

9600 serial communication protocol

9600 series of inverter provides RS232/RS485 communication interface, and adopts MODBUS communication protocol. User can carry out centralized monitoring through PC/PLC to get operating requirements.

F.1 About Protocol

This serial communication protocol defines the transmission information and use format in the series communication and it includes master-polling (or broadcasting) format, master coding method and the content includes function code of action, transferring data and error checking. The response of slave is the same structure, and it includes action confirmation, returning the data and error checking etc. If slave takes place the error while it is receiving the information or cannot finish the action demanded by master, it will send one fault signal to master as a response.

F.2 Application Methods

The inverter will be connected into a "Single-master Multi-slave" PC/PLC control net with RS232/RS485 bus.

F.3 Bus structure

(1) Interface mode

RS232/RS485 Hardware interface

(2) Transmission mode

There provide asynchronous series and half-duplex transmission mode. At the same time, just one can send the data and the other only receives the data between master and slave. In the series asynchronous communication, the data is sent out frame by frame in the form of message.

(3) Topological mode

In Single-master system, the setup range of slave address is 1 to 247. Zero refers to broadcast communication address. The address of slave must be exclusive in the network. That is one condition of one slave machine.

F4 Protocol description

9600 series inverter communication protocol is a kind of serial master-slave communication protocol, in the network, only one equipment, and master can build a protocol, (Named as "Inquire/Command"). Other equipments, slave's response "Inquire/Command" of master only by providing the data or doing the action according to the master's "Inquiry/Command". Here, master is Personnel Computer, Industrial Machine or Programmable logical controller, and the slave is inverter. Master not only visits some slave, but also sends the broadcast information to all the slaves. For the single master "Inquiry/Command", all of slaves will return a signal that is a response; for the broadcast information provided by master, slave needs not feedback a response to master machine.

F5 Communication data structure

ModBus protocol communication data format of 9600 series of inverter is shown as following:

(In RTU mode, messages start with a interval of at least 3.5 character times. This is most easily implemented as a multiple of character times at the baud rate that is being used on the network (shown as T1-T2-T3-T4 in the figure below). The first field then transmitted is the device address. The allowable characters transmitted for all fields are hexadecimal 0 ... 9, A ... F. Networked devices monitor the network bus continuously, including during the silent intervals. When the first field (the address field) is received, each device decodes it to find out if it is the addressed device. Following the last transmitted character, a similar interval of at least 3.5 character times marks the end of the message. A new message can begin after this interval)

The entire message frame must be transmitted as a continuous stream. If a silent interval of more than 1.5 character times occurs before completion of the frame, the receiving device flushes the incomplete message and assumes that the next byte will be the address field of a new message.

Similarly, if a new message begins earlier than 3.5-character times following a previous message, the receiving device will consider it a continuation of the previous message. This will set an error, as the value in the final CRC field will not be valid for the combined messages. A typical message frame is shown below.

RTU frame format

START Frame Start	3.5-character time
Slave addr.	Communication addr. : 1 to 247
Command Code	03:Read slave parameters 06: Write slave parameters
DATA (N-1)	Data: Function code parameter address, the number of function code parameter, Function code parameter,etc.
DATA (N-2)	
.....	
DATA0	

CRC CHK High Order	Detection Value: CAC value
CRC CHK Low order	
END	3.5-character time

Command code: 03H reads N words. (There are 12 characters can be read at the most.)

For example: The inverter start address F002 of the slave 01 continuously reads two consecutive values.

Master command information

ADR	01H
CMD	03H
Start Address High order	F0H
Start Address Low order	02H
Register Number High order	00H
Register Number Low order	02H
CRC CHK Low order	CRC CHK values are to be calculated
CRC CHK high order	

Slave responding information

When FD-05 set to 0

ADR	01H
CMD	03H
Byte Number	00H
The low Order number of byte	04H
Data F002H high order	00H
Data F002H low order	00H
Data F003H high order	00H
Data F003H high order	01H
CRC CHK low order	CRC CHK values are to be calculated
CRC CHK high order	

When FD-05 set to 1

ADR	01H
CMD	03H

The Number of byte	04H
Data F002H high order	00H
Data F002H low order	00H
Data F003H high order	00H
Data F003H low order	01H
CRC CHK low order	CRC CHK values are to be calculated
CRC CHK high order	

Command Code : 06H, write a word

For example: Write 5000 (1388H) into F00AH which slave address is 02H.

Master command information

ADR	02H
CMD	06H
Data Address high order	F0H
Data Address low order	0AH
Data content high order	13H
Data content high order	88H
CRC CHK low order	CRC CHK values are to be calculated
CRC CHK high order	

Slave responding information

ADR	02H
CMD	06H
Data Address high order	F0H
Data Address low order	0AH
Data Content high order	13H
Data Content low order	88H
CRC CHK low order	CRC CHK values are to be calculated
CRC CHK high order	

CRC Checking

In RTU mode, messages include an error-checking field that is based on a CRC method. The CRC field checks the contents of the entire message. The CRC field is two bytes, containing a 16-bit binary value. The CRC value is calculated by the transmitting device, which appends the CRC to the message. The receiving device recalculates a CRC during receipt of the message,

and compares the calculated value to the actual value it received in the CRC field. If the two values are not equal, an error results.

The CRC is started by 0xFFFF. Then a process begins of applying successive eight-bit bytes of the message to the current contents of the register. Only the eight bits of data in each character are used for generating the CRC. Start and stop bits, and the parity bit, do not apply to the CRC.

During generation of the CRC, each eight-bit character is exclusive ORed with the register contents. Then the result is shifted in the direction of the least significant bit (LSB), with a zero filled into the most significant bit (MSB) position. The LSB is extracted and examined. If the LSB was a 1, the register is then exclusive ORed with a preset, fixed value. If the LSB was a 0, no exclusive OR takes place. This process is repeated until eight shifts have been performed. After the last (eighth) shift, the next eight-bit byte is exclusive ORed with the register's current value, and the process repeats for eight more shifts as described above. The final contents of the register, after all the bytes of the message have been applied, is the CRC value.

When the CRC is appended to the message, the low-order byte is appended first, followed by the high-order byte.

```
unsigned int crc_chk_value(unsigned char *data_value, unsigned char length)
{
    unsigned int crc_value=0xFFFF;
    int i;
    while(length--)
    {
        crc_value^=*data_value++;
        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);  
    }  
}
```

The chapter is about communication contents, it's used to control the inverter operation, the status of the inverter and related parameter setup.

Read and write function-code parameters (Some functional code is not changed, only for the manufacturer use.)

The mark rules of Function code parameters address:

The group number and mark of function code is the parameter address for indicating the rules.

High order bytes: F0 to FF

Low order bytes: 00 to FF

For example: P3-12, address indicates to F30C.

Caution:

Group F1: Only for reading parameter, can not be changed parameters

Group FF: Either the parameter can not be read, nor be changed. Some parameters can not be changed during operation, some parameters regardless of what kind of state the inverter in, the parameters can not be changed. Change the function code parameters, pay attention to the scope of the parameters, units, and relative instructions.

Besides, due to EEPROM be frequently stored, it will reduce the lifetime of EEPROM. In the communication mode, and some function code needn't be stored as long as change the RAM value. To achieve this function, change high order F of the function code into zero.

Corresponding function code addresses are indicated below:

High byte: 00~0F

Low byte: 00~FF

For example: Function code F3-12 can not be stored into EEPROM, address indicates to be EEPROM.

This address can only act writing RAM, it can not act reading, when act reading, it is invalid address.

Group FH function parameters:

Some models with extended function, such as MD330 or the models with water supply card, which increase group FH parameters, the communication address of group FH parameter is D0** (non-stored) E0** (stored).

For example: FH-05, it indicates D005H or E005H. FH-20, it indicates D014H or E014H.

Stop/start parameter

Parameter addr.	Parameter description
1000H	Communication setup value(-10000 to 10000)(Decimal)
1001H	Running frequency
1002H	Bus voltage
1003H	Output voltage
1004H	Output voltage
1005H	Output power
1006H	Output torque
1007H	Running speed
1008H	DI input flag
1009H	DO output flag
100AH	AI1 voltage
100BH	AI2 voltage
100CH	AI3 voltage
100DH	Counting value input
100EH	Length value input
100FH	Load speed
1010H	PID setup
1011H	PID feedback
1012H	PLC process
1013H	

Caution:

Communication setting value is the percentage of relative value, and 10,000 correspond to 100.00%, -10000 correspond to -100.00%.

On the frequency dimension of the data, the percentage is the percentage of relative maximum frequency (F0-10). To the torque dimension data, the percentage is relative twice percentage of the inverter rated torque.

Control command input to inverter (write-only)

Command Word Address	Command Function
2000H	0001: Forward operation
	0002: Reverse operation
	0003: Forward jog
	0004: Reverse jog
	0005: Free stop
	0006: Speed-down stop
	0007: Fault reset

Read inverter status :(read-only)

Status Sord Address	Status Word Function
3000 H	0001: Forward operation
	0002: Reverse operation
	0003: Stop

Parameters locking password checksum: (If the return is the 8888H, it indicates the password checksum pass)

Password Address	Contents of Input password
1F00H	*****

Parameter locking command :(write-only)

Address of locking password command	Contents of locking password command
1F00H	0001: lock system command code

Digital output terminal control: (write-only)

Address of locking password command	Contents of locking password command
2001H	BIT0: DO1 output control BIT1: DO2 DO2 output control BIT2: RELAY1 RELAY1 output control BIT3: RELAY2 RELAY2 output control BIT4: FMR FMR output control

Analog output AO1 control: (write-only)

Address of locking password command	Contents of locking password command
2002H	0~7FFF refers to 0% to 100.00%

Analog output AO2 control: (write-only)

Locking password command address	Locking password command contents
2003H	0~7FFF refers to 0% to 100.00%

Pluse output control: (write-only)

Address locking password command	Contents locking password command
2004H	0 to 7FFF (decimal) refers to 0% to 100.00%

Inverter fault description:

Inverter fault address	Inverter fault information
8000 H	0000: No fault 0001: Inverter unit protection 0002: Speed-up over current 0003: Speed-down over current 0004: Constant over current 0005: Speed-up over voltage 0006: Speed-down over voltage 0007: Constant over voltage 0008: Control power supply fault 0009: Under voltage fault 000A: Inverter overload 000B: Motor overload 000C: Input phase failure 000D: Output phase failure 000E: Radiator overheating 000F: External equipment fault 0010: Communication fault 0011: Contactor fault 0012: Current detection fault 0013: Motor tuning fault 0014: PG Fault

Description data of communication fault information (fault code)

Communication fault address	Fault function description
8001	0000: No fault 0001: Password error 0002: Command 0003: CRC checksum error 0004: Invalid address 0005: Invalid address 0006: Parameter change invalid 0007: The system is locked

Group FD Communication parameter description

PD-00	Baud rate		Factory default value	5
	Setup range	0	300BPS	
		1	600BPS	
		2	1200BPS	
		3	2400BPS	
		4	4800BPS	
		5	9600BPS	
		6	19200BPS	
		7	38400BPS	

This parameter is used to set the the data transfer rate between host computer and the inverter. Please note that baud rate of the host computer and the inverter must be consistent. Otherwise, communication is impossible. The higher baud rate is, the faster communication is.

PD-01	Data format		Factory default value	0
	Setup range	0	No check:Data format<8,N,2>	
		1	Even parity Check :data format <8,E,1>	
		2	Odd Parity Check : data format<8,O,1>	

The host computer and inverter setup data format must be consistent, otherwise, communication is impossible.

PD-02	Local Address		Factory default value	1
	Setup range	1~247,0 is broadcast address		

When the local address is set to 0, that is, broadcast address, it can realize the broadcast function of host computer.

PD-03	Response delay		Factory default value	10ms
	Setup range	0~20ms		

Response delay: It refers to the interval time from the inverter finishes receiving data to sending data to the host machine.If the response delay is less than the system processing time, then the response based on the time delay of the system processing time.If the response delay is more than the system processing time, after the system processes the data, it should be delayed to wait until the response delay time is up, then sending data to host machine.

PD-04	Communicaton timeout		Factory default value	0.0 s
	Setup range	0.0 s (inactive), 0.1~60.0s		

When the function set to 0.0 s, the communication timeout parameter is inactive.

When the function code set to RMS, if the interval time between the communication and the next communication is beyond the communication timeout, the system will report communication failure error (Err16). At normal circumstances, it will be set as inactive. If in the continuous communication system, set the second parameter, you can monitor the communication status.

PD-05	Communication protocol selection		Factory default value	0
	Setup range	0	Non-standard MODBUS protocol	
		1	Standard MODBUS protocol	

PD-05=1 : Select standard MODBUS protocol

PD-05=0 : When reading the command, the slave return is one byte than the standard MODBUS protocol's, for details refer to communications Data Structure of this protocol.