逆变器接口升级协议

09/16/25

Revisions History

Date	Rev.	Description of Changes	Modified by
2023-10-04	0.1	New creation	HJH
2023-10-07	0.2	Add version read Add buffer size setting Add 485 support	HJH
2023-10-08	0.3	Modify 485 I/F data transfer packet Add serial info & hw info get command	HJH
2023-10-09	0.4	Add APP version get command Add whole package integrity check	HJH
2023-10-09	0.5	Change to little endian mode	HJH
2023-10-11	0.6	Change 485 address to 0x5B Add CRC and EOP for 485	HJH
2023-10-12	0.7	Simplify the CRC calculation for ROM saving	HJH
2023-10-15	0.8	Add description of CRC, length, version. Add different address for data transfer.	HJH
2023-10-20	0.9	Change length info for the whole file. Add additional status feed back.	HJH
2023-10-27	0.10	Remove the checksum Add information about number of battery Add additional upgrading method	HJH
2023-10-28	0.11	Combine the running command	HJH
2023-12-08	0.12	Fix errors Add response for 485 data transfer	HJH
2023-12-18	0.13	Fix errors	HJH
2023-12-21	0.14	Add description of upgrading flow for safety	HJH

2024-10-22	0.15	Modify the flow chat	HJH
2025-08-14	0.16	Change h/w serial report information	HJH
2025-09-16	0.17	Add CAN I/F feed back for data transfer	HJH

Index

1 通信格式 5
2 通信命令 6
2.1 准备升级 6
2.2 获取 BOOTLOADER 版本 7
2.3 获取硬件的序列号 8
2.4 获取硬件的型号 10
2.5 获取 APP 版本 11
2.6 获取设备当前的每包字节数 12
2.7 设置设备的每包字节数 12
2.8 发送文件字节长度 13
2.9 发送包序列号 14
2.10 发送数据 15
2.11 发送校验数据 16
2.12 发送升级数据传输结束命令 17
2.13 发送运行命令 18
2.14 查询升级状态 19
3 签名校验 20
4 CRC 计算 20
5 升级流程 21

1 通信格式

对于 CAN 接口，采用 CAN 标准帧，速率:500kbps。每包最多 8 字节数据， 如下图：

CAN ID	长度	地址	命令	参数 1	参数 2	参数 3	参数 4	参数 5

其中：

长度：包含除长度字节外的长度信息，包含地址字节，命令字节以及参数字节。

地址：各个 BMS 的设备地址，0 代表主机地址

命令：升级命令

参数：升级参数

对于 485 接口，主机地址为 0X5B，单双工，波特率为 9600。数据宽度为 8 位，停止位 1 位，无校验。

为保证传输的可靠性，添加了两字节的 CRC 和一字节的结束标记（固定为 0x18）。

ID=0x5B	长度	地址	命令	BYTE0	BYTE1	BYTE2	BYTE3	BYTE4
	.....	.....	.....	.....	.....	.....	.....	.....
	BYTEn	CRC (LSB)	CRC (MSB)	EOP (0x18)				

注意：

- 为防止总线冲突，485 主机接收转发送的间隔，需要大于 10ms。
- CAN 协议受字节长度限制，没有添加 CRC 和 EOP 字节定义。
- 使用 485 协议时，数据长度按实际长度信息发送，不需要 8 个字节对齐。
- 485 协议的长度信息不包含 CRC 字节和 EOP。
- 在计算 CRC 值时，CRC 计算的范围是从长度之后（地址信息开始），直至 CRC 字节之前的字节数据，不包含 ID，长度信息，以及 EOP 字节。（如果 CRC 字节也计算进去时，CRC 的结果固定为 0）

2 通信命令

2.1 准备升级

该命令使对应的 BMS 设备进入升级模式。

主机的命令如下：

ID	长度	地址	命令	参数 1	参数 2	参数 3	参数 4	参数 5
0x300(CAN)/0x5B(485)	0x04	XX	0x10	0x8C	0xBE	XX	XX	XX
	CRC (0xE5)	CRC (0x51)	EOP (0x18)					

当 BMS 设备进入升级模式后，响应如下：

CAN ID	长度	地址	命令	参数 1	参数 2	参数 3	参数 4	参数 5
0x370(CAN)/0x5B(485)	0x05	XX	0x50	0xCC	0xFE	电池数量	XX	XX
	CRC (LSB)	CRC (MSB)	EOP (0x18)					

注意：

CRC 和 EOP 仅用于 485 接口

长度不包含 ID 部分，长度本身，以及 CRC 和 EOP

2.2 获取 BOOTLOADER 版本

该命令用于获取 bootloader 程序的版本信息（底层代码的版本）

主机的命令如下：

ID	长度	地址	命令	参数 1	参数 2	参数 3	参数 4	参数 5
0x300(CAN)/0x5B(485)	0x04	XX	0x20	0x8C	0xBE	XX	XX	XX
	CRC (LSB)	CRC (MSB)	EOP (0x18)					

BMS 设备响应如下：

ID	长度	地址	命令	Build	Patch	Minor	Major	HW
0x370(CAN)/0x5B(485)	0x07	XX	0x60	XX	XX	XX	XX	XX
	CRC (LSB)	CRC (MSB)	EOP (0x18)					

其中，软件版本为 Major.Minor.Patch。

Major 表示为重大功能变化，二进制数据表示。

Minor 为软件局部功能变化，二进制数据表示。

Patch 为软件故障修复，二进制数据表示。

Build 为软件构建号，二进制数据表示。

硬件版本用于标识不同的硬件。采用一字节数据二进制数据表示。这个用于方便主机端适配不同的硬件。

注意：

CRC 和 EOP 仅用于 485 接口

该版本号可以在普通模式下访问

2.3 获取电池的序列号

该命令用于获取电池的序列号，便于主机升级管控。

主机的命令如下：

ID	长度	地址	命令	参数 1	参数 2	参数 3	参数 4	参数 5
0x300(CAN)/0x5B(485)	0x04	XX	0x21	0x8D	0xBE	XX	XX	XX
	CRC (LSB)	CRC (MSB)	EOP (0x18)					

BMS 设备响应如下：

ID	长度	地址	命令	序号	参数 1	参数 2	参数 3	参数 4
0x370(CAN)/0x5B(485)	0x07	XX	0x61	0x01	XX	XX	XX	XX
0x370(CAN)	0x07	XX	0x61	0x02	XX	XX	XX	XX
0x370(CAN)	0x07	XX	0x61	0x03	XX	XX	XX	XX
0x370(CAN)	0x07	XX	0x61	0x04	XX	XX	XX	XX
0x370(CAN)	0x07	XX	0x61	0x05	XX	XX	XX	XX
	CRC (LSB)	CRC (MSB)	EOP (0x18)					

硬件序列号为字符表示(Ascall 码)，最大 30 位字符长度。

只需要回复实际长度字符，不足补 0x00，0x00 为字符串的结束符。

对于 485 接口，可以一包返回。

2.4 获取硬件的信息

该命令用于获取 PCB 的序列号，便于主机升级管控。

主机的命令如下：

ID	长度	地址	命令	参数 1	参数 2	参数 3	参数 4	参数 5
0x300(CAN)/0x5B(485)	0x04	XX	0x21	0x8D	0xBA	XX	XX	XX
	CRC (LSB)	CRC (MSB)	EOP (0x18)					

BMS 设备响应如下：

ID	长度	地址	命令	年	月	日	流水号	
0x370(CAN)/0x5B(485)	0x07	XX	0x61	0x01	XX	XX	LSB	MSB
	CRC (LSB)	CRC (MSB)	EOP (0x18)					

其中：
年： 生产的年份 （23 ~ 99），二进制编码
月： 生产的月份（01~12），二进制编码
日： 生产的日期（1~31），二进制编码
流水号：生产的流水号（0000~9999），二进制编码
注意：
CRC 和 EOP 仅用于 485 接口
该序列号可以在普通模式下访问

2.5 获取硬件的型号

该命令用于获取硬件的型号，便于主机升级管控。

主机的命令如下：

ID	长度	地址	命令	参数 1	参数 2	参数 3	参数 4	参数 5
0x300(CAN)/0x5B(485)	0x04	XX	0x22	0x7D	0xBE	XX	XX	XX
	CRC (LSB)	CRC (MSB)	EOP (0x18)					

BMS 设备响应如下：

ID	长度	地址	命令	机种型号				
0x370(CAN)/0x5B(485)	0x07	XX	0x62	XX	XX	XX	XX	XX
	CRC (LSB)	CRC (MSB)	EOP (0x18)					

机种型号为字符表示(ASCII)，最大 5 个字符，不足填 0.

注意：

CRC 和 EOP 仅用于 485 接口

该机种型号可以在普通模式下访问

2.6 获取 APP 版本

该命令用于获取 application 程序的版本信息

主机的命令如下：

ID	长度	地址	命令	参数 1	参数 2	参数 3	参数 4	参数 5
0x300(CAN)/0x5B(485)	0x04	XX	0x23	0x5E	0xBE	XX	XX	XX
	CRC (LSB)	CRC (MSB)	EOP (0x18)					

BMS 设备响应如下：

ID	长度	地址	命令	Build 0	Build 1	Patch	Minor	Major
0x370(CAN)/0x5B(485)	0x07	XX	0x63	XX	XX	XX	XX	XX
	CRC (LSB)	CRC (MSB)	EOP (0x18)					

其中，软件版本为 Major.Minor.Patch。

Major 表示为重大功能变化，二进制数据表示。

Minor 为软件局部功能变化，二进制数据表示。

Patch 为软件故障修复，二进制数据表示。

Build 为软件构建号，二字节二进制数据表示（LSB 在前）。

注意：

CRC 和 EOP 仅用于 485 接口

该版本号可以在普通模式下访问

2.7 获取设备当前的每包字节数

该命令用于获取设备当前的每包字节数（必须是 2 的幂次）。如果没有特别设置，默认为 128 字节。

CAN 主机的命令如下：

ID	长度	地址	命令	参数 1	参数 2	参数 3	参数 4	参数 5
0x300(CAN)/0x5B(485)	0x04	XX	0x28	9C	DE	XX	XX	XX
	CRC (LSB)	CRC (MSB)	EOP (0x18)					

BMS 设备响应如下：

ID	长度	地址	命令	字节 0（LSB）	字节 1	字节 2	字节 3（MSB）	参数 5
0x370(CAN)/0x5B(485)	0x06 0x07	XX	0x68	XX	XX	XX	XX	XX
	CRC (LSB)	CRC (MSB)	EOP (0x18)					

注意：CRC 和 EOP 仅用于 485 接口

2.8 设置设备的每包字节数

该命令用于设置设备的每包字节数（必须是 2 的幂次）。如果超过设备最大允许的字节，设备返回 NG。 系统默认为 128 字节。

主机的命令如下：

ID	长度	地址	命令	字节 0（LSB）	字节 1	字节 2	字节 3（MSB）	参数 5
0x300(CAN)/0x5B(485)	0x06	XX	0x29	XX	XX	XX	XX	XX
	CRC (LSB)	CRC (MSB)	EOP (0x18)					

BMS 设备响应如下：

ID	长度	地址	命令	参数 1	参数 2	参数 3	参数 4	参数 5
0x370(CAN)/0x5B(485)	0x03	XX	0x69	0xA1(OK) 0x01(NG)	XX	XX	XX	XX
	CRC (LSB)	CRC (MSB)	EOP (0x18)					

注意：CRC 和 EOP 仅用于 485 接口

2.9 发送文件字节长度

该命令发送需要传输的文件字节长度。

主机的命令如下：

CAN ID	长度	地址	命令	参数 1	参数 2	参数 3	参数 4	参数 5
0x300(CAN)/0x5B(485)	0x06	XX	0x30	字节 0 (LSB)	字节 1	字节 2	字节 3 (MSB)	-
	CRC (LSB)	CRC (MSB)	EOP (0x18)					

BMS 设备响应如下：

CAN ID	长度	地址	命令	参数 1	参数 2	参数 3	参数 4	参数 5
0x370(CAN)/0x5B(485)	0x07	XX	0x70	0xA1(OK) 0x01(NG)	字节 0 (LSB)	字节 1	字节 2	字节 3 (MSB)
	CRC (LSB)	CRC (MSB)	EOP (0x18)					

注意：CRC 和 EOP 仅用于 485 接口

2.10 发送包序列号

在数据开始传送前，需要发送包的序列号。

主机的命令如下：

ID	长度	地址	命令	参数 1	参数 2	参数 3	参数 4	参数 5
0x300(CAN)/0x5B(485)	0x04 0x06	XX	0x40	序号 0 (LSB)	序号 1 (MSB)	序号 2	序号 3	-
	CRC (LSB)	CRC (MSB)	EOP (0x18)					

注意：

考虑到兼容性，包序号需要能够同时支持包序号和偏移地址模式。设备需要根据字节长度自动判断该序号使用的是包的序列号还是数据地址。当长度为 0x04 时，使用两字节长度的包序列号。如果长度为 0x06 时，使用的则是数据的地址信息。

BMS 设备响应如下：

CAN ID	长度	地址	命令	参数 1	参数 2	参数 3	参数 4	参数 5
0x370(CAN)/0x5B(485)	0x05 0x07	XX	0x80	0xA2(OK) 0x01(NG)	序号 0 (LSB)	序号 1	序号 2	序号 3 (MSB)
	CRC (LSB)	CRC (MSB)	EOP (0x18)					

注意：

当主机使用包序号时，返回的则是包序号。当主机使用地址时，返回的则是偏移地址。

CRC 和 EOP 仅用于 485 接口

2.11 发送数据

当序列号发送完毕后，需要发送实际的数据，每包固定长度为设定的长度，默认为 128 字节。

CAN ID	BYTE0	BYTE1	BYTE2	BYTE3	BYTE4	BYTE5	BYTE6	BYTE7
0x4C0	XX	XX	XX	XX	XX	XX	XX	XX

.....

.....

CAN ID	BYTE120	BYTE121	BYTE122	BYTE123	BYTE124	BYTE125	BYTE126	BYTE127
0x4C0	XX	XX	XX	XX	XX	XX	XX	XX

使用 485 接口时，因为没有包长限制，可以直接发整包数据。

485 ID	BYTE0	BYTE1	BYTE2	BYTE3	BYTE4	BYTE5	BYTE6	BYTE7
0x5C	XX	XX	XX	XX	XX	XX	XX	XX
	.....	.....	.....	.....	.....	.....	.....	.....
	BYTE120	BYTE121	BYTE122	BYTE123	BYTE124	BYTE125	BYTE126	BYTE127
	CRC (LSB)	CRC (MSB)	EOP (0x18)					

注意：当实际包长不足设置的每包字节数时，用 0xFF 补足包长。

BMS 设备响应如下：

CAN ID	长度	地址	命令	参数 1	CRC	CRC	EOP
0x4C0(CAN)/0x5C(485)	0x03	XX	0x8C	0xA2(OK) 0x01(NG)	CRC (LSB)	CRC (MSB)	EOP (0x18)

2.12 发送校验数据

数据发送完毕后，主机下发校验数据（此为每包的数据校验）。
主机的命令如下：

ID	长度	地址	命令	参数 1	参数 2	参数 3	参数 4	参数 5
0x300(CAN)/0x5B(485)	0x04	XX	0x45	CRC (LSB)	CRC (MSB)	XX	XX	XX
	CRC (LSB)	CRC (MSB)	EOP (0x18)					

BMS 设备响应如下：

ID	长度	地址	命令	参数 1	参数 2	参数 3	参数 4	参数 5
0x370(CAN)/0x5B(485)	0x03	XX	0x85	状态	XX	XX	XX	XX
	CRC (LSB)	CRC (MSB)	EOP (0x18)					

注意：

CRC 和 EOP 仅用于 485 接口。

此处 CRC 为命令包的 CRC 数值。

状态表示了 CRC 校验的结果，定义如下：

数值 （1Byte）	描述
0xA3	CRC OK
0x02	CRC 错误
0x03	数据写入错误
0x04	数据大小错误
0x05	错误固件（签名验证错误）

2.13 发送升级数据传输结束命令

数据发送完毕后，主机下发校验数据。
主机的命令如下：

ID	长度	地址	命令	参数 1	参数 2	参数 3	参数 4	参数 5
0x300(CAN)/0x5B(485)	0x05	XX	0x50	CRC Type	CRC (LSB)	CRC (MSB)	XX	XX
	CRC (LSB)	CRC (MSB)	EOP (0x18)					

注意：数据传输结束后，

CRC 和 EOP 仅用于 485 接口。

此处 CRC 为实际文件长度的 CRC 数值。

为保证扩展性，定义了 CRC 计算的种类，目前，仅支持 MODBUS 的 CRC16 计算

CRC Type	描述
0x00	MODBUS CRC16

BMS 设备响应如下：

ID	长度	地址	命令	状态	参数 2	参数 3	参数 4	参数 5
0x370(CAN)/0x5B(485)	0x03	XX	0x90	XX	XX	XX	XX	XX
	CRC (LSB)	CRC (MSB)	EOP (0x18)					

当校验出错后，返回错误代码。

注意：

CRC 和 EOP 仅用于 485 接口

状态表示了 CRC 校验的结果，定义如下：

数值 （1Byte）	描述
0xA4	CRC OK
0x06	CRC 保存错误
0x07	固件长度错误
0x08	CRC 计算错误

2.14 发送运行命令

该命令允许两种升级模式，模式 1 和模式 2。模式 1 仅支持当前设备的升级，并不会执行多个设备的升级模式。而模式 2 命令仅设备主机支持（地址为 0x00）。选择模式 2 时，设备主机首先完成自身的升级，而后，会依次升级设备从机，直至完成。

命令中的参数 1，用于选择升级模式。0x51 选择模式 1，而 0x52 选择模式 2。

主机的命令如下：

CAN ID	长度	地址	命令	参数 1	参数 2	参数 3	参数 4	参数 5
0x300(CAN)/0x5B(485)	0x04	XX	0x60	0x51 0x52	0x52	XX	XX	XX
	CRC (LSB)	CRC (MSB)	EOP (0x18)					

注意：
CRC 和 EOP 仅用于 485 接口
该命令无返回

2.15 查询升级状态

允许主机查询当前升级状态。

主机的命令如下：

ID	长度	地址	命令	参数 1	参数 2	参数 3	参数 4	参数 5
0x300(CAN)/0x5B(485)	0x02	XX	0x61	XX	XX	XX	XX	XX
	CRC (LSB)	CRC (MSB)	EOP (0x18)					

BMS 设备响应如下：

ID	长度	地址	命令	状态	从机	进度	参数 4	参数 5
0x370(CAN)/0x5B(485)	0x04 0x05	XX	0xA1	XX	XX	XX	XX	XX
	CRC (LSB)	CRC (MSB)	EOP (0x18)					

注意：

CRC 和 EOP 仅用于 485 接口

状态表示了当前升级情况，定义如下：

数值 （1Byte）	描述
0xAA	升级完成（全部从机升级完成）
0xF0	升级失败（其他原因）
0xF1	升级失败（从机升级包校验错）
0xF2	升级失败（从机传输包校验错）
0xF3	升级失败（从机传输超时）
0xF4	指令错误
0x0C	升级数据传输中
0x0D	升级数据校验中
0x0E	运行命令执行中

从机字节表示当前升级的从机。

进度字节表示为当前从机升级的进度的百分比。（暂不支持）

3 签名校验

签名信息添加至升级文件的前 512 个字节。当前 512 个字节数据接收后，BMS 设备会自动进行签名验证。只有签名验证通过后，才会返回 OK 的回复。主机程序无需额外的命令。

4 CRC 计算

使用 CRC16/MODBUS，多项式为 $X^{16}+X^{15}+X^{2}+1$。

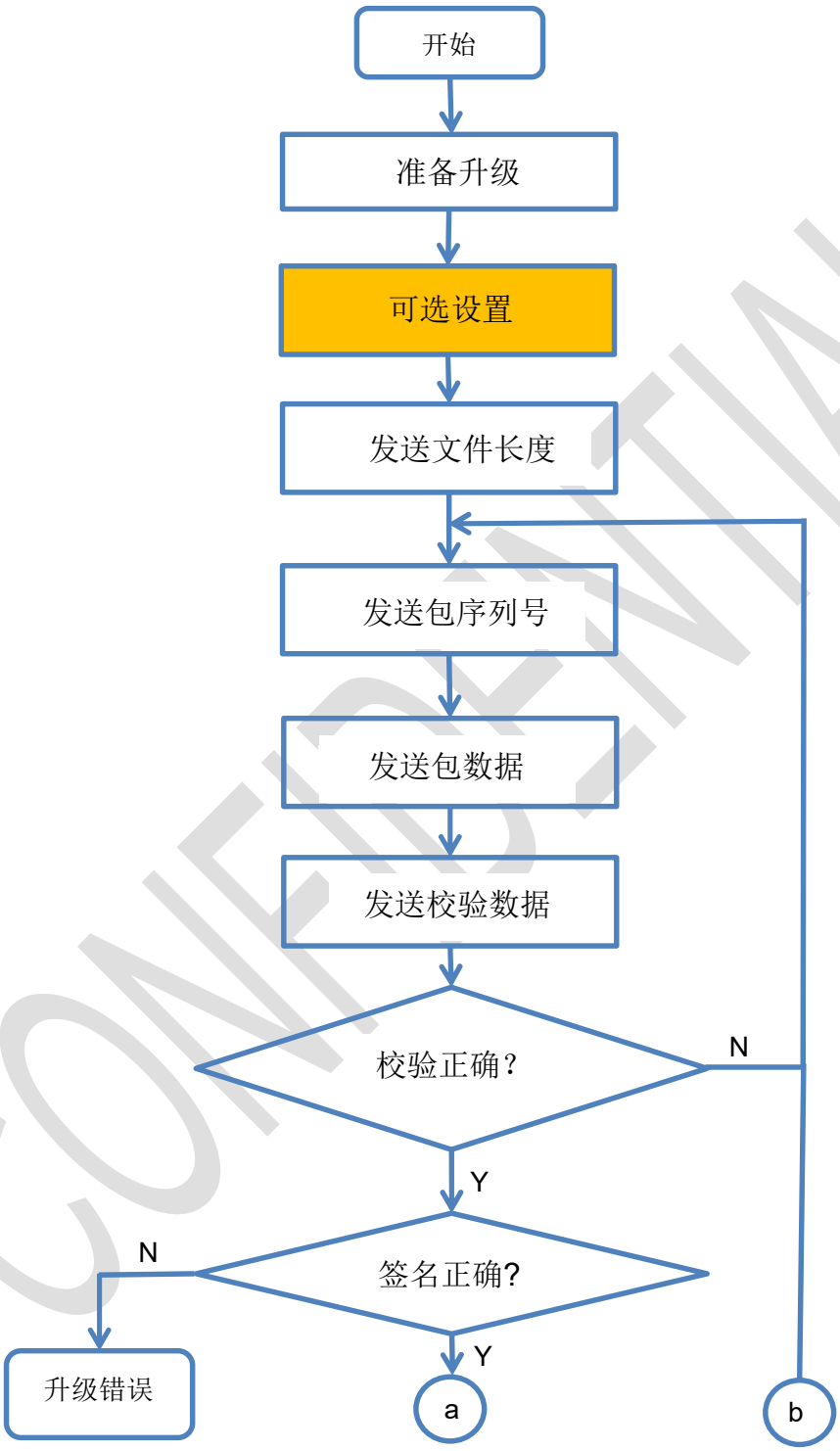
代码如下：

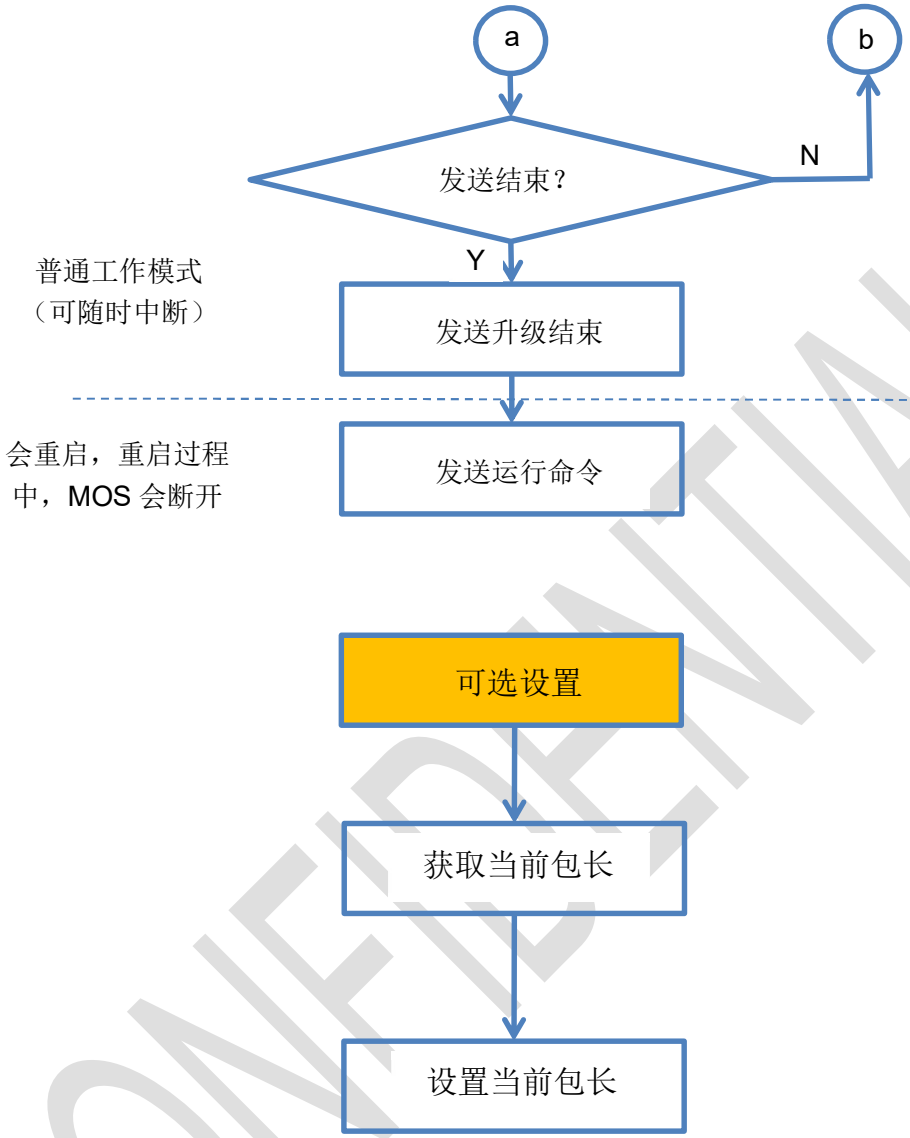
```
uint16_t crc16(uint8_t *ptr, uint32_t len)
{
    unsigned int i;
    uint16_t crc = 0xFFFF;

    while (len--)
    {
        crc ^= *ptr++;
        for (i = 0; i < 8; ++i)
        {
            if (crc & 1)
            {
                crc = (crc >> 1) ^ 0xA001;
            }
            else
            {
                crc = (crc >> 1);
            }
        }
    }

    return crc;
}
```

5 升级流程





注意：

- 可选设置是为了保持主机程序扩展性支持，当前设备默认的为 128 字节的包长。可以跳过，使用默认包长。
- 为保证数据传输的可靠，每包数据会做校验。校验失败，逆变器主机需要重发或停止升级。如果停止升级，BMS 系统处于正常工作模式，可以继续工作。
- 虽然数据传输可以工作在普通模式，但因为涉及到数据存储的操作，且在升级流程最后系统会关闭 MOS 且重启，建议逆变器主机在空闲时（非充/放电状态下）发起升级操作。
- 虽然数据传输可以工作在普通模式，但因为涉及到数据存储的操作，且在升级流程最后系统会关闭 MOS 且重启，建议逆变器主机在空闲时（非充/放电状态下）发起升级操作。

- 为保证系统安全，重启完成后，BMS 会自动开机。此时需要逆变器主机检查版本全部升级无误后，方可使用。