MODBUS Communication Protocol

MS1UE

V2.4.2 · 2025-06-26

Document No.	Document Version	Software Version	Classification
	2.4.2		Public

MODBUS Protocol

1. Overview

This document describes the Modbus communication protocol used by the switching module and related products for communication with supervisory equipment.

2. Scope

This protocol applies to the switching module and related products and provides the basis for their development, testing and use.

3. Reference

Modicon Modbus Protocol Reference Guide PI-MBUS-300 Rev.J

4. Physical Interface

RS485; baud rate: 9600 bit/s; asynchronous serial format: no parity, 8 data bits and 1 stop bit. The data response time is <500 ms, measured from the last byte of the query sent by the host to the first valid byte of the response received from the switching module.

5. Frame Structure

B9	03	30	00	…	3D	5E
Address	Function Code	Data			CRC Checksum	

Modbus RTU mode is used. Each byte is represented by two hexadecimal digits, using 0–9 and A–F.

Address

The switching module address ranges from 1 to 247. The broadcast address is 0x00; the device does not respond to broadcast messages. The USS protocol is used. The host polls the slave devices and initiates every communication transaction. It sends a command to a slave, which returns a response and performs the corresponding action. The slave remains in receive mode except when transmitting a response.

Function Code

The device supports only function codes 0x03 (read data), 0x10 (set user parameters) and 0x16 (bulk read of key data; see Appendix E). The device does not respond to an invalid function code.

Data

Data reported by or written to the device is transmitted by register (data ID). Each register consists of two or more bytes, with an even number of bytes. See Appendix A for the register definitions.

CRC Checksum

The two-byte CRC16 checksum covers the address, function code and data. The transmitting device calculates the CRC and appends it to the frame. A mismatch between the CRC calculated from the received data and the appended CRC indicates an error. See Appendix F for the CRC calculation method.

6. Command Descriptions

Read Data — Function Code 03

The host sends a data query frame. After receiving a valid query, the switching module (referred to below as the device) returns the requested data to the host. The frame formats are shown below.

Query Request Frame

Field Value	Description
B9	Address: 0–247; 0x00 is the broadcast address
03	Function code: 03
18	Starting register address: high byte, then low byte
04	
00	Register count: high byte, then low byte; read 2 registers
02	
CRCLo	CRC low byte
CRCHi	CRC high byte

Normal Response Frame

Field Value	Description	
B9	Address: 0–247	
03	Function code: 03	
08	Response data byte count	
D1HHi	Register 1 bytes, in order: high-high, high-low, low-high, low-low	Register 1: 4 bytes
D1HLo		
D1LHi		
D1LLo		
D2HHi	Register 2 bytes, in order: high-high, high-low, low-high, low-low	Register 2: 4 bytes
D2HLo		
D2LHi		
D2LLo		
CRCLo	CRC low byte	
CRCHi	CRC high byte	

Error Response Frame

Field Value	Description
B9	Address: 0–247
83	Function code: 03
02	Response data byte count
ERRHi	Error information: high byte, then low byte
ERRLo	
CRCLo	CRC low byte
CRCHi	CRC high byte

Note: Setting the most significant bit of the function code to 1 indicates an error.

Write Data — Function Code 10

The host sends a write command. After receiving a valid command, the device writes the data to the specified registers and returns the data unchanged as its response. If the write fails, the device returns an error response frame. The frame formats are shown below.

Write Request Frame

Field Value	Description
B9	Address: 0–247
10	Function code: 10
30	Starting register address: high byte, then low byte
04	
00	Register count: high byte, then low byte; write 3 registers
03	
06	Data byte count
00	Register 1, high byte
AA	Register 1, low byte
1B	Register 2, high byte
12	Register 2, low byte
00	Register 3, high byte
64	Register 3, low byte
CRCLo	CRC low byte
CRCHi	CRC high byte

Note: To ensure reliable communication, no more than 9 bytes may be written to consecutive registers in a single frame.

Normal Response Frame

Field Value	Description
B9	Address: 0–247
10	Function code: 10
18	Starting register address: high byte, then low byte
00	
06	Number of bytes actually written. If the consecutive register range includes read-only registers, this is the sum of the byte counts of all writable registers.
03	Number of registers operated on, corresponding to the write request
CRCLo	CRC low byte
CRCHi	CRC high byte

Error Response Frame

Field Value	Description
B9	Address: 0–247
90	Function code: 10
02	Response data byte count
ERRHi	Error information: high byte, then low byte
ERRLo	
CRCLo	CRC low byte
CRCHi	CRC high byte

Note: Setting the most significant bit of the function code to 1 indicates an error.

Appendix A — Register List (Note 1)

Communication Parameters					
1800H	High byte	Device address	2	R	Ignored by the software when writing
	Low byte	Baud rate: 0: 19200; 1: 9600; 2: 4800; 3: 2400; 4: 1200		R/W	Default: 1 (9600)
1801H	High byte	0: no parity; 2: even parity; 4: odd parity	2	R	
	Low byte	0: 1 stop bit; 1: 2 stop bits			
1802H	Command interval (minimum interval between two commands; default: 10 ms)		2	R/W	Unit: ms
1803H	Response delay (delay from receipt of a command to the device response; default: 20 ms)		2	R/W	Unit: ms
Operating Status					
1804H	Voltage		4	R	2 decimal places; V
1806H	Current (most significant bit = 1 indicates the negative direction; the lower 31 bits contain the absolute value)		4	R	2 decimal places; A
1808H	Power (most significant bit = 1 indicates the negative direction; the lower 31 bits contain the absolute value)		4	R	2 decimal places; kW
180AH	Output energy, current period (continues accumulating unless the host sends a reset command)		4	R/W	2 decimal places; kWh. Write: reset to zero only
180CH	Output energy, previous period (assigned or reset to zero by the user)		4	R/W	2 decimal places; kWh
180EH	Total output energy		4	R	2 decimal places; kWh
1810H	Total operating time		4	R	Unit: min
1812H	Energy settlement time: day, hour, minute (00 DD hh:mm)		4	R/W	
1814H	Date, day of week and time (YYYY.MM.DD WW hh:mm:ss)		8	R/W	
1818H	Temperature at point A (a register value >32767 indicates a negative temperature; temperature = register value − 65536)		2	R	Integer; °C
1819H	Temperature at point B (a register value >32767 indicates a negative temperature; temperature = register value − 65536)		2	R	Integer; °C
181AH-1823H	Reserved				
1824H	Operating status word		2	R	See Appendix C
1825H	Device alarm status word 1 (Note 2)		2	R/W	See Appendix C. Write: reset to zero only
1826H	Device alarm status word 2 (Note 2)		2	R/W	See Appendix C. Write: reset to zero only
1827H	Input energy, current period (continues accumulating unless the host sends a reset command)		4	R/W	2 decimal places; kWh. Write: reset to zero only

1829H	Input energy, previous period (assigned or reset to zero by the user)		4	R/W	2 decimal places; kWh
182BH	Total input energy		4	R	2 decimal places; kWh
182DH	Fault trip count		2	R/W	Write: reset to zero only
182EH~1830H	Reserved				
1831H	Total opening count		4	R/W	Write: reset to zero only
1832H~18B2H	Reserved				
18B3H	Reset all energy values (registers 180AH–180FH and 1827H–182CH)		2	W	Write 0x00AA to reset to zero
183B4H-18FFH	Reserved				
Device Information					
1900H	Manufacturer SN (manufacturer code: 1 byte; production year: 2 bytes; production month: 1 byte; serial number: 4 bytes)		8	R	
1904H	Software Version		4	R	ASCII
1906H	Hardware version		4	R	ASCII
1908H	Production date (YYYY.MM.DD)		4	R	
190AH	Product name		4	R	ASCII
190CH	High byte	Factory-rated current	2	R	Integer; A
	Low byte	Switch width			
190DH	High byte	Rated voltage	2	R/W	Integer; V
	Low byte	Rated current			Integer; A
190EH-1FFFH	Reserved				
2000H	User configuration information 1 (read/write storage only; retained after power-off)		2	R/W	
2001H-2FFFH	Reserved				
Switch Control					
3000H	High byte	Default: 0x00; close priority: 0x01	2	R/W	Close priority: automatically closes after 30 seconds of offline operation
	Low byte	Switch control (0x77 or 0xAA: fully closed; 0x33: standby; 0x55: fully open)			Mechanical version: 0x33 releases the opening handle. Solid-state version: 0x33 opens only the solid-state switch; the handle does not release. Restarting the solid-state version does not change its open/closed state. Both 0x77 and 0xAA close the switch.
3001H	Communication loss alarm delay		2	R/W	Unit: s
3002H	Overcurrent alarm threshold		2	R/W	2 decimal places; A
3003H	High byte	Number of automatic recovery attempts after overcurrent protection	2	R/W	
	Low byte	Automatic recovery interval after overcurrent protection			Unit: min
3004H	Overcurrent protection enable (0x00AA: enable; 0x0055: disable)		2	R/W	
3005H	Overcurrent protection threshold (recovery hysteresis: 1 A)		2	R/W	2 decimal places; A
3006H	Overcurrent protection delay		2	R/W	Unit: 0.1 s

3007H	Undervoltage protection enable (0x00AA: enable; 0x0055: disable)		2	R/W	
3008H	Undervoltage protection threshold (default recovery value: 42 V)		2	R/W	2 decimal places; V
3009H	Undervoltage protection delay		2	R/W	Unit: 0.1 s
300AH~3021H	Reserved				
3022H	High byte	Rental authorization (0x01: authorize; 0x00: revoke authorization)	2	R/W	
	Low byte	One-key function (0x01: enter; 0x00: exit)			
3023H	Overcurrent automatic recovery interval setting 2 (Note 3)		2	R/W	Unit: s
3024H	Undervoltage automatic recovery voltage magnitude setting (Note 4)		2	R/W	2 decimal places; V
3025H~30FEH	Reserved				
30FFH	Energy optical pulse output enable (0xA55A: enable; any other value: disable) (Note 5)		2	R/W	

Note 1 — Consecutive Read Restriction

When using function code 03H to read consecutive registers, the read range must not cross a section marked “Reserved”.

Note 2 — Clearing a Fault After a Protection Trip

If the switch trips due to a protection event, automatic recovery is not configured and the indicator continues flashing, first confirm that the external fault condition has cleared. Then write 0 to the corresponding alarm status word to clear the fault. A closing command may be issued only after the indicator becomes steady.

Note 3 — Overcurrent Automatic Recovery Interval

Register 3023H sets the overcurrent automatic recovery interval in seconds. It is mapped to the minute-based setting in the low byte of register 3003H as follows:

- When the low byte of 3003H is set, 3023H is automatically updated to that value × 60, in seconds.
- When 3023H is set, the low byte of 3003H is automatically updated to the integer part of that value ÷ 60. If the result is 0, it is set to 1.
- The device always uses the value in 3023H as the actual automatic recovery interval.

Existing programs that use the low byte of 3003H require no changes. When using 3023H to configure the interval in seconds, avoid writing to the low byte of 3003H again, as this would overwrite the configured seconds value.

Note 4 — Undervoltage Automatic Recovery Voltage

The undervoltage automatic recovery voltage set in 3024H must be higher than the undervoltage protection threshold set in 3008H.

Note 5 — Energy Optical Pulse Output

Register 30FFH configures the energy optical pulse output for specific customers. When enabled, the normal operating indication is suppressed: the red indicator outputs energy pulses and all other indicators are off. This setting is not retained after power-off and is disabled by default at each power-up.

Appendix B — Message Examples

1. Read the Communication Address

```
18 03 18 00 00 01 BF DC
```

2. Set the Device at Address 0x18 to Standby

```
18 10 30 00 00 01 02 00 33 71 D6
```

Appendix C — Status Word Formats

Communication Error Information (Optional)

bit7	bit6	bit5	bit4	bit3	bit2	bit1	bit0
Data ID error				Baud rate change error	Wrong password or no access	Requested data unavailable	Other errors
bit15	**bit14**	**bit13**	**bit12**	**bit11**	**bit10**	**bit9**	**bit8**
							Invalid data

Note: 0 means the corresponding error has not occurred; 1 means it has occurred. Errors not explicitly defined are classified as “Other errors”.

Operating Status Word (Optional)

bit7	bit6	bit5	bit4	bit3	bit2	bit1	bit0
Fully closed	Standby	Fully open	Emergency switch	Remote switching command			
bit15	**bit14**	**bit13**	**bit12**	**bit11**	**bit10**	**bit9**	**bit8**
Reserved	Battery discharging	Reserved	Switch self-test passed	Offline operation	Rental authorized	Fault protection active	Alarm active

Device Alarm Status Word 1 (Optional)

bit7	bit6	bit5	bit4	bit3	bit2	bit1	bit0
Level 1 overcurrent trip	Reserved	Level 1 overvoltage trip	Under-voltage trip	Reserved	Reserved	Hardware short-circuit fault	Reserved
bit15	**bit14**	**bit13**	**bit12**	**bit11**	**bit10**	**bit9**	**bit8**
Reserved	Reverse-polarity trip	Reserved	Reserved	Point B overtemp. trip	Point A overtemp. trip	Reserved	Level 2 overcurrent trip

Device Alarm Status Word 2 (Optional)

bit7	bit6	bit5	bit4	bit3	bit2	bit1	bit0
Mechanical contact welding alarm	Reserved	Reserved	Point B overtemp. alarm	Point A overtemp. alarm	Overcurrent alarm	Reserved	Reserved
bit15	**bit14**	**bit13**	**bit12**	**bit11**	**bit10**	**bit9**	**bit8**
Comm. loss alarm	Opening/closing failure alarm	Switch address error alarm	Memory error alarm	Reserved	Overcurrent lockout	Reserved	Reserved

Appendix E — Bulk Read of Key Data Packet 1

Use function code 0x16 to read the key data packet in bulk. In the request frame, the starting register address is fixed at 0x1804 and the register count is fixed at 0x0010. The request and response formats are shown below.

Read Request Frame

Field Value	Description
B9	Address: 0–247; 0x00 is the broadcast address
16	Function code: 16
18	Starting register address: high byte, then low byte
04	
00	Register count: high byte, then low byte; read 16 registers
10	
CRCLo	CRC low byte
CRCHi	CRC high byte

Response Frame

Byte Offset	Byte Count	Description
0	1	Address: 0–247; 0x00 is the broadcast address
1	1	Function code, fixed at 16
2	1	Data byte count, fixed at 2A
3~6	4	Voltage; V; 2 decimal places
7~10	4	Current; A; 2 decimal places
11~14	4	Power; kW; 2 decimal places
15~18	4	Output energy, current period; kWh; 2 decimal places
19~22	4	Output energy, previous period; kWh; 2 decimal places
23~26	4	Total output energy; kWh; 2 decimal places
27~30	4	Total input energy; kWh; 2 decimal places
31~32	2	Semiconductor switch temperature; °C; integer
33~34	2	Temperature near the incoming negative terminal; °C; integer
35~36	2	Operating status word
37~38	2	Device alarm status word 1
39~40	2	Device alarm status word 2
41~42	2	High byte: factory-rated current; low byte: switch width
43~44	2	High byte: rated voltage; low byte: rated current
45~46	2	CRC

Appendix F — Bulk Read of Key Data Packet 2

Use function code 0x19 to read the key data packet in bulk. In the request frame, the starting register address is fixed at 0x1804 and the register count is fixed at 0x0010. The request and response formats are shown below.

Read Request Frame

Field Value	Description
B9	Address: 0–247; 0x00 is the broadcast address
19	Function code: 19
18	Fixed at 0x1804
04	
00	Fixed at 0x0010
10	
CRCLo	CRC low byte
CRCHi	CRC high byte

Response Frame

Byte Offset	Byte Count	Description
0	1	Address: 0–247; 0x00 is the broadcast address
1	1	Function code, fixed at 0x19
2	1	Data byte count, fixed at 0x38
3~6	4	Voltage; V; 2 decimal places
7~10	4	Current; A; 2 decimal places
11~14	4	Power; kW; 2 decimal places
15~18	4	Output energy, current period; kWh; 2 decimal places
19~22	4	Output energy, previous period; kWh; 2 decimal places
23~26	4	Total output energy; kWh; 2 decimal places
27~30	4	Input energy, current period; kWh; 2 decimal places
31~34	4	Input energy, previous period; kWh; 2 decimal places
35~38	4	Total input energy; kWh; 2 decimal places
39~42	4	Total opening count
43~44	2	Semiconductor switch temperature; °C; integer
45~46	2	Temperature near the incoming negative terminal; °C; integer
47~48	2	Operating status word
49~50	2	Device alarm status word 1
51~52	2	Device alarm status word 2
53~54	2	High byte: factory-rated current; low byte: switch width
55~56	2	High byte: rated voltage; low byte: rated current
57~58	2	User configuration information 1
59~60	2	CRC

Appendix G — CRC Calculation Code

```
uint16_t CrcCal(uint8_t *data, uint16_t num)
{
   uint8_t   i,j,con1,con2;
   uint16_t  CrcR=0xFFFF, con3=0x00;
   for(i=0; i<num; i++)
   {
      con1=CrcR&0xff;
      con3=CrcR&0xff00;
      CrcR=con3+data[i]^con1;
      for(j=0; j<8; j++)
      {
         con2=CrcR&0x0001;
         CrcR=CrcR>>1;
         if(con2==1)
            CrcR=CrcR^0xA001;
      }
   }
   con1=CrcR>>8;
   con2=CrcR&0xff;
   CrcR=con2;
   CrcR=(CrcR<<8)+con1;
   return CrcR;
}
```