SD-A MODBUS
Communication Protocol

Appendix A: MODBUS Communication Protocol

MSD200A series servo driver supplys RS485 communication interface (CN3), and supports MODBUS communication protocol. User can do centralized control by computer or PLC, set driver motion command, revise or read function code parameter, read driver's working condition and fault information, and so on.

1. Protocoll Content

This communication prtocol defines information content of transmission and use format in serial communication. Including:Polling (or broadcast); Hosts coding method, contents including:Commanding motion's function code, transfering data and error checking. Slae responding also adops same structure, contents including: Motion confirm, returning data, error checking and so on. If slave goes wrong when receive information, or can not finish the motions host required, it will organize a fault information as responding feedback to host.

2. Application Method

Driver connect to "single host and some slaves" PC/PLC control network which have RS232/RS485 BUS.

3. Bus Structure

(1) Interface Method

RS485 hardware interface

(2) Transmission Method

Asynchronous serial, half-duplex transmission method. Only one between host and slave sends datas, the other one only receive datas at the same time. The data is sent by frame and frame in the form of message when in serial asynchronous communication process.

(3) Topological Structure

Single host and some slaves system. Slave address setting range is 1~247, 0 is broadcast communication address. The slave address must be only one in network.

4.Communication Description

MSD200A Serial servo driver communication protocol is an asynchronous serial master - slave ModBus communication protocol.Only one device (host) in the network can establish a protocol (called "query/command").Other devices (slave machines) can only respond to the "query/command" of the host by providing data, or act accordingly according to the "query/command" of the host.Host in this refers to the personal computer (PC), industrial control equipment or programmable logic controller (PLC), etc., slave refers to the MSD200A driver.The host can not only communicate with a slave machine, but also publish broadcast information to all slave machines.The slave machine returns a message (called a response) for each individually accessed host "query/command" and does not need to respond back to the host for the broadcast message sent by the host.

5.Communication Data Structure

MSD200A series servo driver ModBus communication data formate as follows:

In RTU mode, messages are sent at least once every 3.5 characters.Under the network baud rate in the multiple character time, this is the easiest to achieve.The first field of transmission is the device address.The transfer characters available are hexadecimal 0...9,A...F.The network device continuously detects the network bus, including the pause interval.When the first domain (address domain) is received, each device decodes it to determine whether to send it to itself.After the last transmission character, a pause of at least 3.5 characters marks the end of the message.A new message may begin after this pause.

The entire message frame must be transmitted as a continuous stream.If there is a pause of more than 1.5 characters 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 begins with the previous message in less than 3.5 characters, the receiving device will consider it a continuation of the previous message.This will result in an error because the value in the final CRC field cannot be correct.

RTU Frame Format:

Frame header START	3.5 Character time
Slave address ADR	Communication time: 1~247
Command code CMD	03: read slave parameter; 06: write slave parameter
Data content DATA (N-1)	Data content:

Data content DATA (N-2) ..... Data content DATA0	Function code parameter address, number of function code parameters, function code parameter values, etc
CRC CHK high order CRC CHK low order	Test value: CRC value.
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 start address F002 of a drive with a slave address of 01 reads two consecutive values

Host Command information

ADR	01H
CMD	03H
Start address high order	F0H
Start address low order	02H
Caculate numbers high order	00H
Caculate numbers low order	02H
CRC CHK low order CRC CHK high order	To be calculated its CRC CHK value

Slave responds information

When set **PnA.06 ones place is 0:**

ADR	01H
CMD	03H
Byte number high order	00H
Byte number low order	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	To be calculated its CRC CHK value
CRC CHK low order	

PnA.06 ten digit is 1:

ADR	01H
CMD	03H
Number of bytes	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	To be calculated its CRC CHK value
CRC CHK high order	

Command code: 06H, 07H, write a Word (Word), 06H command write function code save after power off, 07H command write function code do not save power off .

For example, write 5000 (1388H) to the F203H address of drive 02H from the slave.

Host Command Information

ADR	02H
CMD	06H
Data address high order	F2H
Data address low order	03H
Data content high order	13H
Data content low order	88H
CRC CHK low order	To be calculated its CRC CHK value
CRC CHK high prder	

Slave respond information

ADR	02H
CMD	06H
Data address high order	F2H
Data address low order	03H
Data content high order	13H
Data content low order	88H
CRC CHK low order	To be calculated its CRC CHK value
CRC CHK high order	

Check mode - CRC check mode: CRC(Cyclical Redundancy Check)

Using the RTU frame format, the message includes a crc-based error detection domain. The CRC domain detects the contents of the entire message. The CRC field is a two-byte, 16-bit binary value. It is computed by the transport device and added to the message. The receiving device recalculates the CRC of the received message and compares it to the value in the received CRC field.

The CRC starts by storing 0xFFFF and then calls a procedure to process the consecutive 8-bit bytes in the message with the values in the current register. Only 8 bits of data per character are valid for CRC, not the start and stop bits or the parity bits.

During CRC generation, each 8-bit character is separately different from the register contents or (XOR), and the result moves towards the direction of the lowest significant bit, and the highest significant bit is filled with 0. LSB is extracted to detect if LSB is 1, the register is separate from the preset value or if LSB is 0, it is not carried out. The process is repeated eight times. After the last bit (bit 8) is completed, the next 8-bit byte is either different or different from the current value of the register alone. The value in the final register is the CRC value after all bytes in the message have been executed.

When a CRC is added to a message, the low bytes are added first, then the high bytes. The CRC simple function is as follows:

```
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);
}
```

Address definition of communication parameter

This part is the content of communication, used to control the operation of the drive, drive state and related parameter setting. **Read abd write function code parameters (some function codes cannot be changed and are only used by the manufacturer) :**

Address labeling rules for function code parameters:

The rule is represented by the function code group number and label as the parameter address:

High order byte: F0~FF(Pn group)、A0~AF(Fn group)、70~7F(U group) 、D0~D1(dn group) 、E0~E4(En group)

Low order byte: 00~FF

Such as: Pn2.16, address is F210;

Note:

PnF group: Neither read parameters nor change parameters;Some parameters cannot be changed while the drive is running.Some parameters cannot be changed regardless of the state of the drive.Change function code parameters, also pay attention to the scope of parameters, units, and related instructions.

In addition, as EEPROM is stored frequently, it will reduce the lifetime of EEPROM. Therefore, some function codes in the mode of communication need not be stored, just change the value in RAM.

If it is a parameter of Pn group, the function can be realized as long as the high order F of the function code address is changed to 0.

The address of the corresponding function code is shown as follows:

HIgh order byte: 00~0F

Low order byte: 00~FF

For example, function code Pn2.16 is not stored in EEPROM, and the address is 02100210;

This address can only do write RAM, invalid address when can not do read action, read.

For all parameters, you can also use the command code 07H to implement this function.。

Stop/Operating parameter part:

Parameter address	Parameter Description
1000	Communication Settings (-10000~10000 decimalism)
1001	Operating frequency
1002	Bus voltage
1003	Output voltage
1004	Output current
1005	Output power
1006	Output torque
1007	Running speed
1008	DI input symbol
1009	DO output symbol
100A	AI1 voltage
100B	AI2 voltage
100C	AI3 voltage
100D	Count input
100E	Length value input
100F	Loading speed
1010	PID setting
1011	PID feedback
1012	PLC step
1013	PULSE iput pulse frequency, unit 0.01KHz
1014	Feedback speed, unit 0.1Hz
1015	Remaining running time
1016	AI1 Voltage before correction
1017	AI2 Voltage before correction
1018	AI3 Voltage before correction
1019	Linear velocity
101A	Current power on time
101B	Current running time
101C	PULSE input pulse frequency,unit 1Hz
101D	Communication setting value
101E	Actual feedback velocity
101F	Master frequency X display
1020	Auxiliary frequency Y display

Note: the communication setting value is the percentage of relative value, 10000 corresponds to 100.00%, and -10000 to -100.00%.

For the data of frequency dimension, this percentage is the percentage of relative maximum frequency (Pn2.05);For torque dimension data, this percentage is Pn1.03 (torque upper limit number setting).

Control command input to drive :(write only)

Command word address	Command function
2000	0001: Running CW
	0002: Running CCW
	0003: JOG CW
	0004: JOG CCW
	0005: Free downtime
	0006: Slowing down
	0007: Fault reset

Read drive status :(read only)

Statusword addre	Status word function
3000	0001: Running CW
	0002: Running CCW
	0003:Downtime

Parameter lock password check :(if it returns 8888H, the password check is passed)

Password address	Enter the contents of the password
1F00	*****

Digital output terminal control :(write only)

Command address	Command content
2001	BIT0: DO1 output control BIT1: DO2 output control BIT2: RELAY1 output control

	BIT3: RELAY2 output control BIT4: FMR output control BIT5: VD01 BIT6: VD02 BIT7: VD03 BIT8: VD04 BIT9: VD05

Analog output A01 control :(write only)

Command address	Command content
2002	0～7FFF is 0%～100%

Analog output AO2 control: (only write)

Command address	Command content
2003	0～7FFF is 0%～100%

PULSE output control: (only write)

Command address	Command content
2004	0～7FFF表示0%～100%

Driver fault description:

Driver fault address	Driver fault information
8000	0000: No fault 0001: Retain 0002: Accelerated overcurrent 0003: Decelerated overcurrent 0004: Constant speed over current 0005: Acceleration overvoltage 0006: Deceleration overvoltage 0007: Constant overvoltage 0008: Buffer resistance overload fault 0009: Under-voltage fault 000A: Driver overloading 000B: Motor overloading 000C: Input lack of phase

	000D: Output lack phase 000E: Module is overheating 000F: External fault 0010: Abnormal communication 0011: Abnormalcontactor 0012: Current detection fault 0013: Motor tuning fault 0014: Encoder/PG card failure 0015: Parameter read-write exception 0016: Driver hardware failure 0017: Short circuit fault of motor to ground 001A: Run time arrival 001B: User-defined faults1 001C: User-defined faults2 001D: Power on time arrival 001E: Off load 001F: Feedback lost when run PID 0028: Fast current limiting timeout failure 0029: Switching motor failure during operation 002A: Excessive speed deviation 002B: Motor overspeed 002D: Motor thermal 0033: Initial position error 0036: Zero lost 0037: When the pulse position is synchronized, the follow-up deviation is too large. 005A: Encoder wire number setting error 005B: No encoder connected

Communication fault information description data (fault code) :

Communication failure address	Failure function description
8001	0000: No fault 0001: Password error 0002: Command code error 0003: CRC checking error 0004: Invalid address 0005: Invalid parameter 0006Invalid parameter change 0007: System locked 0008: In EEPROM operation

PnA group communication parameter description

PnA.00	Communication type		Factory default	0
	Setting range	0	485 communication	
		1	Retain	
		2	Retain	
		3	CAN.LINK card	
		4	Retain	

Select the driver with communication card type.To accommodate different communication protocol processing within the drive.

PnA.01	Baud rate		Factory default	6005
	Setting range	Single digits: MODBUS 0: 300BPS 1: 600BPS 2: 1200BPS 3: 2400BPS 4: 4800BPS 5: 9600BPS 6: 19200BPS 7: 38400BPS 8: 57600BPS 9: 115200BPS		
		Ten digits: Retain		
		Hundred digit: Retain		
		Thousand digit: CAN.LINK Baud rate 0: 20Kbps 1: 50Kbps 2: 100Kbps 3: 125Kbps 4: 250Kbps 5: 500Kbps 6: 1M		

This parameter is used to set the data transfer rate between the host computer and the driver.Note that the baud rate set by the host and driver must be the same, otherwise, the communication cannot proceed.The higher the baud rate, the faster the communication speed.

PnA.02	Data format	Factory default	0

	Setting range	0	No check: data format <8,N,2>
		1	Even checking: data format<8,E,1>
		2	Odd check: data format<8,O,1>
		3	No check: data format<8-N-1>

The data format set by the host computer and the drive must be consistent, otherwise, the communication cannot proceed.

PnA.03	The machine address	Factory default	1
	Setting range	1~247, 0 is broadcast address	

The data format set by the host computer and the drive must be consistent, otherwise, the communication cannot proceed.

The uniqueness of the local address (except the broadcast address) is the basis for point-to-point communication between the host computer and the drive.

PnA.04	Response latency	Factory default	2ms
	Setting range	0~20ms	

Response delay: refers to the intermediate time between the end of the data received by the driver and the data sent to the upper computer. If the response delay is less than the processing time of the system, the response delay shall be subject to the processing time of the system. If the response delay is longer than the processing time of the system, the system shall delay to wait until the response delay time is up before sending data to the computer.

PnA.05	Communication timeout	Factory default	0.0 s
	Setting range	0.0 s (invalid), 0.1~60.0s	

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

When the function code is set to a valid value, if the interval between one communication and the next communication exceeds the communication timeout, the system will report the communication failure error (Err16). Usually, this is set to invalid. If in the continuous communication system, set secondary parameters, you can monitor the communication status.

PnA.06	Data transfer format selection	Factory default	01
	Setting range	Single digit: MODBUS 0: Non-standard MODBUS protocol 1: Satndard MODBUS protocol	
		Ten digit: Retain	

PnA.06=01: Choose standard MODBUS protocol.

When reading commands, the number of bytes returned from the slave machine is one byte more than the standard MODBUS protocol. Please refer to the "5 communication data structure" section of this protocol for details.

PnA.07	Communication read current res		Factory default	0
	Setting range	0	0.01A	
		1	0.1A	

The output unit used to determine the current value when a communication reads the output current