APPENDIX A：APB MODBUS RTU EXTEND Introduction

1. APB MODBUS Protocol Address Type and Function Code List (Note1)

PLC Parameter	Address Range	R/W Attribute	Function Code	Operation Type	Remarks
I0~I127	100 --- 1FF	R	0x01	0x（位）	**Read input status I**
Q0~Q255	200 --- 2FF	R/W	0x01，0x05	0x（位）	**Read and write output status Q**
M0~M1999	2600 --- 35FF	R/W	0x01，0x05	0x（位）	**Read and write M status**
AI0~AI15	4600 --- 467F	R	0x03	4x（字）	**Read analog input AI**
AQ0~AQ15	4680 --- 46FF	R/W	0x03，0x10	4x，5x（字）	**Read and write analog output AQ**
AM0~AM127	4700 ---47FF	R/W	0x03，0x10	4x，5x（字）	**Read and write analog register AM**
D0~D511	4800 --- 67FF	R/W	0x03，0x10	5x（字）	**Read and write register D**
	8000 --- BFFF	R/W	0x03，0x10	4x，5x（字）	**Read and write function block parameters (Note2)**
	C000 --- FFFF	R	0x03	4x（字）	**Read the block running value (Note3)**
	Clock switch parameters` address (calculated independently)	R/W	0x41，0x42		**Read and write the parameters of clock switch block (Note4)**
PLC address	7FFF	R/W	0x03，0x10	4x，5x（字）	**Read and write PLC address (Note5)**
PLC status	0	R	0x01	0x（位）	**Read PLC status (Note6)**
PLC time （year month day hour minute Second）	7FF9 --- 7FFE	R/W	0x03，0x10	4x，5x（字）	**Read and write real-time clock RTC (Note7)**

Note1: Except for clock function block, all read and write operations of APB MODBUS RTU EXTEND communication protocol are standard MODBUS RTU commands, which can communicate with devices that support MODBUS RTU.

Communication parameters: 9600bps, 8 data bits, 1 stop bit, and no parity.

The time interval between frames is 50ms.

Note2: When reading and writing function block parameters, the address calculation formula is: (block number * 32 + block parameter number * 4) +

0x8000

The block parameter is numbered from 0. They are 0, 1, 2, 3…… respectively.

Note3: When reading the block running value, the address calculation formula is: (block number * 32 + block parameter number * 4) + 0xC000

Now only one running value for each block, and the parameter number is 0.

Note4: The address calculation formula for clock switch block is: block number * 256 + group number * 8

The group is numbered from 0, and 32 groups at most.

Note5: When reading and writing PLC address, the MODBUS address range is from 0 to 254, and only low byte of a word is valid.

Note6: When reading PLC status, only the bit0 at address0 can be read now to indicate running or stop status of PLC. 1: running, 0: stop.

Note7: When reading real-time clock, at most 4 words can be read, and 4 words must be written when writing real-time clock. Writing format is: year, month, day, week, hours, minutes and seconds. Sunday~ Saturday is written as 00~ 06.

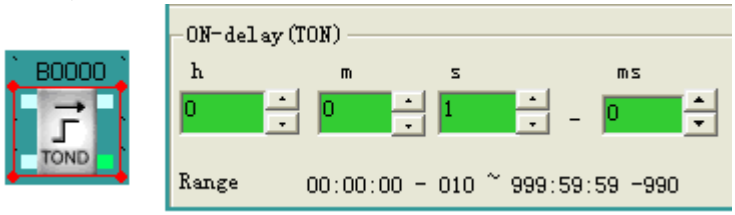
Example: If write 2009-12-15 Friday 10:40:30, then the request frame should be: 01 10 7F F9 00 04 08 **20 09 12 15 05 10 40 30** E7 2C.

1. Examples for Read/Write Operation

Example1: Read/Write On-delay Block Parameter

If block number is B0000, and parameter number is 0, then the address is 0x8000 calculated by the formula: 0*32+0*4+0x8000. Parameter value occupies 2 words.

Read on-delay time parameter 1S (1000MS). It is 0000 03E8 in HEX.



When read time parameter, MODBUS RTU command frame should be:

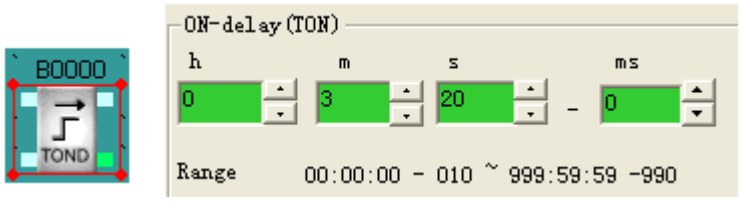
Request Message	
Field Name	Example (Hex)
Device address	01
Function code	03
High byte of the block	80

Response Message	
Field Name	Example (Hex)
Device address	01
Function code	03
The number of returned	04

address	
Low byte of the block address	00
High byte of the block parameter value	00
Low byte of the block parameter value	02
CRC low byte	ED
CRC high byte	CB

bytes	
Parameter value of the block	00
Parameter value of the block	00
Parameter value of the block	03
Parameter value of the block	E8
CRC low byte	FA
CRC high byte	8D

Write on-delay time parameter 3minutes and 20seconds. It is 200000ms, 0003 0D40 in Hex.



When write time parameter, MODBUS RTU command frame should be:

Request Message	
Field Name	Example (Hex)
Device address	01
Function code	10
High byte of the block address	80
Low byte of the block address	00
High byte of the block parameter value	00
Low byte of the block parameter value	02
The number of written bytes	04
Parameter value of the block	00
Parameter value of the block	03
Parameter value of the block	0D

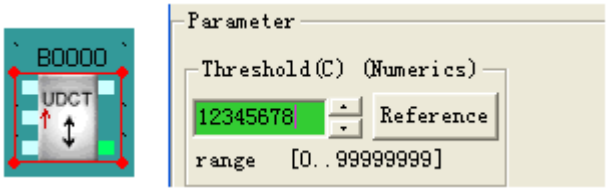
Response Message	
Field Name	Example (Hex)
Device address	01
Function code	10
High byte of the block address	80
Low byte of the block address	00
High byte of the block parameter	00
Low byte of the block parameter	02
CRC low byte	68
CRC high byte	08

Parameter value of the block	40
CRC low byte	ED
CRC high byte	CB

Example2: Read/Write the parameter of universal counter block

If block number is B0000, and parameter number is 0, then the address is 0x8000 calculated by the formula: 0*32+0*4+0x8000. Parameter value occupies 2 words.

Read the universal counter parameter 12345678. It is 00BC 614E (HEX).

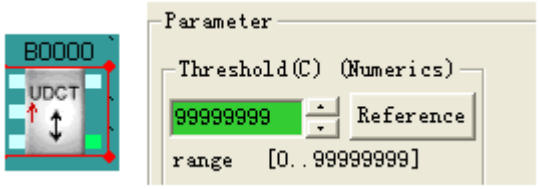


When read counter parameter, MODBUS RTU command frame should be:

Request Message	
Field Name	Example (Hex)
Device address	01
Function code	03
High byte of the block address	80
Low byte of the block address	00
High byte of the block parameter value	00
Low byte of the block parameter value	02
CRC low byte	ED
CRC high byte	CB

Response Message	
Field Name	Example (Hex)
Device address	01
Function code	03
The number of returned bytes	04
Parameter value of the block	00
Parameter value of the block	BC
Parameter value of the block	61
Parameter value of the block	4E
CRC low byte	92
CRC high byte	73

Write the allowed maximum value 9999 9999 to universal counter. It is 05F5 E0FF in HEX.



When write counter parameter, MODBUS RTU command frame should be:

Request Message	Response Message

Field Name	Example (Hex)
Device address	01
Function code	10
High byte of the block address	80
Low byte of the block address	00
High byte of the block parameter value	00
Low byte of the block parameter value	02
The number of written bytes	04
Parameter value of the block	05
Parameter value of the block	F5
Parameter value of the block	E0
Parameter value of the block	FF
CRC low byte	8B
CRC high byte	17

Field Name	Example (Hex)
Device address	01
Function code	10
High byte of the block address	80
Low byte of the block address	00
High byte of the block parameter value	00
Low byte of the block parameter value	02
CRC low byte	68
CRC high byte	08

Example3: Read the parameters of analog monitor

The block number is 5. Its parameters include scale factor, offset value, field value1, and field value2. The parameters numbers are 0, 1, 2, and 3 respectively.

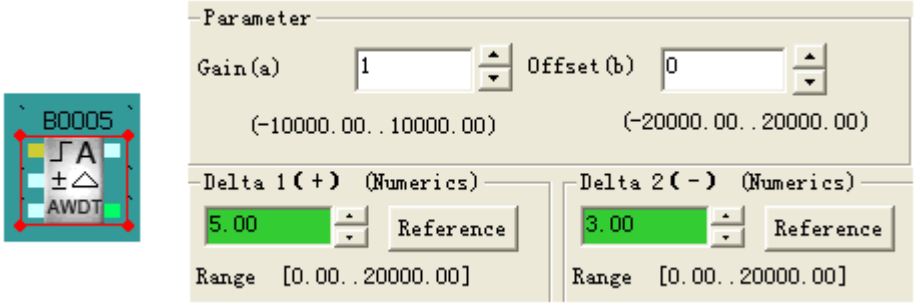
The address is calculated according to the formula: block number * 32 + parameter number * 4 + 0x8000.

Responding address for scale factor is 0x80A0;

Responding address for offset value is 0x80A4;

Responding address for field value 1 is 0x80A8;

Responding address for field value2 is 0x80AC;



When read parameter1, the scale factor of analog monitor block, MODBUS RTU

command frame should be:

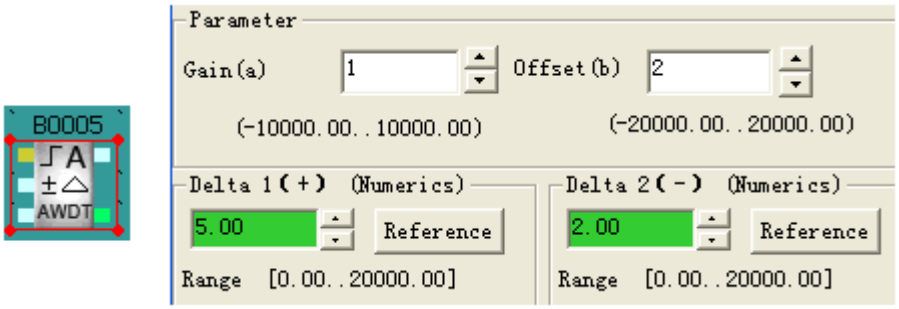
Request Message	
Field Name	Example (Hex)
Device address	01
Function code	03
High byte of the block address	80
Low byte of the block address	A0
High byte of the block parameter value	00
Low byte of the block parameter value	02
CRC low byte	ED
CRC high bite	E9

Response Message	
Field Name	Example (Hex)
Device address	01
Function code	03
The number of returned bytes	04
Parameter value of the block	00
Parameter value of the block	00
Parameter value of the block	00
Parameter value of the block	64
CRC low byte	FB
CRC high bite	D8

The set value 1 in APB software will become 100 times larger than the actual value when it is read through MODBUS protocol.

Example4: Read the running value of analog monitor block

If block number is 5, and parameter number is 0, then the address is 0xC0A0 calculated by the formula: (0*32+0*4) + 0xC000. Parameter value occupies 2 words.



If the input value is 10V, then the theoretical value will be 12 according to the calculation formula: actual value = (Alx· gain value) + offset, and the actual value is 12.01.
The read value through MODBUS protocol is 1201, which is 04B1 in HEX.

MODBUS RTU command frame should be:

Request Message	
Field Name	Example (Hex)

Response Message	
Field Name	Example (Hex)

Device address	01
Function code	03
High byte of the block address	C0
Low byte of the block address	A0
High byte of the block parameter value	00
Low byte of the block parameter value	02
CRC low byte	F8
CRC high bite	E9

Device address	01
Function code	03
The number of returned bytes	04
Parameter value of the block	00
Parameter value of the block	00
Parameter value of the block	04
Parameter value of the block	B1
CRC low byte	38
CRC high bite	87

Example5: Read the running value of off-delay block

If block number is 1, and parameter number is 0, then the address is 0xC020 calculated by the formula: (0*32+0*4) + 0xC000. Parameter value occupies 2 words.

If the running value is 24seconds and 570ms, its decimal value is 24570, and corresponding hexadecimal value is 5FFA.

MODBUS RTU command frame should be:

Request Message	
Field Name	Example (Hex)
Device address	01
Function code	03
High byte of the block address	C0
Low byte of the block address	20
High byte of the block parameter value	00
Low byte of the block parameter value	02
CRC low byte	F9
CRC high bite	C1

Response Message	
Field Name	Example (Hex)
Device address	01
Function code	03
The number of returned bytes	04
Parameter value of the block	00
Parameter value of the block	00
Parameter value of the block	5F
Parameter value of the block	FA
CRC low byte	43

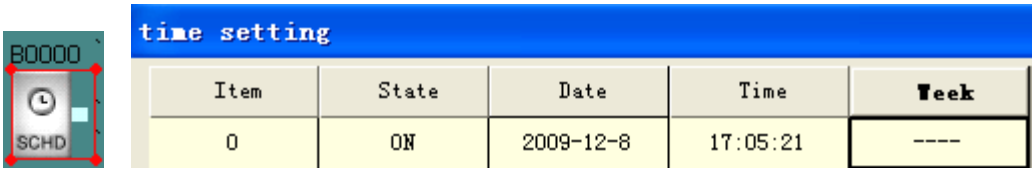
CRC high bite	80

2. Detailed Explanation on Clock Block Operation:

When read/write the clock block parameters, the self-defined function codes are used, and the request/response format is similar to the function codes Ox03, 0x10 of the standard MODBUS RTU.

It is only allowed to read and modify the time of clock block with this command, while the time group cannot be added. In other words, the operation can be executed to the existed time only.

Example1: Read parameters of the clock block



If block number is 0, and read the data of number 0, then the address is calculated by the formula: block number * 256 + group number * 8 = 0. Parameter value occupies 4 words.

If the time data of item 0 is 2009-12-8 17:05:21, and stays in ON state, then MODBUS RTU command frame should be:

Request Message	
Field Name	Example (Hex)
Device address	01
Function code	41
High byte of the block address	00
Low byte of the block address	00
High byte of the block parameter value	00
Low byte of the block parameter value	04
CRC low byte	3C
CRC high bite	06

Response Message	
Field Name	Example (Hex)
Device address	01
Function code	41
The number of returned bytes	08
If clock switch is in ON state, the value is 01; If clock switch is in OFF state, the value is 00;	01
Clock switch mode (see note1)	01
Clock switch date Year	09
Clock switch date Month	12
Clock switch date Day	08
Clock switch date Hour	17
Clock switch date Minute	05
Clock switch date Second	21
CRC low byte	2E
CRC high bite	73

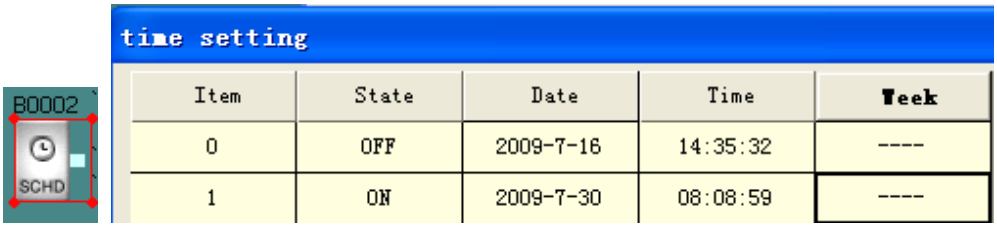
Note1:

Clock switch mode:

01 indicates year
02 indicates month
03 indicates day
04 indicates the fixed date
05~11 indicates from Monday to Sunday
12 indicates from Monday to Thursday
13 indicates from Monday to Friday
14 indicates from Monday to Saturday
15 indicates from Friday to Sunday
16 indicates from Saturday to Sunday

Example1: Modify the data of clock block

The block number is 2, and the clock switch mode is the fixed mode.
Modify the time data of number 1 to be 2009-7-30 08:08:59, and the state is ON.
The address is calculated by the formula: block number * 256 + group number *8.
2 * 256 + 1 * 8=520, and the corresponding hexadecimal value is 0x208.



MODBUS RTU command frame should be:

Request Message	
Field Name	Example (Hex)
Device address	01
Function code	42
High byte of the block address	02
Low byte of the block address	08
High byte of the block parameter value	00
Low byte of the block parameter value	04
The number of written bytes	08
If clock switch is in ON state, the value is 01; If clock switch is in OFF state, the value is 00;	01
Clock switch mode	04

Response Message	
Field Name	Example (Hex)
Device address	01
Function code	42
High byte of the block address	02
Low byte of the block address	08
High byte of the block parameter value	00
Low byte of the block parameter value	04
CRC check low byte	F8
CRC check high byte	7C

Clock switch date Year	09
Clock switch date Month	07
Clock switch date Day	30
Clock switch date Hour	08
Clock switch date Minute	08
Clock switch date Second	59
CRC low byte	7B
CRC high bite	18
