Passenger Flow MODBUS Communication Protocol

1 Communication interface

1.1 Interface standards

Interface standard: RS-485 (EIA/TIA-485)
Hardware connection: 2-wire mode

1.2 Communication parameters

Baud rate: 9600
Data bits: 8
Stop bit: 1
Check digit: n
To enable Modbus function, you need to set the protocol to Modbus-STD on the device side.

2 Communication formats

2.1 Host Transmit Format

地址	功能码	寄存器地址		数据		CRC 低位	CRC 高位
Address	Function	AddrH	AddrL	NumH	NumL	CRCL	CRCH

a, address: address of the corresponding child node, range (1- 247), default address is 01, 0 is broadcast address;
b, Function code: 0x03 to read one or more registers, 0x06 to write a register;
c, register address: AddrH indicates the high byte address of the register to be read, AddrL indicates the low address of the register to be read; see: (2.3 Holding Register Address Resolution) for register address resolution.
d. Data: the number of data to be read by the host, ranging from 1-8;

e, the last two bytes for the CRC checksum check code of the high and low bytes

For example: to read the measurement data to the device whose slave address is 06, the format of the sent data is as follows:

Host sends: 06 03 00 06 00 02 25 BD

2.2 Slave response format

地址	功能码	字节数	数据	**CRC** 低位	**CRC** 高位
Address	Function	byte	D0H,D0L…DNH,DNL	CRCL	CRCH

After the slave receives the data from the host, it unpacks the data and responds to the host only if the address matches.

a. Address code: slave's address (1- 254);

b. Function code: 0x03 read one or more registers, 0x06 write one register;

c, Number of bytes: the number of data sent, i.e., the number of bytes of data D0L-DNH;

d, Data: data sent to the host, the number is equal to the number of bytes;

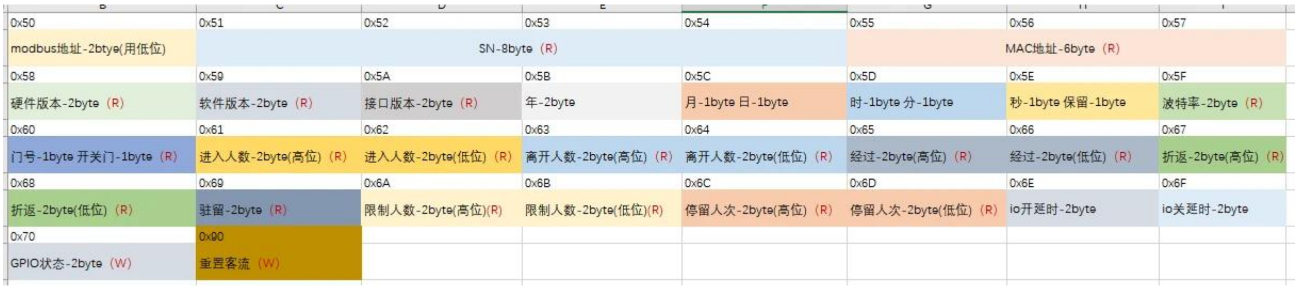
e. The last two bytes are the high and low bytes of the CRC checksum;

For example, the slave responds to the data sent from the host as follows:

Slave response: 06 03 02 00 00 0D 84

Which the fourth fifth data for the data 00 00 said that the slave now measured data for 0, if the measured data for 9968, the data transmitted for 26 F0, that is, the decimal 9968.

2.3 Register Address Data Correspondence Table

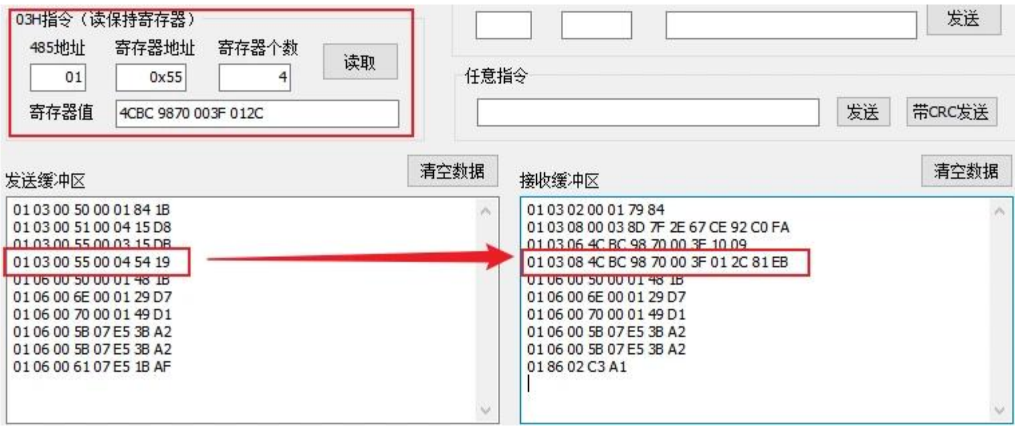


B	C	D	E	F	G	H	I
0x50	0x51	0x52	0x53	0x54	0x55	0x56	0x57
modbus地址-2btye(用低位)	SN-8byte（R）				MAC地址-6byte（R）		
0x58	0x59	0x5A	0x5B	0x5C	0x5D	0x5E	0x5F
硬件版本-2byte（R）	软件版本-2byte（R）	接口版本-2byte（R）	年-2byte	月-1byte 日-1byte	时-1byte 分-1byte	秒-1byte 保留-1byte	波特率-2byte（R）
0x60	0x61	0x62	0x63	0x64	0x65	0x66	0x67
门号-1byte 开关门-1byte（R）	进入人数-2byte(高位)（R）	进入人数-2byte(低位)（R）	离开人数-2byte(高位)（R）	离开人数-2byte(低位)（R）	经过-2byte(高位)（R）	经过-2byte(低位)（R）	折返-2byte(高位)（R）
0x68	0x69	0x6A	0x6B	0x6C	0x6D	0x6E	0x6F
折返-2byte(低位)（R）	驻留-2byte（R）	限制人数-2byte(高位)(R)	限制人数-2byte(低位)(R)	停留人次-2byte(高位)（R）	停留人次-2byte(低位)（R）	io开延时-2byte	io关延时-2byte
0x70	0x90						
GPIO状态-2byte（W）	重置客流（W）						

As shown in the figure, the upper register address corresponds to the data content stored in the lower register;

For example: 0x50 register storage content is modbus address

Example 1:



485地址 01　寄存器地址 0x55　寄存器个数 4

寄存器值 4CBC 9870 003F 012C

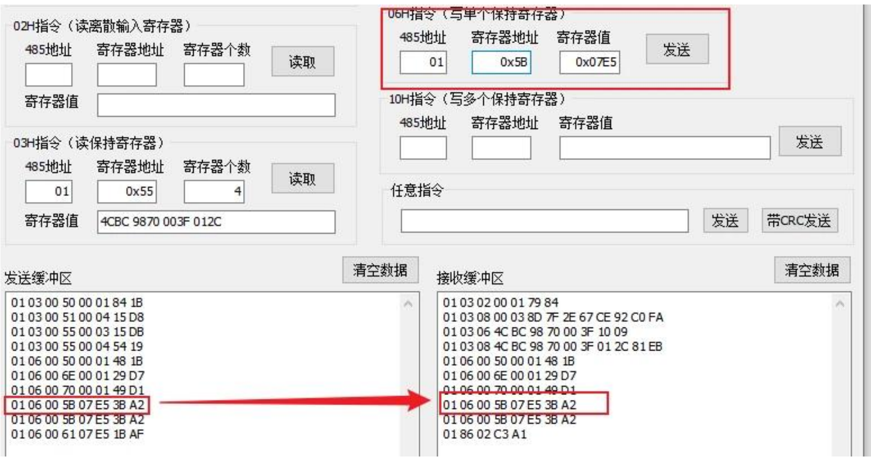
发送缓冲区

```
01 03 00 50 00 01 84 1B
01 03 00 51 00 04 15 D8
01 03 00 55 00 03 15 DB
01 03 00 55 00 04 54 19
01 06 00 50 00 01 48 1B
01 06 00 6E 00 01 29 D7
01 06 00 70 00 01 49 D1
01 06 00 5B 07 E5 3B A2
01 06 00 5B 07 E5 3B A2
01 06 00 61 07 E5 1B AF
```

接收缓冲区

```
01 03 02 00 01 79 84
01 03 08 00 03 8D 7F 2E 67 CE 92 C0 FA
01 03 06 4C BC 98 70 00 3F 10 09
01 03 08 4C BC 98 70 00 3F 01 2C 81 EB
01 06 00 50 00 01 48 1B
01 06 00 6E 00 01 29 D7
01 06 00 70 00 01 49 D1
01 06 00 5B 07 E5 3B A2
01 06 00 5B 07 E5 3B A2
01 86 02 C3 A1
```

Example 2:



03H指令（读保持寄存器）：485地址 01　寄存器地址 0x55　寄存器个数 4

寄存器值 4CBC 9870 003F 012C

06H指令（写单个保持寄存器）：485地址 01　寄存器地址 0x5B　寄存器值 0x07E5

发送缓冲区

```
01 03 00 50 00 01 84 1B
01 03 00 51 00 04 15 D8
01 03 00 55 00 03 15 DB
01 03 00 55 00 04 54 19
01 06 00 50 00 01 48 1B
01 06 00 6E 00 01 29 D7
01 06 00 70 00 01 49 D1
01 06 00 5B 07 E5 3B A2
01 06 00 5B 07 E5 3B A2
01 06 00 61 07 E5 1B AF
```

接收缓冲区

```
01 03 02 00 01 79 84
01 03 08 00 03 8D 7F 2E 67 CE 92 C0 FA
01 03 06 4C BC 98 70 00 3F 10 09
01 03 08 4C BC 98 70 00 3F 01 2C 81 EB
01 06 00 50 00 01 48 1B
01 06 00 6E 00 01 29 D7
01 06 00 70 00 01 49 D1
01 06 00 5B 07 E5 3B A2
01 06 00 5B 07 E5 3B A2
01 86 02 C3 A1
```