T80 series instrument Modbus communication protocol

Serial port: 8 data bits, 1 stop bit, no parity check
Baud rate: 1200, 2400, 4800, 9600

1. RTU mode

When the controller is set to communicate in RTU (Remote Terminal Unit) mode on the Modbus network, each 8Bit byte in the message contains two 4Bit hexadecimal characters. The main advantage of this method is: under the same baud rate, more data can be transmitted than the ASCII method.

Code system
- 8-bit binary, hexadecimal number 0...9, A...F
- Each 8-bit field in the message is composed of two hexadecimal characters

Bits in byte
- 1 start bit
- 8 data bits, the smallest valid bit is sent first
- 1 parity bit, no check no parity bit
- stop bit (when there is parity), 2 Bit (when there is no parity)

Error detection domain
- CRC (cyclic redundancy check)

RTU frame
Using RTU mode, the message transmission must start with a pause interval of at least 3.5 characters. This is the easiest way to achieve various character times under the network baud rate (shown as TI-T2-T3-T4 in the figure below). The first field transmitted is the device address. The transmission characters that can be used are hexadecimal 0...9, A...F. The network device continuously detects the network bus, including the pause interval. When the first field (address field) is received, each device decodes it to determine whether to send it to itself. After the last transmitted character, a pause of at least 3.5 characters marks the end of the message. A new message can start after this pause.

The entire message frame must be transmitted as a continuous stream. If there is a pause of more than 1.5 character time before the frame is completed, the receiving device will refresh the incomplete message and assume that the next byte is the address field of a new message. Similarly, if a new message starts after the previous message in less than 3.5 characters, the receiving device will consider it a continuation of the previous message. This will cause an error, because the value in the final CRC field cannot be correct. A typical message frame is as follows:

Start bit	Device address	Function code	Data	CRC check	Terminator
T1-T2-T3-T4	8Bit	8Bit	n 8Bit	16Bit	T1-T2-T3-T4

RTU message frame

www.finglai.com

2. Example of reading PV parameters in RTU mode

Example 1. Read PV value

Host request						
Address	Function code	Start high-order address	Start low-order address	Registers quantity high address	Registers quantity low address	CRC check
01	03	00	00	00	02	C40B

Slave answer							
Address	Function code	Bytes quantity	Data high byte	Data low byte	Decimal point high byte	Decimal point low byte	CRC check
01	03	04	03	E8	00	01	BB83
The decimal integer represented by the hexadecimal number 03E8.0001 is 1000*10^{-1}=100.0, and the CRC check value depends on the transmission mode.							

Read PV value data as 100.0

Example 2. Read PUH value

Host request						
Address	Function code	Start high-order address	Start low-order address	Registers quantity high address	Registers quantity low address	CRC check
01	03	02	0C	00	02	05B0

Slave answer							
Address	Function code	Bytes quantity	Data high byte	Data low byte	Decimal point high byte	Decimal point low byte	CRC check
01	03	04	13	88	00	01	BF5D
The decimal integer represented by the hexadecimal number 1388.0001 is 5000*10^{-1}=500.0, and the CRC check value depends on the transmission mode.							

Read PV value data as 100.0

When reading data, the address (01) and function code (03) are unchanged, only the starting high-order address and the starting low-order address are different.

www.finglai.com

3. Example of writing parameters in RTU mode

Example 1. Write AH value (AH=100.0)

Host request											
Address	Function code	Start high-order address	Start low-order address	Registers quantity high address	Registers quantity low address	Byte count	Data high	Data low	Point high byte	Point low byte	CRC check
01	10	01	00	00	02	04	03	E8	00	01	BF8F

Slave answer						
Address	Function code	Start high-order address	Start low-order address	Registers quantity high address	Registers quantity low address	CRC check
01	10	01	00	00	02	XX
The decimal integer represented by the hexadecimal number 03E8.0001 is 1000*10^{-1}=100.0, and the CRC check value depends on the transmission mode.						

Example 2. Write SN value (SN=08)

Host request											
Address	Function code	Start high-order address	Start low-order address	Registers quantity high address	Registers quantity low address	Byte count	Data high	Data low	Point high byte	Point low byte	CRC check
01	10	02	00	00	02	04	00	08	00	00	6B0D

Slave answer						
Address	Function code	Start high-order address	Start low-order address	Registers quantity high address	Registers quantity low address	CRC check
01	10	02	00	00	02	XX
The decimal integer represented by the hexadecimal number is 8*1=8, and the CRC check value should be determined according to the transmission mode.						

The Modbus communication protocol is a master-slave protocol. Only one device can send on the line at any time. The master station manages the information exchange, and only it can initiate it. It will successively poll the slave stations, otherwise any slave station can not send messages. Direct communication between slave stations is not possible.

www.finglai.com

Communication address

Parameter	Type	High address	Low address	Decimal point unit
PV	Read	00	00	Decided by DOT value
AH	Read Write	01	00	DOT
DH	Read Write	01	04	DOT
AL	Read Write	01	08	DOT
DL	Read Write	01	0C	DOT
AHH	Read Write	01	10	DOT
DHH	Read Write	01	14	DOT
ALL	Read Write	01	18	DOT
DLL	Read Write	01	1C	DOT
SN	Read Write	02	00	0
DOT	Read Write	02	04	0
PUL	Read Write	02	08	DOT
PUH	Read Write	02	0C	DOT
PBIA	Read Write	02	10	DOT
FILT	Read Write	02	14	3
K1	Read Write	02	18	3
OU-A	Read Write	02	1C	0
PH	Read Write	02	20	0
PL	Read Write	02	24	0
PHH	Read Write	02	28	0
PLL	Read Write	02	2C	0
INPH	Read Write	02	30	0
INPL	Read Write	02	34	0
BAUD	Read Write	02	38	0
ID	Read Write	02	3C	0

www.finglai.com