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 bits: 1
Check digit: n

2 Communication format

2.1 Host send format

address	Function code	Register address		data		**CRC low**	**CRC high**
Address	Function	AddrH	AddrL	NumH	NumL	CRCL	CRCH

a. Address location: the address of the corresponding child node, range (1- 247), the default address is 01, 0 is the broadcast address;
b、Function code: 0x03 read one or more registers, 0x06 write a register;
c、Register address: AddrH represents the high-byte address of the register to be read, AddrL represents the low address of the register to be read; For register address determination, see: (2.3 Maintaining Register Address Determination).
d、Data: The number of data to be read by the host, ranging from 1-8;
e、The last two bytes are the high and low bytes of the CRC check digit
For example, to read measurement data from a device with slave address 06, the data is sent in the following format:
Host send：06 03 00 06 00 02 25 BD

2.2 Slave answer format

Address	Function code	Number of bytes	data	**CRC low**	**CRC high**
Address	Function	byte	D0H,D0L...DNH,DNL	CRCL	CRCH

After the slave receives the host data, it unpacks the data, and only when the address matches will it respond to the host.

a、 Address code: Address of slave (1- 247);

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

c、 Bytes: The number of data sent, that is, the number of bytes of data D0L-DNH;

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

e、 The last two bytes are the high and low bytes of the CRC check digit;

For example, the data response from the slave to the host is as follows:

Slave response: 06 03 02 00 00 0D 84

Among them, the data of the fourth and fifth words is 00 00, which means that the data measured by the slave is now 0, and if the measured data is 9968, the transmitted data is 26 F0, that is, decimal 9968.

2.3 Hold register address definitions

Address	Register information	Value range	R/W	illustrate
0x0000	Modbus address register	1~247	R/W	
0x0001	Device information query		R	Device SN+ Device MAC Hardware version + software version + interface version
0x0002	Device time		R/W	Synchronize the device system time and query the current time of the device
0x0003	Communication baud rate		R	The baud rate is fixed at 9600
0x0004	Open and close door data query		R	Inquiry of door opening and closing signals in bus scenarios Timestamp + opening and closing door status

0x0005	Passenger flow data query		R	Timestamp plus incoming and outgoing passenger flow data

2.4 Register description

Whether it is a read or write instruction, the slave replies to the command if successful, it is unchanged, and if it fails, the highest position is 1.

- Read instruction 03:
  - Successful, the returned command position is still 03
  - Failure, then return the highest position of 03 of the instruction 1, which is 83
- Write the instruction then 06:
  - Successful: 06 Failure: 86

Example (modify slave address 01->02):

01 06 00 00 00 02 08 0B

Successful return: 02 06 00 00 00 02 08 38

Failure return (example): 01 86 01 83 A0

2.4.1 Address register 0x0000 (read, write)

2.4.1.1 Query the modbus address (**use the broadcast address 00 for slave address query, only for forgetting the slave address, the host connects to a single slave to obtain the slave address.**)

Host send: 00 03 00 00 00 01 85 DB

broadcast address	directives	Register address	Number of registers	CRC_L	CRC_H
00	03	0000	0001	85	DB

00 Use broadcast address query

03 Read register instructions

00 00 Register address: 00 00

00 01 Number of registers: 00 01 , 1

85 DB checksum

The device responds: 01 03 02 00 01 79 84

address	directives	length	data	CRC_L	CRC_H
01	03	02	0001	79	84

01 Device address code

03 Read register instruction, failure returns 83, normal is 03

02 Data length

00 01 The data is 00 01, that is, the register address is 01

79 84 check digit

Device response (failed, subsequent instructions are no longer listed separately as failure instructions): 01 83 01 80 F0

address	directives	Exception code	CRC_L	CRC_H
01	83	01	80	F0

01 Device address code

83 Read register instruction, failure returns 83, normal 03

01 Exception code, here 01 is only an example reference, the specific meaning is referred to 2.6 MODBUS exception code

80 F0 check digit

Note: The broadcast address query command will only respond to the query modbus address command (only allow query in the case of single slave connection, multi-slave query data is not trusted), other instructions do not respond

2.4.1.2 Modify the modbus address

Host send：01 06 00 00 00 03 C9 CB

address	directives	Register address	Register value	CRC_L	CRC_H
01	06	0000	0003	C9	CB

Device Response (Success)：03 06 02 00 03 81 49

address	directives	length	data	CRC_L	CRC_H
03	06	02	0003	81	49

2.4.2 Device information query (0x0001) (read-only)

2.4.2.1 Read device information

Host send：01 03 00 01 00 01 D5 CA

address	directives	Register address	Number of registers	CRC_L	CRC_H
01	03	0001	0001	D5	CA

Device Response (Success): 01 03 14 00 07 24 18 69 74 50 21 4C BC 98 60 00 97 01 2C 01 D2 00 64 E0 DF

Address	directives	SN	MAC	hardware	Software	interface	CRC	
01	03	0007241869745021	4CBC98600097	012C	01D2	0064	E0	DF

SN: 0x0007241869745021 corresponds to decimal: 2010012104020001, which is SN

MAC: 4CBC98600097 corresponds to: 4C:BC:98:60:00:97

Hardware version: 0x12C corresponds to decimal 300, divide by 100 to get the version number: 3.0.0

Software version: 0x1D2 corresponds to decimal 466, divide by 100 to get the version number: 4.6.6

Interface version: 0x0064 corresponds to decimal 100, divide by 100 to get the version number: 1.0.0

2.4.3 Device time (0x0002) (read, write)

2.4.3.1 Read the device time:

Host send: 01 03 00 02 00 01 25 CA

Address	directives	Register address	Number of registers	CRC_L	CRC_H
01	03	0002	0001	25	CA

Device response: 01 03 07 07 E5 0C 1F 0C 02 28 C2 89

Address	directives	length	year	month	day	hour	minutes	seconds	CRC_L	CRC_H
01	03	07	07E5	0C	1F	0C	02	28	C2	89

Time conversion: 07E converted to decimal to get 2021, month, day, hour, minute, and second converted to decimal to get the time 2021-12-31 12:02:40

2.4.3.2 Modify the device time

Host send: 01 06 00 02 07 E5 0C 1F 0F 02 28 25 83

Address	directives	length	year	month	day	hour	minutes	seconds	CRC_L	CRC_H
01	06	0002	07E5	0C	1F	0F	02	28	25	83

Device response: 01 06 07 07 E5 0C 1F 0F 02 28 0D D9

Address	directi	length	year	mont	day	hour	minut	secon	CRC_L	CRC_H

s	ves			h			es	ds		
01	06	07	07E5	0C	1F	0F	02	28	0D	D9

2.4.3.3 Synchronize device time

Host send: 00 06 00 02 07 E5 0C 1F 0F 02 28 21 7F

broadcast address	directives	length	year	month	day	hour	minutes	seconds	CRC_L	CRC_H
00	06	0002	07E5	0C	1F	0F	02	28	21	7F

Device Response: None

Note: The broadcast address write command only sets the device time command will take effect, used for multi-slave time synchronization, because the device is unresponsive, it is recommended to send 3 times in a row to ensure successful synchronization

2.4.4 Communication baud rate query (0x0003) (read-only)

2.4.4.1 Read the communication baud rate

Host send：01 03 00 03 00 01 74 0A

Address	directives	Register address	Number of registers	CRC_L	CRC_H
01	03	0003	0001	74	0A

Device response：01 03 02 03 C0 B8 E4

Address	directives	length	baud rate	CRC_L	CRC_H
01	03	02	03C0	B8	E4

Baud rate conversion: 03 C0 -> corresponds to hexadecimal 0x03C0, converted to decimal to get 960. Multiply by 10 to get 9600.

2.4.5 Open and close door data query (0x0004) (read-only)

2.4.5.1 Read open and close door data (only for bus scenarios)

Host send：01 03 00 04 00 01 C5 CB

Address	directives	Register address	Number of registers	CRC_L	CRC_H
01	03	0004	0001	C5	CB

Device response：01 03 0B 07 E5 0C 1F 0C 02 28 01 01 90 A9

Address	directives	length	year	month	day	hour	minutes	seconds	Door number	Open and close the door	CRC_L	CRC_H
01	03	0B	07E5	0C	1F	0C	02	28	01	01	90	A9

Year: 07E5 converted to decimal to get 2021, month, day, hour, minute and second converted to decimal to get the time 2021-12-31 12:02:40

Door number: 01, range 01~ff, currently reserved fixed as 01

Open and close the door: 00 close; 01 Open the door

2.4.6 Passenger flow data query (0x0005) (read-only)

2.4.6.1 Read passenger flow data

Host send: 01 03 00 05 00 01 94 0B

Address	directives	Register address	Number of registers	CRC_L	CRC_H
01	03	0005	0001	94	0B

Device response: 01 03 0B 07 E5 0C 1F 0C 02 28 00 24 00 20 BD 91

Address	directives	length	year	month	day	hour	minutes	seconds	enter	leave	CRC_L	CRC_H
01	03	0B	07E5	0C	1F	0C	02	28	0024	0020	BD	91

Year: 07E5 converted to decimal to get 2021, month, day, hour, minute and second converted to decimal to get the time 2021-12-31 12:02:40

Number of incoming passengers: 00 24 -> corresponds to hexadecimal 0x0024, converted to decimal to get 36

Number of passengers: 00 20 -> corresponds to hexadecimal 0x0020, converted to decimal to get 32

2.4.6.2 Reset footfall data

Host send: 01 06 00 05 00 01 58 0B

Address	directives	Register address	Number of registers	CRC_L	CRC_H
01	06	0005	0001	58	0B

Device Response: 01 06 0B 07 E5 0C 1F 0C 02 28 00 00 00 00 F0 47

Address	directives	length	year	month	day	hour	minutes	seconds	enter	leave	CRC_L	CRC_H

01	06	0B	07E5	0C	1F	0C	02	28	0000	000	F0	47

Year: 07E5 converted to decimal to get 2021, month, day, hour, minute and second converted to decimal to get the time 2021-12-31 12:02:40
Number of incoming passengers: 00 00 -> corresponds to hexadecimal 0x0000, converted to decimal to get 0
Number of passengers: 00 00 -> corresponds to the hexadecimal 0x0000, converted to decimal to get 0
Note: Reset the passenger flow data to return the passenger flow data of the device after the reset, and the entry and exit are 0 if the reset is successful.

2.4.7 Limit number of people data operation (0x0006) (read and write)

2.4.7.1 Read the limit on the number of people

Host send: 01 03 00 06 00 01 64 0B

Address	directives	Register address	Number of registers	CRC_L	CRC_H
01	03	00 06	00 01	64	0B

Device response: 01 03 02 00 0A 38 43

Address	directives	length	Limit the number of people	CRC_L	CRC_H
01	03	02	000A	38	43

Note: Limit the number of people: 00 0A -> corresponds to hexadecimal 0x000A, convert to decimal to get 10

2.4.7.2 Set a limit on the number of people

Host send: 01 06 00 06 00 01 A8 0B

Address	directives	Register address	Number of registers	CRC_L	CRC_H
01	06	00 06	00 01	A8	0B

Device response: 01 06 02 00 01 48 79

Address	directives	length	Limit the number of people	CRC_L	CRC_H
01	06	02	0001	48	79

Note: I mean the number of people: 00 01 -> corresponds to the hexadecimal 0x0001, converted to decimal is get 1

2.4.8 Read IO deferred operation (0x0007) (read-only)

2.5 ModbusCRC16 Verify the code

```
/* CRC16 The code for how it is calculated*/
/* CRC16 =  X16+X15+X2+1 ,In the message, the low position is first, and the high position is the back*/
/* len is msg data + CRC code length*/
uint16_t crc16(uint8_t *msg, uint8_t len)
{
	int i,j;
	unsigned short wCrc;
	wCrc = 0xffff;
	//wCrc = 0x00;
	for(i=0; i<len; i++)
	{
		wCrc ^= msg[i];
		for (j = 0; j < 8; j++)
		{
			if(wCrc & 0x0001)
			{
				wCrc >>= 1;
				wCrc ^= 0xA001;
			}
			else
				wCrc >>= 1;
		}
	}
	return wCrc;
}
```

2.6 MODBUS Exception code

MODBUS Exception code

code	name®	meaning
01	Illegal features	For the server (or slave), the function code received in the query is not an allowable operation. This may be because the function code is only applicable to the new device and is not possible in the selected unit. At the same time, it is also pointed out that the server (or slave) handles such a request in an error state, for example: because it is not configured and asks to return a register value
02	Illegal data address	The data address received in the inquiry is not permissible to the server (or slave). In particular, the combination of reference number and transmission length is invalid. For a controller with 100 registers, a request with offset 96 and length 4 succeeds, and a request with offset 96 and length 5 results in exception code 02.
03	Illegal data values	The value included in the query is not permissible to the server (or slave). This value indicates a failure in the remaining structure of the combined request, for example, the implied length is incorrect. It does not mean that, because the MODBUS protocol does not know the significance of any special value of any particular register, the data item in the register that is committed for storage has a value that is not expected by the application.
04	Slave equipment failure	When the server (or slave) is trying to perform the requested operation, an unrecoverable error occurs.
05	confirmation	Use with programming commands. The server (or slave) has already accepted the request and is processing it, but it takes a long duration for these operations. Returning this response prevents timeout errors from occurring on the client (or master). The client (or master) can continue to send polling program completion messages to determine whether processing is complete.

06	The slave is busy	Use with programming commands. The server (or slave) is processing program commands for long durations. When the server (or slave) is idle, the user (or master) should retransmit the message later.
08	Store parity errors	Used with function codes 20 and 21 and reference type 6 to indicate that the extent does not pass the consistency check. The server (or slave) attempted to read the log file, but found a parity error in memory. The client (or master) can resend the request, but can request service on the server (or slave) device.
0A	Gateway paths are not available	Used with a gateway to indicate that the gateway cannot assign an internal communication path from an input port to an output port for processing requests. This usually means that the gateway is misconfigured or overloaded.
0B	The gateway target device response failed	Used with a gateway to indicate that no response is obtained from the target device. Usually means that the device is not in Network 3.

Release history

Version: V1.0:
Date: 2019-06-08
Description: First draft

Version: V1.1:
Time: 2022-04-28
Description:
1. Add the Clear Passenger Flow command

Version: V1.2:
Time: 2022-09-01
Description:
1. Fix the error of sample data content