JK-BMS: Communication Protocol Between Monitoring Platform and BMS

Version Information

Version	Date	Description	Author
V20191124	Initial Draft		
V20200325	Updated some descriptions, changed 0xA10 to 0xD2, specialized charger switch command		
V20200325	Confirmed the data transfer baud rate to be 115200		
V20200329	Updated and optimized the instruction table, redefined data identifiers		
V20200329	Added command to read all data at once		
V20200427	Added explanation for writing ID and manufacturing date		
V20200429	Added 0xB7 address for software version number		
V20200429	Detailed description for addresses 0x8B and 0x8C		
V20200508	Optimized address 0x84; unit changed from 0.1A to 0.01A		
V20200512	Redefined the name for address 0x81 as internal battery box temperature		
V20200512	Redefined the names for 0xA0 and 0xA1		
V20200512	Added alarm bits to address 0x8B		

Version	Date	Description	Author
V20200526	Added system restart identifier 0xBB		
V20200615	Added 0xB8 identifier, version changed to V2.0		
V20200713	Added 0xBC identifier for factory reset, version changed to V2.1, added 309 fault information		
V20200825	Added 0xBE and 0xBF		
V2.4 20201204	Added 0xC0, redefined current field data	echo	
V2.5 20201217	Added necessary fields for reporting explanation	echo	

Table of Contents

1. Overview

This protocol defines the communication standards between the monitoring platform and the battery terminal, specifying message formats, transmission methods, and communication modes.

2. Referenced Standards

Communications use 2G's GPRS for TCP transmission, 4G's GAT1, SOCKET interface methods, RS232 TTL serial port, with customized communication formats and a baud rate of 115200.

3. Network Topology

This protocol employs a point-to-point or bus architecture involving BMS (Battery Management System), GPS, Bluetooth endpoints, and PC master stations.

4. Protocol Content

4.1 Communication Rules

During communication, the devices have both proactive reporting frames and passive response frames, details of which are as per the communication data format. The minimum interval between each packet is 100 milliseconds, and the longest response packet does not exceed 5 seconds. If the device is in sleep mode, the control end sends activation information to activate the BMS before resuming communication.

4.2 Frame Format

A frame is the basic unit for transmitting information. It includes a start symbol, length, command word, transmission type, information field, end symbol, and checksum. The specific format is as shown in Table 1. Unless explicitly stated, the least significant byte is on the right and the most significant byte on the left. Transmission begins with the most significant bit followed by the least significant bit.

Table 1: Frame Format

Table: Frame Format

Field Number	Frame Unit	Length	Remarks
1	STX	2	Start Frame: 0x4E (78 "N") 0x57 (87 "W")
2	LENGTH	2	Frame Length
3	BMS Terminal No.	4	4-byte ID
4	Command Word	1	Refer to command word explanation
5	Frame Origin	1	0. BMS, 1. Bluetooth, 2. GPS, 3. PC Master Station
6	Transmission Type	1	0. Read Data, 1. Response Frame, 2. BMS Active Upload
7	Frame Info Unit	N	Information field: BMS setting data identification code
8	Record Number	4	The most significant byte is a random code with no meaning (reserved for encryption), the least significant three bytes are the record number
9	End Symbol	1	0X68
10	Checksum	4	Accumulative checksum (the most significant two bytes are for CRC and are not activated, filled with 0; the least significant two bytes are for accumulative checksum)

4.2.1 Frame Start Symbol Field

Two bytes. The first byte is 0x4E and the second byte is 0x57.

4.2.2 Length Field

L: Two bytes, including all data bytes except for the initial two characters, inclusive of the checksum and the length field itself.

4.2.3 BMS Terminal Number

Four bytes in total: FF FF FF FF. The most significant 8 bits are reserved for management backup numbers, and the least significant 24 bits are for the terminal number (the most significant byte is reserved and defaulted to 00, the least significant three bytes are the unique ID number).

4.2.3 BMS Terminal Number

- Consists of four bytes: FF FF FF FF
  - The highest 8 bits are reserved as a management spare number.
  - The lower 24 bits serve as the terminal number.
- Note: The highest byte is reserved and set to default 00, while the lower three bytes serve as a unique ID number.

4.2.4 Command Word Explanation

- A single byte, which defines the transmission function of the frame.

Command Code	Command Function	Remarks
0x01	Activation Instruction	Used to activate the BMS when in sleep mode. Subsequent operations may proceed once a reply is received.
0x02	Write Instruction	Used to configure BMS parameters.
0x03	Read Instruction	Used to read BMS identification data.

Command Code	Command Function	Remarks
0x05	Password Instruction	Must be sent and verified before parameters can be modified.
0x06	Read All Data	Reads the complete set of identification table data in one operation.

4.2.5 Frame Origin Explanation

- A single byte that varies depending on both the sender and receiver.
  - 0: BMS, 1: Bluetooth, 2: GPS, 3: PC Master Station

4.2.6 Transmission Type

- A single byte:
  - 0 represents a request frame.
  - 1 represents a response frame.
  - 2 represents proactive reporting.
- Note: Regardless of who initiates first—whether it be Bluetooth, GPS, PC Master Station, or BMS—the response will always use 1.

4.2.7 Record Number

- The most significant byte is a random code with no meaning (reserved for encryption), and the least significant three bytes are the record number.

4.2.8 End Symbol

- A single byte 0x68

4.2.9 Checksum Field

- The most significant two bytes are for CRC16 and are temporarily unused.

- The checksum is calculated as the sum of all the data bytes from the start symbol to the end symbol.

4.3 Communication Data Format

Example: GPS Read (All, Single) Data Reference

Field No.	Frame Unit	Byte Length	Description
1	STX	2	Start frame: 0x4E (78 "N") 0x57 (87 "W")
2	LENGTH	2	Frame length
3	BMS Terminal No.	4	4-byte ID
4	Command Word	1	Refer to command word explanation
5	Frame Source	1	0. Data Box, 1. Bluetooth, 2. GPS, 3. PC Workstation
6	Transmission Type	1	0. Read data, 1. Response frame, 2. Data Box initiates upload

Field No.	Frame Unit	Byte Length	Description
7	Data Identifier	1	Refer to single data in table 5.1; For all data, fill 0x00
8	Record No.	4	High 1-byte is a random code (reserved for encryption), low 3-bytes are the record sequence number
9	End Identifier	1	0x68
10	Checksum	4	Accumulative checksum

BMS Response

Field No.	Frame Unit	Byte Length	Description
1	STX	2	Start frame: 0x4E (78 "N") 0x57 (87 "W")
2	LENGTH	2	Frame length
3	Terminal No.	4	4-byte terminal ID

Field No.	Frame Unit	Byte Length	Description
4	Command Word	1	Command word
5	Frame Source	1	0. Data Box, 1. Bluetooth, 2. GPS, 3. PC Workstation
6	Transmission Type	1	0. Read data, 1. Response frame, 2. Data Box initiates upload
7	Identifier + Data	1 + N	Identifier + Data
8	Record No.	4	High 1-byte is random (reserved for encryption), low 3-bytes are the record sequence number
9	End Identifier	1	0x68
10	Checksum	4	Checksum

Example: GPS Write Data Reference

Field No.	Frame Unit	Byte Length	Description
1	STX	2	Start frame: 0x4E (78 "N") 0x57 (87 "W")
2	LENGTH	2	Frame length
3	BMS Terminal No.	4	4-byte BMS terminal ID
4	Command Word	1	Refer to the command word description
5	Frame Source	1	0. Data Box, 1. Bluetooth, 2. GPS, 3. PC Workstation
6	Transmission Type	1	0. Read data, 1. Response frame, 2. Data box initiates upload
7	Identifier + Data	1 + N	Identifier + Data
8	Record No.	4	High 1-byte is random (reserved for encryption), low 3-bytes are the record sequence number

Field No.	Frame Unit	Byte Length	Description
9	End Identifier	1	0x68
10	Checksum	4	Checksum

MS Response

Field No.	Frame Unit	Byte Length	Description
1	STX	2	Start frame: 0x4E (78 "N") 0x57 (87 "W")
2	LENGTH	2	Frame length
3	Terminal No.	4	4-byte terminal ID
4	Command Word	1	Command Word (Refer to specific command descriptions)
5	Frame Source	1	0. BMS, 1. Bluetooth, 2. GPS, 3. PC Workstation

Field No.	Frame Unit	Byte Length	Description
6	Transmission Type	1	0. Read Data, 1. Response Frame, 2. BMS Initiates Upload
7	Identifier	1	Write single data (Refer to Table 5.1)
8	Record No.	4	High 1-byte is random (reserved for encryption), low 3-bytes are record number
9	End Identifier	1	0x68
10	Checksum	4	Checksum

Notice for the flag code: (When reading all data, fill the data identification code with 0x00).

5.1 BMS Setting Data Identifier

Direction	Data ID	Description	Bytes	Type	Notes
R	0x79	Single cell voltage	3*n	HEX	
R	0x80	Power management temperature	2	HEX	-40 to 100℃
R	0x81	Internal battery box temperature	2	HEX	-40 to 100℃
R	0x82	Battery temperature	2	HEX	-40 to 100℃
R	0x83	Total battery voltage	2	HEX	
R	0x84	Current data	2	HEX	Discharge and charge currents
R	0x85	Remaining battery capacity	1	HEX	0-100%
R	0x86	Number of temperature sensors	1	HEX	
R	0x87	Battery cycle count	2	HEX	

Direction	Data ID	Description	Bytes	Type	Notes
R	0x89	Total battery cycle capacity	4	HEX	Ah
R	0x8a	Total number of battery series	2	HEX	
R	0x8b	Battery warning information	2	HEX	Various alarms and warnings
R	0x8c	Battery status information	2		
RW	0x8e	Over-voltage protection	2	HEX	1000-15000 (10MV)
RW	0x8f	Under-voltage protection	2	HEX	1000-15000 (10MV)
RW	0x90	Cell over-voltage protection	2	HEX	1000-4500 MV
RW	0x91	Cell over-voltage recovery	2	HEX	1000-4500 MV
RW	0x92	Cell over-voltage protection delay	2	HEX	1-60 seconds

Direction	Data ID	Description	Bytes	Type	Notes
RW	0x93	Cell under-voltage protection	2	HEX	1000-4500 MV
RW	0x94	Cell under-voltage recovery	2	HEX	1000-4500 MV
RW	0x95	Cell under-voltage protection delay	2	HEX	1-60 seconds
RW	0x96	Cell voltage difference protection	2	HEX	0-1000 MV
RW	0x97	Discharge over-current protection	2	HEX	1-1000 A
RW	0x98	Discharge over-current delay	2	HEX	1-60 seconds
RW	0x99	Charge over-current protection	2	HEX	1-1000 A
RW	0x9a	Charge over-current delay	2	HEX	1-60 seconds
RW	0x9b	Balance start voltage	2	HEX	2000-4500 MV

Direction	Data ID	Description	Bytes	Type	Notes
RW	0x9c	Balance start voltage difference	2	HEX	10-1000 MV
RW	0x9d	Active balance switch	1	HEX	0 off, 1 on
RW	0x9e	Power management temperature protection	2	HEX	0-100℃
RW	0x9f	Power management temperature recovery	2	HEX	0-100℃
RW	0xa0	Internal battery box temperature protection	2	HEX	0-100℃
RW	0xa1	Internal battery box temperature recovery	2	HEX	0-100℃
RW	0xa2	Battery temperature protection	2	HEX	0-100℃
RW	0xa3	Battery temperature recovery	2	HEX	0-100℃

Direction	Data ID	Description	Bytes	Type	Notes
RW	0xa4	Battery temperature protection delay	2	HEX	1-60 seconds
RW	0xa5	Maximum charging voltage	2	HEX	1000-15000 MV
RW	0xa6	Minimum discharge voltage	2	HEX	1000-15000 MV
RW	0xa7	Balance voltage	2	HEX	2000-4500 MV
RW	0xa8	Temperature sensor calibration	2	HEX	-500 to 500
RW	0xa9	Total capacity calibration	2	HEX	-1000 to 1000
RW	0xaa	Temperature protection	2	HEX	0-100℃
RW	0xab	Temperature protection recovery	2	HEX	0-100℃
???	0xba	Manufacturer Id	???	???	???

1. For fields ranging from `0x79` to `0xb9`, any field marked with 'R' or 'RW' should be reported. For older versions of the product that haven't implemented this, upgrading is advised. If upgrading is inconvenient, you are suggested to contact technical support at the given phone numbers: 13755639263 or 13480924112.
2. The field `0xBA` is designated for Manufacturer ID naming. This field is primarily intended for use with battery exchange cabinets. If such a requirement exists, this field must be included.