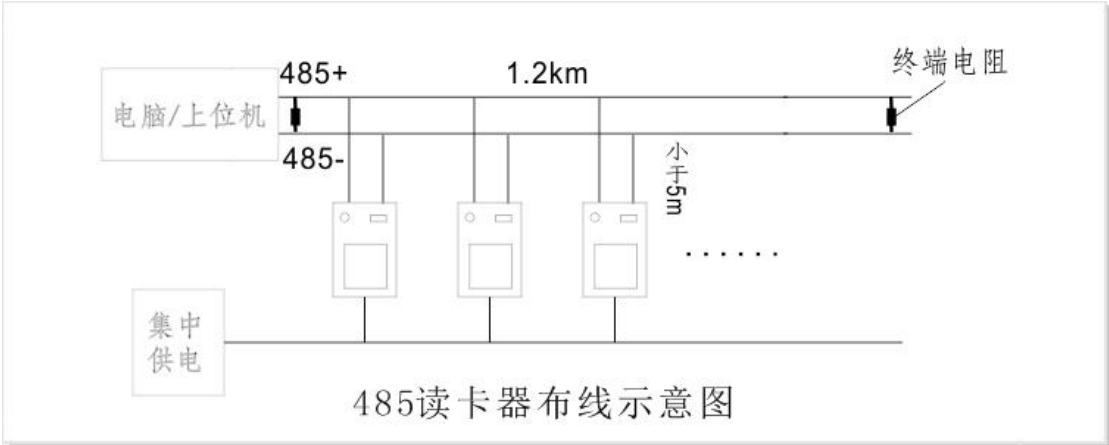
PLC名称	名称	地址	数据类型/格式	功能...	值	值二...	注释
新PLC1		D1300	CHANNEL (十六进制, 通道)		0001 十六进制	0000 ...	
新PLC1		D1301	CHANNEL (十六进制, 通道)		0003 十六进制	0000 ...	
新PLC1		D1302	CHANNEL (十六进制, 通道)		0004 十六进制	0000 ...	
新PLC1		D1303	CHANNEL (十六进制, 通道)		0000 十六进制	0000 ...	
新PLC1		D1304	CHANNEL (十六进制, 通道)		0002 十六进制	0000 ...	
新PLC1		D1305	CHANNEL (十六进制, 通道)		0000 十六进制	0000 ...	
新PLC1		D1306	CHANNEL (十六进制, 通道)		0000 十六进制	0000 ...	
新PLC1		D1307	CHANNEL (十六进制, 通道)		0000 十六进制	0000 ...	
新PLC1		A641.00	BOOL (On/Off, 接点)		0		
新PLC1		A641.01	BOOL (On/Off, 接点)		0		
新PLC1		A641.02	BOOL (On/Off, 接点)		1		
新PLC1		D1350	CHANNEL (十六进制, 通道)		0000 十六进制	0000 ...	
新PLC1		D1351	CHANNEL (十六进制, 通道)		0000 十六进制	0000 ...	
新PLC1		D1352	CHANNEL (十六进制, 通道)		0082 十六进制	0000 ...	
新PLC1		D1353	CHANNEL (十六进制, 通道)		0000 十六进制	0000 ...	
新PLC1		D1354	CHANNEL (十六进制, 通道)		0000 十六进制	0000 ...	
新PLC1		D1355	CHANNEL (十六进制, 通道)		0000 十六进制	0000 ...	
新PLC1		D1356	CHANNEL (十六进制, 通道)		0000 十六进制	0000 ...	

附二：MODBUS 读卡器尺寸与接线示意图

(外壳尺寸，(长×宽×高) 86MM×86MM× 1cm)



接线网络拓补图



接线示意图

文档更新日期：210930