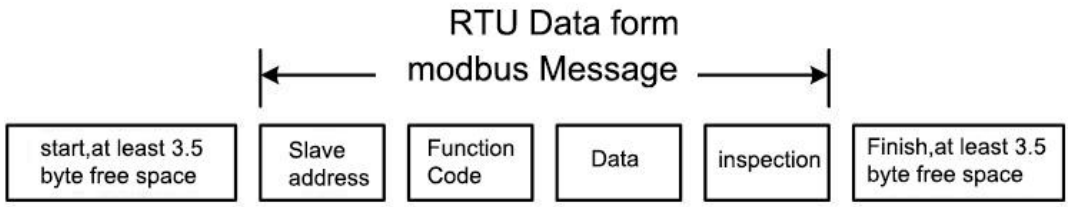
Modbus communication

Max500 adopts the international standard Modbus communication protocol and supports master-slave communication in RTU format. Users can realize centralized control through PC/PLC, screen and other upper computers (setting inverter control commands, operating frequency, modification of related function code parameters, monitoring of inverter working status and fault information, etc.) to meet specific application requirements .

一、 Communication frame structure and function code parameter address reading and writing rules

1. Communication frame structure
The Modbus protocol communication data format of the inverter is RTU (Remote Terminal Unit) mode



Standard structure of RTU frame:

Frame header START	Idle with more than 3.5 character transmission time
Slave address ADR	Mailing address range: 1 ~ 247;
Command code CMD	03: read slave parameters; 06: write slave parameters
Function code address H	The internal parameter address of the inverter is expressed in hexadecimal; it is divided into function code type and non-function code type (such as running state parameters,
Function code address L	Run commands, etc.) parameters, etc., please refer to the address definition; when transmitting, the high byte is first and the low byte is last.
Number of function codes H	
Number of function codes L	The number of function codes read in this frame, if it is 1, it means to read 1 function code. When transmitting, high byte first, low byte
Data H	In the back.
Data L	
CRC CHK low bit	The response data, or the data to be written, is transmitted with the high byte first and the low byte last.
CRC CHK high bit	
END	Detection value: CRC16 check value. When transmitting, the low byte is in front and the high byte is in the back. For the calculation method, please refer to the CRC calibration in this section.

1. Function code parameter address read and write rules

Use function code group number and label as parameter address expression rule:

High byte: F0～FF (P group), A0～AF (A group), 70～7F (U group); low byte: 00～FF
as:
P0-16 function parameter, its communication address is F010H, where F0H represents the function parameter of group P0, 10H represents the hexadecimal data format of the serial number 16 of the function code in the function group
AC-08 function parameter, its communication address is AC08, where ACH stands for the AC group function parameter, 08H stands for the serial number of the function code in the function group
8 hexadecimal data format
Note: PF group: can neither read the parameters nor change the parameters; U group: can only read and cannot change the parameters.
Some parameters cannot be changed when the inverter is in the running state; some parameters cannot be changed no matter what state the inverter is in; to change the function code parameters, pay attention to the parameter range, unit, and related instructions.

Function code group number	Correspondence access address	Communication to modify the function code in RAM
P0～PE group	0xF000 ～ 0xFEFF	0x0000 ～ 0x0EFF
A0 ～ AC group	0xA000 ～ 0xACFF	0x4000 ～ 0x4CFF
U0 group	0x7000 ～ 0x70FF	

Note that because the EEPROM is frequently stored, it will reduce the service life of the EEPROM. Therefore, some function codes do not need to be stored in the communication mode, just change the value in the RAM: if it is a P group parameter, to achieve this function, It can be realized as long as the high bit F of the function code address becomes 0.
If it is a group A parameter, to realize this function, it can be realized by changing the high bit A of the function code address to 4; the corresponding function code address is expressed as follows: High byte: 00～0F (P group), 40～4F(Group A) Low byte: 00～FF
For example: function code P3-12 is not stored in EEPROM, the address is expressed as 030C; function code A0-05 is not stored in EEPROM, and the address is expressed as 4005; this address means that only RAM can be written, not read, read , It is an invalid address. For all parameters, the command code 07 can also be used to realize this function.

Inverter parameter and function address description

1. Pd group communication parameter description

Pd-00	Baud rate	Factory value	5005
	Setting range	One's place: MODUBS baud rate (above the one's place is omitted) 0: 300BPS 5: 9600BPS 1: 600BPS 6: 19200BPS 2: 1200BPS 7: 38400BPS 3: 2400BPS 8: 57600BPS	

		4: 4800BPS 9: 115200BPS

This parameter is used to set the data transmission rate between the host computer and the inverter. Note that the baud rate set by the host computer and the inverter must be the same, otherwise, the communication cannot be carried out.

Pd-01	Data Format	Factory value	0
	Setting range	0: No parity: data format <8, N, 1> 1: Even inspection: data format <8, E, 1> 2: Odd parity: data format <8, O, 1> 3: No check: data format <8, N, 2>	

The data format set by the host computer and the inverter must be consistent, otherwise, the communication cannot be carried out.

Pd-02	Local address	Factory value	1
	Setting range	1～247	

The address of this machine is unique (except the broadcast address), which is the basis for realizing the point-to-point communication between the host computer and the inverter.

Pd-03	Response delay	Factory value	2ms
	Setting range	0～20ms	

Response delay: It refers to the intermediate time from the end of the inverter data receiving to the sending of data to the upper computer. If the response delay is less than the system processing time, the response delay is subject to the system processing time. If the response delay is longer than the system processing time, the system will wait after processing the data until the response delay time expires before going to the upper computer. Send data.

Pd-04	Communication timeout	Factory value	0.0 s
	Setting range	0.0 s (invalid) 0.1～60.0s	

MODBUS、ProPibus-DP、CANopen efficient

When the function code is set to 0.0 s, the communication timeout time 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 time, the system will report a communication failure error (Err16). Under normal circumstances, it is set to invalid. If you set this parameter in a continuous communication system, you can monitor the communication status.

Pd-05	Communication protocol selection	Factory value	30
	Setting range	30: Non-standard Modbus protocol 31: Standard Modbus protocol	

Pd-05=31: Select the standard Modbus protocol.
Pd-05=30: Non-standard Modbus protocol. When reading the command, the number of bytes returned by the slave is one byte more than that of the standard Modbus protocol

Pd-06	Communication reading current Resolution	Factory value	0
	Setting range	0：0.01A 1：0.1A	

Used to determine the output unit of the current value when the communication reads the output current.

1. 1. Address description of other functions

a) a) Shutdown/operation parameter section

Parameter address	Parameter description	Parameter address	Parameter description
0X 1000	* Communication setting value (decimal) -10000～10000	0X 1011	PID feedback
0X 1001	Operating frequency	0X 1012	PLC steps
0X 1002	Bus voltage	0X 1013	PULSE input pulse frequency, unit 0.01kHz
0X 1003	The output voltage	0X 1014	Feedback speed, unit 0.1Hz
… …See the manual for details			

The U0 parameter group and related addresses can be read when monitoring the inverter.

Function code	Name	Smallest unit	mailing address
U0-00	Operating frequency (Hz)	0.01Hz	0X 7000
U0-01	Setting frequency (Hz)	0.01Hz	0X 7001
U0-02	Bus voltage (V)	0.1V	0X 7002
U0-03	Output voltage (V)	1V	0X 7003
U0-04	Output current (A)	0.01A	0X 7004
U0-05	Output power (kW)	0.1kW	0X 7005
U0-06	Output torque (%) Percentage of motor rated torque	0.1%	0X 7006
U0-07	X input state	1	0X 7007
U0-08	Output state	1	0X 7008
U0-09	AI1 voltage (V)	0.01V	0X 7009
U0-10	AI2 voltage (V)	0.01V	0X 700A
U0-11	AI3 voltage (V)	0.01V	0X 700B
……See the manual for details			

Notice:

The communication setting value is the percentage of the relative value, 10000 corresponds to 100.00%, -10000 corresponds to -100.00%. For the frequency dimension data, the percentage is relative to the maximum frequency (P0-10); for the torque dimension data, the percentage is relative to P2-10 (the torque upper limit digital setting).

b) Control commands

When P0-02 (command source) is selected as 2: communication control, the host computer can realize the control of the inverter's start and stop and other related commands through the communication address. The control commands are defined as follows:

Command word address	Command function
0X 2000	0001: Forward running 0002: Reverse running 0003: Forward jog 0004: Reverse jog 0005: Free stop 0006: Decelerate to stop 0007: fault reset

c) Digital output terminal control

When the digital output terminal function is selected as 20: communication control, the host computer can realize the control of the inverter's digital output terminal through the communication address, which is defined as follows:

Digital output terminal control pass News address	Command content
0X 2001	BIT0: Y1 output control BIT1: Y3 output control BIT2: RELAY1 output control BIT3: RELAY2 output control BIT4: Y2 output control

Analog output AO, AO2, high-speed pulse output Y2 control

When the analog output AO, AO2, high-speed pulse output Y2 output function is selected as 12: communication setting, the upper computer can realize the control of the inverter's analog and high-speed pulse output through the communication address, which is defined as follows:

Output control communication address		Command content
AO1	0X2002	0～7FFF means 0%～100%
AO2	0X2003	
Y2	0X2004	

d) Inverter running status

When the communication reads the running status of the inverter, the communication address is fixed at 3000H, and the upper computer can obtain the current running status information of the inverter by reading the address data, which is defined as follows:

Inverter running status communication address	Read status word definition
0X 3000	1: Forward running 2: Reverse running 3: Shutdown

e) Parameter initialization

This function needs to be used when it is necessary to realize the parameter initialization operation of the inverter through the upper computer.

If PP-00 (user password) is not 0, you need to verify the password through communication first. After the verification is passed, the upper computer will initialize the parameters within 30 seconds.

Password	Enter the content of the

address	password
1F00	*****

The communication address for user password verification is 1F00H. Write the correct user password directly to this address to complete the password verification.

The communication address for parameter initialization is 1F01H, and its data content is defined as follows:

Parameter initialization communication address	Command function
0X 1F01	1: Restore factory parameters 2: Clearly record information 4: Restore user backup parameters 501: Backup user current parameters

f) Inverter fault description:

Inverter fault	Inverter fault
0x8000	0000: No fault 0015: Abnormal reading and writing of parameters 0001: reserved 0016: inverter hardware failure 0002: Accelerating over current 0017: Short-circuit fault of the motor to the ground 0003: Deceleration over current 0018: reserved 0004: Constant speed over current 0019: reserved 0005: Accelerating over voltage 001A: Running time reached 0006: Deceleration over voltage 001B: User-defined fault 1 0007: Constant speed over voltage 001C: User-defined fault 2 0008: Buffer resistor overload fault 001D: Power-on time reached 0009: Under voltage fault 001E: Load drop 000A: Inverter overload 001F: PID feedback lost during operation 000B: Motor overload 0028: Fast current limit overtime fault 000C: Input phase loss 0029: Switching motor failure during operation 000D: Output phase loss 002A: Speed deviation is too large 000E: Module overheating 002B: Motor overspeed 000F: External fault 002D: Motor over temperature