

Modbus Protocol

This protocol operate in RS485 hardware for one to many control as well as signal collection under the standard of Modbus RTU.

MODBUS Message

1. Character format

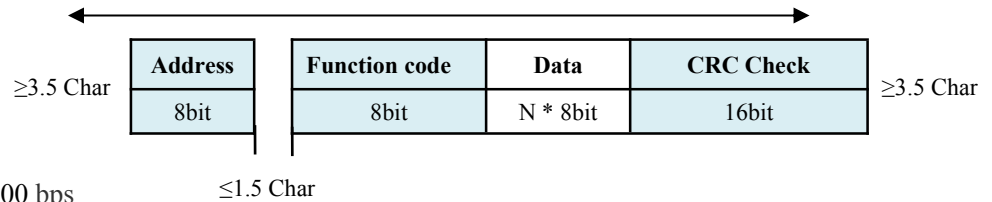
Start: 1Bit

Data: 8Bit

Parity: None

Stop: 1Bit

Baud Rate: 9600 bps、19200 bps



In the RTU, two characters should be spaced out less than 1.5 characters of time; otherwise this frame message would be considered as incomplete and be abandoned by receiver. 3.5 characters of time would be needed between two frame messages.

2. Communication protocol

2.1 Slave equipment ID address

Slave address is the identity for each equipment, The default value is 0x01 and could be altered from range 0x01~0xFF through communication. Among them, 0x00 would be broadcasting address, detailed as table(2.4).

2.2 Read Holding Registers (Function code 0x03)

Host equipment could read data from slave registers numbered in one or many through this function.

Sequence format:

Host reading requests					
Slave ID address	Function code= 0x03	Starting Address	No. of Registers	CRC LO	CRC HI
8Bit	8Bit	16Bit	16Bit	8Bit	8Bit
Slave response sequence					
Slave ID address	Function code= 0x03	Data bytes	Data	CRC LO	CRC HI
8Bit	8Bit	8Bit	N * 8Bit	8Bit	8Bit
Slave inaccurate response sequence					
Slave ID address	Function code= 0x03	Abnormal code= 0x02 or 0x03		CRC LO	CRC HI
8Bit	8Bit	8Bit		8Bit	8Bit

Communication protocol example

Host dispatch sequence: 01 03 00 01 00 02 95 CB
 Slave ID Function Starting address No. of Registers CRC Check

Slave response sequence: 01 03 04 03 E8 00 01 BB 83
 Slave ID Function Byte Count Data CRC Check

Slave inaccurate response sequence: 01 83 02 C0 F1
 Slave ID Function Data length CRC Check

2.3 Preset Single Register (Function code 0x06)

Host could input data to register and could only operate a register a time.

Sequence format:

Host input requests for register sequence					
Slave ID address	Function code = 0x06	Register address	Preset Data	CRC LO	CRC HI
8Bit	8Bit	16Bit	16Bit	8Bit	8Bit
Slave response sequence					
Slave ID address	Function code = 0x06	Register address	Preset Data	CRC LO	CRC HI
8Bit	8Bit	16Bit	16Bit	8Bit	8Bit
Slave inaccurate response sequence					
Slave ID address	False code = 0x86	Abnormal code = 0x02 or 0x03		CRC LO	CRC HI

Modbus Protocol

8Bit	8Bit	8Bit	8Bit	8Bit
------	------	------	------	------

Communication protocol example

Host dispatch sequence: $\frac{01}{\text{Slave ID}}$ $\frac{06}{\text{Function}}$ $\frac{00\ 03}{\text{Register address}}$ $\frac{00\ 01}{\text{Preset data}}$ $\frac{B8\ 0A}{\text{CRC Check}}$

Slave response sequence: $\frac{01}{\text{Slave ID}}$ $\frac{06}{\text{Function}}$ $\frac{00\ 03}{\text{Register address}}$ $\frac{00\ 01}{\text{Preset data}}$ $\frac{B8\ 0A}{\text{CRC Check}}$

Slave inaccurate response sequence: $\frac{01}{\text{Slave ID}}$ $\frac{86}{\text{Function}}$ $\frac{02}{\text{Data length}}$ $\frac{C3\ A1}{\text{CRC Check}}$

2.4 Broadcast preset register (Function code:0x06)

Host could input register data to all slaves of the bus with this function in the address 0x00. Slave no response.

Sequence format:

Host spread broadcast to input register sequence					
Slave ID address = 0x00	Function code= 0x06	Register address	Preset Data	CRC LO	CRC HI
8Bit	8Bit	16Bit	16Bit	8Bit	8Bit
Slave no response					

Communication protocol example

Host dispatch sequence: $\frac{00}{\text{Slave ID}}$ $\frac{06}{\text{Function}}$ $\frac{00\ 05}{\text{Register address}}$ $\frac{00\ 01}{\text{Preset data}}$ $\frac{59\ DA}{\text{CRC Check}}$

Note: The host could manipulate slaves group and could modify slave ID address without knowing this slave ID address. Be careful assimilation of slave address through this function in case.

3. Register Address Table

Register address	Function	Read& write mode	Detail description
0x0001	Pressure value	R	Pressure range is -1000~1000Pa、-10000~10000Pa,the resolution is 1Pa.E.g reading value 0x0000 = 0Pa、0x03E8 = 1000Pa; When pressure value is negative = $-(0x10000 - n(\text{reading value}))$, e.g reading value 0xFFFF = -1Pa,0x FC18 = -1000Pa Pressure range is -100~100Pa,the resolution is 0.1Pa. When pressure value is positive = $n(\text{reading value}) / 10$, e.g reading value 0x0001 = 0.1Pa、0x03E8 = 100.0Pa; When pressure value is negative = $-(0x10000 - n(\text{reading value})) / 10$, e.g reading value 0xFFFF = -0.1Pa、0xFC18 = -100.0Pa
0x0002	Unit setting	R&W	1 = Pa 2 = mmH ₂ O 3 = mbar 4 = inWG 5 = mmHG 6 = daPa 7 = Kpa 8 = hPa (functional when equipped with display) 0 = dial-up switch setting default:0
0x0003	Response time setting	R&W	1 = 0.5s 2 = 1s 3 = 2s 4 = 4s 0 = dial-up switch setting default:0
0x0004	Communication mode setting	R&W	1=9600bps 2=19200bps 0 = dial-up switch setting Default:0
0x0005	Slave ID address setting	R&W	type 0x01~0xFF, 0x00 to set broadcast receiving address default:0x01
0x0006	Zero resetting	R&W	type 1234 (0x04D2) would zero resetting with the data

4. Analysis Of Error Codes

0x02	Illegal register address
0x03	Illegal input data