MODBUS PROTOCOL

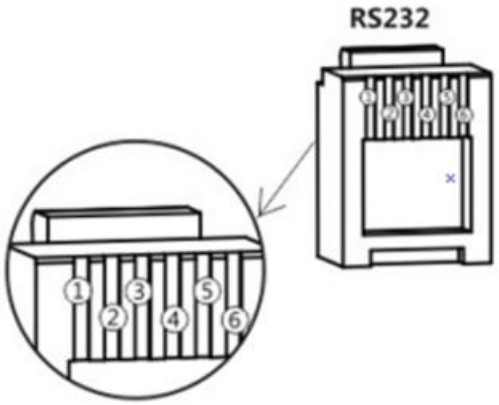
Version	Revision date	Revision contents	Modified by
V3.4	2015-08-06	This version and before,the controller fault information is defined as low 16 bits,and high 16 bits are reserved.	
V3.5	2016-11-09	Changes to the controller fault information is placed in the high 16 bits,and the low 16 bits are reserved.	
V3.6	2017-07-05	In example 4.7,the temperature reading address 0X0102 changed to 0X0103. In example 4.19,the seventh byte of the message is missing the total number of bytes. New:communication line description.	
V3.7	2017-08-09	Add and delete document contents	

Directory

1 Interface specification and serial port configuration information

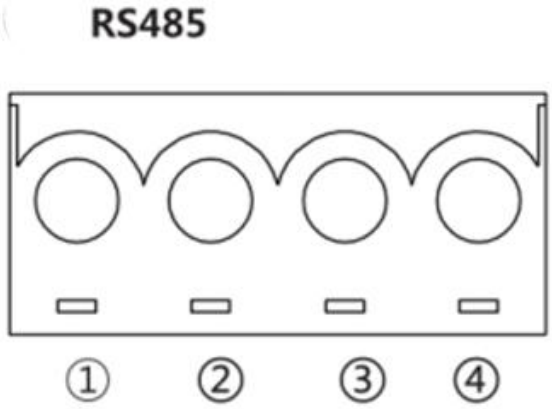
RS232 interface：

Controller communication port RJ12 (6-pin)



No.	Definition
①	Transmitting terminal TX
②	Receiving terminal RX
③	Power supply grounding/signal grounding
④	Power supply grounding/signal grounding
⑤	Power supply positive
⑥	Power supply positive

RS485 interface:



No.	Definition	Parallel operation
①	12V	
②	GND	Black
③	D-	Yellow
④	D+	Red

Serial port rate：9600　　Check bit：NONE　　Data bits：8bit　　Stop bit：1bit

2 Communication protocol format and command analysis

2.1 Format

Start character	Address code	Function code	Data	Error check	End character

2.2 Descriptions

1)start character：>10ms

2)address code：1 byte，range：01H to F7H(decimal 1 to 247)，00His a broadcast address to which all slaves respond but do not return commands.

3)Function code:1 byte

Command name	Accessed data type	Function code	Error code
Read a single or multiple word register	2 bytes	03H	83H
Write a single word register	2 bytes	06H	86H
Write N word registers in a row	2 bytes	10H	90H
Reset to factory defaults	No accessed data	78H	F8H
Clear history	No accessed data	79H	F9H

4)Data:N bytes

5)Error check:2 bytes,it's the CRC checksum of the address code,function code and each byte of the data.

6)End character:>10ms

Note:

1)The data address and the data itself are 2 bytes,with the high byte sent first and then the low byte;for CRC,the low byte is sent first and the high byte is sent next.

2)The error code is the error response function code returned by the client when there is some error in the frame data sent by the server,error code=function code|80H.

2.3 Notes

1)PDU address：(0000 to 0009)/(000A to 001A)/(0100 to 0122)/(E001 to E02D)/(F000 to F3FF),these address segments are not allowed to cross access and modification in the same command!!!

2)The parameters and options of this paper are for the planning and introduction of all the products of this company,so it does not mean that each product has the functions and operation of the following parameters.Refer to the instruction manual for details.

3)Data below suffixed with an "H" are hexadecimal,and the others are decimal.

2.4 Process flow chart

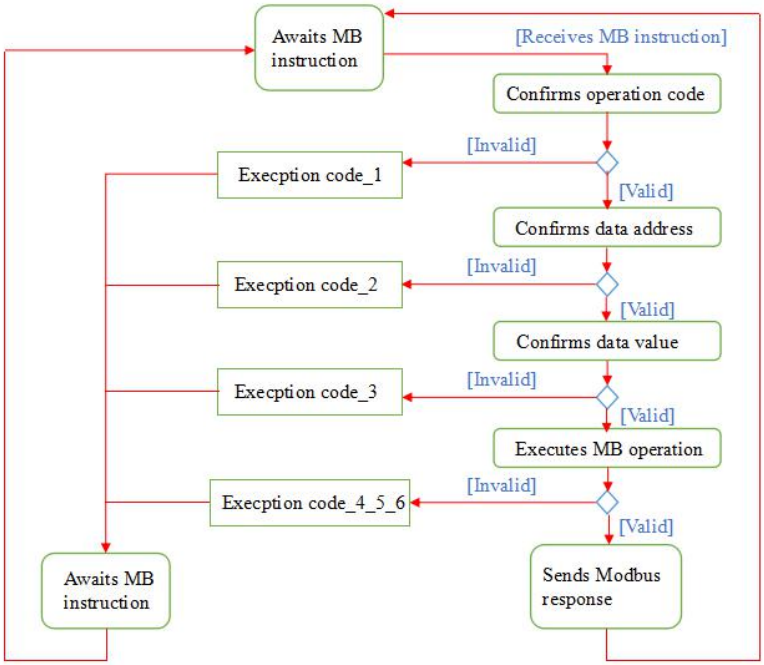


Fig. 8 Modbus process flow chart

1) Exception code descriptions

a、01H -- Function code not supported

b、02H -- PDU start address is not correct or PDU start address + data length

c、03H -- Data length in reading or writing register is too large

d、04H -- Client fails to read or write register

e、05H -- Data check code sent by server is not correct

2）Flow chart of reading register

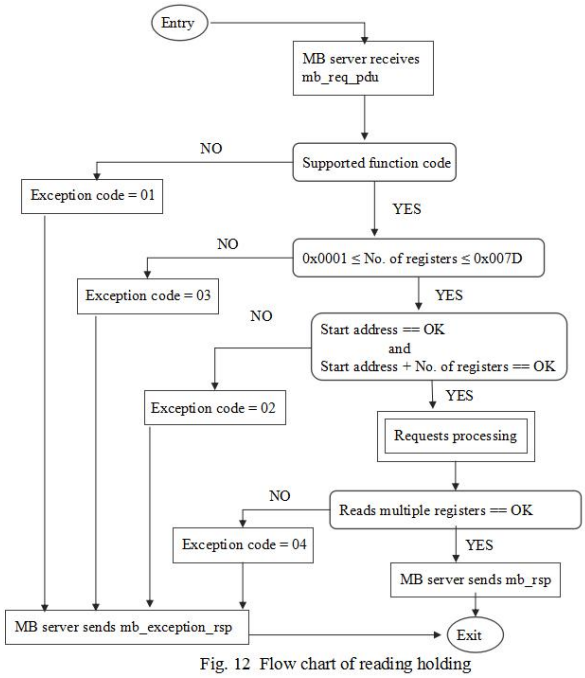


Fig. 12 Flow chart of reading holding

3）Flow chart of writing a single register

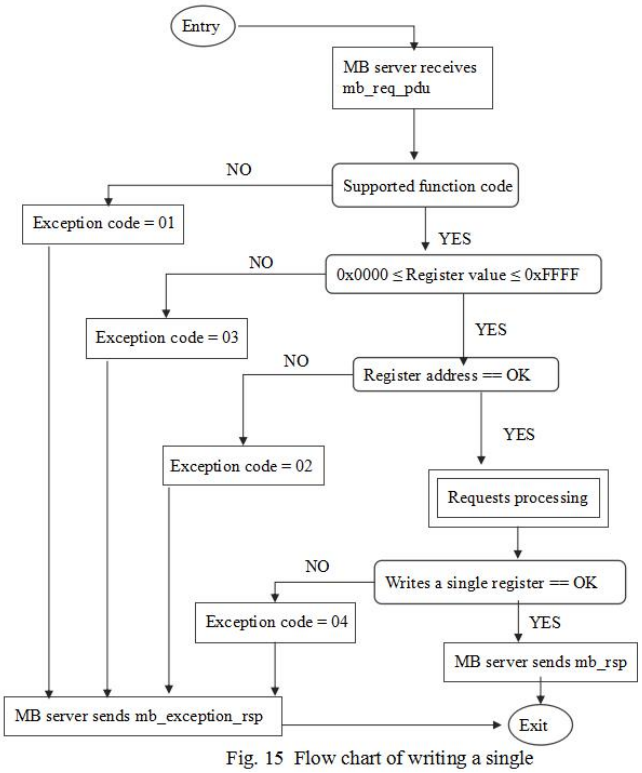


Fig. 15 Flow chart of writing a single

4) Flow chart of writing N registers in a row

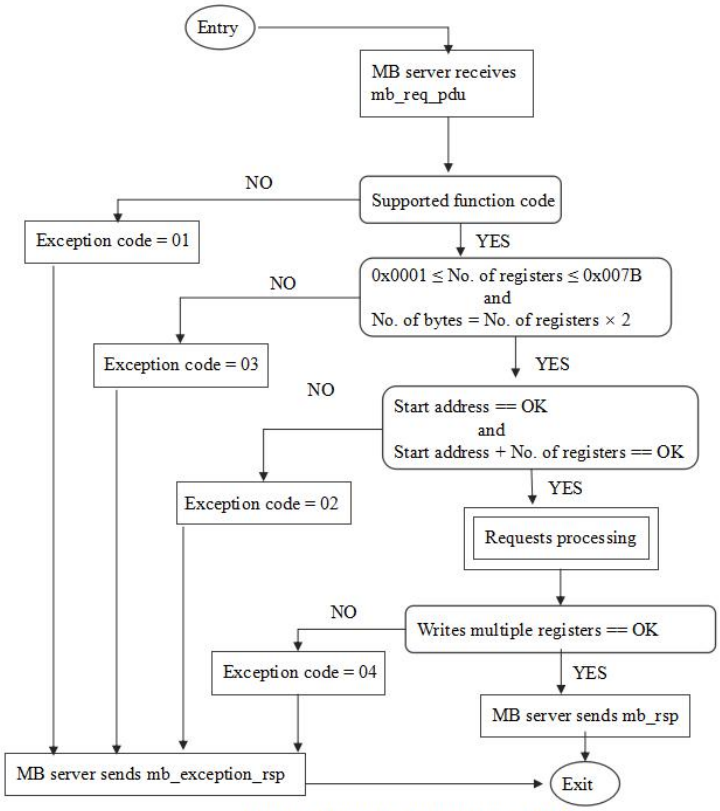


Fig. 17 Flow chart of writing multiple

2.5 Example

1) Read register

Request:

Description	No. of bytes	Command
Device address	BYTE	01H～F7H
Function code	BYTE	03H
Start address	WORD	0000H～FFFFH
No. of read words	WORD	0001H～007DH
Check code	WORD	CRC checksum of all the above bytes

Normal response:

Description	No. of bytes	Command
Device address	BYTE	01H～F7H
Function code	BYTE	03H
Data length	BYTE	01H～FAH
Data content	WORD	Data read out (High byte sent first, low byte sent next)
...	WORD	Data read out (High byte sent first, low byte sent next)
Check code	WORD	CRC checksum of all the above bytes

Exception response:

Description	No. of bytes	Command
Device address	BYTE	01H～F7H
Error code	BYTE	83H
Exception code	BYTE	N (N=1，2，3，4)
Check code	WORD	CRC checksum of all the above bytes

2) Write a single register

Request:

Description	No. of bytes	Command
Device address	BYTE	01H～F7H
Function code	BYTE	06H
Start address	WORD	0000H～FFFFH
Write data in	WORD	0000H～FFFFH
Check code	WORD	CRC checksum of all the above bytes

Normal response:

Description	No. of bytes	Command
Device address	BYTE	01H～F7H
Function code	BYTE	06H
Start address	WORD	0000H～FFFFH
Write data in	WORD	0000H～FFFFH
Check code	WORD	CRC checksum of all the above bytes

Exception response:

Description	No. of bytes	Command
Device address	BYTE	01H～F7H
Error code	BYTE	86H
Exception code	BYTE	N (N=1，2，3，4)
Check code	WORD	CRC checksum of all the above bytes

3) Write N registers in a row

Request:

Description	No. of bytes	Command
Device address	BYTE	01H～F7H
Function code	BYTE	10H
Start address	WORD	0000H～FFFFH
No. of written bytes	WORD	0001H～007DH

No. of written words	BYTE	One time of the No. of bytes
Data content	WORD	Data written in (High byte sent first, low byte sent next)
...	WORD	Data written in (High byte sent first, low byte sent next)
Check code	WORD	CRC checksum of all the above bytes

Normal response:

Description	No. of bytes	Command
Device address	BYTE	01H～F7H
Function code	BYTE	10H
Start address	WORD	0000H～FFFFH
No. of written bytes	WORD	0001H～007DH
Check code	WORD	CRC checksum of all the above bytes

Exception response:

Description	No. of bytes	Command
Device address	BYTE	01H～F7H
Error code	BYTE	90H
Exception code	BYTE	N (N=1，2，3，4)
Check code	WORD	CRC checksum of all the above bytes

4) Reset to factory defaults

Request:

Description	No. of bytes	Command
Device address	BYTE	01H～F7H
Function code	BYTE	78H
Complementary data	WORD	0000H
Complementary data	WORD	0001H
Check code	WORD	CRC checksum of all the above bytes

Normal response:

Description	No. of bytes	Command
Device address	BYTE	01H～F7H
Function code	BYTE	78H
Complementary data	WORD	0000H
Complementary data	WORD	0001H
Check code	WORD	CRC checksum of all the above bytes

Exception response:

Description	No. of bytes	Command
Device address	BYTE	01H～F7H
Error code	BYTE	F8H
Exception code	BYTE	N (N=1，2，3，4)
Check code	WORD	CRC checksum of all the above bytes

5) Clear history

Request:

Description	No. of bytes	Command
Device address	BYTE	01H～F7H
Function code	BYTE	79H
Complementary data	WORD	0000H
Complementary data	WORD	0001H
Check code	WORD	CRC checksum of all the above bytes

Normal response:

Description	No. of bytes	Command
Device address	BYTE	01H～F7H
Function code	BYTE	79H
Complementary data	WORD	0000H

Complementary data	WORD	0001H
Check code	WORD	CRC checksum of all the above bytes

Exception response:

Description	**No. of bytes**	**Command**
Device address	BYTE	01H～F7H
Error code	BYTE	F9H
Exception code	BYTE	N (N=1，2，3，4)
Check code	WORD	CRC checksum of all the above bytes

3 PDU address distribution table

Reserved（20 bytes）								
PDU address	**Bytes**	**R/W**	**Unit**	**Description**	**Data (range)**	**Analysis**	**Return data**	**Parse instance (the data below is decimal data)**
0000H ～ 0009H	20	-		Reserved				
System information（34 bytes）								
000AH	2	R	-	(8 higher bits) max. voltage supported by the system	0CH (decimal 12)	12V	30	The maximum support voltage of the controller system is 48V
					18H (decimal 24)	24V		
					24H (decimal 36)	36V		
					30H (decimal 48)	48V		
					60H (decimal 96)	96V		
					FFH (decimal 255)	Automatic recognition of system voltage		
				(8 lower bits) rated charging current	0AH (decimal 10)	10A	3C	The rated charging current of the controller is 60A
					14H (decimal 20)	20A		
					1EH (decimal 30)	30A		
					2DH (decimal 45)	45A		
					3CH (decimal 60)	60A		
000BH	2	R	-	(8 higher bits) rated discharging current	0AH (decimal 10)	10A	14	The rated discharge current of the controller is 20A
					14H (decimal 20)	20A		
					1EH (decimal 30)	30A		
					2DH (decimal 45)	45A		
					3CH (decimal 60)	60A		
				(8 lower bits) product type	00 (controller) 01 (inverter)		00	Indicates that the product type is the controller type
000CH~ 0013H	16	R	-	Product model				ASCII code
0014H 0015H	4	R	-	Software version			00 01 04 00	The software version of the controller is 01.04.00 (highest byte 00H not used)
0016H 0017H	4	R	-	Hardware version			00 00 05 00	The hardware version of the controller is 00.05.00 (highest byte 00H not used)
0018H 0019H	4	R	-	Product serial number			10 03 00 64	Indicating it's the 100th unit produced in Mar. of 2016

001AH	2	R/W	-	(8 higher bits)Reserved (8 lower bits) device address	1～247		00 01	Indicates that the device address of the controller is 1
Controller dynamic information (7 bytes)								
0100H	2	R	%	(8 higher bits)Reserved (8 lower bits) Battery capacity SOC	0～100	Current battery capacity value	00 37	The battery capacity of SOC is 55 %
0101H	2	R	V	Battery voltage		Battery voltage * 0.1	00 7A	The battery voltage is 12.2V
0102H	2	R	A	Charging current (to battery)		Charging current * 0.01	01 0A	The battery charging current is 2.66A
0103H	2	R	℃	(8 higher bits) Controller temperature (8 lower bits) Battery temperature		b7: sign bit; b0-b6:temperature value	1C 19	The controller temperature is 28℃ The battery temperature is 25℃
0104H	2	R	V	Load dc voltage		Load voltage*0.1	00 7A	The load voltage is 12.2V
0105H	2	R	A	Load dc current		Load current*0.01	04 0B	The load current is 10.35A
0106H	2	R	W	Load dc power		Actual value	00 7E	The load power is 126W
	Solar panel information（6 bytes）							
0107H	2	R	V	Solar panel voltage		Solar panel voltage * 0.1	00 C8	The solar panel voltage is 20V
0108H	2	R	A	Solar panel current (to controller)		Solar panel current * 0.01	01 0A	The solar panel current is 2.66A
0109H	2	R	W	Charging power		Actual value	00 35	The solar panel charging power is 53W
	Battery information（22 bytes）							
010AH	2	R/W	-	Load On/ Off command	0 or 1	1 to turn on the load, 0 to turn off the load	00 01	Turn on the load
010BH	2	R	V	Battery's min. voltage of the current day		Battery's min. voltage of the current day * 0.1	00 70	The current day of battery min. voltage is 11.2V
010CH	2	R	V	Battery's max. voltage of the current day		Battery's max. voltage of the current day * 0.1	00 84	The current day of battery max. voltage is 13.2V
010DH	2	R	A	Max. charging current of the current day		Max. charging current of the current day * 0.01	00 D8	The current day of battery max. charging current is 2.16A
010EH	2	R	A	Max. Discharging current of the current day		Max. discharging current of the current day * 0.01	04 10	The current day of battery max. discharging current is 10.4A

010FH	2	R	W	Max. charging power of the current day		Actual value	00 41	The current day of battery max. charging power is 65W
0110H	2	R	W	Max. discharging power of the current day		Actual value	00 78	The current day of battery max. discharging power is 120W
0111H	2	R	AH	Charging amp-hrs of the current day		Actual value	06 08	The current day of battery charging amp-hrs is 1544AH
0112H	2	R	AH	Discharging amp-hrs of the current day		Actual value	08 10	The current day of battery discharging amp-hrs is 2064AH
0113H	2	R	W	Power generation of the current day		Actual value	03 DE	The current day of Power generation is 990W
0114H	2	R	W	Power consumption of the day		Actual value	01 E3	The current day of Power consumption is 483W
	Historical data information（22 bytes）							
0115H	2	R	days	Total number of operating days			00 08	The system has been running for eight days
0116H	2	R	-	Total number of battery over-discharges			00 01	The battery is over-discharges one time
0117H	2	R	-	Total number of battery full-charges			00 06	The battery is filled six times
0118H 0119H	4	R	AH	Total charging amp-hrs of the battery		Actual value	0001 0203	The battery of total charging amp-hrs is 66051AH
011AH 011BH	4	R	AH	Total discharging amp-hrs of the battery		Actual value	0000 0108	The battery of total discharging amp-hrs is 264AH
011CH 011DH	4	R	W	Cumulative power generation		Actual value	0000 07D0	The solar panel of Cumulative power generation is 2000W
011EH 011FH	4	R	W	Cumulative power consumption		Actual value	0000 03E8	The load of Cumulative power consumption is 1000W

	Load information（2 bytes）								
0120H	2	R	-	Load status	0 or 1	8 higher bits	b7: 0 indicates the load is off, 1 indicates the load is on	E4	Indicates that the load is open and the brightness is 100%. (the brightness is not adjustable at present)
			%	Load brightness	00～64H		b0～b6: brightness value		
			-	Charging state	8 lower bits		00H: charging deactivated	02	The current day of controller is MPPT charging.
							01H: charging activated		
							02H: mppt charging mode		
							03H: equalizing charging mode		
							04H: boost charging mode		
							05H: floating charging mode		
							06H: current limiting (overpower)		
	Controller fault information(4 bytes)								
0121H 0122H	4	R	-	Controller fault and warning information	16 higher bits		B31 reserved B30：circuit, charge MOS short circuit B29：Anti-reverse MOS short		E.g.: A certain bit being 1 indicates some fault occurs to the corresponding item, while a certain bit being 0 indicates the corresponding item is free from faults. When all items function normally, the bits return to 00000000H.
							B28:solar panel reversely connected		
							B27:solar panel working point over-voltage		
							B26:solar panel counter-current		
							B25:photovoltaic input side over-voltage		
							B24: photovoltaic input side short circuit		

						B23: photovoltaic input overpower		
						B22: ambient temperature too high		
						B21: controller temperature too high		
						B20: load overpower or load over-current		
						B19: load short circuit		
						B18: battery under-voltage warning		
						B17: battery over-voltage		
						B16: battery over-discharge		
					16 lower bits	B0-B15 reserved		
EEPROM Controller parameter setting（50 bytes）								
E001H	2			Reserved				
	Battery parameter setting（38 bytes）							
E002H	2	R	AH	Nominal battery capacity				
E003H	2	R/W	-	8 higher bits: system voltage setting 8 lower bits: recognized voltage		12：12V 24：24V 36：36V 48：48V FF: automatic recognition Others:automatic recognition		
E004H	2	R/W	-	Battery type		0=Self-customized, 1=Open, 2=Sealed, 3=Gel, 4=Lithium		
E005H	2	R/W	V	Over-voltage threshold	70～170			Setting range: 7 to 17V E.g.:

E006H	2	R/W	V	Charging voltage limit	70～170			when the over-voltage threshold needs to be set to 17.0 V and one decimal place is to be kept, first multiply the figure by 10, i.e. 17.0V * 10 = 170V, then convert it to a hexadecimal value 00AAH, and next write the value into 0103H.
E007H	2	R/W	V	Equalizing charging voltage	70～170			
E008H	2	R/W	V	Boost charging voltage/ overcharge voltage (lithium batteries)	70～170			
E009H	2	R/W	V	Floating charging voltage/ overcharge recovery voltage (lithium batteries)	70～170			
E00AH	2	R/W	V	Boost charging recovery voltage	70～170			
E00BH	2	R/W	V	Over-discharge recovery voltage	70～170			
E00CH	2	R/W	V	Under-voltage warning level	70～170			
E00DH	2	R/W	V	Over-discharge voltage	70～170			
E00EH	2	R/W	V	Discharging limit voltage	70～170			
E00FH	2	R/W	-	8 higher bits: end-of-charge SOC 8 lower bits: end-of-discharge SOC				Unrealized
E010H	2	R/W	S	Over-discharge time delay	0～120			
E011H	2	R/W	Min	Equalizing charging time	0～300	Step length 10		
E012H	2	R/W	Min	Boost charging time	10～300	Step length 10		
E013H	2	R/W	day	Equalizing charging interval	0～255	0:closed, step length 5		
E014H	2	R/W	mV/℃/2V	Temperature compensation factor	0～5	0:not compensated, step length 1		
E015H～E01CH	16	-		Reserved				
	Mode setting（2 bytes）							

E01DH	2	R/W	-	Load working modes	00H	Sole light control, light control over on/ off of load		
					01H	Load is turned on by light control, and goes off after a time delay of 1 hour		
					02H	Load is turned on by light control, and goes off after a time delay of 2 hours		
					03H	Load is turned on by light control, and goes off after a time delay of 3 hours		
					04H	Load is turned on by light control, and goes off after a time delay of 4 hours		
					05H	Load is turned on by light control, and goes off after a time delay of 5 hours		
					06H	Load is turned on by light control, and goes off after a time delay of 6 hours		
					07H	Load is turned on by light control, and goes off after a time delay of 7 hours		
					08H	Load is turned on by light control, and goes off after a time delay of 8 hours		
					09H	Load is turned on by light control, and goes off after a time delay of 9 hours		
					0AH (decimal 10)	Load is turned on by light control, and goes off after a time delay of 10 hours		

					0BH (decimal 11)	Load is turned on by light control, and goes off after a time delay of 11 hours		
					0CH (decimal 12)	Load is turned on by light control, and goes off after a time delay of 12 hours		
					0DH (decimal 13)	Load is turned on by light control, and goes off after a time delay of 13 hours		
					0EH (decimal 14)	Load is turned on by light control, and goes off after a time delay of 14 hours		
					0FH (decimal 15)	Manual mode		
					10H (decimal 16)	Debugging mode		
					11H (decimal 17)	Normal on mode		
	Light control setting（4 bytes）							
E01EH	2	R/W	Min	Light control delay	0～60			
E01FH	2	R/W	V	Light control voltage	1～40			
E020H	2	-		Reserved				
E021H	2	R/W	-	Special power control	8 higher bits	b3 to b7 not used		
						b1: 1 special power control function enabled 0 special power control function disabled		
						b0: 1 each night on function enabled, 0 each night on function disabled		The position 1 will clear the battery over discharging of mark once every night,and (assuming that the battery over discharging on the same day)at least once allow the system open the load on the night.
					8 lower bits	b3 to b7 not used		
						b2: no charging below 0 °C (1: enabled, 0: disabled)		

						b0 to b1: charging method (00: direct charging, 01: PWM charging)		
Historical data record（FLASH）								
F000H ~ F3FFH	1024	R	-	Historical data of the someday				Function code: Reading the day data is F000H, Read the first 3 days data is F003H, Returns 20 bytes of data block

4 Command parses and paradigms

4.1、Read the voltage and current of the controller system

PDU address	Bytes	R/ W	Data		Meaning
000AH	2	R	8 higher bits: system voltage	0CH (decimal 12)	12V
				18H (decimal 24)	24V
				24H (decimal 36)	36V
				30H (decimal 48)	48V
				60H (decimal 96)	96V
				FFH (decimal 255)	Automatic recognition of system voltage
			8 lower bits: system current	0AH (decimal 10)	10A
				14H (decimal 20)	20A
				1EH (decimal 30)	30A
				2DH (decimal 45)	45A
				3CH (decimal 60)	60A

According to "Table 1", the PDU address is known to be 000AH. Read 1 word (2 bytes)

To send: 01 03 000A 0001 A408

To receive: 01 03 02 181E 324C

Parsing: high byte 18H indicates the controller's system voltage is 24V, and low byte 1EH indicates the system current is 30A.

4.2、To read the controller's model， and the PDU addresses are known to be 000CH to 0013H in sequence and occupy a total of 16 bytes. Assume these addresses store the following data (ASCII) in sequence:

’ ’ , ’ ’, ’ ’, ’ ’, ’M’, ’T’, ’4’, ’8’, ’3’ , ’0’ , ’ ’, ’ ’, ’ ’, ’ ’, ’ ’, ’ ’, ’ ’

To send: 01 03 000C 0008 840F

To receive: 01 03 10 2020 2020 4D54 3438 3330 2020 2020 2020 EE98

Parsing: this controller's model is MT4830 (the ASCII corresponding to 20H is ' ', and space can be neglected)

4.3、To read the controller's software version and hardware version, and the PDU addresses are known to be 0014H, 0015H, 0016H and 0017H in sequence

To send:01 03 0014 0004 040D

To receive:01 03 08 0003 0201 0001 0203 8A54

Parsing: (the highest byte OOH is not used) 030201H indicates the controller's software version is V03.02.01

(the highest byte OOH is not used) 010203H indicates the controller's hardware version is V01.02.03

4.4、To read the controller's product serial number and the PDU addresses are 0018H and 0019H in sequence as shown in "Table 1"

To send: 01 03 0018 0002 440C

To receive:01 03 04 0F01 FFFF A957

Parsing: 0F01 FFFFH is the product serial number, indicating it's the 65535th (hexadecimal FFFFH) unit produced in Jan. of 2015

4.5、To read battery capacity SOC, and the PDU address is known to be 0100H

To send: 01 03 0100 0001 85F6

To receive: 01 03 02 0064 B9AF

Parsing: (the highest byte OOH is not used) the battery capacity SOC is 64H% （decimal 100%)

4.6、To read battery voltage:

Multiply the battery voltage reading by 0.1

The PDU address is known to be 0101H

To send: 01 03 0101 0001 D436

To receive: 01 03 02 007B F867

Parsing: formula (battery voltage = battery voltage * 0.1)

Battery voltage: (007BH, decimal 123), 007BH * 0.1 = 12.3V

4.7、To read the battery's surface temperature and controller temperature, and the PDU addresses are known to be 0103

The high 8 bits represent the temperature of the controller, and the lower 8 bits represent the temperature of the battery.

To send: 01 03 0103 0001 75F6

To receive: 01 03 02 1B19 737E

Analytic: 1B19H represent the temperature of the controller is 1BH (27 ℃), the surface temperature of the battery for 19H(25 ℃)

4.8、To read load voltage, current and power, and the PDU addresses are known to be 0104H, 0105H and 0106H in sequence

To send: 01 03 0104 0003 45F6

To receive: 01 03 06 0078 00C8 00F0 00C5

Parsing:

Formula: load voltage = load voltage * 0.1

0078H is the load voltage, so the actual load voltage is: 0078H * 0.1 = 120 * 0.1 = 12.0V

Formula: load current =load current * 0.01

00C8H is the load current, so the actual load current is: 00C8H * 0.01 = 200 * 0.01 = 2.00A

00F0H is the load power (decimal 240W) which can also be calculated via formula: load voltage * load current

4. 9、To read solar panel voltage, charging current and charging power, and the PDU addresses are known to be 0107H, 0108H and 0109H in sequence

To send: 01 03 0107 0003 B5F6

To receive: 0090 0096 00D8 011E

Parsing:

Formula: solar panel voltage = solar panel voltage * 0.1

00AAH is the solar panel voltage reading, so the actual solar panel voltage is: 0090H * 0.1 = 144 * 0.1 = 14.4V

Formula: solar panel charging current = solar panel charging current * 0.01

0096H is solar panel charging current reading, so the actual solar panel charging current is: 0096H * 0.01= 150 * 0.01 = 1.50A

00D8H is solar panel charging power (decimal 216 W) which can also be calculated via formula: solar panel voltage * solar panel charging current

4. 10、To read the current day's min. battery voltage, max. battery voltage, max. charging current, max. discharging current, max. charging power, max. discharging power, charging amp-hrs, discharging amp-hrs, power generation, power consumption, and the PDU addresses are 010BH to 0114H in sequence as shown in "Table 1"

To send: 01 03 010B 0003 75F5

To receive: 01 03 06 0070 0084 00D8 20CD

Parsing: in the returned command

The 4th and 5th bytes 0070H indicate the current day's min. battery voltage: 0070H * 0.1 = 112 * 0.1 = 11.2V

The 6th and 7th bytes 0084H indicate the current day's max. battery voltage: 0084H * 0.1 = 132 * 0.1 = 13.2V

The 8th and 9th bytes 00D8H indicate the current day's max. charging current: 00D8H * 0.01 = 216 * 0.01 = 2.16V

E.g.: to read the controller's charging amp-hrs and discharging amp-hrs on the current day, and the PDU addresses are known to be 0111H and 0112H respectively

To send: 01 03 00111 0002 31D4

To receive: 01 03 04 0608 0810 7D75

Parsing: the 4th and 5th bytes 0608H are the current day's charging amp-hrs (decimal 1544AH);

Parsing: the 6th and 7th bytes 0810H are the current day's discharging amp-hrs (decimal 2064AH)

4. 11、To read the number of operating days, over-discharges and full-charges, and the PDU addresses are 0115H, 0116H and 0117H respectively.

To send: 01 03 0115 0003 15F3

To receive: 01 03 06 0008 0001 0006 1176

Parsing:

The 4th and 5th bytes 0008H are the number of operating days, indicating the system has operated for 8 days.

The 6th and 7th bytes 0001H are the number of over-discharges, indicating th battery has been over-discharged once.

The 8th and 9th bytes 0006H are the number of full-charges, indicating the battery has been fully charged for 6 times.

4. 12、To read the battery's total charging amp-hrs and discharging amp-hrs, and the PDU addresses are known to be 0118H, 0119H, 011AH and 011BH in sequence

To send: 01 03 0118 0004 C5F2

To receive: 01 03 08 0001 0203 0000 0108 C0A3

Parsing: the 4th to 7th bytes 00010203H are the battery's total charging amp-hrs (decimal 66051AH = 66.051KAH)

The 8th to 11th bytes 00000108H are the battery's total discharging amp-hrs (decimal 264AH = 0.264KAH)

4. 13、To read the controller's cumulative power generation and cumulative power consumption, and the PDU addresses are known to be 011CH to 011FH in sequence and occupy a total of 8 bytes.

To send: 01 03 011C 0004 840F

To receive: 01 03 08 0000 07D0 0000 03E8 550C

Parsing: 000007D0H are the controller's cumulative power generation (decimal 2000 kilowatt-hours)

The 8th to 11th bytes 000003E8H are the cumulative power consumption (decimal 1000 kilowatt-hours)

4. 14、To read load status, brightness and battery status, and the PDU addresses are known to be 0120H

PDU address	Bytes	R/ W	Item	Value		Meaning
0120H	2	R	Load status	0 or 1	High byte	b7:0 indicates the load is off, 1 indicates the load is on
			Load brightness	00 to 64H		b0 to b6: brightness value
			Battery status		Low byte	00H: charging deactivated
						01H: charging activated
						02H: mppt charging mode
						03H: equalizing charging mode
						04H: boost charging mode
						05H: floating charging mode
						06H: constant current (overpower)

To send: 01 03 0120 0001 843C

To receive: 01 03 02 E402 7285

Parsing: E4H is (80H | 64H)

The 4th byte b7 being 1 indicates the street light is on, otherwise it's off, and b0 **to** b6 being 64H indicates the street light's brightness is 100%

The 5th byte 02H indicates mppt charging mode is in operation (for parsing of other statuses, refer to "PDU Address Allocation Table")

4. 15、To read faults and warnings, and the PDU addresses are 0121H and 0122H respectively

PDU address	Bytes	R/ W	Item	byte	Meaning
0121H 0122H	4	R	Controller fault and warning information	16 High bit	B31 reserved
					B30：circuit, charge MOS short circuit
					B29：Anti-reverse MOS short
					B28: solar panel reversely connected
					B27 solar panel working point over-voltage

					B26: solar panel counter-current
					B25: photovoltaic input side over-voltage
					B24: photovoltaic input side short circuit
					B23: photovoltaic input overpower
					B22: ambient temperature too high
					B21: controller temperature too high
					B20: load overpower or load over-current
					B19: load short circuit
					B18: battery over-voltage
					B17: battery under-voltage
					B16: battery over-discharge

To send: 01 03 0121 0002 95FD

To receive: 01 03 04 0101 0000 AA0F

Parsing:

The first four or five bytes for the fault information of the high 16 bit B24, 0101H for 1, said the photovoltaic input side short circuit, B16 1 said the battery over discharge

(for parsing of other fault codes, refer to the "Meaning" column of the "PDU Address Allocation Table")

4. 16、To turn on the load, and knowing the PDU address is 010AH, you need write on/ off command into this address (0001 to turn on the load, 0000 to turn off the load)

To turn on the load:

To send: 01 06 010A 0001 69F4

To receive:01 06 010A 0001 69F4

To turn off the load:

To send: 01 06 010A 0000 A834

To receive:01 06 010A 0000 A834

4. 17、To read street light brightness, and the PDU address is known to be 0120H

To send: 01 03 0120 0001 843C

To receive: 01 03 02 E400 F344

Parsing:

The highest bit is responsible for turning on the street light, and the 7 lower bits of the high byte are for adjusting the brightness value, E4H&7FH = 64H = 100%

4. 18、To set over-voltage threshold, charging limit voltage, equalizing charging voltage, boost charging voltage,

floating charging voltage, boost charging recovery voltage, over-discharge recovery voltage, over-discharge voltage, boost charging time, equalizing charging interval, temperature compensation factor.

The addresses are known to be E005H to E014H in sequence, and occupy a total of 16 words or 32 bytes.

1）、For each setting range, refer to the "Meaning" column of the "PDU Address Allocation Table".

2）、The following table sets the project not all controller support modification, and the controller specification is the subject.

Note: a controller, battery type is SLD, when you issued the following orders, can send the command prompt to success. But your controller is not allowed to change, because the battery type is a custom "User" or "LI" lithium-ion batteries to support some parameter modify command, on the other hand is the controller factory setting parameters)

E.g.:

Item to set	Data processing	Data to send
Over-voltage threshold 17.0V	Multiplied by 10	17.0 * 10 = 170, hexadecimal 00AAH
Charging limit voltage 15.5V	Multiplied by 10	15.5 * 10 = 155, hexadecimal 009BH
Equalizing charging voltage 14.6V	Multiplied by 10	14.6 * 10 = 146, hexadecimal 0092H
Boost charging voltage 14.4V	Multiplied by 10	14.4 * 10 = 144, hexadecimal 0090H
Floating charging voltage 13.8V	Multiplied by 10	13.8 * 10 = 138, hexadecimal 008AH
Boost charging recovery voltage 13.2V	Multiplied by 10	13.2 * 10 = 132, hexadecimal 0084H
Over-discharge recovery voltage 12.6V	Multiplied by 10	12.6 * 10 = 126, hexadecimal 007EH
Under-voltage threshold 17.0 V	Multiplied by 10	12.0 * 10 = 120, hexadecimal 0078H
Over-discharge voltage 11.0V	Multiplied by 10	11.0 * 10 = 110, hexadecimal 006EH
Over-discharge limit voltage 10.5V	Multiplied by 10	10.5 * 10 = 105, hexadecimal 0069H
End of charge and discharge capacity 100%|50%		100<<8|50, hexadecimal 6432H
Over-discharge time delay 5S		Hexadecimal 0005H
Equalizing charging time 60min		003CH
Boost charging time 60min		003CH
Equalizing charging interval 30 days		001EH

Temperature compensation factor 5 mV/ °C/ 2V		0005H

To send: 01 10 E005 0010 20 00AA 009B 0092 0090 008A 0084 007E 0078 006E 0069 6432 0005 003C 003C 001E 0005 9676

To receive: 01 10 E005 0010 E604

4.19、To set load working mode, and the PDU address is known to be E01DH

PDU address	Bytes	R/ W	Item	Value	Meaning
E01DH	2	R/W	Load working modes	00H	Sole light control, light control over on/ off of load
				01H	Load is turned on by light control, and goes off after a time delay of 1 hours
				02H	Load is turned on by light control, and goes off after a time delay of 2 hours
				03H	Load is turned on by light control, and goes off after a time delay of 3 hours
				04H	Load is turned on by light control, and goes off after a time delay of 4 hours
				05H	Load is turned on by light control, and goes off after a time delay of 5 hours
				06H	Load is turned on by light control, and goes off after a time delay of 6 hours
				07H	Load is turned on by light control, and goes off after a time delay of 7 hours
				08H	Load is turned on by light control, and goes off after a time delay of 8 hours
				09H	Load is turned on by light control, and goes off after a time delay of 9 hours
				0AH (decimal 10)	Load is turned on by light control, and goes off after a time delay of 10 hours

				0BH (decimal 11)	Load is turned on by light control, and goes off after a time delay of 11 hours
				0CH (decimal 12)	Load is turned on by light control, and goes off after a time delay of 12 hours
				0DH (decimal 13)	Load is turned on by light control, and goes off after a time delay of 13 hours
				0EH (decimal 14)	Load is turned on by light control, and goes off after a time delay of 14 hours
				0FH (decimal 15)	Manual mode
				10H (decimal 16)	Debugging mode
				11H (decimal 17)	Normal on mode

According to the "PDU Address Allocation Table", if "load is turned on by light control, and goes off after a time delay of 8 hours" needs to be set to, send command 0008H

To send: 01 06 E01D 0008 2FCA

To receive: 01 06 E01D 0008 2FCA

4.20、Read historical data

Function code acquisition method: read the historical data from the N day， (F000H | N),(N=0~3FFH)，Maximum readable 1023 day data.

Read 20 bytes of historical data from the 3 day：F003H = (F000H | 0003H)

To send: 01 03 F003 000A 06CD

To receive:01 03 14 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 A3 67

The returned data is a 100-day historical data block of 20 bytes, beginning with the fourth byte of each successive byte:the current day's min. battery voltage, max. battery voltage, max. charging current, max. discharging current, max. charging power, max. discharging power, charging amp-hrs, discharging amp-hrs, power generation, power consumption

4.21、Reset to factory defaults

To send: 01 78 0000 0001 6000

To receive: 01 78 0000 0001 6000

Parsing: 01 is the id number, 78 is the command to reset to factory defaults, and 6000 is for checking.

4.22、Clear history

To send: 01 79 0000 0001 5DC0

To receive: 01 79 0000 0001 5DC0

Parsing: 01 is the id number, 79 is the command to clear history, and 5DC0 is for checking.