Modbus communication protocol

HE 200 series frequency converter provides RS232/RS485 communication interface and supports Modbus communication protocol.Users can achieve centralized control through the computer or PLC,through the communication protocol to s et the operation order of the frequency converter, modify or read the function code parameters, read the working status and fault information of the frequency converter.

1,the Protocol content

The serial communication protocol defines the content and format of information transmitted in serial communication. The protocol includes: host polling (or broadcast) format; Host coding method,including: required action of the function code, transmission data and error check. The sound of the slave machine should also adopt the same structure, the content includes:
action confirmation, return data and error check. If the slave machine makes an
error when receiving the information, or fails to complete the action required by
the host, it will organize a fault information as a response to the host.

(1) Interface mode

RS485 hardware interface

(2) Transmission method

Asynchronous serial, half duplex transmission mode. Only one host and slave can send data and the other can receive data at the same time. During serial asynchronous communication, data is sent frame by frame in the form of packets.

(3) Topology

Single host multiple slave system. The slave address is set in the range of 1 to 247,0 is the broadcast communication address. The slave address in the network must be unique.

RTU frame format：

Frame header START	3.5 character time
Slave address ADR	Mailing address: 1-247
Command code CMD	03: Read slave machine parameters; 06: Write slave parameters
DATA (N.1)	Data content: Function code parameter address, number of function code parameters, function code parameter values, etc.
DATA（N.2）	
……	
DATA0	
CRC CHK low bit	Detection value: CRC value.
CRC CHK high bit	
END	3.5 character time

CMD (Command Instruction) and DATA (Data Word Description)

Command code: 03H, read N words (Word) (up to 12 words can be read), for example: the starting address F002 of a frequency converter with slave address 01 reads 2 consecutive values

Host Command Information

ADR	01H
CMD	03H
Starting address high bit	F0H
Starting address low order	02H
Number of Registers High	00H
Low register count	02H
CRC CHK low bit	CRC value.
CRC CHK high bit	

Slave response information：

When PD.05 is set to 0:

ADR	01H
CMD	03H
Bytes high	00H
Bytes Low	04H

Data F002H high bit	00H
Data F002H low bit	00H
Data F003H high bit	00H
Data F003H low bit	01H
CRC CHK low bit	CRC value.
CRC CHK high bit	

When PD.05 is set to 1:

ADR	01H
CMD	03H
Bytes	04H
Data F002H high bit	00H
Data F002H low bit	00H
Data F003H high bit	00H
Data F003H low bit	01H
CRC CHK low bit	CRC value.
CRC CHK high bit	

Command code: 06H Write a word (Word), for example: Write 5000 (1388H) to the F00AH address of the slave address 02H frequency converter.

Host Command Information

ADR	02H
CMD	06H
Starting address high bit	F0H
Starting address low order	0AH
Data high bit	13H
Data low bit	88H
CRC CHK low bit	CRC value
CRC CHK high bit	

Slave response information：

ADR	02H
CMD	06H
Starting address high	F0H
Starting address low	0AH
Data high bit	13H
Data low bit	88H
CRC CHK low bit	CRC value
CRC CHK high bit	

Check method -- CRC check method:
CRC simple functions are as follows:

```
unsigned int CRC_Cal_Value(unsigned char *Data, unsigned char Length)
{
    unsigned int crc_value = 0xFFFF;
    int i = 0;
    while(Length..)
    {
        crc_value ^= *Data++;
        for(i=0;i<8;i++)
        {
            if(crc_value & 0x0001)
            {
                crc_value = (crc_value>>1)^ 0xa001;
            }
            else
            {
                crc_value = crc_value>>1;
            }
        }
    }
    return(crc_value);
}
```

2. Address definition of communication parameters

Read and write function code parameters (some function codes can not be changed, only for the use of manufacturers or monitoring). Function code parameters address marking rules:

Function code group number and label as parameters address rules: **High byte: F0~FF (group P), A0~AF (group A), 70~7F (group D) Low byte: 00~FF**

For example, P3.12, the address is F30C; Note:

PF group: Parameters can neither be read nor changed; D: The parameters can only be read and cannot be changed Number.

Some parameters can not be changed when the inverter is in the running state;

Some parameters can not be changed no matter what state the inverter is in; Change the function code parameters, but also pay attention to the range of parameters, units, and related descriptions. In addition, because EEPROM is frequently stored, it will reduce the service life of EEPROM, so some function codes in the mode of communication, do not need to store, as long as the value in RAM can be changed. If it is a P group parameter, to achieve this function, as long as the function code address of the high F into 0 can be achieved. If it is A group parameter, to realize the function, as long as the high A of the function code address into 4 can be realized.

The corresponding function code address is expressed as follows: **High byte: 00~0F (group P), 40~4F (group A) Low byte: 00~FF**

For example, function code P3.12 is not stored in EEPROM, and the address is represented as 030C; Function code A0.05 is not stored in EEPROM, and the address is 4005; This address means that only write RAM, can not do read action, read, as invalid address. For all parameters, you can also use the command code 07H to achieve this function.

Stop/operation parameters section:

Parameter Address（H）	parameter description
1000	Communication set value (-10000~10000) (Decimal)
1001	Operating frequency

1002	Bus voltage
1003	output voltage
1004	Output current
1005	output power
1006	Output torque
1007	running speed
1008	Digital input flag
Parameter Address	parameter description
1009	Digital output flag
100A	AI1 voltage
100B	AI2 voltage
100C	AI3 voltage
100D	Counting value input
100E	Length value input
100F	Load speed
1010	PID setting
1011	PID feedback
1012	PLC steps
1013	High frequency input pulse frequency, unit: 0.01kHz
1014	Feedback speed, unit 0.1Hz
1015	Remaining running time
1016	Voltage before AI1 correction
1017	Voltage before AI2 correction
1018	Voltage before AI3 correction
1019	Linear velocity
101A	Current power-on time
101B	Current running time
101C	High frequency input pulse frequency, in
101D	Communication given value
101E	Actual feedback speed
101F	Main frequency A display
1020	Auxiliary frequency B display

Attention:

The communication given value is a percentage of the relative value, with 10000 corresponding to 100.00% and -10000 corresponding to -100.00%. For frequency dimensional data, this percentage is the percentage of the relative maximum frequency (P010); For torque dimensional data, this percentage

It is P2.10, P2.48, A3.48, A4.48 (the upper torque limit number is given, corresponding to the first and second motors respectively).

Control command input to frequency converter: (write only)

Command word address（H）	Command function
2000	0001：Forward running
	0002：Reverse operation
	0003：Forward jog
	0004：Reverse Jog
	0005：Free stop
	0006：Deceleration shutdown
	0007：Fault reset

Read frequency converter status: (read-only)

status word address（H）	Status word function
3000	0001：Forward running
	0002：Reverse operation
	0003：stop

Parameter lock password verification: (If the return is 8888H, it indicates that the password verification has passed)

Password Address（H）	Enter the content of the password
1F00	*****

Terminal output control: (write only)

command address（H）	Command content
2001	BIT0：Y1 output control BIT1：Y2 output control BIT2：RELAY1 output control BIT3：RELAY2 output control BIT4：Y0 output control BIT5：VDO1 BIT6：VDO2 BIT7：VDO3

Frequency converter fault description:

Frequency converter fault address（H）	Frequency converter fault information
8000	Numeric hexadecimal representation of fault codes