

# 工业测距仪 Modbus RTU 通讯协议

## V1.2

文件修订历史

版本	日期	作者	变更描述
V1.0	2020-03-03	王现运	制定满足基本测量功能的协议版本，基于标准 modbus 通信设计
V1.1	2020-12-03	王现运	增加开关量、模拟量输出、CAN 通讯参数
V1.2	2021-04-12	王现运	增加读取量程和读取多个测量结果数据的命令

## 目录

1、通讯协议介绍 .....	4
1.1 通信物理参数: .....	4
1.2 协议格式 .....	4
1.3 CRC 校验 C 语言实现 .....	5
2、寄存器说明 .....	6
2.1 基础功能寄存器 .....	6
2.2 扩展功能寄存器 .....	6
2.3 错误代码和解决方案 .....	7
3、寄存器使用细节和示例 .....	9
3.1 读取错误状态 .....	9
3.2 读取测量状态 .....	9
3.3 设置测量状态 .....	9
3.4 读取测量距离值 .....	9
3.5 读取设备地址 .....	9
3.6 读取串口通讯参数 .....	10
3.7 设置通讯参数 .....	10
3.8 读取整体偏移量 .....	10
3.9 设置整体偏移量 .....	11
3.10 读取软件版本号 .....	11
3.11 读取测量频率 .....	11
3.12 设置测量频率 .....	11
3.13 读取设备温度 .....	11
3.14 读取设备序列号 .....	12
3.15 读取 DAC 输出模式 .....	12
3.16 设置 DAC 输出模式 .....	12
3.17 读取 DAC 输出最小量程 .....	12
3.18 设置 DAC 输出最小量程 .....	12
3.19 读取 DAC 输出最大量程 .....	12

3.20 设置 DAC 输出最大量程.....	13
3.21 读取开关量输出 1 高电平距离值.....	13
3.22 设置开关量输出 1 高电平距离值.....	13
3.23 读取开关量输出 1 低电平距离值.....	13
3.24 设置开关量输出 1 低电平距离值.....	13
3.25 读取开关量输出 2 高电平距离值.....	14
3.26 设置开关量输出 2 高电平距离值.....	14
3.27 读取开关量输出 2 低电平距离值.....	14
3.28 设置开关量输出 2 低电平距离值.....	14
3.29 读取 CAN 通讯帧模式.....	15
3.30 设置 CAN 通讯帧模式.....	15
3.31 读取 CAN 通讯波特率.....	15
3.32 设置 CAN 通讯波特率.....	15
3.33 读取 CAN 通讯发送 ID.....	16
3.34 设置 CAN 通讯发送 ID.....	16
3.35 读取 CAN 通讯接收 ID.....	16
3.36 设置 CAN 通讯接收 ID.....	16
3.37 保存参数数据.....	17
3.38 读取多个测量结果数据.....	17
附录 A: 使用 modScan32 测试 modbus.....	18
A.1 串口设置.....	18
A.1 寄存器参数设置.....	18

# 1、通讯协议介绍

## 1.1 通信物理参数:

- 波特率：（默认）115200，可使用的常见波特率有：2400，4800，9600，14400，19200，38400，57600，76800，115200；其它波特率可通过设置波特率设置后自行标记记录。
- 奇偶校验：无校验
- 停止位：1 位
- 数据位：8 位

## 1.2 协议格式

采用 MODBUS,RTU 方式，CRC16 位校验。

注：数字后面加 H 表示十六进制数据格式，比如 03H，表示十六进制的 03。

(1)功能码 03H--查询从设备寄存器内容（读操作）

表 1 主设备报文格式

从设备地址	功能码	起始寄存器地址	寄存器个数 (以 2 个字节计算)	CRC 校验
1 字节	(03H) 1 字节	2 字节	n	2 字节

表 2 从设备报文格式

从设备地址	功能码	数据区字节数	数据区	CRC 校验
1 字节	(03H) 1 字节	1 字节	n*2 字节	2 字节

(2)功能码 06H--设置从设备单个寄存器内容（写操作）

表 3 主设备报文格式

从设备地址	功能码	寄存器地址	写入的数据 (以字节为单位)	CRC 校验
1 字节	(06H) 1 字节	2 字节	2 字节	2 字节

表 4 从设备报文格式

从设备地址	功能码	寄存器地址	写入的数据	CRC 校验
1 字节	(06H) 1 字节	2 字节	2 字节	2 字节

说明:

- 整包数据必须连续发送，两个数据包必须间隔 3.5 个字符的静止时间再发送，否则都会解析出错。
- 如果使用 PLC 设备做主设备，则发送的读取寄存器个数以 2 字节为一个寄存器，所以发送的寄存器个数是字节长度的一半。

- 有效的从设备地址范围为 0-247（十进制），其中设备地址 0 为广播地址，所有从机都可收到，1-247 为从机的寻址范围。
- 功能码的有效范围 1-255（十进制），本协议使用的功能码有 03(读),06(写)。
- 地址和数据中包含的 16 位或者 32 位数据，则发送时高字节在前，低字节在后。
- CRC 校验数据是两个字节，低 8 位在前，高 8 位在后。该校验数据由设备地址、功能码和数据通过 1.2.1 的 CRC 计算公式计算得出。接收设备重新计算收到消息的 CRC，并与接收到的 CRC 域中的值比较，如果两值不同，则有误。

### 1.3 CRC 校验 C 语言实现

//计算 CRC 校验值

```
unsigned short CRC16 ( unsigned char *arrbuff ,int len)
{
    unsigned short  crc = 0xFFFF;
    int i, j;
    for ( j=0; j<len;j++)
    {
        crc=(unsigned short)(crc ^arrbuff[j]);
        for ( i=0; i<8; i++)
        {
            if ((crc & 1) > 0)
            {
                crc = (unsigned short)(crc >> 1);
                crc = (unsigned short)(crc ^ 0xa001);
            }
            else
            {
                crc = (unsigned short)(crc >> 1);
            }
        }
    }
    return (crc);
}
```

## 2、寄存器说明

### 2.1 基础功能寄存器

表 5 基础功能寄存器定义表

寄存器地址	寄存器内容	寄存器字节长度	寄存器状态	说明
0000H	错误状态码	2	只读	=0 无故障 >0 有故障，具体错误代码请看表 6
0001H	运行状态	2	读写	0 空闲，停止测量 1 激光指示 2 正在测量
0002H	测量距离值	4	只读	4 字节无符号整型数据，高位在前，低位在后，单位 0.1mm，0 为无效数据
0003H	设备地址	2	读写	有效范围 1-247
0004H	串口通讯参数	4	读写	高 8 位为校验参数： 00 无校验 01 奇校验 02 偶校验 低 24 位为波特率： 有效范围 2400-115200
0005H	距离偏移量	2	读写	有符号整数，单位 0.1mm
0006H	软件版本号	2	只读	当前软件版本号
0007H	测量频率设置	2	读写	=0 单次 =1 5Hz =2 10Hz =3 20Hz =4 30Hz
0008H	设备温度	2	只读	单位 0.1℃
0009H	序列号	4	只读	唯一序列号

### 2.2 扩展功能寄存器

表 6 扩展功能寄存器定义表

寄存器地址	寄存器内容	寄存器字节长度	寄存器状态	说明
000AH	DAC 输出模式	2	读写	模拟量输出功能 =0 关闭 =1 0-5V =2 0-10V =3 4-20mA

				=4 0-20mA =5 0-24mA
000BH	DAC 输出最小量程	4	读写	有效数据范围 0-900000
000CH	DAC 输出最大量程	4	读写	有效数据范围 0-900000
000DH	开关量输出 1 高电平距离值	4	读写	有效数据范围 0-900000
000EH	开关量输出 1 低电平距离值	4	读写	有效数据范围 0-900000
000FH	开关量输出 2 高电平距离值	4	读写	有效数据范围 0-900000
0010H	开关量输出 2 低电平距离值	4	读写	有效数据范围 0-900000
0011H	开关量入功能	2	读写	=0 关闭 =1 悬空或高电平启动测量，低电平停止测量 =2 悬空或高电平停止测量，低电平启动测量
0014H	CAN 通讯帧模式	2	读写	=0 标准帧 =1 扩展帧
0015H	CAN 通讯波特率	2	读写	单位 KHz，有效数据为： 20,50,80,100,125,250,500,600,800,1000
00016H	CAN 通讯发送 ID	4	读写	标准帧模式，ID 有效范围为 0-7FF,H 扩展帧模式 ID 有效范围为 0-1FFFFFFFH
0017H	CAN 通讯接收 ID	4	读写	标准帧模式，ID 有效范围为 0-7FF,H 扩展帧模式 ID 有效范围为 0-1FFFFFFFH
0018H	保存参数	2	写	把设定的参数存入存储器，掉电保存
0019H	获取多个测量结果参数	12	读	获取测量的距离、信号强度和内部温度值。三个参数都是 4 个字节长度表示的整数。
0028H	读取最大量程	4	读	获取设备最远测量距离
0029H	读取最小量程	4	读	获取设备最近测量距离

## 2.3 错误代码和解决方案

表 6 错误代码定义表

错误代码	含义
220	内部通信故障

252	温度过高(60℃)
253	温度过低(-10℃)
254	目标测距值超出量程范围
255	目标反射信号弱或者超量程
256	目标反射信号过强
257	环境光过强

### 3、寄存器使用细节和示例

设备为测距传感器，主机为控制接收端。以下以设备地址=19H(十进制为 25)作为示例，设备发送即主机接收的数据。

#### 3.1 读取错误状态

方向	数据	含义
主机->设备	19 03 00 00 00 01 87 D2	读取错误状态
设备->主机	19 03 02 00 00 98 46	无错误
	19 03 02 00 FF D8 06	错误代码 255

#### 3.2 读取测量状态

方向	数据	含义
主机->设备	19 03 00 01 00 01 D6 12	读取测量状态
设备->主机	19 03 02 00 00 98 46	激光关闭，停止测量
	19 03 02 00 01 59 86	激光开启，指示模式
	19 03 02 00 02 19 87	正在测量

#### 3.3 设置测量状态

方向	数据	含义
主机->设备	19 06 00 01 00 02 5A 13	启动测量
	19 06 00 01 00 01 1A 12	打开激光
	19 06 00 01 00 00 DB D2	停止测量
设备->主机	19 06 00 01 00 02 5A 13	已启动测量
	19 06 00 01 00 01 1A 12	已打开激光
	19 06 00 01 00 00 DB D2	已停止测量

#### 3.4 读取测量距离值

方向	数据	含义
主机->设备	19 03 00 02 00 02 66 13	读取测量距离
设备->主机	19 03 04 00 00 3D 9B 33 09	单位 0.1mmm. 测量结果 00003D9BH，换算成 10 进制结果为 1.5771m
	19 03 04 00 00 00 00 62 32	测量结果为 0，距离无效

#### 3.5 读取设备地址

方向	数据	含义
主机->设备	19 03 00 03 00 01 77 D2	读取设备地址
	或 00 03 00 03 00 01 75 DB	如果不知道设备地址可以使用广播地址 0
设备->主机	19 03 02 00 19 59 8C	地址为 0019H

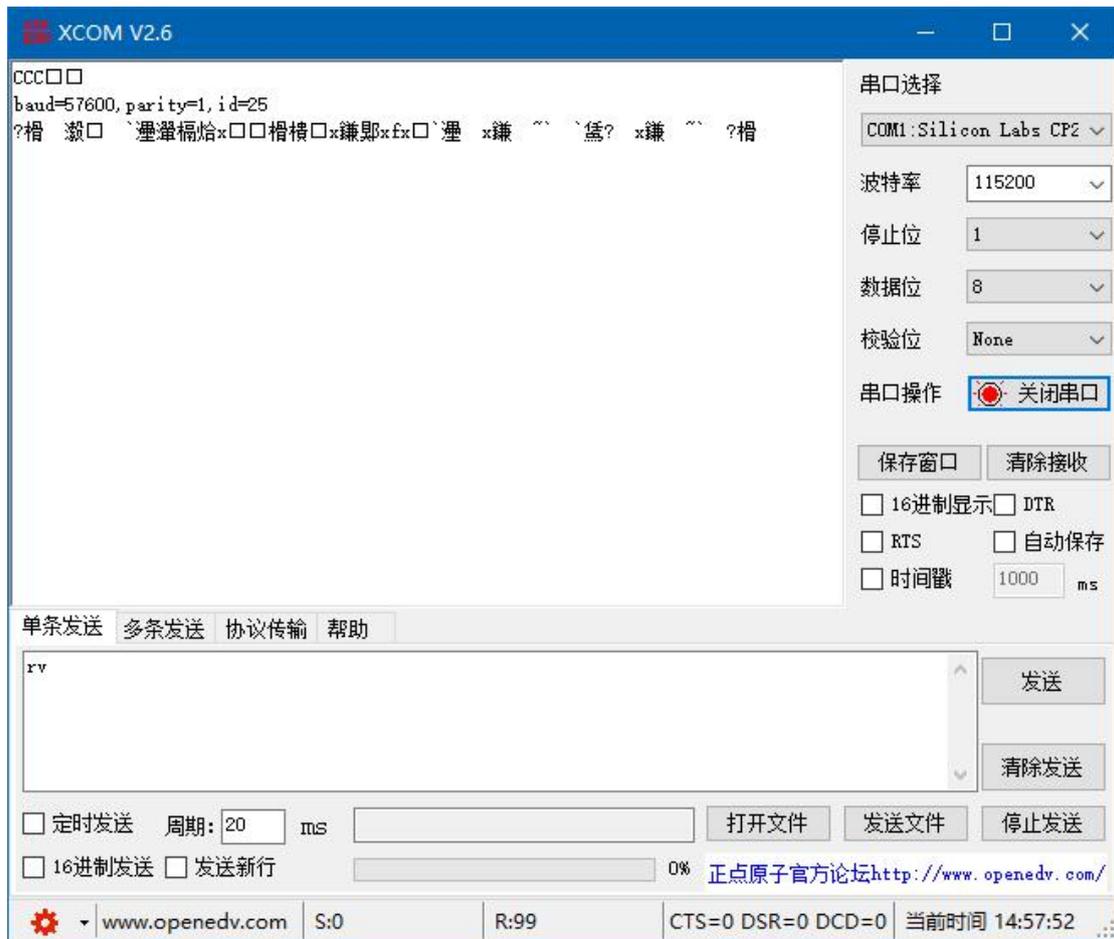
### 3.6 读取串口通讯参数

方向	数据	含义
主机->设备	19 03 00 04 00 01 C6 13	读取串口通讯参数
设备->主机	19 03 04 00 01 C2 00 62 92	00H:无校验 01C200H: 波特率 115200

### 3.7 设置通讯参数

方向	数据	含义
主机->设备	19 06 00 04 01 00 E1 00 5F 01	01H:奇校验 00E100H:波特率 57600
设备->主机	19 06 00 04 01 00 E1 00 5F 01	01H:奇校验 00E100H:波特率 57600

使用说明：使用修改波特率时，必须知道当前波特率，否则指令不会被设备正确识别。如果不知道具体波特率，可把串口接收调试工具调为默认参数 115200，无校验，首次上电会通过串口输出当前设置的串口通讯参数和设备 ID，如下图所示：



### 3.8 读取整体偏移量

方向	数据	含义
主机->设备	19 03 00 05 00 01 97 D3	读取设备整体偏移量

设备->主机	19 03 02 FF 03 99 B7	偏移量单位为 0.1mm 返回的数据 FF03H, 十进制为-253,
--------	----------------------	--

### 3.9 设置整体偏移量

方向	数据	含义
主机->设备	19 06 00 05 FE FC DA 32	整体偏移量单位 0.1mm 设置整体偏移量为 FFFC, 十进制为-260, 有效的范围为 [- 20000~ 20000]
设备->主机	19 06 00 05 FE FC DA 32	整体偏移量单位 0.1mm 设置整体偏移量为 FFFC, 十进制为-260

备注:偏移量为有符号整数, 负数表示实测值比真实值大, 需要减去的数值。比如 -260 的意思就是输出值=实测值-260.

### 3.10 读取软件版本号

方向	数据	含义
主机->设备	19 03 00 06 00 01 67 D3	读取软件版本号
设备->主机	19 03 02 00 66 18 6C	版本号为 0066H, 十进制表示是 102

### 3.11 读取测量频率

方向	数据	含义
主机->设备	19 03 00 07 00 01 36 13	读取测量频率
设备->主机	19 03 02 00 00 98 46	单次
	19 03 02 00 01 59 86	5Hz
	19 03 02 00 02 19 87	10Hz
	19 03 02 00 03 D8 47	20Hz
	19 03 02 00 04 99 85	30Hz

### 3.12 设置测量频率

方向	数据	含义
主机->设备	19 06 00 07 00 02 BA 12	设置频率参数为 0002H, 表示 10Hz
设备->主机	19 06 00 07 00 02 BA 12	频率参数为 0002H, 表示 10Hz

### 3.13 读取设备温度

方向	数据	含义
主机->设备	19 03 00 08 00 01 06 10	读取设备温度
设备->主机	19 03 02 00 CA 18 11	该温度值采用有符号 16 位整数表示, 单位为 0.1℃, 数值为 00CAH, 表示 20.2℃

### 3.14 读取设备序列号

方向	数据	含义
主机->设备	19 03 00 09 00 02 17 D1	读取序列号，2 个寄存器长度
设备->主机	19 03 04 00 00 04 51 A1 0E	序列号为 00000451H,十进制为 1105

### 3.15 读取 DAC 输出模式

方向	数据	含义
主机->设备	19 03 00 0A 00 01 A7 D0	读取 DAC 输出模式
设备->主机	19 03 02 00 03 D8 47	模式参数为 0003H，4-20mA 输出，该参数为出厂默认值

模拟量输出模式参数含义如下，只能选择下面的参数，其它参数无效

- =0 关闭
- =1 0-5V
- =2 0-10V
- =3 4-20mA
- =4 0-20mA
- =5 0-24mA

### 3.16 设置 DAC 输出模式

方向	数据	含义
主机->设备	19 06 00 0A 00 03 EA 11	设置 DAC 输出模式为 0003H,即 4-20mA 输出
设备->主机	19 06 00 0A 00 03 EA 11	频率参数为 0002H，表示 10Hz

### 3.17 读取 DAC 输出最小量程

方向	数据	含义
主机->设备	19 03 00 0B 00 02 B6 11	读取 DAC 输出模拟量最小值
设备->主机	19 03 04 00 00 01 F4 62 25	模式参数为 DAC 输出模拟量最小值为 000001F4H,即 500

注释：最小量程范围为 0-900000。

### 3.18 设置 DAC 输出最小量程

方向	数据	含义
主机->设备	19 06 00 0B 00 00 01 F4 42 BB	设置 DAC 输出模拟量最小值为 000001F4H, 即 500
设备->主机	19 06 00 0B 00 00 01 F4 42 BB	

### 3.19 读取 DAC 输出最大量程

方向	数据	含义

主机->设备	19 03 00 0C 00 02 07 D0	读取 DAC 输出模拟量最大值
设备->主机	19 03 04 00 09 EB 10 FD 0C	模式参数为 DAC 输出模拟量最小值为 0009EB10H，即 650000

注释：最大量程范围为 500-900000。

### 3.20 设置 DAC 输出最大量程

方向	数据	含义
主机->设备	19 06 00 0C 00 09 EB 10 68 52	设置 DAC 输出模拟量最大值为 0009EB10H，即 650000
设备->主机	19 06 00 0C 00 09 EB 10 68 52	

说明：本设备的 DAC 输出为 16 位精度，DAC 输出的分辨率为：

$$(D_{max}-D_{min})/65535DAC。$$

输出数据以最小量程为下限，以最大量程为上限，量程范围内为线性关系。

比如，4-20mA 输出模式，假如测量距离为 d，则 DAC 输出数据为：

$$I_{out} = \frac{d - D_{min}}{D_{max} - D_{min}} * 16 + 4$$

### 3.21 读取开关量输出 1 高电平距离值

方向	数据	含义
主机->设备	19 03 00 0D 00 02 56 10	读取开关量输出 1 高电平距离值
设备->主机	19 03 04 00 00 03 E8 62 8C	参数为 000003E8H，即 1000

### 3.22 设置开关量输出 1 高电平距离值

方向	数据	含义
主机->设备	19 06 00 0D 00 00 03 E8 CA 12	设置开关量输出 1 高电平距离值 000003E8H，即 1000
设备->主机	19 06 00 0D 00 00 03 E8 CA 12	

### 3.23 读取开关量输出 1 低电平距离值

方向	数据	含义
主机->设备	19 03 00 0E 00 02 A6 10	读取开关量输出 1 低电平距离值
设备->主机	19 03 04 00 00 01 F4 62 25	参数为 000007D0H，即 2000

### 3.24 设置开关量输出 1 低电平距离值

方向	数据	含义
主机->设备	19 06 00 0E 00 00 07 D0 8D 00	设置开关量输出 1 低电平距离值 000007D0H, 即 2000
设备->主机	19 06 00 0E 00 00 07 D0 8D 00	

### 3.25 读取开关量输出 2 高电平距离值

方向	数据	含义
主机->设备	19 03 00 0F 00 02 F7 D0	读取开关量输出 2 高电平距离值
设备->主机	19 03 04 00 00 07 D0 61 9E	参数为 000007D0H, 即 2000

### 3.26 设置开关量输出 2 高电平距离值

方向	数据	含义
主机->设备	19 06 00 0F 00 00 07 D0 B0 C0	设置开关量输出 2 高电平距离值 000003E8H, 即 1000
设备->主机	19 06 00 0F 00 00 07 D0 B0 C0	

### 3.27 读取开关量输出 2 低电平距离值

方向	数据	含义
主机->设备	19 03 00 10 00 02 C6 16	读取开关量输出 2 低电平距离值
设备->主机	19 03 04 00 00 03 E8 62 8C	参数为 000003E8H, 即 1000

注释：最小量程范围为 0-900000。

### 3.28 设置开关量输出 2 低电平距离值

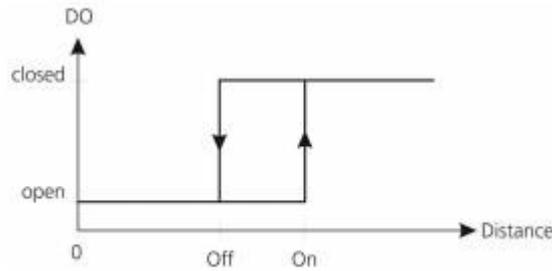
方向	数据	含义
主机->设备	19 06 00 10 00 00 03 E8 26 10	设置开关量输出 2 低电平距离值 000003E8H, 即 1000
设备->主机	19 06 00 10 00 00 03 E8 26 10	

开关量参数说明：

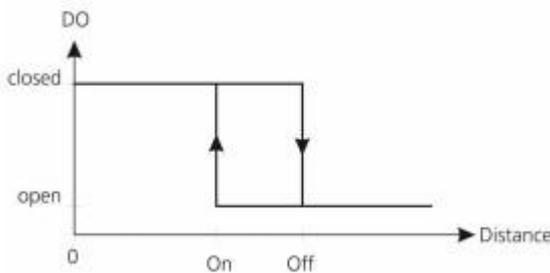
可以为设备 2 路开关量输出单独设置参数，配置参数有两种情况，即(1:ON > OFF, 2: ON < OFF)。设备根据设定的开关数值参数，自动判断属于哪种模式。

1) 迟滞参数：ON 电平 > OFF 电平

随着距离的增加，当距离超过 ON 时打开数字输出高电平。随着距离的减小，当距离下降时，开关关闭输出低电平。



2) 迟滞参数: ON 电平 < OFF 电平



随着距离的增加，当距离超过 OFF 时打开数字输出低电平。随着距离的减小，当距离下降时，输出高电平。

### 3.29 读取 CAN 通讯帧模式

方向	数据	含义
主机->设备	19 03 00 14 00 01 C7 D6	读取 CAN 通讯帧模式
设备->主机	19 03 02 00 00 98 46	参数 0000H 普通帧
	19 03 02 00 01 59 86	参数 0001H 普通帧

### 3.30 设置 CAN 通讯帧模式

方向	数据	含义
主机->设备	19 06 00 14 00 01 0B D6	设置 CAN 通讯帧模式为扩展帧
设备->主机	19 06 00 14 00 01 0B D6	参数 0001H 普通帧

### 3.31 读取 CAN 通讯波特率

方向	数据	含义
主机->设备	19 03 00 15 00 01 96 16	读取 CAN 通讯帧波特率
设备->主机	19 03 02 00 7D 58 67	参数 007DH, 单位为 K, 十进制含义为 125K

### 3.32 设置 CAN 通讯波特率

方向	数据	含义
主机->设备	19 06 00 15 00 FA 1B 95	设置 CAN 通讯帧波特率为 00FAH,单位 K, 即 250K
设备->主机	19 06 00 15 00 FA 1B 95	

CAN 通讯波特率仅限于以下几种：20,50,80,100,125,250,500,600,800,1000，单位 K。

### 3.33 读取 CAN 通讯发送 ID

方向	数据	含义
主机->设备	19 03 00 16 00 02 26 17	读取 CAN 通讯接收 ID
设备->主机	19 03 04 00 00 02 86 E2 F0	参数 00000286H，十进制为 646

发送 ID 的有效范围和帧模式有关。

普通帧，取值范围为：0-7FF

扩展帧，取值范围为：0-1FFF FFFF

### 3.34 设置 CAN 通讯发送 ID

方向	数据	含义
主机->设备	19 06 00 16 00 00 02 86 2E 6C	设置 通讯 发送 ID 为 00000286H，十进制为 646
设备->主机	19 06 00 16 00 00 02 86 2E 6C	

发送 ID 的有效范围和帧模式有关。

普通帧，取值范围为：0-7FF

扩展帧，取值范围为：0-1FFF FFFF

### 3.35 读取 CAN 通讯接收 ID

方向	数据	含义
主机->设备	19 03 00 17 00 02 77 D7	读取 CAN 通讯接收 ID
设备->主机	19 03 04 00 00 03 06 E2 C0	参数 00000306H，十进制为 774

发送 ID 的有效范围和帧模式有关。

普通帧，取值范围为：0-7FF

扩展帧，取值范围为：0-1FFF FFFF

### 3.36 设置 CAN 通讯接收 ID

方向	数据	含义
主机->设备	19 06 00 17 00 00 03 06 13 9C	设置 通讯 发送 ID 为 00000306H，十进制为 774
设备->主机	19 06 00 17 00 00 03 06 13 9C	

发送 ID 的有效范围和帧模式有关。

普通帧，取值范围为：0-7FF

扩展帧，取值范围为：0-1FFF FFFF

注：CAN 通讯协议详见《工业测距传感器 CAN 通讯协议》

### 3.37 保存参数数据

方向	数据	含义
主机->设备	19 06 00 18 00 01 CB D5	保存参数到内部存储器，掉电保存
设备->主机	19 06 00 18 00 01 CB D5	保存成功

只有使用该命令后，设置的参数才会掉电保存，否则重新上电需要重新配置。

### 3.38 读取多个测量结果数据

方向	数据	含义
主机->设备	19 03 00 19 00 06 17 D7	读取距离，信号强度和温度
设备->主机	19 03 0C 00 00 3C FA 00 00 AB 1A 00 00 01 04 71 54	00 00 3C FA 为距离值 15610 00 00 AB 1A 为强度值 43802 00 00 01 04 为温度值 260

该命令用于同时获取多个测量参数，距离值单位 0.1mm，强度值单位 uV,温度值单位 0.1℃

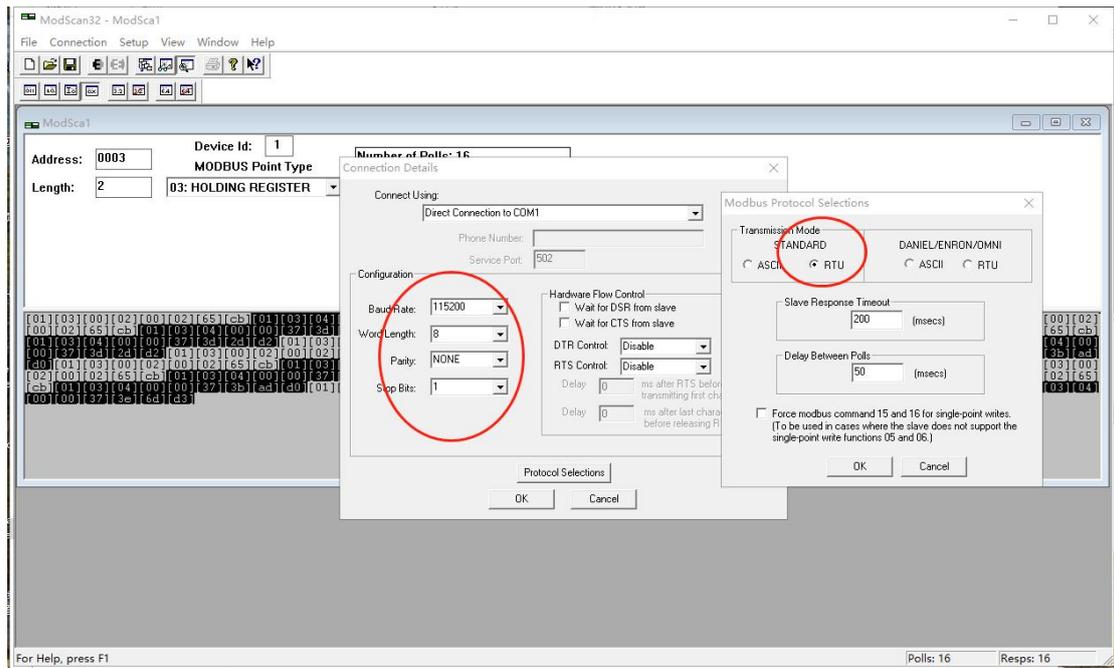
# 附录 A: 使用 modScan32 测试 modbus

## A.1 串口设置

电脑端串口 1 和传感器相连。

通信参数：115200，8 位数据长度，1 停止位，无校验

通信模式：RTU



## A.1 寄存器参数设置

Device id: 设备的从地址

Address: 寄存器地址，modscan 会自动把寄存器地址减 1 后再发送，所以读取距离参数寄存器 2 时，需要填写 Address 为 3。

Length: 寄存器长度，数据为传感器发回数据自己长度/2.

选用 03, HOLDING REGISTER。读取距离数据

菜单：setup->display Options->show traffic 显示如下数据

