Battery Management System (BMS)

Protocol for Lithium Battery Pack

Modbus Protocol

Author:
ShenZhen Daren
High tech electronics Co.,LTD.

Version:
V1.0.2

Contents

List of Figures

List of Tables

1 Profile

1.1 Instruction

The document stipulates the protocol for command control and data exchange between the lithium battery (slave node) and the monitoring module (master node).
Functions defined in the protocol include:

1. The master node obtains the information by sending a read command.
2. The master node configures the relevant parameters and controls actions by sending a write command(This protocol does not support write command temporarily).

The master node is the host in the communication process. The information exchange is done by a question-and-answer method. The information and parameters of the slave node use register addresses as storage addresses. The master node executes the read/write command by accessing the registers. The protocol supports the networking of one master node and multiple slave nodes. Slave nodes are identified by addresses. On the same communications bus, addresses of slave nodes must be unique.

2 Modbus Protocol Basic Defination

2.1 CRC parity

CRC applies to all bytes in front of the CRC code, which consists of 16 bits. The reference code is as follows:

```
unsigned short modbus_crc(unsigned char *addr, int num) {
    unsigned short CRC = 0xFFFF;
    int i;
    while (num--) {
        CRC ^= *addr++;
        for (i = 0; i < 8; i++) {
            if (CRC & 1) {
                CRC >>= 1;
                CRC ^= 0xA001;
            }else {
                CRC >>= 1;
            }
        }
    }
    return CRC;
}
```

2.2 Communication Parameters

Baud Rate : 9600 bps;
Parity Bit: None;
Data Bits: 8;
Stop Bits: 1;
Communication slave address depend on BMS code Dial switch value. It's range: 0∼15.
The BMS code switch show as below picture:

Such as:

- Slave address 0: 1,2,3,4 all are down.
- Slave address 1: 1 is up, 2,3,4 are down.
- Slave address 2: 2 is up, 1,3,4 are down.
- Slave address 15: 1,2,3,4 all are up.

3 Frame format of communication data

3.1 List of function code

Function code	Meaning	Notes
0x04	Read command	support to read single or multi-resister sequentially
0x10	Write command	support to write single or multi-resister sequentially

Table 1: function code

Note:

1. Function code 0x04 means that slave node upload battery pack information collected to host node when slave node accept command 0x04 from host node.

3.2 Read the collected information frame format

Note:

1. Type of command 0x04;
2. MSB means high significant byte, LSB means low significant byte.
3. Each register store two bytes; Register data type is one byte of data, it is required to store in LSB.

3.2.1 Host node sending frame format

Item	0	1	2	3	4	5	6	7
Field definition	ADDR	CMD	MSB	LSB	MSB	LSB	LSB	MSB
Explanation	Controller address	Type of command(0x04)	Beginning register address		Resister number n		CRC parity	

Table 2: Read command

For example: Query from host to BMS module:

0x00	0x04	0x10	0x00	0x00	0x17	0xb5	0x15
0x01	0x04	0x10	0x00	0x00	0x17	0xb4	0xc4
...	...	...	...	...	...	...	...
0x0E	0x04	0x10	0x00	0x00	0x17	0xb4	0x3b
0x0F	0x04	0x10	0x00	0x00	0x17	0xb5	0xea

Table 3: Query from host to BMS module

Item	0	1	2	3	4	5	6	7	8	...	L +1	L+2	L+3	L+4
Field definition	ADDR	CMD	MSB	LSB	MSB	LSB	Length	MSB	LSB	...	MSB	LSB	LSB	MSB
Explanation	Controller address	Type of command	Data addr		Data length		Length L=n*2	First register's value		...	Last register's value		CRC parity	

Table 4: write command

3.2.2 Normal response for reading register

Item	0	1	2	3	...	L +1	L+2
Field definition	ADDR	CMD	LSB	MSB	$BYTE_1$ ...$BYTE_n$	LSB	MSB
Explanation	Controller address	Type of command	Length L=n*2		data	CRC parity	

Table 5: The format of normal response for reading frame from slave node

3.2.3 Normal response for writing register

Item	0	1	2	3	4
Field definition	ADDR	CMD+128	Rtn Code	LSB	MSB
Explanation	Controller address	Type of command+128	Rtn Code	CRC parity	

Table 6: The format of normal response for writing frame from slave node

Note: CRC parity range is the check of all bytes before CRC field.

3.3 Rtn Code

Rtn Code	NAME	Remark
0	legal function code	Operation success
1	Illegal function code	Function that does not exjst
2	Illegal function address	Register address that does not exist
3	Illegal data operation	Its operation is not allowed

Table 7: Rtn Code

4 Data Information

4.1 Data acquisition

Note:

1. if the reading data is invalid value, reported 0xFFFF
2. Each register stores two bytes.

Relative Address	**Name**	**Bytes**	**Data Type**	**Unit**	**Range**	**Remark**
0x1000	Voltage of battery Pack	2	uint16	10mV	0~655.35V	
0x1001	Current of battery Pack	2	int16	10mA	-327.68~327.67A	
0x1002	Full capacity	2	uint16	10mAh	0~655.35Ah	Checking how many energy BMS can charge
0x1003	Average of cell temperature	2	int16	0.1℃	-40.0~120.0℃	
0x1004	Env temperature	2	int16	0.1℃	-40.0~120.0℃	
0x1005	Warning Flag	2	HEX	bit	0000~FFFF	See section 5.1

Relative Address	Name	Bytes	Data Type	Unit	Range	Remark
0x1006	Protection Flag	2	HEX	bit	0000∼FFFF	See section 5.2
0x1007	Fault/Status	2	HEX	bit	0000∼FFFF	See section 5.3
0x1008	SOC	2	uint16	0.1%	0∼100%	
0x1009	SOH	2	uint16	0.1%	0∼100%	
0x100A	Full charged capacity	2	uint16	10mAh	0∼655.35Ah	
0x100B	Cycle Count	2	uint16	Cycles	0∼65535	
0x100C	Max allowable charging current	2	int16	10mA	-327.68∼327.67A	
0x100D	Max cell voltage	2	uint16	mV	0∼65535mV	
0x100E	Min cell voltage	2	uint16	mV	0∼65535mV	
0x100F	Max allowable discharging current	2	int16	10mA	-327.68∼327.67A	
0x1010	Max cell temperature	2	int16	0.1℃	-40.0∼120.0C	
0x1011	Min cell temperature	2	int16	0.1℃	-40.0∼120.0C	
0x1012	FET temperature	2	int16	0.1℃	-40.0∼120.0C	
0x1013	Work mode	2	int16	N/A	0∼3	See section 5.4
0x1014	Nominal Float voltage	2	uint16	10mV	0∼655.35V	
0x1015	Design capacity	2	uint16	10mAh	0∼655.35Ah	
0x1016 ∼ 0x1020	Reserved	22	-	-	-	
0x1021 ∼ 0x1028	Model of product	16	ASCII	-	-	
0x1029	software version	2	HEX	-	-	
0x102A	hardware version	2	HEX	-	-	
0x102B∼ 0x1034	BMS SN	20	ASCII	-	-	BMS serial number
0x2000	Reserved	2	uint16			
0x2001∼ 0x2015	Pack SN No.	20	ASCII			Pack serial number ”0123456789 0123456789”
0x2016∼ 0x2051	Cell Voltage	30x2	uint16	1mV	0-65535mV	Each two bytes represent one cell voltage 30 cells in total
0x2052	Remaining capacity	2	uint16	0.01Ah	0-655.35Ah	Checking how many energy BMS can use
0x2053	Disable charge MOS	2	ENUM			0: Normal 1: Force switch off
0x2054	Disable discharge MOS	2	ENUM			0: Normal 1: Force switch off

Table 8: Data acquisition

4.2 Information of product

Note:

1. The data of Model of product is same as register 0x1021 ~ 0x1028,the data length is less than 15 ASCII characters, fill it with 0x20;
2. The data of software version is same as register 0x1029;
3. The data of hardware version is same as register 0x102A;
4. The data of Serial number is same as register 0x102B ~ 0x1034, the data length is less than 15 ASCII characters, fill it with 0x20;

	Number of bytes	Example	Note
Model of product	15 (max number of bytes)	P16S50A-6232	ASCII transmission
sofware version	2 (fixed)	0x0100, version: V1.00	16 hexadecimal code
hardware version	2 (fixed)	0x0120, version: v1.20	16 hexadecimal code
serial number	20 (fixed)	20161111011800400000	ASCII transmission

Table 9: Information of product

5 Description

5.1 Warning Flag

Byte Order	**Bit Order**	**Description**	**Remark**
Byte0(Fault)	Bit0	1: battery cell overvoltage alarm; 0: not occuring	
	Bit1	1: battery cell low voltage alarm; 0: not occuring	
	Bit2	1: battery pack overvoltage alarm; 0: not occuring	
	Bit3	1: battery pack low voltage alarm; 0: not occuring	
	Bit4	1: charing over current alarm; 0: not occuring	
	Bit5	1: discharging over current alarm; 0: not occuring	
	Bit6	1: battery high temperature alarm; 0: not occuring	
	Bit7	1: battery low temperature alarm; 0: not occuring	
Byte1(Status)	Bit0	1: Environment high temperature alarm; 0: not occuring	
	Bit1	1: Environment low temperature alarm; 0: not occuring	
	Bit2	1: MOSFET high temperature alarm; 0: not occuring	

Table 10 continued from previous page

	Bit3	1: low capacity alarm; 0: not occuring	
	Bit4	Reserved	
	Bit5	Reserved	
	Bit6	Reserved	
	Bit7	Reserved	

Table 10: Warning Flag

5.2 Protection Flag

Byte Order	Bit Order	Description	Remark
Byte0	Bit0	1: battery cell overvoltage protection; 0: not occuring	
	Bit1	1: battery cell low voltage protection; 0: not occuring	
	Bit2	1: battery pack overvoltage protection; 0: not occuring	
	Bit3	1: battery pack low voltage protection; 0: not occuring	
	Bit4	1: short circuit protection; 0: not occuring	
	Bit5	1: over current protection; 0: not occuring	
	Bit6	1: charging high temperature protection; 0: not occuring	
	Bit7	1: charging low temperature protection; 0: not occuring	
Byte1	Bit0	1: discharging high temperature protection; 0: not occuring	
	Bit1	1: discharging low temperature protection; 0: not occuring	
	Bit2	Reserved	
	Bit3	Reserved	
	Bit4	Reserved	
	Bit5	Reserved	
	Bit6	Reserved	
	Bit7	Reserved	

Table 11: Protection Flag

5.3 Fault/Status Flag

Byte Order	Bit Order	Description	Remark
Byte0(Fault)	Bit0	1: front end sampling communication fault; 0: not occuring	
	Bit1	1: temperature sensor break; 0: not occuring	
	Bit2	Reserved	

	Bit3	Reserved	
	Bit4	Reserved	
	Bit5	Reserved	
	Bit6	Reserved	
	Bit7	Reserved	
Byte1(Status)	Bit0	1: state of charge; 0: not occuring	
	Bit1	1: state of discharge; 0: not occuring	
	Bit2	1: charge MOSFET is ON; 0: charge MOSFET is OFF	
	Bit3	1: discharge MOSFET is ON; 0: discharge MOSFET is OFF	
	Bit4	1: charge limit current function is ON; 0: charge limit current function is OFF	
	Bit5	Reserved	
	Bit6	Reserved	
	Bit7	Reserved	

Table 12: Fault/StatusFlag

5.4 Work Mode Definition

No.	**Work Mode Value**	**Work Mode**	**Description**
1	0	IDLE	Stand by mode
2	1	CHG	Charging process
3	2	DISCH	Discharging process
4	3	FAIL	BMS has an unrepairable failure

Table 13: Work Mode Definiation

6 Change log

Table 14: Change log

Date	Version	Description	Reviser	Reviewer
2021-01-04	V1.0.0	First edition	Donn1e	Jy Chen
2022-06-19	V1.0.2	Remove BCop, adding MOS operation	Donn1e	