

SR MODBUS RTU Protocol Operating Guide

1. SR MODBUS RTU Communication Parameter Settings

Item	Content
Communication parameters	9600bps or19200bps\8bits \1stop\ None
Communication port	RS232/485 communication port
Communication mode	RS232/485
Communication distance (max.)	15m/500m (twisted-pair cable)

2. SR MODBUS RTU Data Format

Host machine: PLC address byte (one byte) + MODBUS request frame + CRC
(The PLC response timeout of host machine is suggested to be 2 seconds.)

PLC response: PLC address byte (one byte) + MODBUS response frame + CRC

Notes: 1. The content of [...] occupies two bytes;

2. * indicates invalid;

3. PBCD compressed BCD format;

4. When setting station number and baud rate, PLC needs to be restarted.

5. When communicating with SR via Modbus, if it is necessary to program the multifunctional clock switch, please set the maximum value in the program to it, or an error will occur during communication.

6. When write or read dual-register value, the high word is prior to the low word

3. MODBUS RTU Address table

No	Type	Address range	Modbus address range	Command code	Properties
1	Input I (I0-I127)	0x0000- 0x007F	0x0000- 0x007F	0x01	Read only
2	Output Q (Q0-Q127)	0x0100- 0x017F	0x0100- 0x017F	0x01	Read only
3	M(M0-MI127)	0x0200- 0x027F	0x0200- 0x027F	0x01	Read only
4	Virtual key V	0x1300-0x137F	0x1300-0x137F	0x01	Read only
5	Remote control Y (Y1-Y6)	0x1301- 0x1306	0x1300- 0x1306	0x01	Read only
8	Timer operating value The maximum data length:2 words; Data content: [****11111 11111111] [11111111 11111111] indicates invalid 1 indicates valid data; Data range: 0-536870911	0x2000- 0x23FF	Occupied block number * 2 +0x2000	0x03	Read 2 register only

	(10ms)				
9	Counter operating value The maximum data length:2 words; Data content: [*****1111 11111111] [11111111 11111111] Data format:HEX;	0x2400- 0x27FF	Occupied block number *2+0x2400	0x03	Read 2 register only
10	Timer parameter The maximum data length: 1 word; Data content: PBCD; Integral part; Decimal part; Data range: 00.00 - 99.99	0x2800-0x2BFF	Occupied block number * 2+0x2800	0x03/0x06/ 0x10	Read/Write single register
11	Counter parameter The maximum data length: 2 words; Data content: [***** 11111111 [11111111 11111111]	0x2C00-0x2FFF	Occupied block number * 4+0x2C00	0x03/0x06/0x10	Read/Write
12	Analog comparison parameter; The maximum data length: 1 word; Data range: 0-65535 HEX	0x3000- 0x33FF	Occupied block number * 2 +0x3000	0x03/0x06/ 0x10	Read/Write
13	Timer comparison parameter; The maximum data length:1 word; Data content: PBCD; Integral part; Decimal part; Data range: 00.00 - 99.99	0x3400- 0x37FF	Occupied block number * 2 +0x3400	0x03/0x06/ 0x10	Read/Write

14	Counter comparison parameter; The maximum data length: 2 words; Data content: [**** **** 11111111] [11111111 11111111]	0x3800-0x3BFF	Occupied block number * 4 +0x3800	0x03/0x06/ 0x10	
15	Multifunctional clock ON parameter The maximum data length: 2 words; Hour/Minute; Second/Arbitrary value; Data content: [**** **** 11111111] [11111111 11111111]	0x3C00-0x3FFF	Occupied block number * 4 +0x3C00	0x03/0x06/ 0x10	Read/Write dual-register
16	Multifunctional clock OFF parameter The maximum data length: 2 words; Hour/Minute; Second/Arbitrary value; Data value: Data format : PBCD; [**** **** 11111111] [11111111 11111111]	0x4000-0x43FF	Occupied block number * 4 +0x4000	0x03/0x06/ 0x10	Read/Write dual-register
17	Phone number The maximum data length: 8 words; Data content: please refer to the introduction to operation for details;	0x4400-0x4BFF	Occupied block number * 16 +0x4400	0x03/0x06/0x1 0	Read/Write several registers

18	Playing voice message The maximum data length is: 1 word; Data content: Read: 00**-99** Write: 0000-0099 Data format: PBCD When 15** is read, which indicates the 15 th section phonetic When 0015 is written, which indicates the 15 th section	0x4C00-0x4CFF	0x4C00-0x4CFF	0x03/0x06/0x10	Read/Write single register
19	PLC station number The maximum data length: 1 word; Data content: 0000-00FF Data format: HEX	0x4D00	0x4D00	0x03/0x06	Read/Write
20	PLC baud rate The maximum data length: 1 word; Data content: **00-**FF Data format: HEX Please refer to the introduction to operation for details.	0x4D01	0x4D01	0x03/0x06	Read/Write

4. Introduction to operation

4.1. Choose the corresponding communication ports, and set the communication parameters.

4.2. Read the baud rate of SR. **00 indicates the baud rate is read or set as 9600dps; other values indicate the baud rate is read or set as 19200.

The format of SR request data and response data from master station is shown as following list.

Query message	
Field Name	Example (Hex)
Device address	01
Function code	03
Register address Hi	4D
Register address Lo	01
NO.of registers Hi	00
NO.of registers Lo	01
CRC Lo	C2
CRC Hi	A6

Response message	
Field Name	Example (Hex)
Device address	01
Function code	03
Count of returned bytes	02
Register data Hi (4D01)	00
Register data Lo (4D01)	00
CRC Lo	B8
CRC Hi	44

4.3. Read SR address

The format of SR request data and response data from master station is shown as following list.

Query message	
Field Name	Example (Hex)
Device address	00
Function code	03
Register address Hi	4D
Register address Lo	00
NO. of registers Hi	00
NO. of registers Lo	01
CRC Lo	92
CRC Hi	B7

Response message	
Field Name	Example (Hex)
Device address	01
Function code	03
Count of returned bytes	02
Register data Hi (4D01)	00
Register data Lo (4D01)	01
CRC Lo	79
CRC Hi	84

4.4. Read SR input I (I0-I127)

For example: Read the status of 8 consecutive inputs from I0.

The status of input I0-I7 is: 0 1 0 0 0 0 0 0

The format of SR request data and response data from master station is shown as following list.

Query message	
Field Name	Example (Hex)
Device address	00
Function code	01
Starting address of coil Hi	00
Starting address of coil Lo	00
Quantity of coils Hi	00

Response message	
Field Name	Example (Hex)
Device address	01
Function code	01
Quantity of returned bytes	01
Data(coil M0-M127)	02
CRC Lo	D0

Quantity of coils Lo	08
CRC Lo	3D
CRC Hi	CC

CRC Hi	49


4.5 . Read input value of SR analog. If the value of IA1 is 5V, the corresponding MODBUS address is 1A11, and the value of single register is read.
the format of SR request data and response data from master station is shown as following list.

Query message	
Field Name	Example (Hex)
Device address	
Function code	
Starting address of register Hi	
Starting address of register Lo	
NO.of registers Hi	00
NO. of registers Lo	01
CRC Lo	82
CRC Hi	D7

Response message	
Field Name	Example (Hex)
Device address	01
Function code	03
Count of returned bytes	02
Data Hi (register 1A11)	00
Data Lo (register 1A11)	31
CRC Lo	84
CRC Hi	44

Note: The real voltage value is read as $4.9V = (3*16+1)/10$.




4.6. Read the operation value of timer  in SR program. If the operation value of B3 is 29.20S, and the corresponding MODBUS address is 2006, the values of two consecutive registers are read.
The format of SR request data and response data from master station is shown as following list.

Query message	
Field Name	Example (Hex)
Device address	01
Function code	03
Starting address of register Hi	20
Starting address of register Lo	06
NO.of registers Hi	00
NO. of registers Lo	02
CRC Lo	2F
CRC Hi	CA

Response message	
Field Name	Example (Hex)
Device address	01
Function code	
Count of returned bytes	04
Data Hi (register 2006)	-
Data Lo (register 2006)	00
Data Hi (register 2007)	0B
Data Lo (register 2007)	68
CRC Lo	FC
CRC Hi	ED



4.7. Read the set value of timer  in SR program. If the set value of B3 is 50.00S, and the corresponding MODBUS address is 2806, the value of single register is read.
The format of SR request data and response data from master station is shown as following list.

Query message	
Field Name	Example (Hex)
Device address	01
Function code	
Starting address of register Hi	28
Starting address of register Lo	06
Quantity of registers Hi	00
Quantity of registers Lo	01
CRC Lo	6D
CRC Hi	AB


Response message	
Field Name	Example (Hex)
Device address	01
Function code	
Count of returned bytes	02
Data Hi (register 2806)	50
Data Lo (register 2806)	00
CRC Lo	84
CRC Hi	44

Set the value of timer to be 34.00S, and the format of SR request data and response data from master station is shown as following list.

Query message	
Field Name	Example (Hex)
Device address	01
Function code	
Starting address of register Hi	28
Starting address of register Lo	06
Data Hi (register 2806)	34
Data Lo (register 2806)	00
CRC Lo	D7
CRC Hi	6B

Response message	
Field Name	Example (Hex)
Device address	01
Function code	
Starting address of register Hi	28
Starting address of register Lo	06
Data Hi (register 2806)	34
Data Lo (register 2806)	00
CRC Lo	D7
CRC Hi	6B




- 4.8. Read the current value of counter  in SR program. If the current value of B4 is 131, and the corresponding MODBUS address is 2408, the values of two consecutive registers are read, and the data format is HEX.

The format of SR request data and response data from master station is shown as following list.

Query message	
Field Name	Example (Hex)
Device address	01
Function code	
Starting address of register Hi	24
Starting address of register Lo	08
No. of registers Hi	00
No. of registers Lo	02
CRC Lo	4E
CRC Hi	09

Response message	
Field Name	Example (Hex)
Device address	01
Function code	
Count of returned bytes	04
Data Hi (register 2408)	-
Data Lo (register 2408)	00
Data Hi (register 2409)	00
Data Lo (register 2409)	83
CRC Lo	BB



- 4.9. Read the set value of counter  in SR program. If the set value of B4 is 16, and the corresponding MODBUS address is 2C10, the values of two consecutive registers are read and written.

When read the set value of counter, the format of SR request data and response data from master station is shown as following list.

Query message	
Field Name	Example (Hex)
Device address	01
Function code	
Starting address of register Hi	20
Starting address of register Lo	10
NO.of registers Hi	00
NO.of registers Lo	02
CRC Lo	CD
CRC Hi	5E

Response message	
Field Name	Example (Hex)
Device address	01
Function code	
Count of returned bytes	04
Data Hi (register 2C10)	-
Data Lo (register 2C10)	00
Data Hi (register 2C11)	00
Data Lo (register 2C11)	16
CRC Lo	7B
CRC Hi	FD


When set the value of counter to be 579, the format of SR request data and response data from master station is shown as following list.

Query message	
Field Name	Example (Hex)
Device address	01
Function code	
Starting address of register Hi	2C
Starting address of register Lo	10
NO.of registers Hi	00
NO. of registers Lo	02
Count of written bytes	04
Data Hi (register 2C10)	00
Data Lo (register 2C10)	00
Data Hi (register 2C11)	05
Data Lo (register 2C11)	79
CRC Lo	FC
CRC Hi	D0

Response message	
Field Name	Example (Hex)
Device address	01
Function code	10
Starting address of register Hi	2C
Starting address of register Lo	10
NO.of registers Hi	00
NO. of registers Lo	02
CRC Lo	48
CRC Hi	9D

- 4.10. When using MODBUS protocol to modify the ON/OFF parameters of multifunctional clock, the function block number of multifunctional clock has to be set as the maximum block number used in the program.



Read the ON parameter of multifunctional clock  in SR program. If the ON time is

15:35:45, and the corresponding MODBUS address is 3C28, the values of two consecutive registers are read.

The format of SR request data and response data from master station is shown as following list.

Query message	
Field Name	Example (Hex)
Device address	01
Function code	
Starting address of register Hi	3C
Starting address of register Lo	28
NO.of registers Hi	00
NO. of registers Lo	02
CRC Lo	48
CRC Hi	53

Response message	
Field Name	Example (Hex)
Device address	01
Function code	
Count of returned bytes	04
Data Hi (register 3C28)	15
Data Lo (register 3C28)	35
Data Hi (register 3C29)	45
Data Lo (register 3C29)	-
CRC Lo	DC
CRC Hi	A1




Read the ON parameter of multifunctional clock in SR program. If the ON time is 18:47:26, and the corresponding MODBUS address is 3C28, the values of two consecutive registers are read.

The format of SR request data and response data from master station is shown as following list.

Query message	
Field Name	Example (Hex)
Device address	01
Function code	
Starting address of register Hi	3C
Starting address of register Lo	28
NO.of registers Hi	00
NO. of registers Lo	02
Count of written bytes	04
Data Hi (register 2C10)	18
Data Lo (register 2C10)	47
Data Hi (register 2C11)	26
Data Lo (register 2C11)	00
CRC Lo	5D
CRC Hi	C5

Response message	
Field Name	Example (Hex)
Device address	01
Function code	10
Starting address of register Hi	3C
Starting address of register Lo	28
NO.of registers Hi	00
NO. of registers Lo	02
CRC Lo	CD
CRC Hi	90



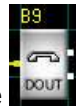
4.11. Read the phone number set through dialing function block , if the phone number is 025 52801556-223, the corresponding MODBUS address is 4490, the values of eight consecutive registers are read.

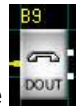
The format of SR request data and response data from master station is shown as following list.

Query message	
Field Name	Example (Hex)
Device address	01
Function code	
Starting address of register Hi	44
Starting address of register Lo	90
NO.of registers Hi	00
NO. of registers Lo	08
CRC Lo	5D
CRC Hi	C5

Response message	
Field Name	Example (Hex)
Device address	01
Function code	03
Quantity of responded bytes	10
Data Hi (register 4490)	02
Data Lo (register 4490)	55
Data Hi (register 4491)	28
Data Lo (register 4491)	01
Data Hi (register 4492)	55
Data Lo (register 4492)	6B
Data Hi (register 4493)	22
Data Lo (register 4493)	3A
Data Hi (register 4494)	00
Data Lo (register 4494)	00
Data Hi (register 4495)	00
Data Lo (register 4495)	00
Data Hi (register 4496)	00
Data Lo (register 4496)	00
Data Hi (register 4497)	00
Data Lo (register 4497)	00
CRC Lo	47
CRC Hi	46

The maximum data length is 8 words, and 30bits phone numbers can be read (including 0B,0A), in which each B indicates waiting one time occupies 2 seconds, and A indicates end. The data format is PBCD.



- 4.12. Read and write voice message , which is set as the fifth section in program. The corresponding MODBUS address is 4C09, and the single register is read. The low bits of the data are invalid.

Query message	
Field Name	Example (Hex)
Device address	01
Function code	
Starting address of register Hi	4C
Starting address of register Lo	09
NO.of registers Hi	00
NO. of registers Lo	01
CRC Lo	42
CRC Hi	98

Response message	
Field Name	Example (Hex)
Device address	01
Function code	
Count of returned bytes	02
Data Hi (register 4C09)	05
Data Lo (register 4C09)	-
CRC Lo	3B
CRC Hi	19