Catalogue

1: Modbus protocol Introduction

BMS supports standard industrial modbus protocol. Customers can obtain the BMS-related information provided below in accordance with the standard modbus protocol. The following description is an example of sending and responding to read registers.

Send

The send data must contain the starting address and the number of the register to be read. Note that register addresses start at 0. The following is an example of reading register address 107-109 from slave device No. 1. The sent byte stream is: 0x11 0x03 0x00 0x6B 0x00 0x03 0x74 0x17

Send	
section name	Example (HEX format)
Slave address	0x01
function code	0x03
start address	0x00 0x6B
Quantity (high byte) 00	0x00 0x03
Check(CRC)	0x74 0x17

Response:

The register is transmitted by multiple two bytes, the low byte is in the front and the high byte is in the back, the response byte stream for the above read request is: 01 03 06 94 11 F2 FF 00 00 C3 2A

Response	
section name	Example (HEX format)
Slave address11	0x1

function code	0x03
number of bytes	0x06
address 107	0x94 0x11
address 108	0xF2 0xFF
address 109	0x00 0x00
Check(LRC 或者CRC)	0xC3 0x2A

2：Protection board modbus information

The BMS protection board is used as a slave station, the baud rate is 9600, no parity bit, the default modbus address is 0x01, and the read register function code is 0x03.

3：The verification function of the secondary development

```
const u16 CRCtbl[256] = {
    0x0000, 0xC0C1, 0xC181, 0x0140, 0xC301, 0x03C0, 0x0280, 0xC241,
    0xC601, 0x06C0, 0x0780, 0xC741, 0x0500, 0xC5C1, 0xC481, 0x0440,
    0xCC01, 0x0CC0, 0x0D80, 0xCD41, 0x0F00, 0xCFC1, 0xCE81, 0x0E40,
    0x0A00, 0xCAC1, 0xCB81, 0x0B40, 0xC901, 0x09C0, 0x0880, 0xC841,
    0xD801, 0x18C0, 0x1980, 0xD941, 0x1B00, 0xDBC1, 0xDA81, 0x1A40,
    0x1E00, 0xDEC1, 0xDF81, 0x1F40, 0xDD01, 0x1DC0, 0x1C80, 0xDC41,
    0x1400, 0xD4C1, 0xD581, 0x1540, 0xD701, 0x17C0, 0x1680, 0xD641,
    0xD201, 0x12C0, 0x1380, 0xD341, 0x1100, 0xD1C1, 0xD081, 0x1040,
    0xF001, 0x30C0, 0x3180, 0xF141, 0x3300, 0xF3C1, 0xF281, 0x3240,
    0x3600, 0xF6C1, 0xF781, 0x3740, 0xF501, 0x35C0, 0x3480, 0xF441,
    0x3C00, 0xFCC1, 0xFD81, 0x3D40, 0xFF01, 0x3FC0, 0x3E80, 0xFE41,
    0xFA01, 0x3AC0, 0x3B80, 0xFB41, 0x3900, 0xF9C1, 0xF881, 0x3840,
    0x2800, 0xE8C1, 0xE981, 0x2940, 0xEB01, 0x2BC0, 0x2A80, 0xEA41,
```

```
    0xEE01, 0x2EC0, 0x2F80, 0xEF41, 0x2D00, 0xEDC1, 0xEC81,0x2C40,
    0xE401, 0x24C0, 0x2580, 0xE541, 0x2700, 0xE7C1, 0xE681,0x2640,
    0x2200, 0xE2C1, 0xE381, 0x2340, 0xE101, 0x21C0, 0x2080,0xE041,
    0xA001, 0x60C0, 0x6180, 0xA141, 0x6300, 0xA3C1, 0xA281,0x6240,
    0x6600, 0xA6C1, 0xA781, 0x6740, 0xA501, 0x65C0, 0x6480,0xA441,
    0x6C00, 0xACC1, 0xAD81, 0x6D40, 0xAF01, 0x6FC0, 0x6E80,0xAE41,
    0xAA01, 0x6AC0, 0x6B80, 0xAB41, 0x6900, 0xA9C1, 0xA881,0x6840,
    0x7800, 0xB8C1, 0xB981, 0x7940, 0xBB01, 0x7BC0, 0x7A80,0xBA41,
    0xBE01, 0x7EC0, 0x7F80, 0xBF41, 0x7D00, 0xBDC1, 0xBC81,0x7C40,
    0xB401, 0x74C0, 0x7580, 0xB541, 0x7700, 0xB7C1, 0xB681,0x7640,
    0x7200, 0xB2C1, 0xB381, 0x7340, 0xB101, 0x71C0, 0x7080,0xB041,
    0x5000, 0x90C1, 0x9181, 0x5140, 0x9301, 0x53C0, 0x5280,0x9241,
    0x9601, 0x56C0, 0x5780, 0x9741, 0x5500, 0x95C1, 0x9481,0x5440,
    0x9C01, 0x5CC0, 0x5D80, 0x9D41, 0x5F00, 0x9FC1, 0x9E81,0x5E40,
    0x5A00, 0x9AC1, 0x9B81, 0x5B40, 0x9901, 0x59C0, 0x5880,0x9841,
    0x8801, 0x48C0, 0x4980, 0x8941, 0x4B00, 0x8BC1, 0x8A81,0x4A40,
    0x4E00, 0x8EC1, 0x8F81, 0x4F40, 0x8D01, 0x4DC0, 0x4C80,0x8C41,
    0x4400, 0x84C1, 0x8581, 0x4540, 0x8701, 0x47C0, 0x4680,0x8641,
    0x8201, 0x42C0, 0x4380, 0x8341, 0x4100, 0x81C1, 0x8081, 0x4040
};
static u16        MODBUS_CalCRC(const u8 buff[], const u8 len)
{
  u8 i;
  u16 crcval = 0xffff; u16
  temp = 0;
  for(i=0;i<len;i++)
  {
    temp = (crcval>>8)^CRCtbl[(crcval&0xFF)^buff[i]];
```

```
      crcval = temp;
    }
    return crcval;
  }
```

4：BMS Protection board communication example

1. Example: read voltage, current, instantaneous power information.

Read:

Read 5 starting at address 76 (decimal) (i.e. read 10 bytes)

The sending byte stream is (hexadecimal): 01 03 00 4C 00 05 44 1E

Send byte stream explanation: 01 is the BMS address, 03 is the function code, 00 4C is the read address, 00 05 is the length to be read, and 44 1E is the check. Therefore, the read register range is 76-80 (decimal, starting from 0x004C). According to the register table in Chapter 5, address 76 (decimal) represents voltage, and address 78 (decimal) represents current. , the address 90 (decimal) is the instantaneous power, and the three information can be obtained by this visit.

Response:

BMS response byte stream (hexadecimal): 01 03 0A 9C 17 01 00 02 00 00 00 00 00 C9 2A

Response byte stream explanation: 01 is the BMS address, 03 is the function code, 0A is the number of bytes of the response content (the read length is 5 (decimal), so the returned byte length is 10 (decimal)), 9C 17 01 00 02 00 00 00 00 00 is the response content, C9 2A is the check. 9C 17 01 00 means the voltage is 71.580V (0x0001179C), 02 00 00 00 means the current is 0.02A (0x00000002), 00 00 means the instantaneous power is 0W (0x0000).

2. Example, read BMS cell voltage information.

Read:

Read 20 starting at address 81 (decimal) (that is, read 40 bytes). Host sends byte stream (all in hexadecimal): 01 03 00 51 00 14 14 14
Send byte stream explanation: 01 is the BMS address, 03 is the function code, 00 51 is the read address, 00 14 is the length to be read, and 14 14 is the check. Therefore, the range of registers to be read is 81-100 (decimal, starting from 0x0051). According to the register table in Chapter 5, it means that 20 cell voltages are read.

Respond

BMS respond (all in hexadecimal): 01 03 28 EC 0D ED 0D ED 0D E3 0D EF 0D EF 0D 22 0E 23 0E 24 0E 1F 0E 21 0E 1E 0E 21 0E 21 0E 80 0D 2D 0E 86 0D 2D 0E 83
0D 27 0E 8B B2

Explanation of the response byte stream: 01 is the BMS address, 03 is the function code, 28 is the number of bytes of the response content (the read length is 20 (decimal), so the returned byte length is 40 (decimal)) , EC 0D ED 0D ED 0D E3 0D EF 0D EF 0D 22 0E 23 0E 24 0E 1F 0E 21 0E 1E 0E 21 0E 21 0E 80 0D 2D 0E 86 0D 2D 0E 83 0D 27 0E is the response content, 8B B2 is the check. EC 0D represents the first string voltage 3.564V (0x0DEC), ED 0D means the second string voltage 3.565V (0x0DED), ... and so on, 27 0E means the lower twenty strings voltage 3.623V (0x0E27).

3. Example, read string number and battery type information

Send:

Read 1 starting at address 75 (decimal) (that is, read 2 bytes). Host sends byte stream (all in hexadecimal): 01 03 00 4B 00 01 F4 1C

Send byte stream explanation: 01 is the BMS address, 03 is the function code, 00 4B is the read address, 00 01 is the read length, and F4 1C is the check. Therefore, the read register 75 (0x004B), according to the register table in Chapter 5, shows that the low bit of address 75 represents the number of battery strings, and the high bit of 75 represents the battery type.

Response:

BMS response (all in hexadecimal): 01 03 02 0D 00 BC D4

Response byte stream explanation: 01 is the BMS address, 03 is the function code, 02 is the number of bytes of the response content (the read length is 1 (decimal), so the returned byte length is 2 (decimal)), 0D means the number of battery strings is 13,00 means the battery type is ternary, BC D4 is the check.

4. Example, read the temperature number of cells, MOS and equilibrium

send:

Read 2 starting at address 52 (decimal) (that is, read 4 bytes). Host sends byte stream (all in hexadecimal): 01 03 00 34 00 02 85 C5
Send byte stream explanation: 01 is the BMS address, 03 is the function code, 00 34 is the read address, 00 02 is the read length, and 85 C5 is the check. Therefore, the range of registers to be read is 52-53 (decimal). According to the register table in Chapter 5, the high bit of the 52 (decimal) address represents the number of cell temperatures, and the low bit of the 53 (decimal) address represents the number of cell temperatures. The number of MOS temperature, the high bit of 53 (decimal) address represents the number of equilibrium temperature.

Response:

BMS response (all in hexadecimal): 01 03 04 00 02 01 00 5A 63

Response byte stream explanation: 01 is the BMS address, 03 is the function code, 04 is the number of bytes of the response content (the read length is 2 (decimal), so the returned byte length is 4 (decimal)), 02 means there are 2 cell temperatures, 01 means 1 MOS temperature, 00 means 0 equilibrium temperature, 5A 63 is

the check.

5. Example, read temperature information

send:
Read 5 starting at address 112 (decimal) (that is, read 10 bytes). Host sends byte stream (all in hexadecimal): 01 03 00 70 00 02 C5 D0
Send byte stream explanation: 01 is the BMS address, 03 is the function code, 00 70 is the read address, 00 02 is the read length, and C5 D0 is the check. Therefore, the read register range is 112-113 (decimal). According to the register table in Chapter 5, the low bit of the 112 (decimal) address represents the equilibrium temperature, the high bit represents the MOS temperature, and the low bit of the 113 (decimal) address represents the cell temperature 1, and the high bit of the 113 (decimal) address represents the cell temperature 2.

Response:

BMS response (all in hexadecimal): 01 03 04 45 45 45 45 0D 89

Response byte stream explanation: 01 is the BMS address, 03 is the function code, 0A is the number of bytes of the response content (the read length is 5 (decimal), so the returned byte length is 10 (decimal)), 45 means the temperature at equilibrium is 29 degrees Celsius (69(0x45)-40), 45 means the temperature at MOS is 29 degrees Celsius, 45 means cell temperature 1 is 29 degrees Celsius, and 45 means cell temperature 2 is 29 degrees Celsius. 0D 89 is the check.

6. Example, read rated capacity, actual capacity, SOC and SOH

send:

Read 2 words starting at address 44 (decimal) (that is, read 4 bytes). Host sent (all in hexadecimal): 01 03 00 76 00 03 E4 11
Send byte stream explanation: 01 is the BMS address, 03 is the function code, 00 76 is the read address, 00 03 is the read length, and E4 11 is the check. Therefore, the read register range is 118-120 (decimal). According to the register table in Chapter 5, the 118 (decimal) address represents the rated capacity, the 119 (decimal) address represents the actual capacity, and the low bits of the 120 (decimal) address represent SOC, and the high bits represent SOH.

Reception:

BMS response (all in hexadecimal): 01 03 06 5A 00 5A 00 00 64 3E BC

Response byte stream explanation: 01 is the BMS address, 03 is the function code, 06 is the number of bytes of the response content (the read length is 3 (decimal), so the returned byte length is 6 (decimal)), 5A 00 means rated capacity 9.0AH, 5A 00 means actual capacity is 9.0AH, 00 means SOC is 0 (decimal), 64 means SOH is 100 (decimal), 3E BC is check.

7. Example, read running status information

send:

Read 2 words starting at address 152 (decimal) (that is, read 4 bytes). Host sent (all in hexadecimal): 01 03 00 98 00 02 45 E4

Send byte stream explanation: 01 is the BMS address, 03 is the function code, 00 98 is the read address, 00 02 is the read length, and 45 E4 is the check. Therefore, the read register range is 152-153 (decimal). According to the register table in Chapter 5, the address of 152 (decimal) represents the system operating state 1.

Reception:

BMS response (all in hexadecimal): 01 03 04 53 01 30 00 AE B7

Response byte stream explanation: 01 is the BMS address, 03 is the function code, 04 is the number of bytes of the response content (the read length is 2 (decimal), so the returned byte length is 4 (decimal)), 53 01 30 00 means the system status value is 0x00300153, the analytical meaning is that the discharge switch is closed, the charging switch is closed, the precharge switch is disconnected, the load access status is unknown, the charger insertion status is unknown, ... the current status is idle, AE B7 is check.

8. Example, read the alarm information

Send:

Read 2 words starting at address 156 (decimal) (that is, read 4 bytes). Host sent (all in hexadecimal): 01 03 00 9C 00 02 04 25
Send byte stream explanation: 01 is the BMS address, 03 is the function code, 00 9C is the read address, 00 02 is the read length, and 04 25 is the check. Therefore, the read register range is 156-157 (decimal). According to the register table in Chapter 5, the address of 156 (decimal) represents the alarm flag information.

Reception:

BMS response (all in hexadecimal): 01 03 04 00 00 00 00 FA 33

Response byte stream explanation: 01 is the BMS address, 03 is the function code, 04 is the number of bytes of the response content (the read length is 2 (decimal), so the returned byte length is 4 (decimal)), 00 00 00 00 means that the alarm flag information value is 0x00000000, and the specific analysis is that there is no single-string overvoltage alarm, no single-string undervoltage alarm...no charging switch failure alarm, FA 33 is check.

9. Example, read single string overvoltage protection value

send:
Read 1 word starting at address 169 (decimal) (that is, read 2 bytes). Host send (all in hexadecimal): 01 03 00 A9 00 01 54 2A

Send byte stream explanation: 01 is the BMS address, 03 is the function code, 00 A9 is the read address, 00 01 is the read length, and 54 2A is the checksum. Therefore, the read register range is 169 (decimal). According to the register table in Chapter 5, the 169 (decimal) address represents a single-string overvoltage protection value.

Reception:

BMS response (all in hexadecimal): 01 03 02 68 10 96 48

Response byte stream explanation: 01 is the BMS address, 03 is the function code, 04 is the number of bytes of the response content (the read length is 1 (decimal), so the returned byte length is 2 (decimal)), 68 10 means that the single string overvoltage protection value is 0x1068, which is 4200mV, and 96 48 is the check.

5： MODBUS Address table description

Modbus address table description:

1. Read-write property: R means read-only, W means write-only. R&W means support for read and write.
2. The return value of each corresponding register occupies 2*length bytes, which are encoded by BMS.
3. In the received data, the low order is in the front, and the high order is in the back.

Register name	Address	Length	read-write property	Meaning and coding description
SA address (sa)	0	1	R&W	Module RS485 address
Internal reservation	1	1	R	
SN Serial Number (sn)	2	4	R	8byte hexadecimal
switch type(switchSerial)	6	1	R	L: 0 means different mouth, 1 means same mouth H: reserved
Hardware model(hwTypeName)	7	13	R	26 characters ASCII (null terminated, actual available 25)
prTypeName	20	18	R	36 characters ASCII (null terminated, actual available 35)
Hardware version number(hwVer)	38	1	R	L: Hardware version number, decimal H: reserved
MadeDate	39	2	R	39: year, decimal 40L: month, decimal 40H: day, decimal
DevName	41	6	RW	A string of ASCII codes of length 12.
Device password(devPwd)	47	2	RW	4-length string ASCII (English characters, number).
Internal reservation	49	1	R	
Internal reservation	50	1	R	
Internal reservation	51	1	R	

switchType&BatTempNum	52	1	R	L: switch type 0-mos; 1-relay 1; 2-relay 2; 3-magnetic hold 1; 4-magnetic hold 2; H: Number of cell temperature
mosTempNum&balaTempNum	53	1	R	L: mos temperature number 0 - non-mos board, no mos temperature. 1-mos board with 1 mos temperature. H: The number of equilibrium temperatures. 0 - no equilibrium temperature 1- Equilibrium has 1 temperature
Internal reservation	54	1	R	
Internal reservation	55	1	R	
minCells&maxCells	56	1	R	L: maximum cell strings H: minimum cell strings
maxCurt	57	1	R	uint16_t number, unit: 1A
Internal reservation	58	1	R	
Internal reservation	59	1	R	
Internal reservation	60	1	R	
Internal reservation	61	1	R	
Boot version number and firmware version number (bootVer&binVer)	62	1	R	L: boot version number H: Firmware version number
Internal reservation	63	2	R	
Internal reservation	65	3	R	
reserved	68	3	R	
total running time(ticks)	71	2	R	A uint32_t number, unit s.
Number of restarts(rstTimes)	73	1	R	uint16_t number
Internal reservation	74	1	R	

CellsNum&batType	75	1	RW	L: The number of battery strings. H: battery type code. Battery Type Code: 0- Ternary Lithium 1- Iron Lithium 2- Lithium Titanate
total voltage(sysVol)	76	2	R	total system voltage, number of uint32_t, unit 1mv
sysCurt	78	2	R	The current total system current, the number of int32_t, the unit is 0.01A. Positive numbers represent discharge current, negative numbers represent charging current.
Instantaneous power(power)	80	1	R	unit 1w
Array of cell voltage values (cellVols)	81	30	R	A sequence of uint16_t of length 30. Sequence 0 represents the voltage of a single string of 0, sequence 1 Represents the voltage of a single string 1… unit mv
Serial number of the highest voltage and lowest voltage(maxVolInd&minVolInd)	111	1	R	L: serial number of the highest voltage string H: serial number of the lowest voltage string
Mos Temp&balanceTemp	112	1	R	L: temperature at mos H: temperature at equilibrium The temperature offset is -40
batTemps	113	4	R	A sequence of uint8_t of length 8. Sequence 0 means cell temperature 0, sequence 1 means Indicates the cell temperature 1 … The temperature offset is -40
Maximum & Minimum Cell Temperature Serial Number (minTempInd&maxTempInd)	117	1	R	L: Minimum cell temperature single serial number H: Maximum cell temperature single string serial number

ratedCap	118	1	RW	uint16_t number, unit 0.1AH
actCap	119	1	RW	uint16_t number, unit 0.1AH
Remaining power percentage & battery health status score (Soc&Soh)	120	1	RW	L: soc number, range 0-100 H: SOH number, range 0-100
remainWh	121	2	R	uint32_t number, unit: WH
remainChrgTime	123	1	R	uint32_t number, unit: minutes
remainDsgTime	124	1	R	uint16_t number, unit: minutes
capLearnTimes	125	1	R	uint16_t number
learned capacity value (capLearndVal)	126	1	R	uint16_t number, last learned actual capacity
Capacity Learning Status & Cycle Times (capLearnState&recycleCnt)	127	1	R	L: capacity learning state H: Number of times of capacity learning
A discharge or charge of electricity (CaptyOnOnce)	128	1	R	The number of uint32_t, the capacity that has been charged or discharged at a time, that is, the power that has been switched from the state to the current discharged or charged in, unit 0.1AH
Charge request current (chrgReqCurt)	129	1	R	L: unit 0.1C H: reserved
Current Calibration 1 Slope (curtCaliGain1)	130	1	RW	Current Calibration 1 Slope
Current Calibration 1 Offset (curtCaliOffset1)	131	1	RW	Current Calibration 1 Offset
Internal reservation	132	1	RW	
Internal reservation	133	1	RW	
reserved	134	4		
Balance Mode & Balance Status (balaMode&balaState)	138	1	RW	L: equalization mode code 0 - automatic equalization 1- Odd string equalization 2- Even string equalization 3- Static Equalization 4- Specify Equalization H: equalization status code, currently reserved for processing 0 - equalization not started 1- Equilibrating 2- Equilibrium ends

Number of strings performing equalization (balaCellsMask)	139	2	R	32bit mask information, bit0 corresponds to single string 0, bit1 corresponds to single string 1… bit encoding: 0- Indicates that the single string is not equalizing 1- Indicates that a single string is being equalized
balaEnVol	141	1	RW	The number of uint16_t, equalizing the allowable turn-on voltage (single string voltage is larger than it to equalize balance), unit mv
balaEnDiff	142	1	RW	The number of uint16_t, equalizing the allowable turn-on voltage difference (the difference between the single string voltage and the lowest voltage larger than it can be balanced), unit mv
Static Equalization Voltage	143	1	RW	Number of uint16_t, static equalization voltage (In static equalization mode, all single strings are equalized to this voltage), in mv
reserved	144	5	R	reserved
reserved	149	1	RW	reserved
keyMode&panelType	150	1	RW	L: key mode 0- Self-reset button 1- Self-locking button, press to work, pop up to sleep H: Light board type 0 - Broken LCD 1-5LED lights 4LED lights

System Enable Flag(sysEnFlg)	151	1	RW	Bit0: reserved Bit1 (beepEn): Buzzer function on/off Bit2 (dsgWkEn): Discharge wake-up function on/off Bit3-4 (dsgWkSensCh): Discharge wake-up current selection mode Bit5 (chrgWkEn): enable/disable the charging wake-up function (only test can be disabled) Bit6 (commWkEn): enable/disable communication wake-up function Bit7 (keyWkEn): enable/disable key wakeup function (only for testing) Bit8 (rtcWkEn): Enable/disable timing wake-up function (only for testing) Bit9 (keyAdvEn): enable/disable the advanced function of self-reset button Bit10 (auSleepEn): Automatic sleep function is enabled (can be disabled only for testing) Bit11 (auPanelOffEn): The lamp panel automatically turns off when discharging Bit12(bleWkEn): Bluetooth wake-up function is enabled /closure

system runtime status1(runState1)	152	2	R	Bit0 (dsgOn): Discharge switch status Bit1 (chrgOn): Charge switch status Bit2 (preChrgOn): Precharge switch status Bit3-4 (loadPlugIn): Load access status (0-remove, 1-insert, 2-unknown) Bit5-6 (chrgPlugIn): Charger access status (0-shift Divide, 1-Insert, 2 Unknown) Bit7-9 (runLedFunc): Running light status (0-constant off, 1-constantly on, 2-flashing 1, 3-flashing 2, 4-flashing 3) Bit10-12 (warnLedFunc): Warning light status (0-off, 1-on, 2-flashing 1, 3-flashing 2, 4-flashing 3) Bit13-15 (socLedFunc): Status of battery light (0-off, 1-1 grid, 2-2 grid, 3-3 grid, 4-4 grid, 5-5 grid) Bit16 (keyUpDown): button status Bit17-19 (beepFunc): buzzer status (0-no sound, 1-always beep, 2-beep 1, 3-beep 2, 4-beep 3) Bit: 20 (rs485Conn): RS485 communication status Bit21 (canConn): CAN communication status Bit22 (bleConn): BLE communication status Bit23 (shellConn): Debug serial port connection status Bit24 (manual): Manual mode status Bit25 (noDetTemp): Temperature not checking status Bit26-27 (curtState): Current state (0-idle, 1-charge, 2-discharge) Bit28-29 (spsState): Protection state (0-no protection, 1-charge protection, 2-discharge protection, 3-charge and discharge protection)

reserved	154	2	R	reserved
System warning and protection flags (sysAlarmFlg)	156	2	R	Bit0 (ovFlg) : Single string overvoltage flag Bit1 (uvFlg) : Single string undervoltage flag Bit2 (uvKillFlg)： Storage mode trigger Bit3 (sumOvFlg) : Total voltage overvoltage flag Bit4 (sumUvFlg) : Total voltage undervoltage flag Bit5 (ocChrgFlg) :Charge overcurrent flag Bit6 (ocDsg1Flg) :Discharge overcurrent 1 flag Bit7 (ocDsg2Flg) :Discharge overcurrent 2 flag Bit8 (scFlg) :short circuit flag Bit9 (otChrgFlg) :Battery charging over temperature symbol flag Bit10 (utChrgFlg) :Battery charging low temperature flag Bit11 (otDsgFlg) :Cell discharge over temperature flag Bit12 (utDsgFlg) :Cell discharge low temperature flag Bit13 (otMosFlg) :Mos Over temperature flag Bit14 (usSocFlg) :soc low alarm Bit15 (fullFlg) : full protection flag Bit16 (emptyFlg) :Vent protection flag Bit17 (bqOvFlg) :bq Single string overvoltage flag Bit18 (bqUvFlg) :bq Single string undervoltage flag

				Bit19-23 (rsv): Reserve Bit24 (invalidFlg) :failure flag （The AND results of the failure flags below) Bit25 (bqInvlidFlg) :Bq failure flag Bit26 (eeInvlidFlg):Ee failure flag Bit27 (vInvalidFlg): voltage failure flag Bit28 (tInvalidFlg):temperature failure flag Bit29 (cInvalidFlg):Current failure flag Bit30 (dsgSwInvalidFlg):discharge switch Failure flag Bit31 (chrgSwInvalidFlg): Charging switch invalid flag
reserved	158	8		reserved
Low battery warning judgment mode &soc warning value(usWarnMode&usSocWarn)	166	1	RW	L: Low soc judgment mode. 0 - judged by soc 1- Judging by the low voltage value of a single string 2- Both are judged, and either condition is satisfied. H: soc warning value
Single low pressure warning value(usVolWarn)	167	1	RW	Single string low voltage warning value, unit mv
reserved	168	1		reserved
Single overvoltage protection value(ovWarn)	169	1	RW	uint16_t number, unit mv
Cell overvoltage protection recovery value(ovrWarn)	170	1	RW	uint16_t number, unit mv
Cell overvoltage protection delay time & recovery delay time(ovDelay&ovrDelay)	171	1	RW	L: Single-string overvoltage protection delay time H: Single-string overvoltage recovery delay time Units

Single unit under voltage protection value(uvWarn)	172	1	RW	uint16_t number, unit mv
Cell undervoltage protection recovery value(uvrWarn)	173	1	RW	uint16_t number, unit mv
Cell undervoltage protection delay time & recovery time(uvDelay&uvrDelay)	174	1	RW	L: Undervoltage protection delay time H: Undervoltage recovery delay time Unit S
Entering storage mode cell voltage threshold (uvKillVol)	175	1	RW	uint16_t number, unit mv
Internal reservation	176	1	RW	uint16_t number in 0.01A
Entering Storage Mode Delay Time(killDelay)	177	1	RW	A uint16_t number in s.
Total overvoltage protection value(sumOvWarn)	178	1	RW	uint16_t number in 0.01V
Total overvoltage protection recovery value(sumOvrWarn)	179	1	RW	uint16_t number in 0.01V
Total Overvoltage Protection & Recovery Delay Time(sumOvDelay&sumOvrDelay)	180	1	RW	L: Total voltage overvoltage protection delay time H: Overvoltage protection recovery delay time Unit S
Total undervoltage protection value(sumUvWarn)	181	1	RW	uint16_t number in 0.01V
Total undervoltage protection recovery value(sumUvrWarn)	182	1	RW	uint16_t number in 0.01V
Total Brownout Protection & Recovery Delay Time(sumUvDelay&sumUvrDelay)	183	1	RW	L: key under-voltage protection delay time H: total voltage under-voltage recovery delay time Unit S
Full protection overall voltage(fullWarn)	184	1	RW	uint16_t number in 0.01V
full protection current(fullCurt)	185	1	RW	uint16_t number in 0.01A
Full protection delay time/time limit(fullDelay&fullLimit)	186	1	RW	L: delay time, unit s H: number of times limit

Internal reservation	187	1		
Internal reservation	188	1	RW	(Unit 1mv)
Internal reservation	189	1	RW	(Unit 0.01A)
Internal reservation	190	1	RW	Internal reservation
Charge overcurrent protection value(ocChrgWarn)	191	1	RW	uint16_t number, 0.01A, absolute value.
Internal reservation	192	1	RW	Internal reservation
Internal reservation	193	1	RW	Internal reservation
Discharge overcurrent 1 protection value(ocDsg1Warn)	194	1	RW	Number of uint16_t, unit: 0.01A
Discharge overcurrent 2 protection value(ocDsg2Warn)	195	1	RW	Number of uint16_t, unit: 0.01A
Internal reservation	196	1	RW	Internal reservation
Internal reservation	197	1	RW	Internal reservation
Internal reservation	198	1	RW	Internal reservation
Short circuit protection delay time (scDelay)	199	1	RW	L: reserved H: Hardware short-circuit protection delay parameter
Battery charging high temperature protection value & recovery value (otChrgWarn&otrChrgWarn)	200	1	RW	L: Charging high temperature protection value H: Charging high temperature recovery value
Cell charging low temperature protection value & recovery value (utChrgWarn&utrChrgWarn)	201	1	RW	L: charging low temperature protection value H: charging low temperature recovery value
Cell discharge high temperature protection value & recovery value(otDsgWarn&otrDsgWarn)	202	1	RW	L: Discharge high temperature protection value H: Discharge high temperature recovery value
Cell discharge low temperature protection value & recovery value (utDsgWarn&utrDsgWarn)	203	1	RW	L: Discharge low temperature protection value H: Discharge low temperature recovery value

MOS over temperature protection value & recovery value (otMosWarn&otrMosWarn)	204	1	RW	L: MOS over-temperature protection value H: MOS over-temperature recovery value
MOS over temperature protection delay time (otMosDelay)	205	1	RW	L: MOS over temperature protection delay time H: reserved
Short circuit protection current (scCurt)	206	1	RW	uint16_t number, 0.01A, absolute value.
Idle into sleep time(idleSleepT)	230	1	R	Internal reservation

Figure 1 modbus protocol

6：Set BMS parameters

6.1 Basic Format

Basic format of a command，PC -> BMS

ID	COM	AddrH	AddrL	LenH	LenL	DxL	DxH	CRCH	CRCL
Id number, default 1	0X11	0	1	0	2	XX	XX	XX	XX

ID：Address of BMS

COM：Function code, fixed as 0X11

AddrH/AddrL:corresponding different commands.

LenH/LenL:written data

CrcH/CrcL:Check.

BMS responsed：

ID	COM	AddrH	AddrL	Len	DxL	DxH	CRCH	CRCL
SA	0X11	0	XX	2	XX Success or failure recovery value	XX Success or failure recovery value	XX	XX

6.2 Common Commands

6.2.1 Setting SOC

Example: SOC set to 16% and write byte stream is：01 11 00 78 00 02 01 10 81 50

ID	COM	AddrH	AddrL	LenH	LenL	DxL	DxH	CRCH	CRCL
Id number, default 1	0X11	0	0x78	0	2	fixed at 0x1	Input range: 0-100 Unit: 1%/bit	XX	XX

6.2.2 Setting Capacity

Example: the capacity is set to 60AH and the write byte stream is：01 11 00 76 00 02 **58 02** 52 CC

ID	COM	AddrH	AddrL	LenH	LenL	DxL	DxH	CRCH	CRCL
Id number, default 1	0X11	0	0x76	0	2	Input range: 1-6000. Unit: 0.1ah/bit		XX	XX

6.2.3 Setting the String Number

Example: Capacity set to 15 strings and write byte stream is：01 11 00 4B 00 02 01 **0F** C4 9C

ID	COM	AddrH	AddrL	LenH	LenL	DxL	DxH	CRCH	CRCL
Id number, default 1	0X11	0	0x4B	0	2	fixed at 1	Input range: 3-25	XX	XX

6.2.4 Setting the Battery Type

Example: Set battery type lithium iron, and write byte stream is：01 11 00 4B 00 02 00 **01** 44 C8

ID	COM	AddrH	AddrL	LenH	LenL	DxL	DxH	CRCH	CRCL
Id number, default 1	0X11	0	0x10	0	2	fixed at 0	Input range: 0-2 Unit: 0:Ternary 1: Lithium iron 2: Lithium Titanate	XX	XX

6.2.5 Set the overvoltage protection value

Example: set single series overvoltage 4100mV and write byte stream is：01 11 00 A9 00 02 04 10 7E 12

ID	COM	AddrH	AddrL	LenH	LenL	DxL	DxH	CRCH	CRCL
Id number, default 1	0X11	0	0xA9	0	2	Input range: 2000-4500 Unit: 0.001V/bit		XX	XX

6.2.6 Set the undervoltage protection value

Example: set the single-string undervoltage to 3000mv and write byte stream is：01 11 00 AC 00 02 B8 0B 82 D9

ID	COM	AddrH	AddrL	LenH	LenL	DxL	DxH	CRCH	CRCL
Id number, default 1	0X11	0	0xAC	0	2	Input range: 1500-3900 Unit: 0.001V/bit		XX	XX

6.2.7 Set the charging high temperature protection value

Example: Set charging temperature to 50 ° C and write byte stream is：01 11 00 C8 00 02 01 5A 41 7D

ID	COM	AddrH	AddrL	LenH	LenL	DxL	DxH	CRCH	CRCL
Id number, default 1	0X11	0	0xC8	0	2	Input range: 70-165 Unit: 1°/bit, where the offset is 40. actual value = Enter value - 40		XX	XX

6.2.8 Set charging low temperature protection value

Example: Set charging temperature to 0 ° c and write byte stream is：01 11 00 C9 00 02 01 28 FC 98

ID	COM	AddrH	AddrL	LenH	LenL	DxL	DxH	CRCH	CRCL
Id number, default 1	0X11	0	0xC9	0	2	Input range: 0-80 Unit: 1°/bit, where the offset is 40. actual value = Enter value - 40		XX	XX

6.2.9 Set the discharge high temperature protection value

Example: Set discharge temperature to 50 degrees and write byte stream is： 01 11 00 CA 00 02 01 5A 38 BD

ID	COM	AddrH	AddrL	LenH	LenL	DxL	DxH	CRCH	CRCL
Id number, default 1	0X11	0	0xCA	0	2	Input range: 70-165 Unit: 1°/bit, where the offset is 40. actual value = Enter value - 40		XX	XX

6.2.10 Set the discharge low temperature protection value

Example: Set the discharge low temperature to 0 degrees, and write the byte stream is： 01 11 00 CB 00 02 01 28 85 58

ID	COM	AddrH	AddrL	LenH	LenL	DxL	DxH	CRCH	CRCL
Id number, default 1	0X11	0	0xCB	0	2	Input range: 70-165 Unit: 1°/bit, where the offset is 40. actual value = Enter value - 40		XX	XX

6.2.11 Set the discharge overcurrent protection value

Example: Set the discharge overcurrent to 40A, and the write byte stream is: 01 11 00 C2 00 02 A0 0F 60 D3

ID	COM	AddrH	AddrL	LenH	LenL	DxL	DxH	CRCH	CRCL
Id number, default 1	0X11	0	0xC2	0	2	Input range: 1-65535 Unit：0.01A		XX	XX

6.2.12 Set charging overcurrent protection value

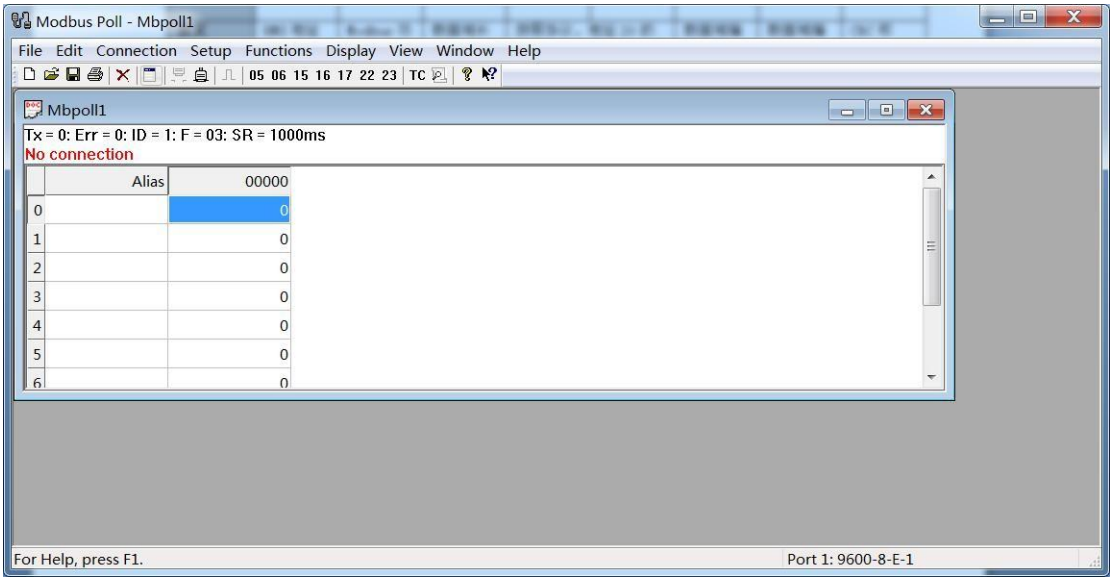
Example: Set charging overcurrent 20A and write byte stream: 01 11 00 BF 00 02 D0 07 28 DF

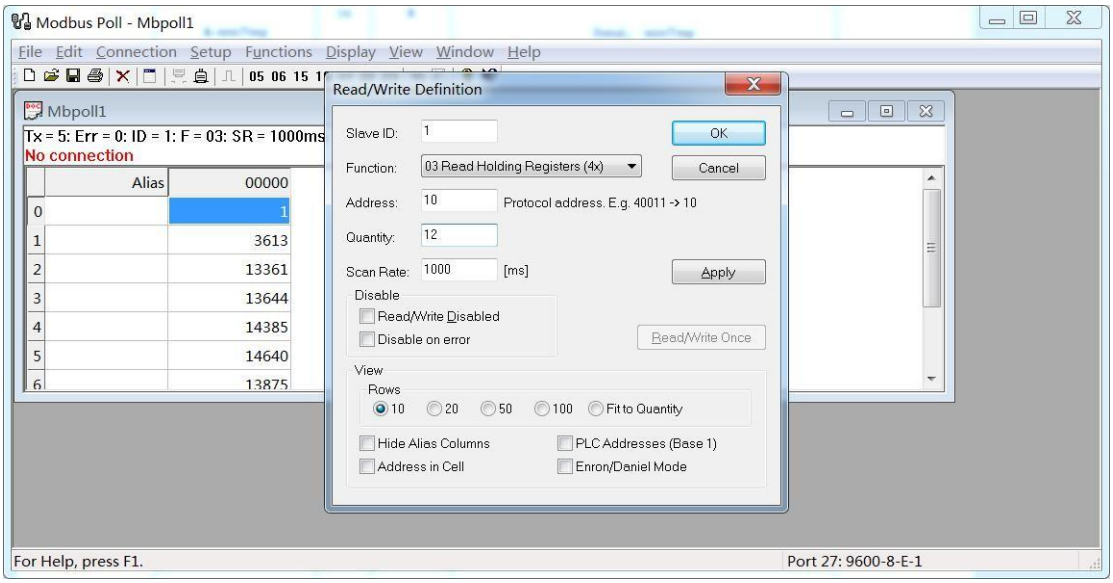
ID	COM	AddrH	AddrL	LenH	LenL	DxL	DxH	CRCH	CRCL
Id number, default 1	0X11	0	0xBF	0	2	Input range: 1-65535 Unit: 0.01A		XX	XX

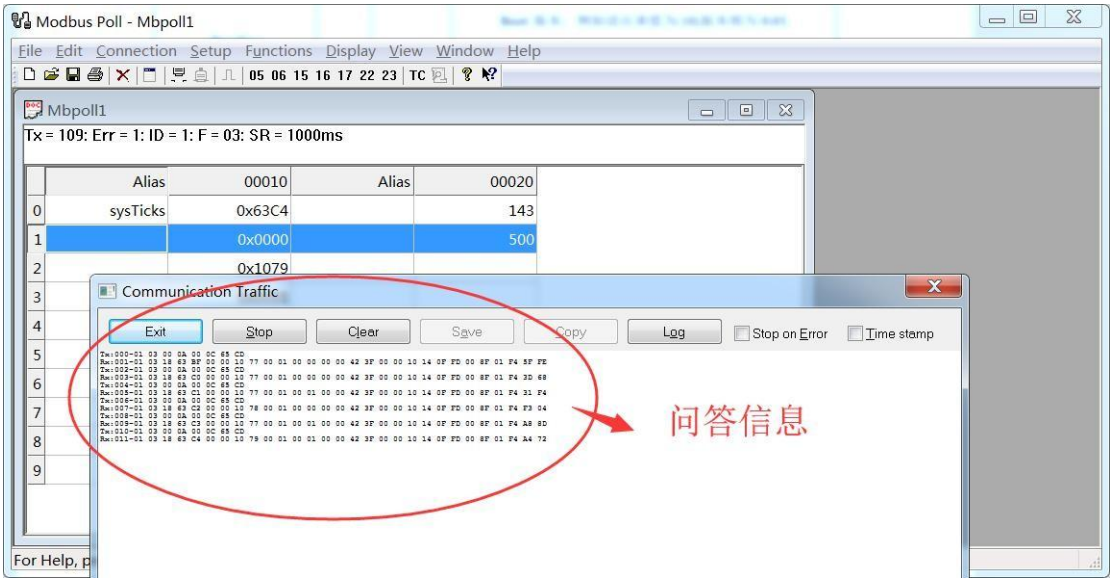
7： MODBUS Common test software

Users can download the MODBUS POLL software by themselves. This software can directly calculate the CRC, and can also obtain the information of any address. The maximum number of registers accessed each time cannot exceed 35 registers, otherwise the BMS cannot response.

1. Modbus Poll




Modbus Poll - Mbpoll1
File Edit Connection Setup Functions Display View Window Help
Mbpoll1
Tx = 5: Err = 0: ID = 1: F = 03: SR = 1000ms
No connection
Alias 00000
0 1
1 3613
2 13361
3 13644
4 14385
5 14640
6 13875
Read/Write Definition
Slave ID: 1
OK
Function: 03 Read Holding Registers (4x)
Cancel
Address: 10
Protocol address. E.g. 40011 -> 10
Quantity: 12
Scan Rate: 1000 [ms]
Apply
Disable
Read/Write Disabled
Disable on error
Read/Write Once
View
Rows
10 20 50 100 Fit to Quantity
Hide Alias Columns
PLC Addresses (Base 1)
Address in Cell
Enron/Daniel Mode
For Help, press F1.
Port 27: 9600-8-E-1


Modbus Poll - Mbpoll1
File Edit Connection Setup Functions Display View Window Help
Mbpoll1
Tx = 109: Err = 1: ID = 1: F = 03: SR = 1000ms
Alias 00010 Alias 00020
0 sysTicks 0x63C4 143
1 0x0000 500
2 0x1079
Communication Traffic
Exit Stop Clear Save Copy Log Stop on Error Time stamp
问答信息