ICS XX.XX.XX
CCS XX

团　　体　　标　　准

T/ CAAMTB XX—2022

电动汽车用电池管理系统设计规范

Design specification of power battery management system for electric vehicles

征求意见稿

2022－XX－XX 发布　　2022－XX－XX 实施

中国汽车工业协会　　发布

目　　次

前　　言

本标准根据GB/T　1.1-2020给出的规则起草。

本文件某些内容可能涉及专利，本文件的发布机构不承担识别这些专利的责任。

本标准由中国汽车动力电池产业创新联盟提出。

本文件由中国汽车工业协会归口。

本文件起草单位：东软睿驰汽车技术（武汉）有限公司、广州汽车集团股份有限公司、国联汽车动力电池研究院有限责任公司、宁德时代新能源科技股份有限公司、中国第一汽车股份有限公司、蜂巢能源科技(无锡)有限公司、华霆（合肥）动力技术有限公司、上海捷能汽车技术有限公司、天津力神电池股份有限公司、江苏高泰昊能科技有限公司、江铃汽车股份有限公司、郑州宇通客车股份有限公司。

本文件主要起草人：刘木林、吴清平、商国平、卜凡涛、邵迪迪、魏咏梅、葛长青、王子冬、王军、刘岩、赵坤、张放南、劳力、朱玉龙、刘彩秋、张伟峰、李启东、佟丽翠、董冰、白福永、唐海波、马小利、赵海陆。

本文件为首次发布。

1 范围

本规范描述了电动汽车动力蓄电池管理系统的设计架构、各个功能项的设计及注意事项、安全相关专题设计、产品开发过程管理、产品测试及生产要求等，同时附录部分提供了一些安全设计的案例。

本规范适用于电动汽车用锂离子动力蓄电池的管理系统，其他类型动力蓄电池的管理系统可参考执行。

2 规范性引用文件

下列文件对于本文件的应用是必不可少的，凡是注日期的引用文件，仅所注日期的版本适用于本文件。凡是不注日期的引用文件，其最新版本（包括所有修改单）运用于本文件。

GB/T XXXXX 电动汽车安全指南

GB/T XXXXX 电动汽车用电池管理系统技术条件

GB/T XXXXX 电动汽车用电池管理系统功能安全要求及实验方法

GB/T 19596 电动汽车术语

GB/T 18384 电动汽车 安全要求

GB XXXXX 电动汽车动用动力蓄电池安全要求

GB/T 31467 电动汽车用锂离子动力蓄电池包和系统

GB/T 34590 道路车辆 功能安全

GB/T 32960 电动汽车远程服务于管理系统技术规范

GB/T 18487 电动汽车传导充电系统

GB/T 27930-2015 电动汽车非车载传导式充电机与电池管理系统之间的通信协议

GB/T 34658-2017 电动汽车非车载传导式充电机与电池管理系统之间的通信协议一致性测试

GB/T 20234-2015 电动汽车传导充电用连接装置

GB/T 17619 机动车电子电器组件的电磁辐射抗扰性限值和测量方法

IEC 61851 电动车辆充电系统

ISO 15118 道路车辆-车辆到电网的通信接口

ISO 26262 道路车辆-功能安全

ISO/IEC 15504 信息技术-软件过程评估

ISO 16750 道路车辆-电气和电子装备的环境条件和试验

3 术语和定义

GB/T 19596 界定的以及下列术语和定义适用于本文件。

3.1

电池控制单元 battery management unit, BMU

包括供电电路、CPU 电路、CAN 通信电路、控制电路等。

3.2

电池检测单元 Cell Module Controller, CMC

负责检测电池单体的电压、温度，单体电池间电量的均衡功能等。

3.3

高压检测单元 high voltage monitor unit, HVMU

负责进行单体电池电压的采集、系统总压的采集、绝缘电阻的监测。

3.4

模拟前端 analog front end，AFE

采集单节电池电压及温度等模拟信号的集成电路。

3.5

电动车辆通信控制器 electric vehicle communication controller，EVCC

安装在电动车辆端的主要实现不同通信协议间转换功能的控制器。

3.6

供电设备通信控制器 supply equipment communication controller，SECC

安装在供电设备端的主要实现不同通信协议间转换功能的控制器。

4 BMS 边界、接口、功能汇总及架构设计

4.1 边界、接口

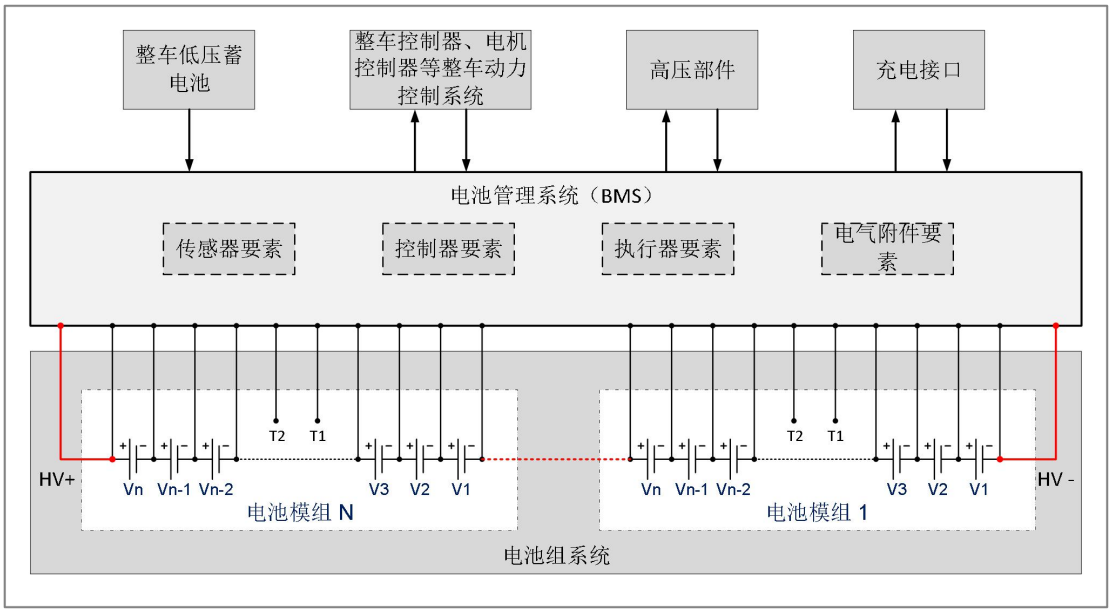


图 4.1 BMS 的边界及接口图

4.1.1 BMS 的要素

BMS 主要要素包括：传感器要素、控制器要素、执行器要素及电气附件要素。

BMS 传感器要素用于测量电池包内部的相关信息，包括但不限于：电芯单体的电压及表面温度、电芯模组电压，电池组电流， 电池组总电压，电池组内部自定义采样点电压、电池组内部自定义采样点温度等。

BMS 控制器要素主要对于传感器要素采集的信息或收到的其他外围系统发送信息进行逻辑判断及算法计算，并与其他外围系统进行信息交互，或控制执行器要素进行工作。

BMS 执行器要素主要根据控制器要素的决策及指令，执行相关动作，典型的动作包括：主负接触器开关控制、主正接触器开关控制、预充电接触器开关控制、冷却水泵控制、冷却风扇控制。

电气附件要素主要对电池包进行安全保护，典型附件包括，保险丝、服务开关等。

4.1.2 BMS 的行为影响假设

BMS 电源部分来源于整车低压蓄电池，影响低压蓄电池能量消耗。

BMS 电源如果部分来源于高压电池组，则影响高压电池组能量消耗。

BMS 影响对外通讯总线上其他系统的工作，如整车动力控制系统（整车控制器、电机控制器等），根据 BMS 预测的功率值作为上限进行动力控制。

4.1.3 BMS 与其它相关项或要素的相互作用

BMS 与整车动力控制系统（如整车控制器、电机控制器）交互，影响整车功率输出。

BMS 与充电接口进行交互，控制交流充电过程，影响车载交流充电回路的工作。

BMS 与充电接口进行交互，控制直流充电过程，影响直流充电回路的工作。

4.1.4 其它相关项、要素和环境要求 BMS 提供的功能

整车动力控制系统要求 BMS 提供电动汽车充电管理功能、电动汽车放电管理功能、电动汽车高压安全监控及保护功能。

电池组系统要求 BMS 提供电动汽车充电管理功能、电动汽车放电管理功能、电动汽车静置（高压断开）状态管理功能、电动汽车高压安全监控及保护功能。

充电接口要求 BMS 提供电动汽车充电管理功能、电动汽车高压安全监控及保护功能、电动汽车高压安全监控及保护功能。

4.1.5 BMS 要求其它相关项、要素和环境提供的功能

BMS 要求整车动力控制系统提供驾驶意图判断功能（上电、上高压、下高压指令）。

BMS 要求整车动力控制系统根据所估计的最大充放电功率限制整车功率输入输出电池包。

BMS 要求电池组系统提供能量输入输出功能。

BMS 要求车载充电系统提供交流充电能量输入管理功能。

BMS 要求直流充电系统提供直流充电能量输入管理功能。

BMS 要求整车动力控制系统、车载充电机等高压部件提供高压互锁接口。

4.1.6 功能在所涉及的系统和要素间的分配

BMS 的电动汽车电池包能量输入输出管理功能的实现涉及 BMS 内部要素包括：传感器要素、控制器要素、执行器要素及电气附件要素。涉及的外部系统包括：整车低压蓄电池、整车动力控制系统、充电系统、电池组系统。

BMS 电动汽车高压安全监控功能的实现涉及 BMS 内部要素包括：传感器要素、控制器要素、执行器要素及电气附件要素。涉及的外部系统包括：整车低压蓄电池、整车动力控制系统、充电系统、电池组系统。

BMS 电动汽车储能电芯安全监控功能的实现涉及 BMS 内部要素包括：传感器要素、控制器要素、执行器要素及电气附件要素。涉及的外部系统包括：整车低压蓄电池、电池组系统。

4.2 BMS 功能总述

BMS 主要包括以下功能，如下表所示，主要分为：电池状态监测、电池状态分析、控制功能、电池安全保护、能量控制管理以及信息管理等 6 大类别，但是在具体项目实施过程中 BMS 的部分功能可能会由不同控制器（例如 VCU）去实现，此种架构称之为广义 BMS 功能划分，被划分到其他控制器的 BMS 功能也需要满足该规范中所提要求。

表 4.2 BMS 功能列表

序号	功能分类	功能	说明

1	电池状态监测	电池单体电压监测	实时监控单体电压值
2		电池总电压监测	根据单体电压值计算总电压
3		充放电电流监测	监测电流大小及方向
4		电池温度监测	通过温度传感器监控部分电池单体温度
5		冷却板进出水口温度监测	监测冷却板在进水口和出水口的温度
6	电池状态分析	SOC 估算	精确计算动力电池剩余荷电值
7		SOP 估算	估算当前电池充放电功率预测
8		SOH 估算	估算动力电池寿命
		SOE 估算	估算动力电池剩余能量
9	控制功能	接触器控制	根据上、下电逻辑准确完成继电器控制
		充放电控制	根据充放电逻辑准确完成继电器控制
		冷却控制	根据冷却需求请求冷却系统的开关
10	电池安全保护	故障诊断及处理	根据故障定义判断故障等级及采取相应措施
11		绝缘电阻监测及漏电保护	监测动力电池对车身绝缘电阻值并能进行报警和保护
12		碰撞断电功能	能够进行碰撞判断及断电功能。能够接收和识别整车碰撞 CAN 信号和硬线型号，并采取相关对策断开动力电池对外输出高压。
13		高压互锁	监测接插件的连接状态
14		继电器状态检测	对电池包内部所有继电器状态进行检测
15		主熔断器状态检测	对主熔断器的状态进行检测
16		CAN 通讯失效保护	对通讯失效进行识别和处理
17	能量控制管理	均衡控制	实现均衡功能
18		电池充电控制管理	实时估算动力电池最大允许充电电流值
19		电池放电管理	实时估算动力电池最大允许放电电流值
20	信息管理	CAN 通讯	符合整车 CAN 通讯协议要求
21		Bootloader 功能	通过 CAN 总线实现在线升级功能
22		故障记忆	存储动力电池故障信息
23		BUS-OFF 功能	实现 CAN 总线故障关断功能
24		内部电源管理功能	按照双方商定的低压下电流程图执行
25		蓄电池电压监测	实时监控蓄电池 12v 电压值
26		远程监控	按照通讯协议要求，能够向 T-BOX 发送相关监控信息；

			支持 CAN 唤醒和 BOOT Loader

4.3 BMS 拓扑结构类型及分析

从 BMS 硬件开发的角度，BMS 硬件电路主要可分为三大功能模块，电池检测单元（Cell Module Controller，CMC）、高压检测单元（high voltage monitor unit，HVMU）负责进行单体电池电压的采集、系统总压的采集、绝缘电阻的监测。和电池控制单元（battery management unit，BMU）包括供电电路、CPU 电路、CAN 通信电路、控制电路等。BMS 的拓扑结构根据 CMC、HVMU 和 BMU 的电路板的构成关系分为集中式 BMS 和分布式 BMS。

CMC、HVMU 和 BMU 设计在同一电路板上为集中式 BMS，也叫一体式 BMS、一体机等叫法。实现 BMS 全部 6 大类功能。因集中式 BMS 硬件的高压区域和低压区域在同一电路板上，所以设计时需注意高低压的隔离。集中式 BMS 一般成本较低，占用电池箱的空间较小，但是集中式 BMS 一般只适用于电池数量不多，电池包体积较小的情况，如果电池数量较多，集中式 BMS 所能提供的接口数量会受到局限，同样的采样线过多、过长也会带来其他潜在安全隐患。

分布式 BMS 一般由一个 BMU、一个 HVMU 和多个 CMC（集中式或分布式）组成。其中 CMC 也分为集中式和分布式两种，集中式 CMC 指单个 CMC 采集板包含一个或多个模拟前端芯片，可采集多个电池模组信息，分布式 CMC 由多个 CMC 采集板构成，每个采集板上的模拟前端芯片数目不定，与电池模组相对应采集。

其中 BMU 主要实现 6 大类功能中的以下功能：

电池状态分析；

控制功能；

电池安全保护；

能量控制管理；

信息管理。

其中 HVMU 主要实现以下功能：

（1） 对整个电池包系统的总电压和总电流进行监测。

（2） 其中 CMC 主要实现以下功能：

（3） 对电池模组的电压和温度进行监测；

（4） 对电池进行具体的均衡控制等。

按照 BMU 和 CMC 之间的通讯方式可将分布式 BMS 分为星型分布式 BMS、总线式 BMS 和菊花链分布式 BMS 示意图分别如下图，图 4.3-1 所示。

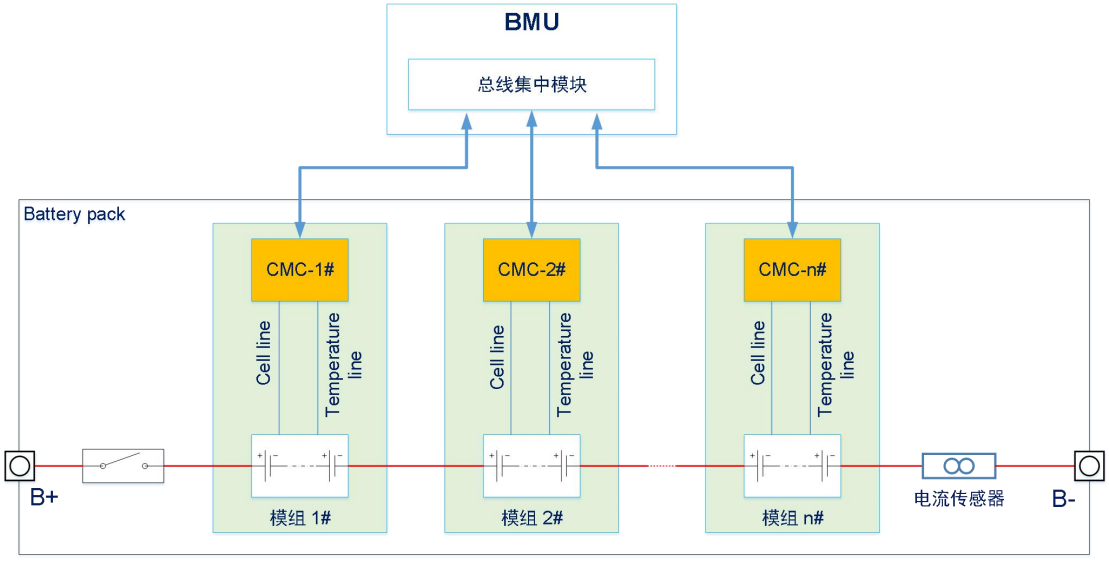


图 4.3-1　星型分布式 BMS

上图所示为星型分布式 BMS 的 BMU 与 CMC 的关系示意，从外观结构上看，BMU 处于中央位置，每个 CMC 通过通讯总线与之相连，通常情况，BMU 会带有一个总线集中模块，使得每个 CMC 可以共享通道。

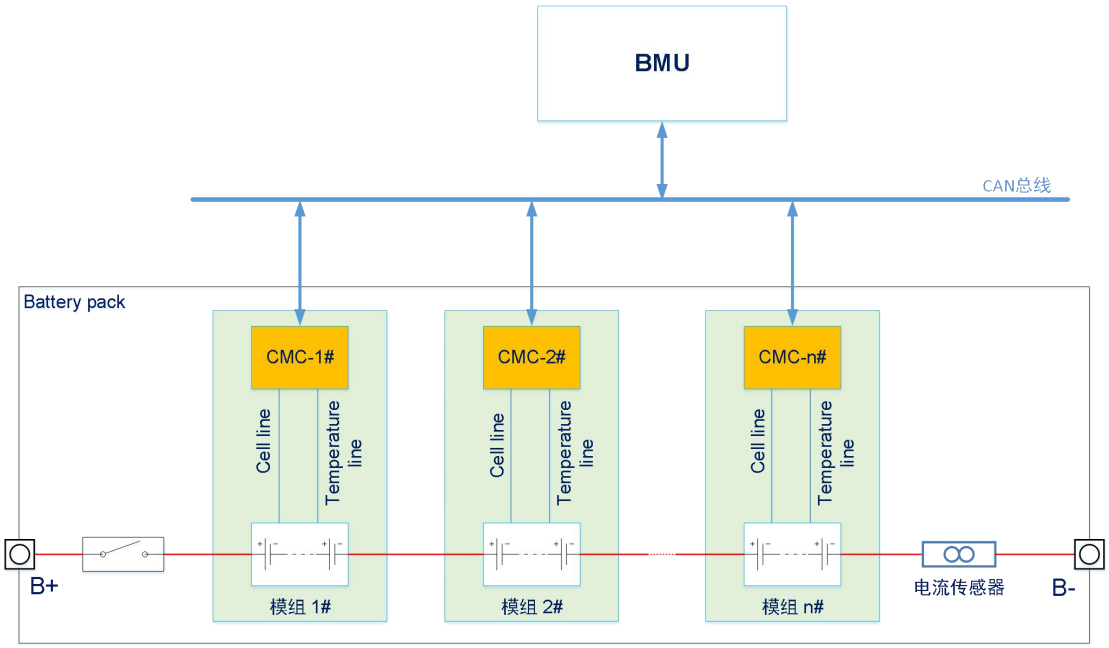


图 4.3-2　总线式 BMS

上图所示为 CAN 总线式 BMS 的 BMU 与 CMC 的关系示意，CAN 总线是汽车上较为常见的一种总线，总线式拓扑结构在电动大巴上较为常见，总线式 BMS 的每一块采集板 CMC，由电压/温度采集回路、单片机 MCU、通信隔离回路等模块构成，CMC 与 CMC 之间通过 CAN 总线链接，从而实现与 BMU 的信息交互。在内部为 CAN 总线的 BMS 系统中，每个 CMC 都独立的处理自己的数据，因此所有的 CMC 功率消耗基本没有差别。

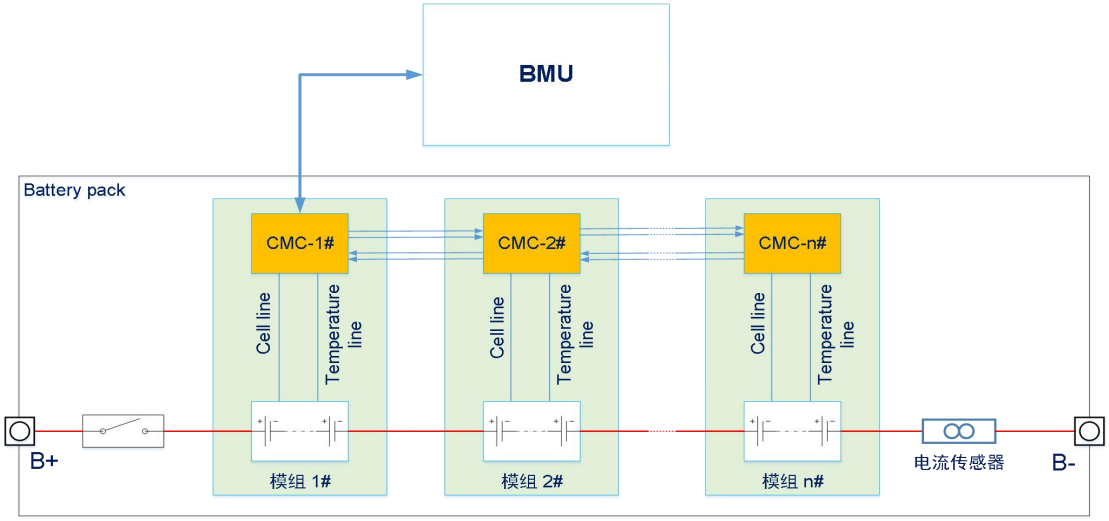


图 4.3-3　菊花链分布式 BMS

上图所示为菊花链分布式 BMS 的 BMU 与 CMC 的关系示意图，CMC 之间通过菊花链式通讯依次相连形成一个环形拓扑结构，在内部通讯方式菊花链通讯的 BMS 系统中，每个 CMC 都有一个“输入”和“输出”接口，每一个 CMC 的输入与下一个的 CMC 的输出接口连接，CMC #n-1 会将数据发送给 CMC #n，CMC #n 会将自身的数据和#n-1 的数据发送给 CMC #n+1。因此相对于 CAN 总线，菊花链的一个优点是如果菊花链中间断开，后面的 CMC 照样可以继续通讯，传

递数据，同时缺点也很明显，跟 BMS 主控制器的那个 CMC 任务是最繁重的，功耗也最大，进一步会引起模组间 Cell 电压差，SOC 差等问题。

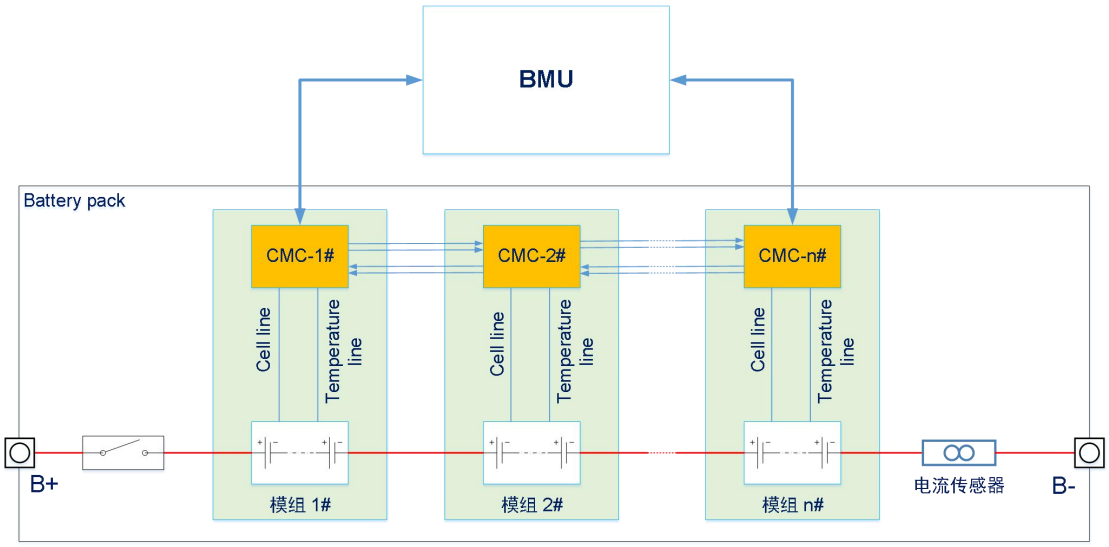


图 4.3-4　菊花链分布式 BMS

在这个菊花链环形架构中，主控制器能够周期形的改变通讯方向，因此 CMC 的平均功耗差不太多，功耗差异会得到极大的改善，而且该环形回路的另外一个好处是，在回路中，不管哪个位置通讯线路断开，都不影响数据传输。如果环状打破在一个特定的链接，然后传输可以通过反向路径，从而确保所有节点始终处于连接状态中的单一故障的情况下被发送。是由一个环路连接的最后一个设备返回到第一个。菊花链不适合长距离通讯，在 HEV 车型中应用更多，大巴车上更多的是 CAN 总线。

（1）其他分布式 BMS 类型：一个 BMU（HVMU 功能集成到 BMU 中）和多个 CMC（集中式或分布式），要注意的是，此方案设计时需注意 BMU 电路板低压和高压的隔离。

（2）广义分布式 BMS：电池包内只有 CMC 和 HVMU，其他功能在整车上其他控制器中实现

5 BMS 安全设计专题

5.1 电池热失控预防及报警机制的设计

5.1.1 诱发热失控的原因

锂电池的热失控主要是由于电池内部产热速率远大于散热速率，在电池内部积累了大量的热量，从而引发单体电池的着火或爆炸。单体电池的热失控又会扩散到整个电池系统，导致整个电池系统甚至整车的起火或爆炸事故。

引发单体锂电池热失控的原因主要分三类：

（1）电池设计缺陷及电池生产制造问题。

（2）电池滥用。如过充、过放后再充电、过温、过流等。

（3）机械损伤。如碰撞。

5.1.2 热失控的预防措施

针对诱发热失控的三类原因，电池设计和机械损伤问题无法通过 BMS 的设计来解决，但是对于电池滥用问题可以通过 BMS 的合理设计来避免。BMS 对于热失控相关的预防措施主要有以下几个方面：

（1）防止电池过充。

在充电的过程中实时监控电池系统中每一个串联单体的电压，不允许超过电池厂规定的充电限制电压（如三元锂电池的 4.2V）。

建议将防止电池过充作为 BMS 的一个功能安全目标，建议设定为 ASIL C 等级。

（2）防止电池过放后再充电。

在放电的过程中实时监控电池系统中每一个串联单体的电压，不允许低于电池厂规定的放电限制电压。

建议将防止电池过放作为 BMS 的一个功能安全目标，建议设定为 ASIL C 等级。

（3）防止过温。

BMS 需实时监控各个单体电池的温度。应设置几级过温报警阀值，当温度超过相应的阀值将采取限制功率输出、断开充放电接触器等措施。

建议将防止电池过放作为 BMS 的一个功能安全目标，建议设定为 ASIL C 等级。

（4）充放电功率限制

在电池充放电过程中，不允许超过电池厂规定的在特定 SOC 及温度条件下的最大允许可充电、放电功率值。同时由于 SOC 的估算误差、温度的测量误差及各单体电池间的不一致性，BMS 要留有足够的余量。特别是对于低温环境下的充电电流，一定不能超过电池厂规定的最大充电电流。建议低温环境下先对电池进行加热再进行充电。

5.1.3 热事件报警机制设计

根据国标“电动乘用车动力蓄电池热事件报警要求”，在电池包发生热事件之前 15 分钟，BMS 需对热事件进行报警。本规范推荐的热失控报警机制设计方法及需要注意的事项如下。

热事件的报警设计分为信号的采集和处理、报警条件的判断、休眠状态下异常唤醒共三个部分。热事件报警设计相关的信号包括温度信号、电压信号、气体压力及成分信号。针对各信号的采集和处理如下。

5.1.3.1 信号的采集和处理

（1）温度信号的采集及处理

数量要求。原则上要求每个单体电池都要有一个温度测量点。如果通过仿真及实验可以验证单个温度测量点能有效反映多个单体电池的温度，则可适当减少温度传感器的数量。需注意的是隔热板的两侧需要分别有两个温度传感器进行测量。

编号要求。温度采集点编号应与单体电池电压采集编号一致。如果是一个温度传感器对应多节单体电池，也需要明确指示出具体所测量的电池单体的编号（与电压测量编号一致）。

传感器需采取一些保护措施，以抵御热失控发生瞬间的高温及液体喷溅。尽量保证在热失控发生后短时间内（推荐 5 秒），传感器能正常使用。（另外，即使温度测量失效也要准确把失效信号报出来）

对温度信号的范围和精度要求与国标“电动汽车用电池管理系统技术条件”的要求相同，同时本标准对采样周期及分辨率也有相应的要求。汇总如附表 5.1-1 所示。

表 5.1-1　温度采集上报要求

指标	要求	备注
范围	-40℃~125℃	
误差	在-20℃~65℃范围（包含-20℃和 65℃），误差不大于+/-2℃；其他范围误差不大于+/-3℃	
分辨率	≤0.5℃	
采集及上报周期	上报周期不大于 200ms 采样周期不大于上报周期	
超范围处理方式	超上限报 125℃。 超下限报-40℃。	

a)　温度极值计算

BMS 应能计算出电池包所有温度点的最大值和最小值以及对应的位置标号。对温度极值的要求与附表 A.1 要求相同。

b)　温度信号有效性

BMS 需对温度信号的有效性进行判断，并且要求在热失控发生后的 5 秒内能够及时、准确的报出。温度信号有效性的判断，推荐使用以下三种方法：

方法一：如果 BMS 的采集芯片有功能安全机制建议开启温度检测通道的校验，设置 FTTI 时间应不大于 5 秒。如果采集芯片报温度采集故障则认为温度采样为无效值。

方法二：同一个点的两个温度传感器比较。对两个温度值（Tn 和 Tn′）做差值，然后取绝对值大于 5℃，该逻辑维持 5 秒认为温度采样失效。

表 5.1-2 温度有效性判断方法二

T 失效置位条件	｜Tn － Tn′｜＞5℃,维持 5 秒
T 失效清楚条件	｜Tn － Tn′｜≤5℃,维持 5 秒

方法三：相邻温度传感器比较，只针对极值点。（主要是防止单一温度条件的误报）当两个极值点温度差在 20℃（可标定）以上时，最高温度点的相邻温度点与最小温度点差值在 5℃（可标定）内，维持 5 秒判断该最大温度失效。温差小于 20℃并维持 5 秒故障清除。

（2）电压信号的采集及处理

模组电压测量要求。为了进行单体电压测量有效性的校验，BMS 除了测量每个串联单体电池之外，还需要对电池模组电压进行测量。

传感器需采取一些保护措施，以抵御热事件发生瞬间的高温及液体喷溅。尽量保证在热失控发生后短时间内（推荐 5 秒），传感器能正常使用。（另外，即使电压测量失效也要准确把失效信号报出来）

对单体电压信号的范围和精度要求与国标“电动汽车用电池管理系统技术条件”的要求相同，同时本标准对采样周期及分辨率也有相应的要求。汇总如表 5.1-3 所示。

表 5.1-3 单体电压采集上报要求

指标	要求	备注
误差	≤10mV	
分辨率	≤1mV	
采集及上报周期	上报周期不大于 100ms 采样周期不大于上报周期	

另外，对模组电压的检测精度要求为+/-0.5FS（满量程）。其他要求同表 2.

a) 单体电压极值计算。BMS 应能计算出电池包所有单体电压的最大值和最小值以及对应的位置标号。对单体电压极值的要求与表 3 要求相同。

b) 单体电压信号有效性。BMS 需对单体电压信号的有效性进行判断，并且要求在热失控发生后的 5 秒内能够及时、准确的报出。对单体电压信号有效性的判断建议使用以下两种方法：

方法一：如果 BMS 的采集芯片有功能安全机制建议开启单体电压检测通道的校验，设置 FTTI 时间应不大于 5 秒。如果采集芯片报单体电压采集故障则认为单体电压采样为无效值。

方法二：模组电压比较法。将模组内所有单体电压值求和，与模组总压进行比较，如果差值大于+/-0.5V 并维持 2 秒（可标定）认为该模组中的单体电压检测失效。

（3）气压测量要求

a) 布置位置。对于良好连通的一个电池包可放置一个气压测量点。多个箱体的 PACK 结构需要在每个箱体中都放置一个气压测量点。

b) 在同一测量点需要有两个气压传感器进行测量，建议两个传感器型号不同。

c) 需保证在热失控发生 5 秒内（具体时间可标定），气压测量功能正常。

（4）通信异常判断

如果采集板与主控板之间的通信异常，则存在热事件发生后采集板损坏的可能。因此建议对通信状态进行监测，推荐的方法包括 CRC、Time out、Rolling counter 三种校验方法。

5.1.3.2 报警条件的判断

热事件发生前一段时间温度信号有一些较明显特征，但也不一定能确认出现这些特征就一定会发生热事件。温度相关的条件包括：

（1）某个温度值大于或等于一定值（推荐温度值 60℃）并且持续一定时间（推荐时间 3 秒）。

（2）温度最大值与最小值的差大于一定值（推荐温度值 20℃）并且持续一定时间（推荐时间 3 秒）。

（3）最高温度值在一定时间内（推荐时间 5 秒）的温升大于或等于一定值（推荐 2℃）。

只要出现三个条件中的任何一个条件就应该引起注意，有可能会发生热事件。相应的处理上仅做低级预警提示、数据的记录及上报给上一级控制单元，不做其他任何实质性措施。另外该预警的一个重要作用是通过车载终端上报大数据监控中心，通过人工分析热事件的可

能性有多大，从而采取进一步措施。

根据实验数据分析，在热事件发生的时刻，如果 BMS 的所有测量值均有效，则可以检测到的故障子条件包括：温度过高，温升过快，电压过低，压降过快，气压波动（可选项）这些信号又分为温度类，电压类，气压类，如果出现任意两类条件同时满足，则可判断发生热事件。另外，由于热事件发生时短时间内大量发热有可能对 BMS 的各个传感器及采集板造成损坏，导致信号的失效。因此一个失效信号组合一个其他类别的故障信号也可判断发生热事件。现将所有热事件报警的组合列举如下表：

表 5.1-3 热失控报警条件汇总

组合类别	序号	条件列举及描述
温度和电压	1	条件①和③同时成立，即温度过高同时电压过低
	2	条件①和④同时成立，即温度过高同时压降过快
	3	条件②和③同时成立，即温升过快同时电压过低
	4	条件②和④同时成立，即温升过快同时压降过快
温度和气压	5	条件①和⑧同时成立，即温度过高同时气压波动
	6	条件②和⑧同时成立，即温升过快同时气压波动
电压和气压	7	条件④和⑧同时成立，即压降过快同时气压波动
	8	条件③和⑧同时成立，即电压过低同时气压波动
失效和其他	9	条件⑤成立，同时条件③④⑧中任意一个成立
	10	条件⑥成立，同时条件①②⑧中任意一个成立，
	11	条件⑦成立，同时条件①②③④⑤中任意一个成立

条件 1——温度过高

置位条件：如果有某个温度值大于或等于一定值（推荐温度值 60℃）并且持续一定时间（推荐时间 3 秒）。

清除条件：该温度值小于一定值（推荐温度值 60℃）持续一定时间（推荐时间 10 分钟）。

条件 2——温升过快 2 级

置位条件：最高温度值在一定时间（推荐 1 秒）内的温升大于或等于一定值（推荐 5℃）。

清除条件：一定时间内（推荐 5 秒）没有新的置位条件则故障清除，如果有新的置位则重新计时一定时间（推荐 5 秒）。

条件 3——电压过低

置位条件：某个电压值在小于等于一定值（推荐 2V）并且维持一定时间（推荐 2 秒）。

清除条件：该电压值大于一定值（推荐 2V）并且维持一定时间（推荐 2 秒）。

条件 4——压降过快

置位条件：最低电压在一定时间（推荐 2 秒）之内下降一定值（推荐 1V）。

清除条件：每隔一定时间（推荐 2 秒）重新判断。

条件 5——温度检测失效

具体方法参照附录 1 部分，另外故障需维持一定时间（推荐 5 秒）。

条件 6——电压检测失效

具体方法参照附录 2 部分，另外故障需维持一定时间（推荐 5 秒）。

条件 7——通信异常

具体方法参照本标准 3.2.3 节，另外故障需维持一定时间（推荐 5 秒）。

条件 8——气压波动（可选项）

置位条件：两个气压传感器测量值在一定时间（推荐 5 秒）时间间隔内都出现过气压大于一定值（推荐值 120KPa）的情况。

清除条件：信号维持一定时间（推荐 5 秒）后无置位条件则故障清除。

车辆处于停泊状态时，如电池发生热失控，BMS 应被唤醒，唤醒信号可以是温度、电压、气压、可燃气体成分等。

5.2 电池异常事件唤醒 BMS 功能的设计

电动汽车在静止过程中，由于 BMS 处于断电状态下，无法对动力电池状态进行实时监控，如果发生电池欠压、过温等严重异常事件时，BMS 无法及时有效地发出报警信息来保证用户的人身安全。为了保证用户的人身安全，及时获取动力电池当前状态，BMS 需要具备电池异常事件唤醒启动的功能。建议的方法包括

（1）设计一个独立的低功耗传感器，实时监测电池状态，一旦监测到严重故障则唤醒 BMS。

（2）利用采集芯片的功能安全机制在 UV/OT 等条件下通过 fault IO 唤醒 BMS。

（3）通过整车和 BMS 低功耗设计实现 24 小时实时监控。

以上三种方式均需要整车为 BMS 提供常电供给，BMS 应具备硬件唤醒、CAN 唤醒、定时唤醒、下电维持运行、唤醒信号输出等功能。以下是此三种方法的详细设计要求：

（1）电池异常监测低功耗传感器唤醒

参数采集：能够对多种参数进行测量，包括箱内温度、气体种类及含量、烟雾浓度、箱内气压、电池间压紧力等；传感器至少能够测量三种以上参数；

异常分析：通过温度变化率及限值、气体种类及占比变化率、烟雾浓度变化及限值、箱内气压变化率及限值、电池间压紧力变化率及限值等，判定动力电池是否出现异常。依据不同参数因子形成分级报警机制，具体要依据模型和实验数据。

异常报警：无故障状态下，传感器处于低功耗模式运行实时监测各类参数。一旦监测到异常事件，触发传感器进入正常工作模式，全速监测并分析故障现象。确认故障发生应及时唤醒 BMS，通过 BMS 唤醒 VCU 或者 T-BOX，进行声音报警，显示信息报警以及远传异常事件发生时的重要数据。从监测到异常事件到触发报警时间建议小于 5s；

性能要求：低功耗工作电流推荐值小于或等于 10mA（在 12V 电压下），睡眠电流推荐值小于或等于 100uA（在 12V 电压下）；

数据存储：能够将异常事件数据（发生前后）进行存储，可以存储 100 条以上事件，先进先出；

可靠性要求：异常事件误报率建议小于 100ppm

（2）前端采集芯片基于功能安全机制唤醒

采用具有功能安全睡眠模式下故障唤醒机制、菊花链级联输出故障信号的前端采样芯片。在睡眠模式下，当电池出现电源过压/欠压、电池欠压/过温、断线等异常状态时，能够将异常信号通过级联输出接口 Fault IO 唤醒 BMS，BMS 读取电池数据，分析并存储故障信息（BMS 能够将异常事件数据（发生前后）进行存储，可以存储 500 条以上事件，先进先出；同时能够存储故障发生时一段时间的数据，数据冻结密度为 500ms。）。同时，BMS 通过硬件或者 CAN 唤醒激活 VCU 或者 T-BOX 发送故障信息到监控平台，严重故障信息（对车辆周围人员可能造成人身伤害）可以通过 VCU 进行整车声光告警提示安全风险。BMS

性能要求：工作电流建议小于或等于 15mA（在通信关闭且均衡关闭的情况下），睡眠电

流建议小于或等于 100uA；

（3）通过整车和 BMS 低功耗设计实现 24 小时实时监控

BMS 系统架构要求：建议电池采集模块采用菊花链通信方式替代 CAN 通信方式，降低系统工作功耗。

电源管理设计要求：

总电源供给采用双电源冗余设计，动力电源 DC/DC 作为主电源，蓄电池电源作为辅助电源，当主电源电量不足时，自动切换到蓄电池电源。当蓄电池电源电量不足时，则关闭 24 小时实时监控功能，并上报电源欠压故障事件。

在泊车静止场景下，整车 VCU 电源关闭，T-BOX 可以允许 BMS 直接通过整车 CAN 进行数据传输。一旦 BMS 监测到故障现象，通过 CAN 唤醒整车 T-BOX 正常工作，BMS 主动上报故障记录三次以后停止上报。T-BOX 在一段时间未接收到 CAN 信息则自动进入休眠模式。

BMS 电源管理设计：采取分布式电源管理策略，电源 A 为能够实时监测电芯状态（电压、温度等）基本电路如主控制器电路、整车 CAN 电路、电芯电压/温度采集电路等供电。电源 B 为充电 CAN 电路、控制管理电路、粘连检测电路、绝缘检测电路等供电。在泊车静止场景下，电源 A 持续工作，电源 B 工作停止（由主控制器根据需求定时关闭或开启），从而达到系统低功耗的目的。

根据任务需求动态调整功能模块工作模式（正常运行、低速运行、待机、休眠、关断）：在泊车静止场景下 T-BOX 处于休眠状态下，每 20S 通过 CAN 唤醒激活一次传输电芯电压、温度等参数。随着故障的严重程度动态调整激活唤醒时间；在满足电芯参数采集及数据传输的条件下尽可能降低主控制工作频率，延长电芯参数传输周期（建议大于等于 1s）。关断充电 CAN、控制器管理等电路，定期开启（建议大于等于 5min）和系统安全相关的电路如绝缘检测电路；降低电芯采样频率和参数更新周期，当检测到参数异常再恢复正常采样功能。

所有电子器件尽可能选择低功耗器件；主控器芯片、通信芯片等需要具备待机、休眠、唤醒功能。

优化软件系统架构、软件结构、分析算法，占用较小资源来进一步降低系统功耗满足 24 小时实时监控的需求。

5.3 BMS 的功能安全要求

国标《电动汽车用电池管理系统功能安全要求及试验方法》规定的安全目标如下：

表 5.4 国标要求的 BMS 功能安全目标

序号	安全目标	ASIL	安全状态	FTTI
1	防止电池单体过充导致热失控	C	断开高压回路	见下文备注
2	防止电池单体过放后再充电导致热失控	C	断开充电回路	
3	防止电池单体过温导致热失控	C	断开高压回路	
4	防止动力蓄电池系统过流导致热失控	C	断开高压回路	

对上表补充说明如下：

（1）不同类型的电池发生热失控的风险大小有可能不同，由此对应的安全目标也可能存在差异。在实际测试的基础上，可以对上表的 ASIL 等级进行调整。

（2）FTTI 代表从故障发生到可能发生危害事件的最短时间间隔，需要在最严苛的工况

下，通过实际测试的方法得到这个时间，以此作为功能安全开发的输入指标，每一个安全目标都需要单独测试。

（3）其它可能的安全目标包括：

a）防止高压互锁故障导致触电；

b）防止绝缘故障导致触电；

c）防止碰撞后电池被破坏导致触电。

这些安全目标可能的 ASIL 等级范围包括 QM、ASIL A 和 ASIL B，跟高压的幅值、电池包的结构、车型的布置等多方面因素有关，具体可根据 GB/T 34590《道路车辆 功能安全》的要求进行分析，然后得出结论。

由于功能安全是基于过程的开发方式，即：将产品从概念到报废的全部生命周期划分为若干阶段，在每个阶段都规定了需要执行的工作任务，同时给出了相应的技术方法和指标，作为该阶段通过的条件。所以，功能安全开发应遵照 GB/T 34590《道路车辆 功能安全》执行，本节仅根据国标《电动汽车用电池管理系统功能安全要求及试验方法》所规定的安全目标概述典型的系统架构。

系统可分为传感器、处理器和执行器三个部分：

（1）传感器：

对于 ASIL C 的安全目标，传感器需要采用冗余、比较的方式，比如同时采集两路电流传感器的数据，在软件里进行相互比较，以确认数据的有效性。不同通道的传感器应彼此隔离，同时应尽量采用异构设计，比如霍尔电流传感器与分流器冗余，以减少共因失效。

如果采用专用芯片作为采样输入，则要求芯片自身对应的安全功能达到 ASIL C 以上的安全等级。有的芯片支持对单体过、欠压的监控功能达到 ASIL C，也有其它芯片支持更多的安全监控比如过温监控、过流监控等，可根据项目需要进行选择。采样芯片选定后，需要根据芯片厂家提供的安全手册进行开发，满足安全手册里规定的限制条件，启用规定的安全机制。

（2）处理器：

单片机最小系统典型的实现方式是一个 MCU 搭配一个 SBC。这两个芯片自身对应的安全功能都要求达到 ASIL C 以上的安全等级。然后需要根据芯片的安全手册进行开发，满足安全手册里规定的限制条件，启用规定的安全机制。

软件方面，底层软件建议使用 AUTOSAR 架构，同时需要启用规定的安全机制如 E2E 校验、存储分区等。应用层软件可参照 EGAS 标准，按照三层监控的架构进行功能和模块分解

（3）执行器：

与功能安全相关的执行器主要是高压继电器。为了保证有效断开及减少共因失效，建议采用两个独立的高压继电器，并将不同继电器的驱动电路进行隔离。如果采用集成的驱动芯片，则建议将高驱和低驱分开，使用不同的芯片。

5.4 电池漏液及爆喷检测功能设计

5.4.1 对电池漏液故障的检测及报警

（1）BMS 具备电池漏液故障的检测功能

BMS 设计增加 CO 气体传感器装置，当电池包内电池发生漏液后，电池会产生 CO 等气体，当 CO 扩散到 BMS 的 CO 气体传感器装置时，传感器输出端有电流输出，BMS 采样电路根据电流大小进行 CO 浓度检测，当气体浓度发生变化时，气体传感器的输出电流也随之变化，BMS 针对不同的检测结果可以分为不同严重故障等级。

（2）报警后处理措施

BMS 对不同故障等级进行报警，可以采取不同的故障处理方式，对车辆可以采取降功率、跛行或者请求下高压处理，甚至需要带载切断高压处理等方式。

5.4.2 电芯爆喷检测功能

对电芯的爆喷检测推荐采用以下方法：电池系统设计时增加每个电芯正负极爆喷检测回路，所有电芯的检测回路串联，当电芯发生爆喷时，正负极对应的检测回路在高温热质的作用下熔断，检测回路变为断路，输出相关信号，BMS对车辆采取降功率、跛行或者请求下高压处理，甚至切断高压处理等方式。

5.5 安全相关信号检测要求汇总

（1）绝缘电阻

动力电池包或高压系统的绝缘电阻，与人员触电、电池包热失控防护均有较强的相关性。当高压系统或电池包绝缘失效时，极大地增加了人员触电的危险性；同时，若电池包进水或高压系统双点绝缘失效，则车辆有较高的起火自燃风险。

（2）高压互锁

高压互锁反映了高压接插件的连接状态，若高压接插件脱落，则高压裸露，存在短路、人员触电等风险；若高压接插件连接状态不良，因接触电阻增大可能使局部过热引起车辆自燃。

（3）碰撞信号监测

接收整车碰撞信号，并及时切断动力电池高压输出，防止因碰撞产生的高压系统破损引起的人员触电或短路起火风险。

（4）温度监测

电芯的温度监测，防止因过温引起的电芯热失控，同时温度是热失控报警中的关键信号

（5）水冷系统进出水口温度监测

电池包水冷系统进出水口温度监测，防止电池包加热功能误启动，使电池包过温发生热失控。

（6）电压监测

电芯、模组和 Pack 的电压监测，防止因过充引起的电芯热失控，同时电压是热失控报警中的关键信号。

（7）电流监测

当监测到高压回路中产生异常大电流时，应及时进行故障动作，切断高压输出。高压短路能够瞬间释放大量的热，若未及时断开高压输出，可能会引起车辆自燃。

（8）气压监测

对电池包内部压力的监测，能够为电池包热失控报警提供有力的信号证据，使热失控报警信号加快报出。

（9）继电器状态监测

继电器物理上决定了动力电池的能量是否能够向外输出，若继电器出现不期望的动作，如粘连故障，则存在较高的人员触电风险。

（10）高压系统母线电压监测

监测高压系统中正负极母线间电压，在动力电池切断高压输出后，系统中仍存储者较多的电能，需通过系统主被动放电功能将电能释放。对其电压的监测可在放电功能异常时提醒用户，降低人员触电的风险。

5.6 电池箱进水或冷却液泄露检测功能设计

若动力电池中的电芯出现电解液泄露，可能会造成不同模组之间外短路，引发电池起火；

若液冷扁管中的冷却液发生泄漏，不同位置电芯在冷却液的作用下形成电势差电解冷却液，从而加剧单体电芯外壳腐蚀造成电芯电解液泄漏，同样可能引发上述危险。所以BMS应具备电池箱进水或冷却液泄露检测功能。

进水检测实现方式：电池系统设计增加电池包底板多个检测线路，当电池箱进水或冷却液泄露后，底板上积聚的水使相互之间断路的检测回路变为通路，输出相关信号，BMS采样电路根据检测回路信号持续时间进行检测，不同的检测结果可以分为不同严重故障等级。BMS对不同故障等级进行报警，可以采取不同的故障处理方式，对车辆可以采取降功率、跛行或者请求下高压处理，甚至切断高压处理等方式。

5.7 电池维护提醒功能设计

5.7.1 纯电动车辆电池维护提醒功能设计

（1）正常运营车辆：正常情况下，每天运营车辆都要有一次满充电，以便对 SOC 进行充满矫正，消除累计误差。若连续 3 天未充满，BMS 宜提醒客户进行满充电，可以在仪表短时间提醒，也可通过智能推送方式直接发送到客户手机提醒，车辆充满后提醒消除。

正常运营车辆，在整车产品服务手册或者售后服务手册要求的时间周期内，未进行电池维护保养，BMS 宜具备提醒功能，可以在仪表短时间提醒，也可通过智能推送方式直接发送到客户手机提醒，电池维护保养后，提醒消除。

正常运营车辆，BMS 检测到电池系统一致性差异过大，影响系统有效容量使用， BMS 宜提醒客户进行均衡保养，可以在仪表短时间提醒，也可通过智能推送方式直接发送到客户手机提醒，均衡保养后提醒消除。

（2）长期停放车辆：在整车产品服务手册或者售后服务手册要求的时间周期内，车辆长期停放未运营，BMS 宜具备定时唤醒并识别和提醒电池维护功能，避免因长时间停放，影响电池一致性。在 BMS 定时唤醒时，当电池电量 SOC 低于 8%时，BMS 宜具备提醒充电维护功能，避免电池过放。提醒方法，可通过智能推送方式直接发送到客户手机，电池正常运营或者维护保养后，提醒消除。

5.7.2 插电式车辆的电池维护提醒功能设计

（1）正常运营车辆：插电式车辆需要定期满充电，以便对 SOC 进行充满矫正，消除累计误差。若连续 1 个月未充满，BMS 宜提醒客户进行满充电，可以在仪表短时间提醒，也可通过智能推送方式直接发送到客户手机提醒，车辆充满后提醒消除。

正常运营车辆，在整车产品服务手册或者售后服务手册要求的时间周期内，未进行电池维护保养，BMS 宜具备提醒功能，可以在仪表短时间提醒，也可通过智能推送方式直接发送到客户手机提醒，电池维护保养后，提醒消除。

正常运营车辆，BMS 检测到电池系统一致性差异过大，影响系统有效容量使用， BMS 宜提醒客户进行均衡保养，可以在仪表短时间提醒，也可通过智能推送方式直接发送到客户手机提醒，均衡保养后提醒消除。

（2）长期停放车辆：在整车产品服务手册或者售后服务手册要求的时间周期内，车辆长期停放未运营，BMS 宜具备定时唤醒并识别和提醒电池维护功能，避免因长时间停放，影响电池一致性。在 BMS 定时唤醒时，当电池电量 SOC 低于 8%时，BMS 宜具备提醒充电维护功能，避免电池过放。提醒方法，可通过智能推送方式直接发送到客户手机，电池正常运营或者维护保养后，提醒消除。

（3）针对插电式车辆频繁按照纯电动模式行驶，造成部分电池异常衰减的风险。BMS 应能识别出电池按照纯电动工况工作的模式，在纯电动模式下，当放电量大于一定值，BMS 宜按照制定的策略对充放电功率进行限制，并在仪表显示“请切换至混动模式”，当司机切换至混动模式后，解除功率限制，取消仪表提醒。

另外,燃料电池车辆、无轨电车车辆等混合动力车型，动力电池维护提醒功能参照插电式车型设计。

5.8 电池维护接口及方法

5.8.1 电池保养维护的意义及内容

与传统燃油车的维护进行对比，电动车虽然没有需要换空气滤清器、换发动机机油的需求，但是对电池系统的维护同样具有重要意义。对于电动车来说，就目前动力电池的技术水平而言，我们对电动汽车的高压绝缘性能、动力电池系统的健康度和安全性等性能的管控措施有效性还需要评估,因此也应给予必要的维护。电动车的维护主要是针对电池组进行维护，通过降低单体电池的一致性差异进而提高整个电池包的可用容量及车辆的续航里程。

5.8.2 电池维护接口

关于电池维护接口方面要求，可参照的标准为：《电动汽车传导电池维护用连接装置标准》。其中规定了连接装置（电池包插座、插头）的技术要求，包括使用环境、结构要求、绝缘防护要求、防水防尘等级等。另外，包括锁止装置、连接线缆等也都进行了技术规范。该标准还规定了对电池维护接口的试验方法及验收准则。

5.8.3 均衡维护方法设计

对单体电芯的均衡补电是电动车维护保养过程中最重要的一项内容。如何在短时间内，将带电量较低的电芯进行补电，同时又不会出现过充电及补电不足的问题。这是评价均衡维护方法是否高效、安全的一个标准。

根据客户对维护时间长短的接收程度不同,我们设计了两种快速均衡补电方法和标准均衡补电方法。快速均衡补电方法没有给整个电池包进行满充电的过程，因此速度较快。完成的时间取决于最低电量单体电芯的电量，通常在半个小时左右时间即可完成。标准均衡补电方法需要先进行满充电过程，如果电池的电量较低会需要长时间的充电过程。

快速均衡补电流程见图 5.8.3.1。其中做几点说明：第一，是否完成均衡的判断依据通常可根据单体 SOC 或单体电压进行判断，考虑到单体 SOC 的计算精度问题，另外部分 BMS 由于算力限制没有该功能。同时根据单体电压进行判断又具有方法简单可靠的特点。因此该方法选用单体电压作为均衡完成的判断依据。第二，由于电池极化电容的存在，该方法在充电的过程中进行。目的是使各单体的极化电压差尽量小，从而尽量减少补电不足的问题。

标准均衡补电流程见图 5.8.3.2。与快速均衡补电流程的区别是加入了为电池充满电的过程，同时判断均衡完成的依据变为达到充电限制电压。使用该方法完成均衡后，电池单体的一致性会更好。如果在时间可接受的前期下建议使用此方法。

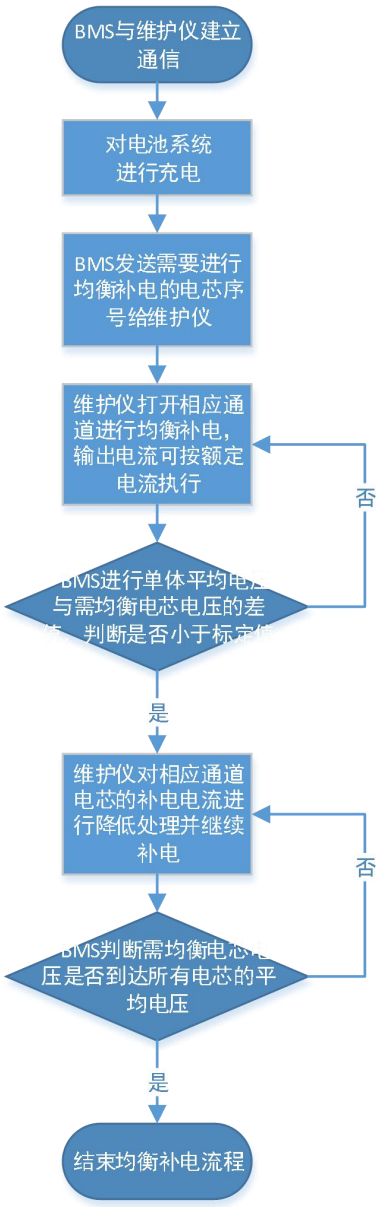


图 5.8.3.1 快速均衡补电流程

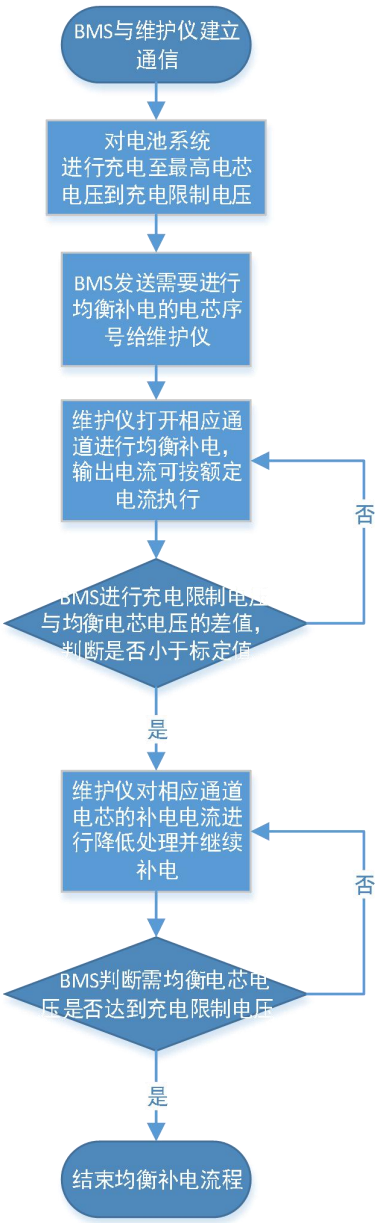


图 5.8.3.2 标准均衡补电流程

6 BMS 基础硬件设计

6.1 电源设计

电源模块为 BMS 提供初始化和正常工作所需的驱动能力，电源模块的设计需要考虑以下内容：

（1）电源供电是否达到要求。

（2）电源模块需有电压采样电路。

（3）接触器需独立供电。

（4）需有隔离、防串扰措施。

（5）静态电流控制，建议小于或等于 200μA。

（6）需设置防反接、瞬态抑制、滤波等保护电路。

6.2 唤醒及休眠功能设计

唤醒和休眠电路设计过程中需要注意以下事项：

（1）通常采用 CAN 唤醒，包括固定 ID 唤醒，但有可能丢失第一帧数据。

（2）唤醒方式也可以采用硬线唤醒等。

（3）休眠时需保持长时间的监控需求。

（4）定时唤醒及功耗要求。

（5）唤醒源之间需采用隔离电路。

对于部分关键电路，须对唤醒源进行保护（稳压管），防止电压过大。

6.3 存储器设计考虑

在存储器选型时，主要考虑以下因素：

（1）低功耗性；

（2）快速读写；

（3）数据保存时间（建议 20 年以上）；

（4）可擦写次数；

（5）可靠性。

6.4 RTC 设计考虑

可设计 RTC 电路、或通过其他方式得到相对时间。RTC 模块在设计时，需要考虑以下因素：

（1）实时性；

（2）高精度；

（3）低功耗；

（4）看门狗功能；

（5）定时输出中断；

（6）定时唤醒功能。

关于实时时钟电源的设计有以下三个方案，对于其优劣、利弊分析如下：

a）使用纽扣电池作为时钟的电源。优势在于设计简单、成本较低。问题在于，使用寿命过低，一般纽扣电池使用年限为 3 年，如果到年限之后时钟信息无法保存，造成 OCV 校准无法进行等后果。

b）使用电容作为电源。优势同样为设计简单、成本低。问题在于，掉电后时钟的保持时间较短。但是如果配合 BMS 接常电使用，同时保证静态功耗的情况下，该问题可以接受。

c）使用可充电的锂电池作为电源。优势使用时间长、寿命长，不存在以上两方法的缺点。但是问题在于一个是成本高，另外还需要加入充电控制电路，设计复杂，增加了风险点。

7 基础软件设计

7.1 AUTOSAR 设计要求

采用 Autosar 架构进行软件开发需注意以下一些事项：

（1）开发流程方面要注意满足其他相关标准，如 IATF16949，A-SPICE，ISO26262 等。

（2）确定 Autosar 开发模式，选择合适的开发工具链

（3）应用层开发：对 ECU 功能进行分解，并进行 SWC 的划分， 同时确定 SWC 各项属性，

以及接口数据的定义，如接口类型、数据类型等。

（4）MCAL 部分：结合 ECU 所需要的处理器及其外设、 传感器、 执行器等参数信息以及硬件设计的需求和约束，对 MCAL 进行配置，实现对 MCU 资源的驱动和管理。其中要考虑对硬件资源分配的优先设计要求，以避免 MCAL 部分再次配置的麻烦。

（5）服务层部分：根据 ECU 设计方案将系统服务、内存服务、通讯服务进行配置和开发，实现底层部分数据的匹配和调度。其中要考虑对通讯协议的优先设计要求，以避免服务层部分再次配置的麻烦。

（6）RTE 部分：实现底层资源管理和应用层 Runnable 的调度，并将底层数据与应用层数据进行映射，使应用层和底层进行融合使之成为一个完整的系统。其中要考虑对资源调度的优先设计要求，以避免 RTE 层部分再次配置的麻烦。

7.2 BootLoader 设计要求

设计 Bootloader 程序时，一般需要考虑如下要点：

（1）确定通讯方式，如 CAN、Uart 等。

（2）设计 Bootloader 与升级上位机间的数据交互协议，一般设计为国际规范性协议如 UDS 等；

（3）提供内部 Flash 或外部存储器的相关操作（擦除、写入、读取）；

（4）提供程序正确性判断算法。

（5）提供程序跳转功能。

（6）在代码更新过程中，出现电压异常、通讯异常等状况，重新上电后软件能够再次被更新。

7.3 UDS 协议设计要求

UDS 协议中需包含如下基本服务：

（1）诊断会话控制；

（2）ECU 复位；

（3）安全访问；

（4）通讯控制；

（5）在线测试；

（6）DTC 设置；

（7）局部标志读数据；

（8）局部标志写数据；

（9）输入输出控制服务；

（10）清除故障码；

（11）读取 DTC 码；

（12）读取控制器码及程序版本信息；

故障代码的设计一般参照 ISO 15031-6。

7.4 CCP/XCP 协议设计要求

CCP 与 XCP 协议设计时需要考虑以下内容：

（1）根据系统的特性合理选择观测变量

（2）设计合理的观测数据的周期以保障不影响 ECU 正常工作

（3）合理设计和选择可标定数据

（4）具有真实物理意义或关键数据能够直接进行读写操作；

（5）能够保存标定数据，并可通过刷写的方式进行数据标定；
（6）设计合理的内存管理方案以对标定数据进行存储和保护；
（7）设计对非常正常数据的处理规范和策略。

8 高压采集功能设计

8.1 电压采集

8.1.1 功能简介

BMS 的高压采样由高压模块完成，主要采集电池总压、母线电压，为策略计算分析提供数据。BMS 可以依据当前采集的电压数据、实时监测电池内总压和高压器件的状态。

8.1.2 电压采集需求

电池包内的高压器件包括母线上的保险丝、多个继电器、高压 MSD 等。这些器件依赖于 BMS 来判断其运行状态，因此需要采集高压器件两端电压来做诊断。

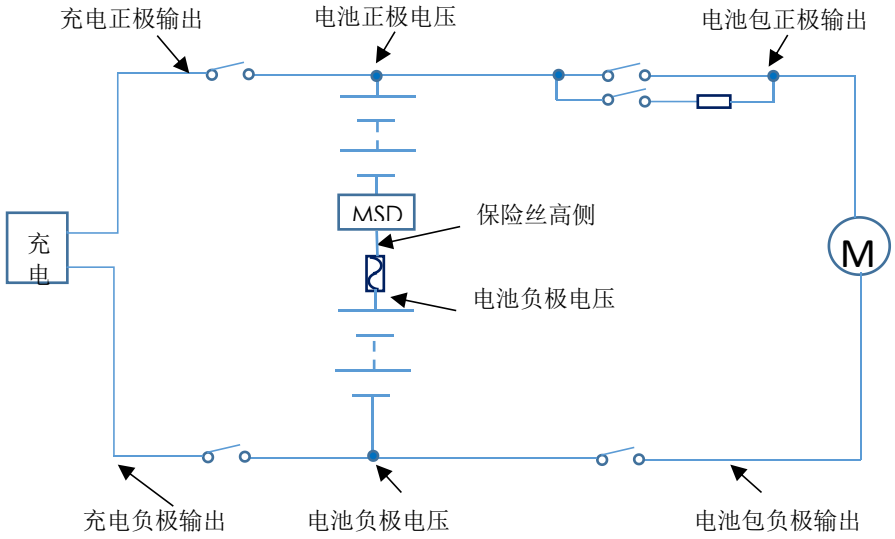


图 8.1 高电压采集点

8.1.3 采集电路要求

鉴于采样电路处于高压模块，其元器件选型参数必须符合电池包高压环境下正常工作范畴，高压采样点应该覆盖母线全线。包括相关开关的前后端。

高低压之间隔离必须满足确保无击穿或放电，需考虑下列内容。

（1）耐压测试:基本的规定是 2×待测物的工作电压+1000V
（2）爬电距离
（3）电气间隙

由于采集电压的数量较多，可通过给采集电路配备开关或其他方式，确保互相之间保持独立采样，不能因为同时采样或者分开采样而出现异常采样现象。设计上需要避免采集电路工作时，使车辆可触摸处带虚电，存在安全隐患，如快充口。

总电压检测精度需不低于满量程的±1%，误差不超过±5V。

采样电路的漏电流的考虑：

（1）在高压采集模块不工作时，少或不消耗电池电量，可以对所有有源输入的监测回路加分断开关，以免在停车时因采样电路漏电消耗电池。

（2）如使用高阻值分压电阻，可减小漏电流。此时应注意 ADC 转换时的采样电流流经采样电阻上形成压降影响采样精度，在靠近 ADC 输入端加入旁路电容。

（3）如加入稳压管保护的，应考虑稳压管漏电流，并选择低漏电流的稳压管。

（4）另外，电路板受污染或滤波电容失效，有可能增加漏电流。应考虑相关保护。

高压电压采样最常见的电路是电阻分压。由于多路高压采样电路的接入，可能会引发串扰。这里的串扰不同于电磁兼容的串扰，是指连接高压采集模块后，在工作状态或非工作状态可能会使原来不该带电的部件或触点带电了，因为对有源信号通过采集电路流通到无源部件。有源信号指电池输出开关前、直接接电池的信号，包括电池正极电压、保险丝两端电压、（如有）高压 MSD 两端电压。这类的采集电路在非工作状态应与其他电路保持分断。对于 EV 快充口，在快充继电器未闭合的条件下，应确保快充口不会接触触电，快充继电器主触点后端的电压采样电路应使用独立开关与其他电路保持分断。

高压采样的电压值，通常通过比较为动力控制策略提高判断依据，因此要求高的采样频率，在相近的时间内完成采样。

8.1.4 采样信号处理

采样信号通过分压、滤波电路，经过 ADC 转换后，传输给底层或应用层后，还需要对采集电压进行处理。底层或应用层需要首先判断采集电压是否是有效值，然后根据电压值进行策略分析，判断是否存在故障以及是否需要采集相关策略措施。策略包括但不限于下列：

（1）电池总压与 BMS 采集到的单体电压之和比较，压差应在允许范围内。否则认为数据无效。

（2）继电器主触点两侧的电压比较，用于判断是否与继电器控制状态一致。是否有异常断开或粘连、正常断开，是否可靠闭合。

（3）保险丝两侧电压比较，特别是运行过程，以确认保险丝的状态，是否有熔断或熔断风险。

8.2 电流采集

电流采样可由磁电式电流传感器、分流器等方案。推荐对于功能安全等级要求较高的系统，可以使用双电流传感器校验策略并在设计中避免共因失效。

电流采集主要关注以下问题：

（1）充放电模式可识别，明确电流方向是充电还是放电；

（2）电流精度；应满足±3% FS（满量程）；

（3）判断采集电流是否有效；

（4）根据采集电流进行故障判断和采取保护策略。

（5）电流更新的速率不低于 50Hz。

8.3 绝缘检测

8.3.1 功能简介

绝缘检测是用于检测电池包高压对整车车身地之间的绝缘状态，车辆启动、行驶或充电工况如绝缘失效，均需报警，避免人员有触电危险。

8.3.2 绝缘要求

电池管理系统不工作时与动力电池相连的带电部件和其供电电源的端子之间的绝缘电阻值应不小于 10 MΩ，工作时与动力电池相连的带电部件和其供电电源的端子之间的绝缘电阻值应满足以下要求：在动力电池最大工作电压下，直流电路绝缘电阻应不小于 100 Ω/V，交流电路应不小于 500 Ω/V。

电池管理系统所检测的状态参数精度要求如下表所示：

表 8.3 绝缘检测精度要求

绝缘监测条件	电池包电压＞400V	电池包电压＜400V
检测精度	-20% ~ +20%	-30% ~ +30%
备注：绝缘电阻小于等于50 kΩ时，检测精度应满足±10 kΩ		

8.3.3 检测方法

BMS 检测绝缘的方法主要有：

（1）国标 GB18384 推荐的平衡桥电阻法，电路参数匹配及设计注意事项。

（2）交流注入法测绝缘，设计注意事项及 EMC 实验经验。

BMS 具备绝缘问题失效点定位功能。

8.3.4 交流注入法检测绝缘简介

从电气层面看，认为电动车辆包含两个电气系统：

（1）以车辆底盘（12V 铅酸电池负极）为电压基准的低压系统

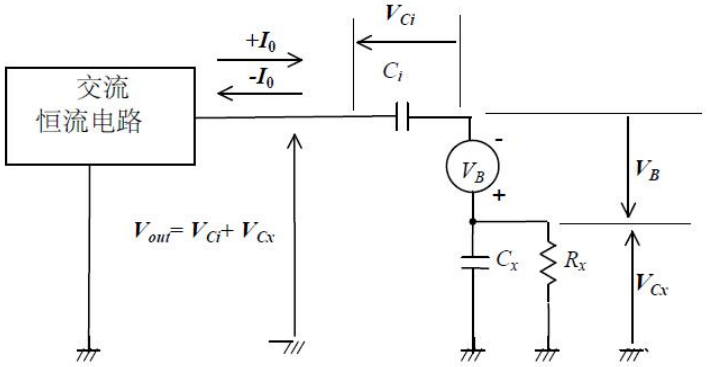
（2）以动力电池总负为电压基准的高压系统

车况良好时，系统间电气隔离。当隔离失效或裂化时，高压系统可能与低压系统建立电流回路，产生人员触电及其它风险。

系统间的绝缘电阻值可一定程度上表征系统间隔离情况，并将其量化表达。因此，电动车辆必须具有绝缘电阻检测能力，对潜在隔离风险进行监测与应对。

与国标规定的直流法相比较，交流注入法的一个明显的优势是在没有高压接入时也可以准确测量到绝缘电阻。特别是对于电动汽车启动过程中，在闭合电池包主接触器之前就可以测出整车的绝缘电阻值，当整车的绝缘状态不佳时可以通过软件策略控制整车不上高压电。

交流注入法的原理简要介绍如下



上图为交流注入法绝缘检测方案的等效原理图，其中：

交流恒流电路为绝缘注入与回检模块

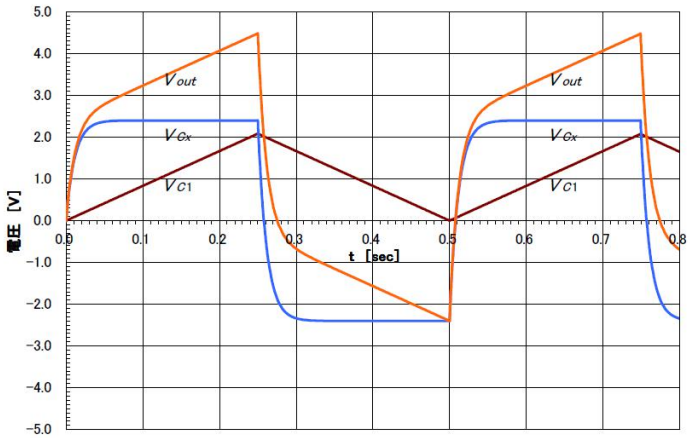
I0 为注入恒流电流，一般设置为 20uA 左右

Ci 为隔离电容，一般设置为 2uF 左右

VB 为动力电池系统总压

Rx 为等效绝缘电阻

Cx 为等效浮游电容
VoutPP 为注入电压峰值



当注入模块以 Ts 周期交流注入电流时，各点电压如图变化。
并根据 KVL 定律：

$$V_{out}(T_s)=V_{ci}(T_s)+V_{cx}(T_s)-V_B=\frac{I_0}{C_i}T_s+R_xI_0\left(1-\varepsilon^{-T_s/\tau_x}\right)-V_B$$

$$V_{out}(2T_s)=V_{ci}(2T_s)+V_{cx}(2T_s)-V_B=-R_xI_0\left(1-\varepsilon^{-T_s/\tau_x}\right)-V_B$$

解方程得：

$$R_x=\frac{V_{out}PP}{2I_0}-\frac{T_S}{C_i}$$

设计注意要点：
（1）实际 Ci 电容耐压值应尽量大，并考虑高压系统降额。
（2）VB 在行车过程中可能产生波动，以非稳态因素引入计算误差。
（3）CX 值为车辆寄生容值，应做充分标定工作后引入计算。
（4）绝缘检测时注意系统间干扰（例如：充电桩接入时）。

9 采集板功能设计

9.1 采集板功能设计

采集板根据当前技术状态，可以通过 CAN、菊花链等通信方式与控制板或者其他采集板进行通信，负责串联电压采集、电池温度采集、加热片等其他温度采集，并对电池以及 PACK 的部分连接问题进行诊断。

采集板可以分为集中式和分布式。集中式采集板本身成本低，结构紧凑，但线束相对复杂；分布式采集板一般随模组进行设计，采集板间通过 CAN、菊花链等通信模式进行通信，线束简单，但成本一般相对会高一点。

9.2 基本功能要求

（1）低压供电建议使用 12V 和 24V 兼容系统，系统供电宽电压范围为 6-32V 可工作。低压功耗分工作功耗和休眠功耗，工作功耗一般不高于 100mA，休眠功耗一般不高于 200uA；

（2）采样供电，可以选择使用被采样电池供电，也可以使用低压隔离供电。如果采用

被采样电池供电，要求工作状态电池功耗不超过 15mA，休眠状态电池功耗不超过 100uA，且每路电池功耗偏差需要控制在 10%以内；

（3）单体采集范围 0-5V，精度需要控制在电池全工作温度范围（-40~65℃）内 3mV 误差，采样周期不超过 50ms；

（4）温度采集范围不低于-40~125℃，精度要求不低于 1℃@(-20℃~45℃)，2℃@(-40℃~125℃)，采样周期不超过 500ms；

（5）需求考虑单体单体与电流的同步采集方案，要求单体电压与电流采集可以同步采样，同步误差不超过 5ms；

（6）与主控通信周期可以调节，周期最低不少于 50ms，且在出现报警时具体呗可以立即上报功能；

（7）地址自分配要求，推荐采集板能够提供地址自分配功能，能够根据物理电池单体的排布顺序自动分配采集板地址，进而能够通过采集板上报次序来与实际电池排布顺序一一对应；

（8）均衡功能要求，要求采集板能够提供电池单体均衡功能，可采用被动均衡或者采用主动均衡方案；

（9）具有电池过压报警、欠压报警、过温报警、欠温报警等保护性报警功能。

9.3 可靠性要求

（1）设计上，均衡需要考虑均衡热失控的可能，建议对均衡区域进行温度采样，来辅助判断均衡热失控；

（2）隔离耐压要求，要求低压与高压，高压与外壳之间，不低于 1000+2U 的隔离耐压要求；

（3）均衡要求：支持温度采样；

（4）隔离耐压特性：AC≥2U+1000V，需要考虑高压供电系统（电池电压）与低压供电系统；高压供电系统对壳体；低压供电系统对壳体；高压供电系统之间，即接插件相邻两个管脚之间的耐压；

（5）绝缘电阻特性：≥10MΩ（系统对外壳）；

（6）EFT 抗扰特性：满足 ISO_7637-3 标准中等级 A 要求，EFT 抗扰除了考虑低压供电系统，还需要考虑高压系统，即所有采样输入接口都需要满足此抗扰要求；

（7）防火等级：满足 UL94-V0；

（8）ESD 抗扰特性：满足 GB 17626.2-2006 标准中 4 级 A 类要求（接触放电±8kV，空气放电±15kV）；

（9）浪涌(冲击)抗扰特性：满足 GB 17626.5-2008 标准中 3 级 A 类要求（测试电压±2KV）；

（10）单线（多线）开路试验：满足 GB/T 28046.1-2011 标准中等级 A 要求；

（11）短路保护试验：满足 GB/T 28046.1-2011 标准中等级 A 要求；

（12）RE（传导发射），CE（辐射发射）特性：满足 GB/T 18655-2010 标准中等级 3 要求；

（13）环境抗扰特性：高温（低温）运行试验满足 GB/T 28046.4-2011 标准中等级 A 要求；

高温（低温）存储试验满足 GB/T 28046.4-2011 标准中等级 A 要求；温度梯度试验满足 GB/T 28046.4-2011 标准中等级 A 要求；稳态湿热试验满足 GB/T 28046.4-2011 标准中等级 A 要求；耐机械振动冲击特性：满足 GB/T 28046.3-2011 标准中等级 A 要求；

（14）供电电压抗扰特性：供电电压叠加交流电压试验满足 ISO 16750-2：2012 标准中

等级 A 要求；供电电压缓降和缓升试验满足 ISO 16750-2：2012 标准中等级 C 要求；供电电压瞬时下降试验满足 ISO 16750-2：2012 标准中等级 A 要求；供电电压骤降的复位性能试验满足 ISO 16750-2：2012 标准中等级 C 要求；供电电压启动特性试验满足 ISO 16750-2：2012 标准中等级 A 要求；

（15）辐射抗扰特性：GB/T 17619-1998 标准中带状线测试法满足等级 A 要求；大电流注入测试法（BCI）满足等级 A 要求；自由场测试法满足等级 A 要求；

（16）耐盐雾特性：满足 QCT 897-2011 标准中等级 A 要求。

9.4 策略要求

（1）推荐系统硬件需要有全时均衡的能力，尽可能的延长均衡时间；

（2）系统需要考虑提供采集板内自主均衡和采集板间均衡策略；

（3）建议采集板存储电池模型以及保护相关参数，方便车电分离使用方案；

（4）为降低大串数应用时主控负担，建议采集板进行 SOC、SOH、SOP 等估算，然后主控进行综合。

9.5 诊断标准

采集板需要提供以下诊断，但不限于以下：

（1）采样断线；

（2）温度断线、温度短路；

（3）均衡开路、均衡短路；

（4）采样 AFE 失效；

（5）采样 AFE 不准确；

（6）采集 AFE 通讯不可靠。

10 高压控制

10.1 高压系统安全设计

为了保证高压系统和使用人员的安全，电池系统高压架构应当考虑正常和异常情况下的高压电路断开和保护的需求，包括但不限于：

（1）在电池系统处于高压下电状态时（非故障状态），所有的接口及高压连接电缆均处于不带电状态，避免由于线缆破损或操作不当导致的触电或短路事故；

（2）根据外部负载电容的预充需求，电池系统设计合适的预充电路，以保证继电器或开关的使用寿命；

（3）在电池系统处于过充/过温/过放等问题时，电池系统应能主动的断开对外的高压连接，保证电池系统的安全；

（4）高压系统中存在相应的设计，应对电池使用过程中可能出现的过流，短路等情况，避免高压连接无法断开的情况发生；特别的，由于当前常用方案中的继电器的特性，尤其应当注意短路情况下的电路保护；

（5）当出现由于某种原因导致的继电器或开关的非预期闭合，电池系统应避免人员对电池系统的操作导致的触电事故。

10.2 电池高压控制系统设计

为了完整实现高压控制功能，BMS 需要设计相应的软件和硬件对高压系统进行相应的高压采样，高压系统控制及高压系统故障诊断。

采样部分详见本规范第 8 章，本章节不再赘述。本章节将从高压系统控制功能和高压系统故障诊断两方面描述 BMS 的设计。

10.2.1 高压系统控制

继电器作为高压控制系统里最常见，也是最普遍的执行器件，BMS 控制其完成了电池系统高压系统的绝大部分控制功能，本章节将着重介绍继电器控制功能的设计。

BMS 应当通过提供独立的高边驱动及低边驱动完成对继电器的控制。

BMS 的高低边设计应当考　虑实际驱动时的功率大小需求，包括瞬时功率和持续功率。

通常情况，不建议使用单独的高边或低边，配合 GND 或电源去控制继电器，避免由于单点失效导致的继电器的无法断开；

BMS 必须对高边输出进行过压/欠压/过流等故障进行诊断。

当使用系统外部输入的电源配合低边进行继电器控制时，BMS 必须对电源进行过压/欠压诊断，　确保继电器稳定，可靠的闭合。

为了保证继电器断开时的性能，BMS 必须根据继电器的参数设计合适的续流电路。

在设计过程中，BMS 应当基于生产/运输/安装/售后维护的需求，设计相应的功能，以满足产品全生命周期的产品需求

10.2.2 高压系统诊断

BMS 应当对高压系统进行实时的监控和诊断，以保证高压系统正常的运行，并在高压系统发生故障时，及时的采取相应的措施保证系统安全。

BMS 进行的高压系统诊断主要包括对 BMS 自身硬件的高压诊断以及对电池高压系统的诊断。其中，BMS 对于自身的高压系统（高压采样，绝缘采样，电流采样等）诊断由其他章节进行详细介绍，本章节不再赘述。本章将主要从几个核心器件和功能的角度，介绍电池高压系统诊断的开规范。

10.2.2.1 继电器故障诊断

为了防止继电器出现非预期的闭合或者非预期的断开，导致产品安全问题和系统功能丧失，BMS 需要具备继电器诊断功能，以配合高压系统控制。

BMS 必须对继电器的触点进行诊断，确认继电器的闭合状态，并识别继电器是否存在粘连和开路等故障。

BMS 应当在合适的时机对继电器的触点进行诊断，具体如下：

（1）在继电器闭合前，应当对继电器的触点进行粘连诊断；

（2）在继电器闭合后、断开前，应当对继电器的触点进行开路诊断；

（3）在继电器断开后，应当对继电器的触电进行粘连诊断

（4）特别的，对于输出到电池系统外部的回路，当回路中继电器数量≥2 时，闭合任意一个继电器前，都应对回路内其他继电器进行粘连诊断；

上述诊断时机在存在重合的情况，根据失效模式及发生概率和发生失效后的风险，在同一时段的诊断，可以考虑只进行一次。

BMS 可以根据需求设计线圈诊断功能，对线圈的短地/短电源/开路进行诊断。

为了保证能提前识别继电器在正常使用过程中的失效风险，BMS 应当能够根据继电器的实际使用数据，评估其寿命情况，并在继电器达到使用寿命后，提示进行维护和更换。

10.2.2.2 预充故障诊断

对于存在预充电路的电池系统，为了避免控制不当或其他故障导致预充电路损坏及预充

失败，BMS 应当具备预充故障诊断的功能。

预充故障诊断应从预充电路损坏的失效模式分析，至少包括以下几种故障诊断：

（1）预充短路/预充过流；

（2）预充回路开路；

（3）预充超时；

在不同的系统设计方案中，还可能存在如下失效模式，在 BMS 设计过程中，应当进行分析和论证，并针对存在失效可能的情况，增加相应诊断：

（1）预充次数过多导致电阻过热；

（2）预充电阻阻值异常（偏大/偏小）。

10.2.2.3 熔断器状态诊断

BMS 应当对电池系统内部的熔断器的状态进行监控，当出现故障后，应当提示更换。

10.3 电池系统高压状态控制及管理

通过 10.1 章节所述的控制及诊断功能，BMS 可以完成电池系统高压状态的控制和管理，本章节将从系统行为上介绍电池高压的控制和状态管理。

10.3.1 电池系统高压状态控制

一般来说，电池系统最主要的高压状态控制行为有两个：高压上电以及高压下电。根据系统架构不同，还可能存在充电控制，加热控制等。本章节将着重介绍高压上电及高压下电。

10.3.1.1 高压上电

高压上电指的是：电池系统通过一系列的动作，完成与外部高压负载系统建立高压连接的过程。通常这一系列的动作主要是由 BMS 控制，整车系统配合完成的。

通常，BMS 控制的高压上电流程至少包含以下几个步骤：

（1）BMS 确认当前状态可以进行高压上电，并将可用状态反馈给整车 VCU；

（2）VCU 根据 BMS 反馈的状态及高压上电需求，发送高压上电指令；

（3）BMS 在收到高压上电指令后，通过一系列高压系统的控制和诊断，完成整个预充过程；

（4）BMS 将已经完成上电的状态反馈给整车 VCU；

（5）VCU 根据电池状态，确认高压上电完成，并开启用电器件。

为了保证安全 BMS 在确认电池状态是否可以进行高压上电时，至少应当保证以下几点状态得到确认：

（1）电池系统无高压安全风险，包括但不限于：高压环路互锁正常，电池系统/整车系统绝缘状态正常，电池系统并未发生过碰撞，热失控等异常；

（2）电池系统功能处于正常的可用状态，电池系统不可用状态包括但不限于：过压、欠压、过温、低温以及其他电池厂家定义的禁止电池使用的状态；

（3）BMS 及高压控制系统未出现不允许高压上电的故障，包括但不限于：电源电压处于正常工作范围、电流/电压/温度采样功能正常，内外部通讯功能正常以及其他 BMS 厂家定义的禁止电池使用的状态；

BMS 与整车进行状态机高压上电指令交互的报文建议增加校验，校验方式可以选择 CRC 或 Rolling Count 等形式。

BMS 应当对预充过程中可能导致预充功能失效的故障进行诊断及处理，避免引发其他问题，如继电器粘连，预充电阻损坏，包括但不限于：

（1）当出现主回路正极/负极继电器粘连等故障时，BMS 应当停止预充；

（2）当出现预充短路、过流、预充电阻过热，预充超时等故障时，BMS 应当停止预充；

（3）整个预充过程中，BMS 应当持续监控系统或继电器的供电电压，避免由于瞬间功率过大导致的继电器不可靠闭合以及其他功能异常；

（3）判断外部电容预充完成的条件应当参考主回路继电器所能承受的最大冲击电流及电压；

BMS 接收到高压上电指令到反馈上电完成状态的时间，根据整车负载端 X 电容及预充电阻型号不同，会存在一定的差异，通常建议控制在 1S 以内。

10.3.1.2 高压下电

高压下电指的是电池系统断开与外部负载连接的过程，高压下电通常有两种原因：

（1）整车系统已经结束所有的高压负载工作，不再需要高压供电了；

（2）电池系统由于各种原因，无法继续使用，必须要断开与负载的高压连接；

根据上述两种原因，可以将高压下电分为两类：正常高压下电和紧急高压下电。

正常的高压下电一般由整车发起。在高压下电前，通常所有用电器件均已关闭，BMS 控制继电器按照流程依次断开并完成相应的诊断。下电完成后，BMS 应将下电完成状态发送给整车，整车再进行负载电容泄放。

紧急高压下电通常由于电池系统出现了无法继续使用的故障，BMS 此时应按照与整车协商一致的通讯协议将故障信息和紧急下电需求发送给整车。在允许的情况下，BMS 应等待整车关断用电器件并发送下电命令后，控制继电器按照流程依次断开并完成相应的诊断。下电完成后，BMS 应将下电完成状态发送给整车，整车再进行负载电容泄放。

为了避免 BMS 等待整车高压下电命令时，电池包出现安全事故，BMS 应对所有需要紧急高压下电的故障的断电时间进行评估， 并设置最长等待时间。超过该等待时间时，BMS 应当强制断开继电器，确保电池包关闭高压输出。

在分析紧急高压下电故障的断电时间时，应当按照最坏情况进行分析，并将故障从发生到能被探测到的时间计算到等待时间内。

BMS 可以在等待高压断电期间，降低电池系统允许使用功率，减小电池系统发生安全事故的风险。

10.3.2 电池系统高压状态管理

BMS 应当将电池系统的高压状态实时反馈给整车。

以下以常见的电池系统为例，介绍 BMS 应反馈的几种电池系统高压状态，不同电池系统可能略有出入，但至少应包含以下状态：

（1）Initial / Wake up

初始状态，BMS 在唤醒后发送的状态。在此状态中，BMS 可以进行自检及电池状态检测。

（2）Standby / Ready

等待高压上电状态，此时 BMS 应已经确认电池系统处于正常状态，可以进行高压上电。通常情况，在没有整车命令的情况下，BMS 不允许独立进行高压上电。

（3）Pre-Charging

预充状态，此时电池系统正在完成预充，建立电池包与负载的高压连接。

（4）Discharging

放电状态，电池系统正常工作状态中的一种，BMS 应当在确认高压连接建立后，再发送该状态。在该状态下执行高压下电，应确认高压连接完全断开后，再跳转到其他状态。

（5）Charging / AC Charging / DC Charging

充电状态，电池系统正常工作状态中的一种，BMS 可以根据不同类型的充电方式区分将 Charging 状态区分为 AC Charging/DC Charging。由于不同厂家对于充电状态定义存在差异，故该状态进入和退出条件应以 BMS 厂商与整车厂协商达成的一致意见为准。

（6）Shut Down / Power Off

高压下电状态，BMS 应在确认电池系统已经完成高压连接断开后，再发送此状态。

（7）Error

故障状态，故障状态通常可以使用故障等级或故障代码表示。当电池系统出现故障时，BMS 可以按照与整车协商一致的通讯协议，将故障等级或故障代码发送给整车，以便整车采取相应的处理措施。

根据不同的电池系统架构及整车需求，还存在如下特例：

（1）如果 BMS 不参与任何的充电控制和判断，可以将放电状态和充电状态合并为一个；

（2）根据整车需求，BMS 可以将热管理状态作为电池系统状态中的一种发送给整车；

（3）上述状态不一定需要通过状态机实现，也可以通过不同的 CAN 信号表示，但需要注意不同的状态可能存在的矛盾。

BMS 将电池系统的高压状态反馈给整车是为了更好的实现整车对于电池系统的管理，所以只要不违法上述原则，允许对上述技术方案进行修改，以适应不同的技术方案需求。

11 BMS 核心算法设计

11.1 SOC 估算方法

SOC 估计方法有很多，现在具备工程化的几种方法如下:安时积分法、带 OCV 修正的安时积分法、离线卡尔曼滤波法及在线卡尔曼滤波法等。安时积分法的精度依赖于电流传感器的精度以及初始 SOC 精度；带 OCV 修正的安时积分法成功解决了初始 SOC 精度不准的问题，得到了广泛的应用，但 SOC 估计精度仍然收到电流传感器精度的影响，导致不可忽略的电流累积误差;离线卡尔曼滤波法可以解决 SOC 精度完全依赖于电流精度的困境,通过电压反馈，实现了 SOC 估计的实时修正，提高了 SOC 估计精度，但 SOC 估计精度更多依赖于等效电路模型参数矩阵的精度，这种方法提出了大量的试验需求，延长了 BMS 开发周期；为了解决这个问题，提出了在线卡尔曼滤波法，对等效电路模型参数在线辨识，降低了离线参数辨识的试验量，缩短了 BMS 开发周期，增强了 SOC 估计方法对电池全生命周期、全工况的适应性，进而提高了 SOC 估计精度。

提高 SOC 估计精度考虑的几个方面：

（1）不同电芯材料体系

不同材料体系采用不同的 SOC 估计方法，以匹配不同的材料体系的 SOC-OCV 曲线特点，也应有不同的 SOC 估计精度要求；

（2）电芯不一致性

电池由于生产水平、使用条件、老化等因素造成的电芯一致性变差给 SOC 估计精度带来较大影响，应充分考虑电芯不一致性带来的影响，对电池单体的最大 SOC 及最小 SOC 分别估计，并在充电过程用最大 SOC 作为充电截至的参考条件之一，在放电过程用最小 SOC 限制电池的放电功率，避免部分电芯长期处于过流状态带来的安全风险；

（3）电池老化

随着电池使用，电池会发生不同程度老化，SOC 估计方法应该具备适应电池全生命周期使用的高精度估计能力，但不同老化阶段的 SOC 估计精度可以不同，建议：对于三元电池，BOL 阶段 SOC 全工况误差宜在 3%以内，EOL 阶段 SOC 全工况误差宜在 5%以内。对于磷酸铁锂电池，全生命周期全工况 SOC 误差在 5%以内

（4）电池使用工况

不同电池使用工况对电池 SOC 估计精度也有较大影响，SOC 估计方法应具备对电池使用工况的适应能力，不同电池使用工况的影响应该可以通过 SOC 估计方法予以消除；

（5）硬件

影响 SOC 估计精度的直接因素是电池电流、电压及温度的采集精度，对于依赖等效电路模型参数矩阵的 SOC 估计方法，SOC 估计精度强烈依赖于电池电流、电压及温度的采集精度，对于等效电路模型参数在线辨识的 SOC 估计方法，SOC 估计精度强烈依赖于电池电流和电压采集精度，对温度采集精度不敏感。

电池是一个复杂的非线性、柔性的电化学系统，SOC 估计精度受到以上多种因素影响，建议 SOC 使用区间的高端及低端各留一部分缓冲区间，以确保电池时刻工作在安全区域。

11.2 SOE 估算方法

SOC 用于表征电池的剩余电量。但是在实际的应用中，用户更关注的是车辆的剩余行驶里程。由于在放电工况下动力电池的端电压呈现下降趋势，使得动力电池在 SOC 较大区间内的能量（W·h）供给能力降低，进而在电动汽车运行过程中 SOC 指标表现出加快下降的趋势。以 SOC 作为充电指标参量，容易导致充电时机的误判，给电动汽车用户造成诸多不便。

动力电池的能量状态（State of Evergy, SOE）作为电动汽车 W·h 单位尺度上剩余能量的比例参数，是电池能量供给能力的直接描述，将其作为电动汽车用户充电指标参量更具优势。SOE 定义为电池当前剩余可用能量与电池满充状态剩余可用能量之比。本节提供两个计算 SOE 的方法。

11.2.1 查表法得到 SOE

SOE 估算使用“平均温度/SOC(最小 SOC)---电芯剩余能量”表格查表计算得到，计算结果乘以电芯节数，再乘以当前电芯 SOH（SOH 限制在 100%-80%之间）。SOE 估算使用平均温度（TBD），计算过程中，查表时平均温度要加入 0.1℃/s（TBD）的变化速率。在无平均温度情况下（计算稍慢）使用最大最小温度的平均值作为平均温度。

表 11.2.1 某型号电池 SOE 对应表（单位 W.h）

SOC / 温度	0	0.2	0.4	0.6	0.8	1
-25	0	24.6103	51.72155	79.86129	109.3153	140.2862
-10	0	29.48648	60.64468	92.67259	126.1121	161.3263
0	0	29.28783	60.32606	92.27443	125.6382	160.7908
10	0	31.84803	65.38884	99.83321	135.7732	173.715
25	0	33.89219	69.63318	106.295	144.518	184.9309
40	0	35.18943	72.4253	110.6339	150.4577	192.6159
50	0	35.59268	73.36346	112.1456	152.5686	195.3828

表格 11.2.1 为某种型号电池的 SOE 对应 SOC/温度表格。仅作为方法描述的示例。实际使用中请注意几个方面：1、在实验条件允许的情况下，表格数据的密度越大越好。上表中 SOC 的密度为 20%，温度大约为 10℃。一般情况下，可将数据密度提高到 SOC 做到 5%，温度差 5℃。2、以上仅一个表格，为初始状态下的对应关系。在 SOH 衰减的条件下还应该有相应的表格进行对应。

11.3 SOH 估算方法

电池管理系统中用 SOH 表征电池的健康状况，SOH 的定义为：电池包在 25° C 下以额定

电流放电至截止电压的总容量，比上BOL情况25°C下以额定电流放电至截止电压的总容量。

本章节推荐一种在线计算的方法来计算SOH。当满足特殊工况要求时，利用公式deltaAh = 电池容量 * deltaSOC计算得到电池容量。该方法的执行流程见下图11.3.1。

在线计算法通过公式 电池容量 = deltaAh / （SOC1 - SOC2）

SOC1：t1时刻电芯的SOC

SOC2：t2时刻电芯的SOC

deltaAh：t1时刻到t2时刻电池的总充放电容量。

在容量计算公式中，为提高容量计算的精度，SOC1与SOC2应当是由静态（1小时静置）查OCV曲线的方式得到，而非SOC模块实时计算的结果。

其中，当同时满足以下条件时，认为获取的SOC1与SOC2以及累计的充放电电量delta Ah有效，并进行电池容量的计算：

1. SOC1与SOC2均在0%与100%之间

2. |SOC1-SOC2|大于等于30%，且小于100%

3. t1时刻到t2时刻之间的（|充电容量|+|放电容量|）应小于等于3*电池容量，防止安时积分的累计误差影响容量计算精度

4. t1时刻到t2时刻之间的时间间隔不应超过3天，防止电池自放电影响容量计算精度

5. t1时刻到t2时刻之间不应出现电流无效故障

计算完成之后应当将SOC1，SOC2，累计充放电电量delta Ah，t1时刻开始的（|充电容量|+|放电容量|，t1时刻开始的累计时间全部清零，避免影响下次计算。

在线计算法在获得新的有效delta Ah与delta SOC之后，应当采用最小二乘法更新电池容量值，将获取的一组delta Ah与deltaSOC视为一组最新测量数据，将电池容量视为待估算的系数，利用最新的测量数据delta Ah，deltaSOC对历史估算得到的电池容量Q进行迭代更新。

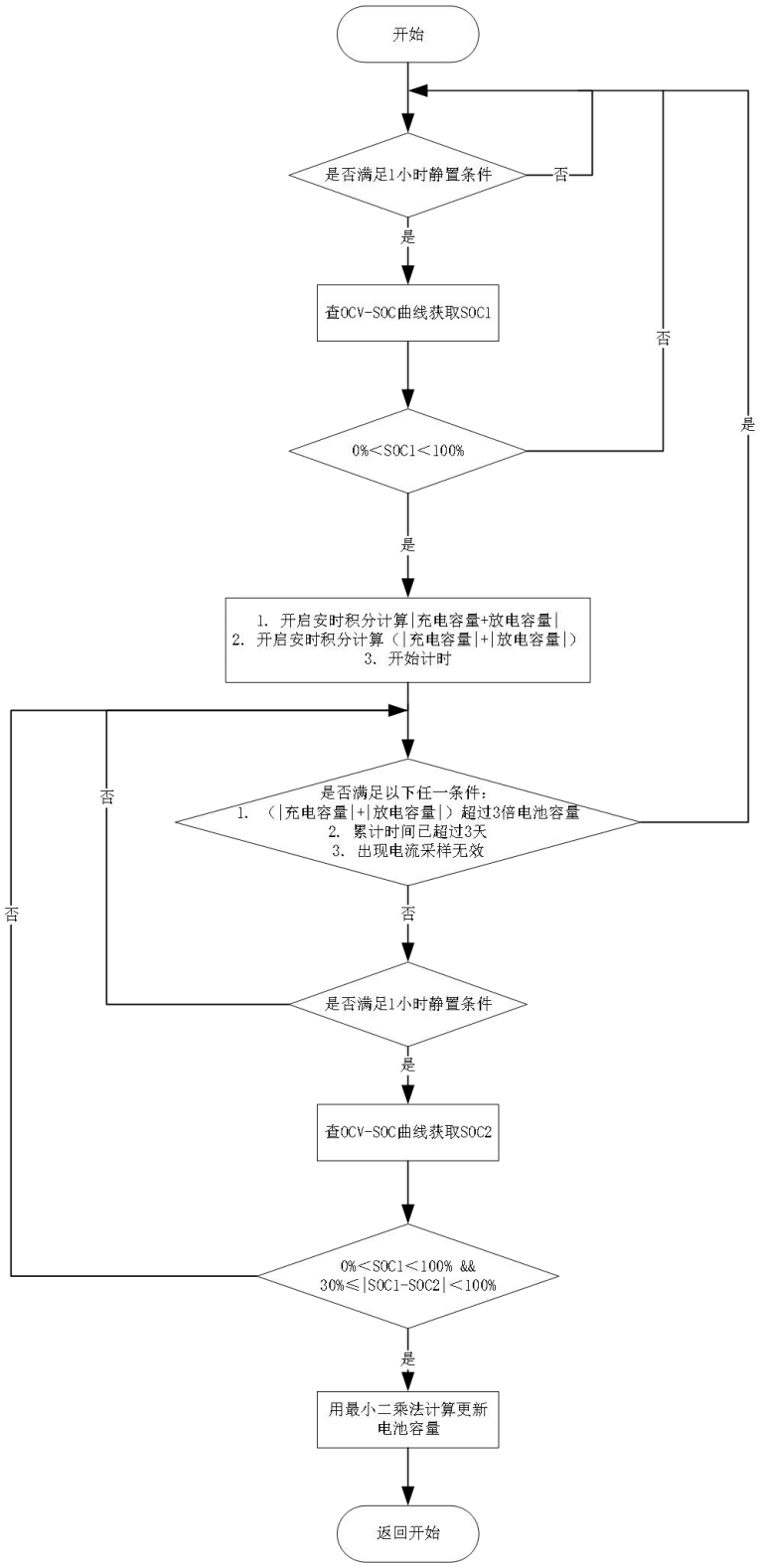


图 11.3.1　SOH 在线计算法流程图

最小二乘法的状态公式为：

$y=Qx+\varepsilon$

y: delta Ah

x: delta SOC
Q: 电池容量
ε：噪声
则带遗忘因子的最小二乘法的递推公式为：

$$k(i)=\frac{P(i-1)x(i)}{\lambda+x(i)P(i-1)x(i)} \quad (1)$$

$$\mathrm{P(i)}=\frac{1}{\lambda}(P(i-1)-k(i)x(i)P(i-1)) \quad (2)$$

$$\varepsilon(\mathrm{i})=y(i)-Q(i-1)x(i) \quad (3)$$

$$\mathrm{Q(i)}=Q(i-1)+k(i)\varepsilon(i) \quad (4)$$

其中：
$k(i)$: 状态方程的误差增益
$P(i)$: 修正系数，INIT：1000000（可标定）
λ:*遗忘因子*，default：0.98（可标定）

11.4 SOP 功能设计

11.4.1 SOP 功能概述及安全设计

SOP估算策略主要是BMS在运行过中要不超过电芯实际输入输出能力。确保电芯在高温情况下限制输出功率，不出现大功率放电造成电芯热失控；确保电芯在低温情况下限制输出功率，不出现大功率放电造成电芯放电析锂；确保电芯在高SOC情况下限制回馈功率，不出现大功率回充造成电芯过充；确保在超高温、超低温情况下限制输入输出功率不允许充放电；同时还需要满足整车运行所需能量。

电池管理系统中功率限值的计算策略，该数据通过CAN发送给整车，向整车提供电池在当前状态下的充电以及放电能力。功率限值应当是考虑了电池的电量，温度，使用工况，故障情况等之后的综合评估结果。通常情况下，有以下几类功率限值的定义：

（1）2s功率限值：2s功率限值又可分为2s放电功率限值P(2s放电)与2s充电功率限值P(2s充电)，实时反馈当前电池能输出的最大充放电功率，若电池以该充电(放电)功率充电(放电)2s及以下，不会造成过压(欠压)故障。

（2）10s功率限值：10s功率限值又可分为10s放电功率限值P(10s放电)与10s充电功率限值P(10s充电)，若该电池以该充电(或放电)功率充电(放电)10s及以下，不会造成过压(欠压)故障。

（3）30s功率限值：30s功率限值又可分为30s放电功率限值P(30s放电)与30s充电功率限值P(30s充电)，若该电池以该充电(或放电)功率充电(放电)30s及以下，不会造成过压(欠压)故障。

（4）持续功率限值：持续功率又可分为持续放电功率限值P(持续放电)与持续充电功率限值P(持续充电)，通常定义为电池可以以该功率进行持续地充电(或放电)，直至电池达到100%SOC（或0%SOC），而不会造成过压（或欠压）故障。

其中，2s，10s，30s功率限值为软件计算的目标结果，持续功率限值为与电池状态相关的电池属性参数，应用在2s，10s，30s功率限值计算中
本策略的目标即为用较合理，考虑较全面的方式实时计算2s，10s，30s充放电功率限值。

11.4.2 SOP 估算方法

功率限值计算整体可以分为两大部分，第一部分为静态功率限值，第二部分为动态功率限值。

静态功率限值指当电池处在稳定状态，在特定的温度以及SOC的状态下，充电功率以及放电功率的限值，静态功率限值通常通过查表取得，功率限值表通过线下标定得到（通常由电芯供应商提供），Pack的功率限值表需要将电芯的功率限值表经过计算处理之后得到。

动态功率限值指的是在静态功率限值的基础之上，考虑历史工况，故障状况，电池的老化状况之后，计算出的电池实际的充电功率限值以及放电功率限值大小。

功率计算策略可参考以下流程图执行（推荐的策略）：

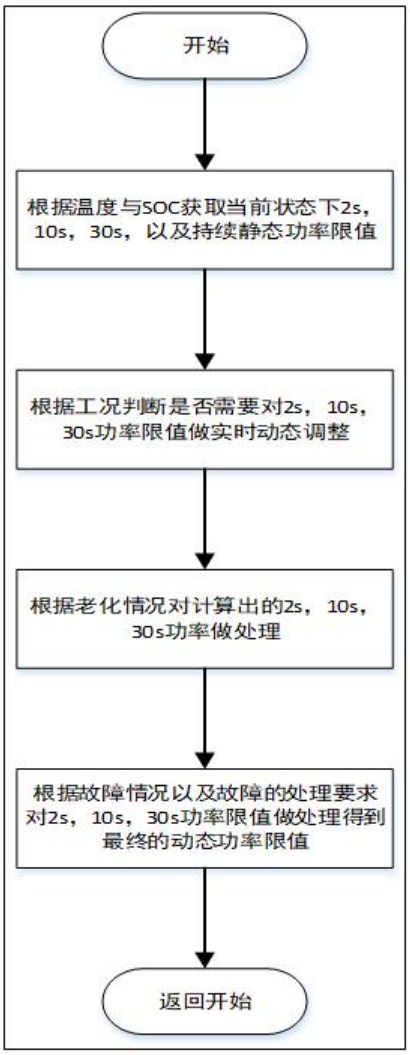


图 11.4 SOP 估算策略流程图

出于安全角度考虑SOP估算策略需注意以下三个方面:

（1）SOP查表估算值是通过当前温度与SOC二维查表查出当前温度与SOC下最大峰值功率和持续功率。其中表格内数据采用二次线性插值的方法进行查表，超范围数值采用边沿值数据；SOP查表估算考虑了电芯单体温度不一致性对SOP估算的影响，对单体最高温度，与单体最低温度同时输入进行查表，然后取两者较小值，确保不论是高温还是低温都不会伤害到电芯；最低单体SOC进行查表，确保最低单体在当前功率下放电也不会出现过放。在充电的情况下，最高单体SOC进行查表，确保最高单体在当前功率下充电（回馈）也不会出现过充。

（2）随着电芯的老化，电芯的实际输入输出能力会逐步降低，这时候我们引入电池健康状态SOH来参与当前SOP估算，根据SOH，同比例降低持续和峰值功率，确保老化后实

际SOP计算值也在电芯允许范围内。

（3）电芯测试数据有峰值功率和持续功率，峰值功率是短时间内输出，电池能达到的最大输出功率值；持续功率是长时间输出时，电池能维持的功率值。基于峰值功率和持续功率，我们可以采用能量积分的方式进行功率切换。

11.5 均衡功能设计

11.5.1 均衡功能概述及安全注意事项

单体电芯间电量的均衡功能主要有两种方式：主动均衡和被动均衡。主动均衡主要是给带电量低的单体电芯进行补电。按硬件实现方式分为电容式、电感式及 DC/DC 形式的主动均衡。硬件结构复杂，成本高，均衡效率较高。主要应用于电池容量较高的电池系统中，比如纯电动大客车上多采用主动均衡。被动均衡主要依靠放电电阻给带电量高的单体电芯进行放电。硬件结构简单，成本低，虽然均衡效率没有主动均衡方式高，但在电池容量不是特别高，有足够的时间进行均衡的场景非常适用，因此在电动乘用车上广泛使用。下面主要说明被动均衡的安全设计注意事项及相关的被动均衡策略设计。

在设计被动均衡策略时应着重注意以下几点安全事项：

（1） 避免由于均衡的开启导致单体电芯出现过放电现象。

（2） 对于均衡区域的温度要进行实时监控，防止温度过高造成的一系列问题。

（3） 对均衡回路要进行开路及短路的诊断。

另外，还需要防止由于均衡条件的误判导致加剧电池间电量的不一致性，从而降低整个电池包可用电量，降低整车的续航里程及使用寿命。因此一个准确、实时、高效率的均衡处理策略至关重要。下面就被动均衡控制策略做设计规范。

11.5.2 被动均衡控制策略设计

均衡策略主要涉及三大部分，分别为均衡计算，均衡控制与均衡诊断。均衡计算主要包含均衡时间的计算以及剩余均衡时间的更新。均衡控制主要指系统根据当前开启关闭均衡的条件及控制策略执行均衡。均衡诊断主要指的是对均衡回路的实时诊断，系统应当根据当前的均衡控制命令以及均衡结果实时反馈均衡状态。均衡计算，均衡控制，均衡诊断时间的相互关系可用以下的流程图表示：

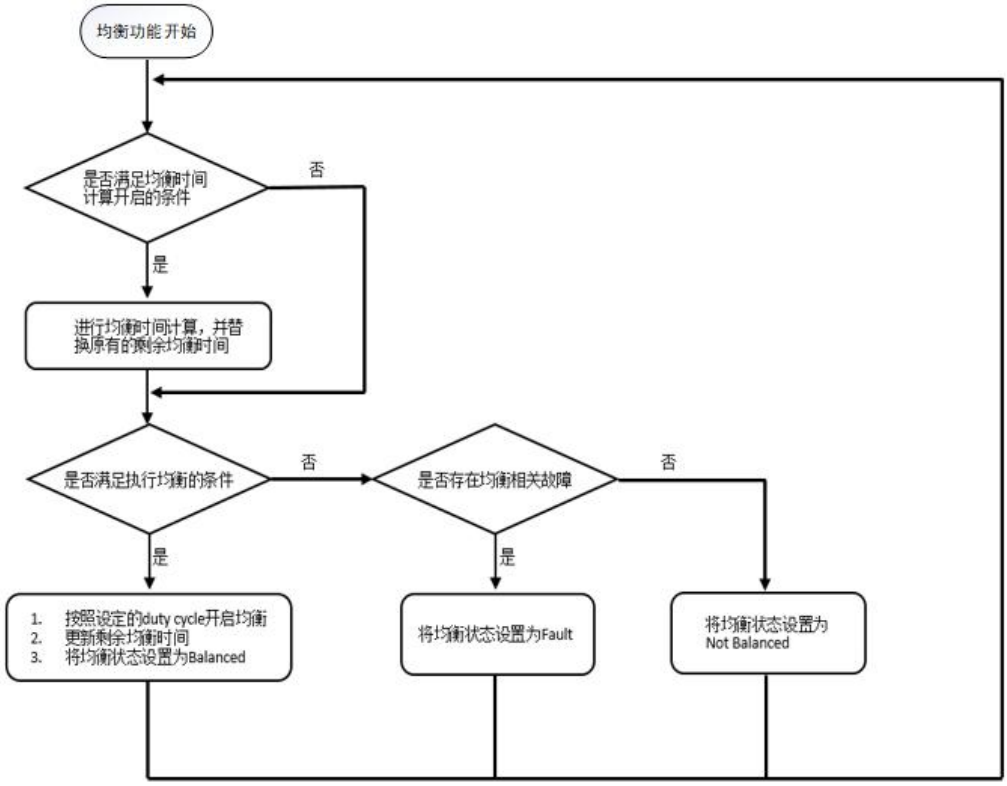


图 11.5 均衡计算、控制、诊断的执行流程

对于以上图中涉及的各个条件说明如下

（1）均衡时间计算开启的条件有：

a）所有电芯电压均有效：

b）电芯处在稳态（电芯休眠超过 1h（可标定））或准稳态（整车唤醒状态下充放电电流小于 2A（可标定）持续超过 3min（可标定））。

（2）均衡时间的计算方法：

电芯均衡时间 = 电芯容量*ΔSOC/平均均衡电流（可标定，建议值：100mA）

其中：

电芯均衡时间指的是分别计算的每个电芯的均衡时间

电芯容量指的是被计算均衡时间的电芯的相应容量

ΔSOC指的是被计算的电芯的SOC与所有电芯中最小SOC的差。

平均均衡电流根据均衡前端的设计确定，default为100mA

（3）电芯的剩余均衡时间应当持续按照下述方式更新：

剩余均衡时间 = 总的均衡需求时间 - 累计均衡开启时间*70%（可标定）

若新的一轮电芯均衡时间计算被触发，则应将所有的电芯剩余均衡时间替换成新一轮计算得到的各电芯总的均衡需求时间。电芯剩余均衡时间应当存储NVM，若上电检测到NVM存储故障，则应将所有的剩余均衡时间全部恢复到default值（default：0）。

（4）对于整个BMS系统，当满足以下这些条件的时候，均衡可以开启：

a）主板供电应当在9（可标定）到16V（可标定）之间，主板对从板的供电应当在9到16V之间；

b）所有电芯电压采样均有效；

c）最小电芯电压应当大于等于2.8V（可标定）（电压的判定需要添加滤波）；

d）最小电芯SOC应当大于等于15%（可标定）（考虑2%SOC的滞回）；

e）若在慢充模式下，最大电芯SOC应当小于等于95%（可标定）（考虑2%SOC的滞回）；
f）当前系统不处在快充模式；
h）所有模组温度采样均有效；
i）模组最高温度小于等于53℃（可标定）（温度考虑5℃的滞回）；
j）模组最低温度大于等于-30℃（可标定）（温度考虑5℃的滞回）；
k）Pack没有绝缘检测故障；
l）没有均衡故障，包括均衡开路，均衡电阻短路，均衡区温度故障；
m）当前处在IGN ON状态。

（5）单体电芯均衡开启的条件

对于单体电芯，其均衡开启的条件为：

a）该电芯剩余均衡时间大于等于 1h（可标定）；

b）该电芯电压大于最小 SOC 所对应的电芯电压，且压差大于等于 60mV（可标定）。

（6）电芯均衡的执行

a）从板应当按照子网上从主板周期性发出的均衡控制命令执行均衡,报文周期为 1s（可标定）；

b）从板应当对均衡控制命令作超时诊断，若连续 5 个报文周期（default：5s，可标定）未收到均衡指令，判断发生报文超时，从板应强制均衡关闭，并将报文超时故障通过子网的均衡故障状态报文发出到主板；

c）若从板收到有效的开启均衡命令，则应当按照 70%（可标定） duty cycle 的方式执行均衡。

即每100ms（可标定，电芯电压采样周期），在电芯电压采样前20ms关闭均衡，在电芯电压采样之后10ms开启均衡。若均衡与电芯电压采样同时进行，会导致被均衡的电芯电压偏低，被均衡电芯相邻的电芯电压偏高。

a）若从板收到有效均衡指令，且均衡指令为关闭均衡，则应当关闭对应电芯的均衡；

b）在收到下一帧有效的均衡控制命令或确认存在均衡控制命令超时故障之前，应当维持当前均衡执行状态。

11.5.3 均衡相关的诊断

11.5.3.1 均衡区温度诊断

（1）从板的模拟前端应当具备检测均衡区温度的功能，检测周期为100ms（可标定）

（2）从板应当对均衡区温度采样作有效性判断，若采样得到的模拟值超出有效的模拟量范围，则判断该均衡区温度采样无效，将该前端控制的均衡关闭，该均衡区温度维持上一时刻有效值，均衡温度的采样故障状态应通过子网的报文发送到主板。若采样有效，则从板应将其实际采样得到的均衡区温度通过子网的报文发送到主板。

（3）若均衡温度采样有效，并且温度超过97℃（可标定），则认为发生均衡过温故障，应将均衡强制关闭,并且应当维持均衡关闭，直到温度降到85℃（可标定）及以下。

（4）从板应根据发生均衡区温度采样故障或者均衡区过温故障的模拟前端的数量将其故障状态通过报文发送到主板，详细如下：

- 当前无模拟前端的均衡区温度发生采样无效或过温故障；
- 当前部分模拟前端的均衡区温度发生采样无效或过温故障；
- 当前全部模拟前端的均衡区温度发生采样无效或过温故障。

11.5.3.2 均衡回路开路诊断

从板应当具备周期性进行均衡回路开路诊断的功能,且该诊断需要在特殊的诊断模式下

进行（诊断模式下，无法进行正常的电芯电压采样或均衡），若发生均衡回路开路故障，应将该均衡回路强制关闭，将其故障状态通过子网的均衡状态信号发送到主板。

11.5.3.3 均衡电阻短路诊断

从板应当具备周期性进行均衡电阻短路诊断的功能，该诊断在正常运行模式，均衡开启时周期性进行（对正常的采样及均衡没有影响）。从板应当周期性地判断短路的状态，若发生故障，则将该故障对应的均衡回路关闭，将其故障通过子网的均衡状态信号发送到主板。

12 充电控制

充电过程是车辆与充电系统协同配合并实现电能传递的过程，充电失控易引发动力电池的安全事故，应注重充电过程的安全风险管理。

车辆 BMS 作为充电主控侧，充电设备为被控侧，执行 BMS 充电指令，结合电动汽车及动力电池管理系统充电特性输出，宜进一步优化充电模式及充电特性控制要求，通过数据交互及可信度判别，形成与充电特性安全边界相适配的保护机制。提倡对电池系统、充电系统应具备健康状况监测、诊断及设置故障预警功能，且当电池系统出现安全风险状况时具有相应的保护措施。

电动汽车在充电过程中应建立故障风险监测及相应保护控制措施，在故障模式下应具备安全事故不扩散的控制能力；

建立全过程的安全防控机制，设计阶段应充分重视充电设备对安全相关标准技术要求的执行，充分运用功能保护设计有效减低系统功能失效安全风险，制造阶段应重视产品生产制造质量水平提升和产品检验、认证检测和入网管理，建设阶段应严格执行充电设施建设竣工质量要求，运营阶段应提高运行维护保障能力和安全管理水平。

BMS 在功能设计上应遵循功能安全设计思想，如具备防死机、呆滞和 CPU 处理的自恢复能力，确保 BMS 与充电控制单元通信的可靠，通信连接上应具有心跳侦测、数据纠错、以及必要的容错能力，避免充电过程中如通信处理器或控制处理器故障形成假报文传递、关键参数畸变等状况，并能有效控制因此产生的充电功能失效而造成充电失控风险。

采用传导充电的电动汽车，BMS 设计应该遵守 GB/T 18487.1-2015 的相关要求。

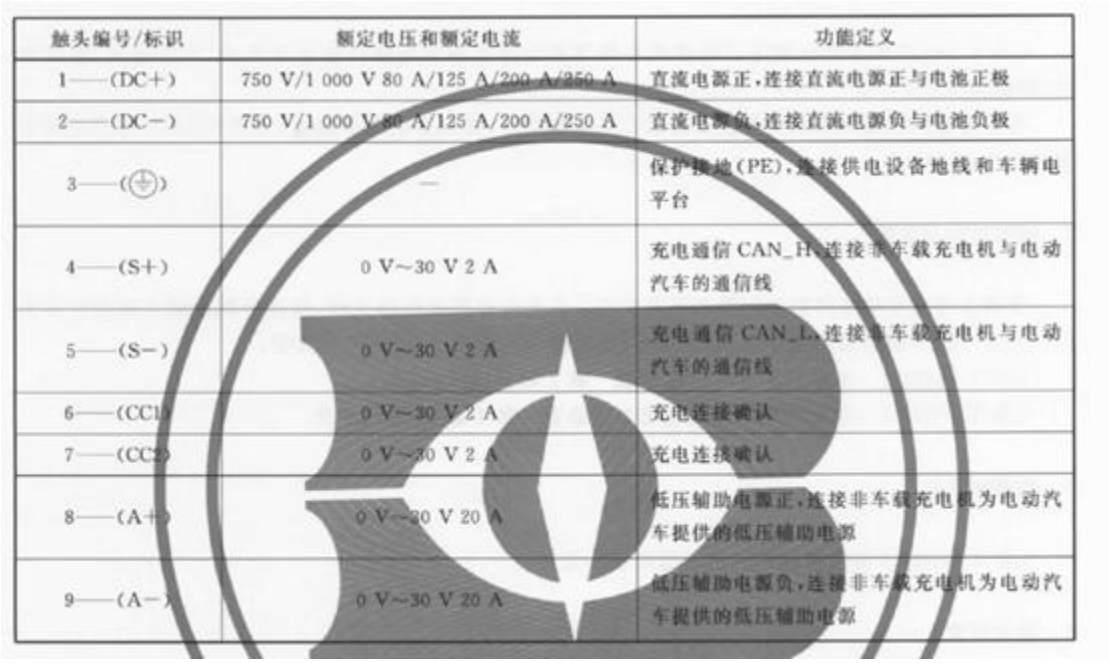
12.1 国家标准直流充电设计

对于采用直流充电的电动车辆，电池管理系统应满足 GB/T18487-2015、GB/T27930-2015、GB/T 34658-2017 相关要求，能通过与非车载充电机的实时通讯或者其他信号交互方式实现对充电过程的控制和管理，实现对电池系统的充电与安全保护功能。

12.1.1 接口要求

充电连接方式采用 GB/T 18487.1 -2015 中的连接方式 C，该充电方式中电源线和连接器同电动车辆连接，电源线和连接器永久地固定在充电机(站)上。

BMS 充电插座应该按照 GBT-20234.3-2015 进行设计，其与充电机的接口功能如表所示：



触头编号/标识	额定电压和额定电流	功能定义
1——(DC+)	750 V/1 000 V 80 A/125 A/200 A/250 A	直流电源正，连接直流电源正与电池正极
2——(DC−)	750 V/1 000 V 80 A/125 A/200 A/250 A	直流电源负，连接直流电源负与电池负极
3——(⏚)	—	保护接地(PE)，连接供电设备地线和车辆电平台
4——(S+)	0 V~30 V 2 A	充电通信 CAN_H，连接非车载充电机与电动汽车的通信线
5——(S−)	0 V~30 V 2 A	充电通信 CAN_L，连接非车载充电机与电动汽车的通信线
6——(CC1)	0 V~30 V 2 A	充电连接确认
7——(CC2)	0 V~30 V 2 A	充电连接确认
8——(A+)	0 V~30 V 20 A	低压辅助电源正，连接非车载充电机为电动汽车提供的低压辅助电源
9——(A−)	0 V~30 V 20 A	低压辅助电源负，连接非车载充电机为电动汽车提供的低压辅助电源

图 12.1-1 国标 GBT-20234.3-2015 对充电接口的要求

12.1.2 控制引导电路

BMS 直流充电安全保护系统的控制引导电路应满足 GB/T18487.1-2015 附录 B 中的相关要求，BMS 应能监测接触器 K5 和 K6 的状态并控制其接通和关断。

12.1.3 硬件参数

上拉电压 U2 应为 12V 或者 24V，R4、R5 应为 1K。

BMS 应使用充电枪的输出 A+，A-作为充电快充唤醒源；

12.1.4 与充电机的通信

电池管理系统充电功能兼容 GB/27930-2011 和 GB/27930-2015 标准要求，实现新老国标充电机均可以正常充电；分为握手、配置、充电和充电结束四个阶段；BMS 应使用单独一路 CAN 通道与充电机进行通信。

BMS 在与充电机的通讯协议上应按照主机厂的要求进行国标 GB/T 34658-2017 规定的一致性测试。

12.1.5 充电控制过程

12.1.5.1 插充电枪识别

车辆插头与车辆插座插合后，BMS 应能识别到，并通过 VCU 使车辆应该处于不可状态。

12.1.5.2 充电准备就绪

车辆接口完成，绝缘检测逻辑按照 GB/T 27930-2015 进行，在 K5，K6 闭合之前，由充电机进行绝缘检测，BMS 不参与；在 K5，K6 合闸之后的充电过程中，BMS 负责整个系统的绝缘电阻检测，单边绝缘电阻值低于 100Ω/V 时不允许充电。充电机完成自检后，BMS 与非车载充电机控制装置进入配置阶段，BMS 控制闭合 K5 和 K6，使充电回路导通。

BMS 允许对电池包进行快充的温度范围一般是 0-45℃，否则执行高压辅助模式进行电池包热管理，将电池包温度恢复到 5-40℃范围内。

BMS 应在快充过程中进行电池包热管理，将电池包温度维持在 0-45℃范围内；快充充电阶段分为恒流模式和恒压模式两个阶段。

12.1.5.3 充电阶段

充电前，BMS 先对电池电压进行检测，当检测电池深度放电等原因出现电压过低时，先要用小电流对其进行修复性充电；若检测电池电压在正常范围内，则可跳过涓充这一步，直接进入恒流充电模式。BMS 应该根据电池 SOP 实时调整需求的充电电压和充电电流，并和充电机共享各自状态信息。在充电过程中，BMS 应该实时监测 PE 接地情况。

BMS 具备过流和过充保护措施及故障报警功能。

BMS 宜具备检测充电机响应速率的能力，当充电机的降流速率较低时，BMS 应适当提前调整充电电流，防止个别单体过压。

12.1.5.4 正常条件下充电结束

BMS 应根据电池系统是否达到满充状态或是否收到“充电机中止充电报文”来判断是否结束充电。在满足以上充电结束条件时，BMS 周期发送 BMS 中止充电报文，在确认充电电流小于 5A 后，断开 K5 和 K6。

12.1.5.5 非正常条件下充电中止

在充电过程中，如果车辆出现不能继续充电的故障，则 BMS 应向非车载充电机发送 BMS 中止充电报文，并在 300ms（可根据故障等级确定）内断开 K5 和 K6。

12.1.6 绝缘检测功能

BMS 应具备绝缘监测功能，在 K5 和 K6 闭合之后，BMS 应周期性对整个系统进行绝缘监测。充电 DC+、PE 之间的绝缘电阻，与 DC-、PE 之间的绝缘电阻（两者取小值 R），当 R>500Ω/V 视为安全；100Ω/V<R<500Ω/V 时，应进行绝缘异常报警，但仍可正常充电；当 R<100Ω/V 视为绝缘故障，应停止充电。

12.1.7 故障诊断及保护

BMS 应具备充电继电器故障检测与报警功能,BMS 应具备充电插座温度传感器故障检测、高温报警和降流功能，BMS 应具备 DC/DC 故障检测与报警功能，BMS 应具备电池热管理系统的故障检测、报警及对应的请求充电电流变化功能。

12.1.8 充电连接控制时序

直流充电连接过程和控制时序参见下图:

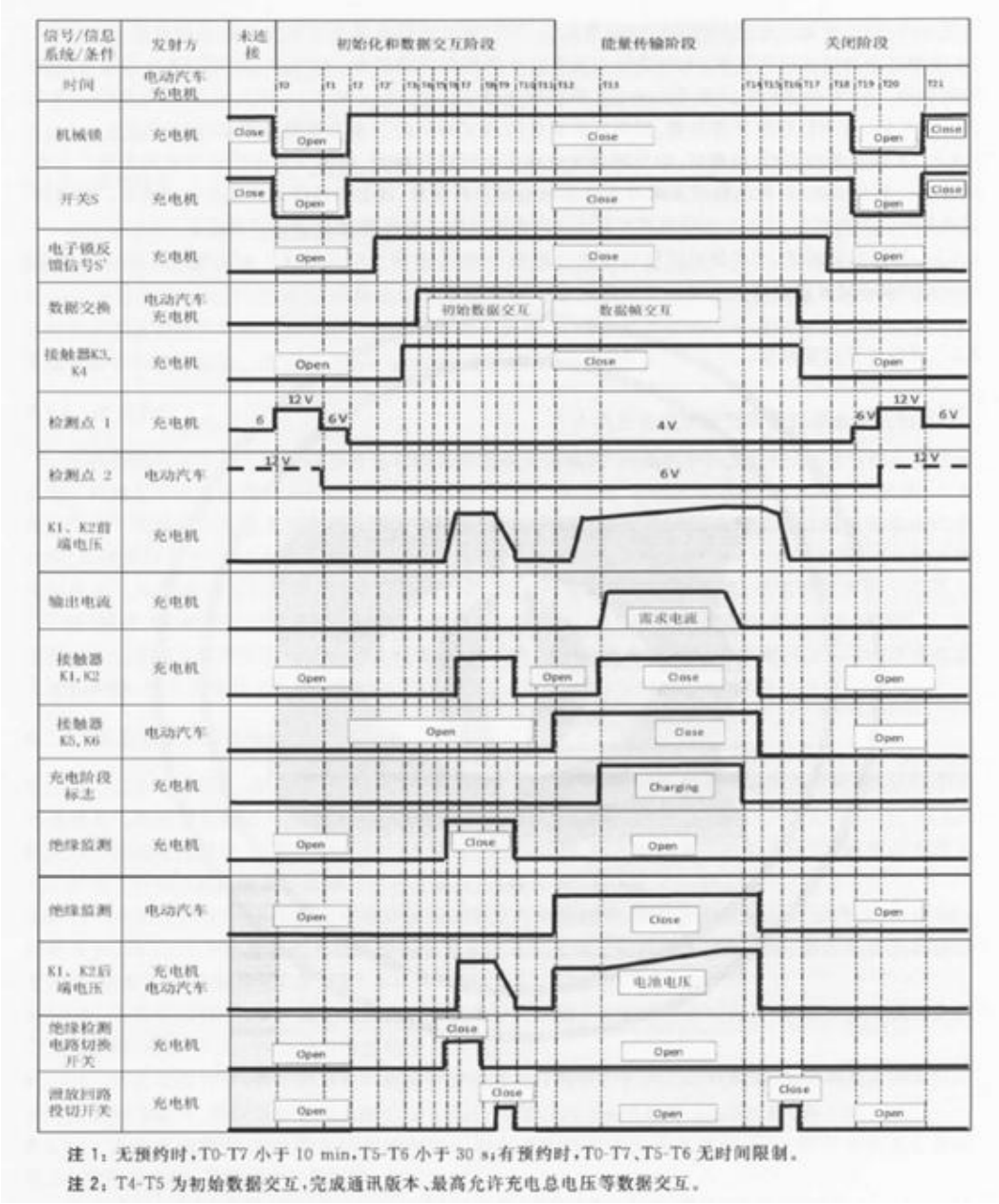


图 12.1.2 直流充电连接过程和控制时序图

12.1.9 直流双枪充电

目前尚无直流双枪充电的国家标准，现有的标直流充电，存在电流偏移量（目前国标规定是-400A），充电过程中增加枪数量，如果电池需求充电电流大于 400A，电流偏移量可能就要自适应更改了， BMS 应根据整车厂要求进行设计，不区分主副充电口，两个充电插座共用一个 BMS 充电 CAN 接口，若要实现双枪充电，两把枪必须均插入车辆插座后，方可进行正常的充电流程和宇通自定义电流偏移量兼容协议 BFC/CFC 交互，充电过程中不再允许增加充电枪，以充电握手前检测到的充电枪数量为准。

（国标直流充电，存在电流偏移量（目前国标规定是-400A），充电过程中增加枪数量，如果电池需求充电电流大于 400A，电流偏移量可能就要自适应更改了，目前国标协议还不支持这样的变动）

针对欧洲地区的直流双枪充电，需要区分主副充电口，先插入的枪为主充电枪，先插入的座为主充电插座，充电过程中允许增加充电枪。由于两个充电口均存在 EVCC，双枪充电时 BMS 需要打开主充电口的 EVCC，副充电口的 EVCC 需要关闭。

直流双枪充电时，主桩与主充电口负责通讯，副桩和副充电口不通讯。主副充电回路的定义如下：充电插座和充电桩都不预先定义主副，先插的枪为主充电枪，先插入的座为主充电插座；先插枪的桩由用户通过充电桩接口定义为主桩，后插枪的桩由用户通过充电桩接口定义为副桩；两把枪的先后顺序时间差大于等于 2s；如果用户把先插入的枪设置为副桩则不能充电；如果用户没有设置主桩和副桩的属性，则只能单枪充电。

对 BMS 的要求如下：BMS 与先插入的枪正常建立通讯连接并进行正常的充电流程，过程中当检测到另一把枪插入时，后插入的充电插座定义为副座，副座电子锁上锁，上锁成功后即闭合副回路正负继电器。如果过程中没有检测第二把充电枪插入，按照正常单枪模式充电；BMS 确认副座回路正负极继电器闭合后，根据充电桩充电能力的提升，提升充电请求电流；当充电完成后，BMS 同时断开主回路与副回路的充电继电器、粘黏检测与电子锁解锁。

12.2 国家标准交流充电设计

对于采用交流充电的电动车辆，电池管理系统应满足 GB/T18487-2015 相关要求，能通过与车载充电机的实时通讯或者其他信号交互方式实现对充电过程的控制和管理，实现对电池系统的充电与安全保护功能。

电动车辆交流充电机(站)和电动车辆之间可采用三种不同的连接方式:

方式 A：供电电缆和插头永久性固定于电动车辆(EV)上;

方式 B：使用带有电动车辆连接器和电源连接器的独立活动电缆;

方式 C：供电电缆和连接器永久性固定于充电机(站)上。

12.2.1 接口要求

BMS 充电插座应按照 GBT-20234.2-2015 进行设计，其与充电机的接口功能如下表所示：

表 12.2-1 国标定义：触头电气参数值及功能定义

触头编号/标识	额定电压和额定电流	功能定义
1——(L1)	250 V 10 A/16 A/32 A	交流电源(单相)
	440 V 16 A/32 A/63 A	交流电源(三相)
2——(L2)	440 V 16 A/32 A/63 A	交流电源(三相)
3——(L3)	440 V 16 A/32 A/63 A	交流电源(三相)
4——(N)	250 V 10 A/16 A/32 A	中线(单相)
	440 V 16 A/32 A/63 A	中线(三相)
5——(⏚)	—	保护接地(PE)连接供电设备地线和车辆电平台
6——(CC)	0 V～30 V 2 A	充电连接确认
7——(CP)	0 V～30 V 2 A	控制导引

12.2.2 控制导引电路功能要求

当电动汽车使用充电模式 2 和充电模式 3 进行充电时，BMS 侧控制导引电路应满足 GB-T18487.1-2015 中附录 A 的要求；

开关 S2 为车辆内部开关，在车辆接口与供电接口完全连接，并且配置了电子锁的接口被完全锁止之后，当车载充电机自检测完成后无故障时，并且电池组处于可充电状态时，S2 闭合；开关 S3 为车辆插头的内部常闭开关，与插头上的下压按钮联动，按下按钮解除机械锁止功能的同时，S3 处于断开状态。

12.2.2.1 确认连接与电子锁

BMS 通过检测点 3 与 PE 之间的电阻值来判断车辆插头与车辆插座是否完全连接。完全连接后，大于 16A 电流的应加入枪锁控制，如果车辆插座内配备了电子锁，电子锁应在开始供电（K1 与 K2 闭合）前锁定车辆插头，并在整个充电流程中保持锁止；若不能锁止，应该报警，并限制充电电流。

12.2.2.2 充电连接装置载流能力与供电设备供电功率的识别

BMS 通过测量检测点 3 与 PE 之间的电阻值来确认当前充电连接装置的额定容量；通过测量检测点 2 的 PWM 信号占空比确认当前供电设备的最大供电电流。占空比与充电电流限值的映射关系如下。

表 12.2-2 国标定义：电动车辆检测的占空比与充电电流限值映射关系

PWM 占空比 D	最大充电电流 I_{max}/A
$D<3\%$	不允许充电
$3\%\leqslant D\leqslant 7\%$	5%的占空比表示需要数字通信，且需在充电前在充电桩和电动汽车之间建立。没有数字通信不允许充电
$7\%<D<8\%$	不允许充电
$8\%\leqslant D<10\%$	$I_{max}=6$
$10\%\leqslant D\leqslant 85\%$	$I_{max}=(D\times 100)\times 0.6$
$85\%<D\leqslant 90\%$	$I_{max}=(D\times 100-64)\times 2.5$ 且 $I_{max}\leqslant 63$
$90\%<D\leqslant 97\%$	预留
$D>97\%$	不允许充电

12.2.2.3 充电过程的监测

充电过程中，BMS 应对检测点 3 与 PE 之间的电阻值及检测点 2 的 PWM 信号占空比进行监测。

12.2.2.4 充电的停止

在充电过程中，当充电完成或因为其他原因不能满足继续充电的条件时，BMS 应及时检测出，发出相应等级的报警，并中止充电。

12.2.2.5 充电过程的工作控制程序

12.2.2.5.1 确认车辆接口已完全连接

BMS 通过测量检测点 3 与 PE 之间的电阻值来判断车辆插头与车辆插座是否完全连接。未连接时，S3 处于闭合状态，CC 未连接，检测点 3 与 PE 之间的电阻值为无限大；半连接时，S3 处于断开状态，CC 已连接，监测点 3 与 PE 之间的电阻值为 RC+R4;完全连接时，S3 处于闭合状态，CC 已连接，监测点 3 与 PE 之间的电阻值为 RC。BMS 应能识别到完全连接后，应通过一定的方案使车辆应该处于不可行驶的状态。

12.2.2.5.2 充电准备就绪

在充电机自检完成，且没有故障的情况下，并且电池组处于可充电状态时，BMS 闭合开关 S2。要求只有当电池单体温度在 0~45℃（可标定量）范围内时，才能够直接进行充电，否则需要首先进行热管理使电池单体温度满足充电要求。
要求慢充充电过程中，允许开启热管理（加热和制冷）功能。

12.2.2.5.3 充电阶段

BMS 通过判断检测点 2 的 PWM 信号占空比确认供电设备的最大供电能力，并且通过判断点 3 与 PE 之间的电阻值来确认电缆的额定容量。BMS 根据对供电设备当前提供的最大供电电流值、车载充电机的额定输入电流值及电缆的额定容量进行判断，将其最小值设定为车载充电机当前最大允许输入电流。

充电过程中，当接收到检测点 2 的 PWM 信号时，车载充电机最大允许输入电流设置取决于供电设备的可供电能力、充电线缆载流值和车载充电机额定电流的最小值。
充电前，BMS 先对电池电压进行检测，当检测电池深度放电等原因出现电压过低时，先要用小电流对其进行修复性充电；若检测电池电压在正常范围内，则可跳过涓充这一步，直接进入恒流充电模式。BMS 具备过流和过充保护措施及故障报警功能。

控制电路中如果没有配置开关 S2，则应采用单枪充电，且最大充电电流不超过 8A。
在充电过程中，BMS 应周期性监测检测点 2 和检测点 3，以确定供电接口和车辆接口的连接状态，监测周期不大于 50ms；同时，BMS 应对检测点 2 的 PWM 信号进行不间断检测，当占空比有变化时,BMS 应根据 PWM 占空比实时调整车载充电机的输出功率,检测周期不应大于 5s。

12.2.2.5.4 正常条件下充电结束

BMS 应根据电池系统是否达到满充状态或者驾驶员对车辆实施了停止充电的指令时，车辆控制装置断开开关 S2，并使车载充电机处于停止充电状态。

12.2.2.5.5 非正常条件下充电中止

在充电过程中，BMS 通过检测 PE 与检测点 3 之间的电阻值（对于连接方式 B 和连接方式 C)来判断车辆插头和车辆插座的连接状态,如判断开关 S3 由闭合变为断开(状态 A 或 B)，则 BMS 应控制车载充电机在 100ms 内停止充电，然后断开 S2。

在充电过程中，BMS 对检测点 2 的 PWM 信号进行监测，当信号中断时，则 BMS 控制车载充电机在 3s 内停止充电，然后断开 S2。

充电过程中，如果漏电断路器动作，则车载充电机处于失电状态，BMS 控制 S2 断开。当高压电网交流 220V 中断一段时间后又重新恢复时，要求 BMS 具备充电自恢复功能。

12.2.6 故障诊断及保护

BMS 应具备充电继电器故障检测与报警功能,BMS 应具备充电插座温度传感器故障检测、高温报警和降流功能，BMS 应具备 DC/DC 故障检测与报警功能。

12.3 欧美标准的充电设计

12.3.1 欧美国家充电标准介绍

国际电工委员会（International Electro technical Commission, IEC）对电动汽车传导充电系统制定了如下标准；

（1） IEC61851－1（电动车辆充电系统 第1部分：总体要求）规定了直流电动车辆充电站与电动车辆之间控制直流充电的数字通信的基本要求；

（2） IEC61851－21－1（电动车辆充电系统 车载充电机EMC要求）规定了车载交流充电机EMC方面的要求；

（3） IEC61851－21－2（充电系统 非车载充电系统EMC要求）规定了非车载交流充电机EMC方面的要求；

（4） IEC61851－22（交流充电桩标准）规定了交流充电桩的相关标准；IEC61851－23（直流充电桩标准）规定了直流充电桩的相关标准；

（5） IEC61851－24（直流充电通信要求）规定直流电动车辆充电站与电动车辆之间控制直流充电的数字通信的基本要求，该标准规定采用了ISO15118/DIN70121协议标准；

（6） DIN70121是德国标准化学会指定的直流充电的数字通信协议；

（7） ISO 15118是国际标准化组织（International Organization for Standardization，ISO）指定的道路车辆到电网的通信接口标准；

（8） ISO15118、DIN70121基于PLC通信，和国标GB/T 27930一样都是针对电动汽车充电设施的充电接口通信这种特定应用场景设计的通信协议；

（9） 而GB/T27930基于CAN通信。GB/T 27930是针对我国国标GB/T20234.3的直流充电接口制定的协议，而ISO15118除了传统传导式充电外，还涉及到了V2G（向电网回馈电能）和无线充电部分内容。

IEC61851-1中定义了全球的三种不同的充电系统，包括国标、日标和欧美标准（system C联合充电系统）。在欧洲以ISO15118、DIN70121（未来将被ISO15118取代）及IEC61851作为充电通信标准的联合充电系统（CCS），采用CP线上的电力线载波技术（PLC），在基础的控制引导之上增加了高层数字通信（当CP线上PWM占空比为5%时）。ISO15118参考OSI网络模型，物理层和数据链路层基于Homeplug Green PHY标准，上层通信协议引入互联网技术，如SLAC、TCP/IPv6、TLS及XML-EXI等，从而实现在大数据量高速传输的基础上，满足通信信息安全和未来的应用扩展。在ISO15118的通信协议的基础上，可实现交直流充电管理、即插即充、负载均衡管理、能量回馈等应用，并为无线充电及大功率充电的高层数字通信进行了定义。对于美国地区，则使用SAE J2847和SAE J2931系列标准定义了充电通信的场景及协议。下图为欧美充电系统的标准分布。

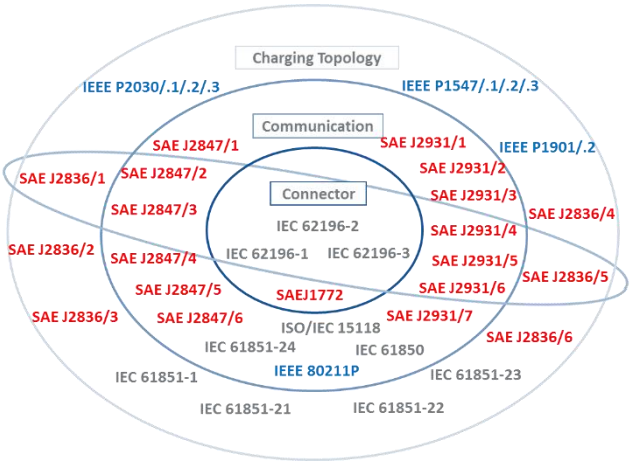


图12.3-1 欧美充电标准分布图

12.3.2 欧美标直流充电

12.3.2.1 欧标直流充电

12.3.2.1.1 欧标单枪直流充电

12.3.2.1.1.1 欧标直流充电与国标直流充电的区别

欧标的直流充电系统采用系统 C（Combined Charging System,联合充电系统），不同于中国采用的系统 B，具体区别如下：

（1） 系统 C 的充电接口中没有系统 B 中的低压辅助电源接口。

（2） 直流充电系统，欧洲充电接口配置采用 FF 配置,不同于中国采用的 BB 配置。

（3） 充电过程中的绝缘检测由充电机执行，BMS 不负责充电过程中的绝缘检测;

（4） 整车端与桩端的通讯方式为 PLC 通讯，使用控制导向引线建立控制导向回路，使用 PWM 调制通信；而系统 B 采用 CAN 通信方式；

（5） 充电插座与充电枪有电子锁机构，BMS 负责电子锁的上锁与解锁控制，而系统 B 中充电机负责电子锁的上锁和解锁控制;

为了兼容欧标的充电桩，国内电动车 BMS 可以通过充电 CAN 接口与 EVCC 通讯，EVCC 再与桩端的 SECC 进行 PLC 通讯；BMS 负责对 EVCC 模块的电源供电，EVCC 应在 BMS 检测到充电枪插入后立即上电或插入前上电；BMS 应具备 EVCC 故障诊断功能，故障诊断包括但不限于 EVCC 电源故障、PLC 通讯超时、EVCC 设备故障等；BMS 应具备电子锁的故障诊断功能，故障诊断包括不限于上锁、解锁判断，工作电压判断等。

12.3.2.1.1.2 通信转换模块介绍

某型号国标 CAN 转欧标动力线载波的 EVCC 为通讯转换模块的电气参数如下：

（1） 允许工作电压范围：16~32V；

（2） 标称工作电压：24V；

（3） 冲击电流：<3A(24V,10ms)；

（4） 工作电流：<300mA；

（5） 波特率：500kbps；

（6） 终端电阻：120±5Ω；

（7） 电力载波通信芯片 ：QCA7005

下图为 PLC 模块（EVCC）与 BMS 的典型参考连接：

其中，控制引导线 CP（PLC 载波信号）、PP（连接确认信号）需连接 PLC 模块，枪锁电机控制和检测、充电口温度检测可选择性的接入 PLC 模块，也可由其他控制器负责。

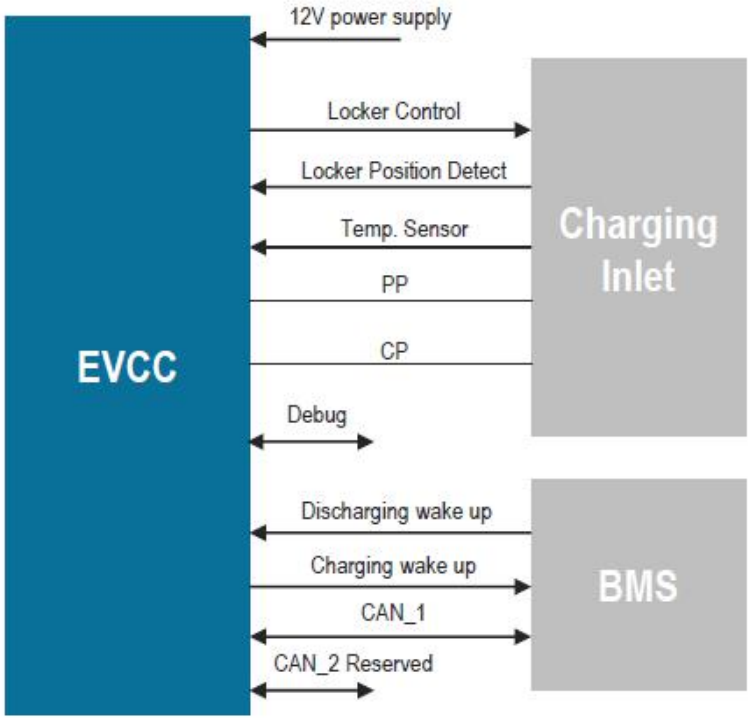


图 12.3-2 EVCC 接口图

12.3.2.1.1.3 通讯协议介绍

欧标 BMS 与桩端的数字通讯协议采用 IEC 61851-24 标准，报文类型有如下几种：

（1） EVCC 查询 BMS 的状态信息，报文类型为 COMMAND；

（2） BMS 回复 COMMAND 的报文类型为 CONFIRM；

（3） EVCC 通知 BMS 充电桩的状态信息报文类型为 INDICATION;

（4） BMS 回复确认收到该信息的报文类型为 RESPONSE；

报文交互：

（5） 一个 COMMAND 和一个或多个 CONFIRM 构成一次完整的交互；

（6） 一个 INDICATION 和一个或无 RESPONSE 构成一次完整交互；

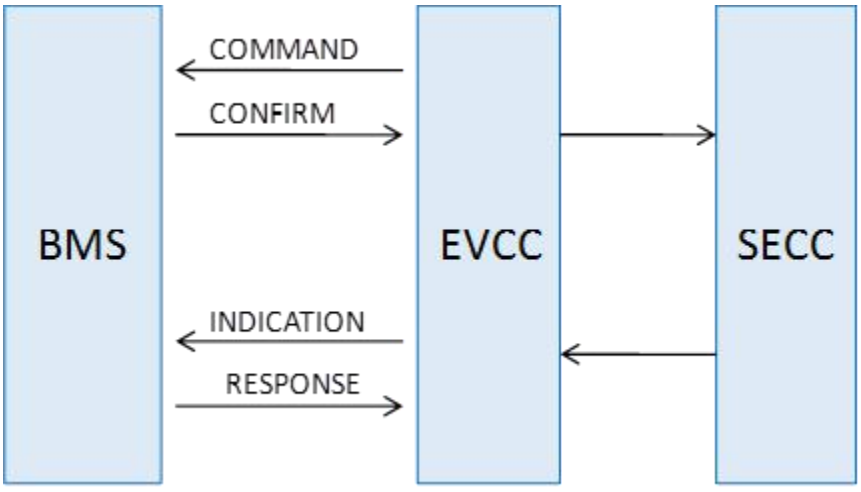


图 12.3-3 报文交互示意图

状态查询报文 COMMAMD: MsgID0x0001；根据查询的类型分为 4 种：

a、 充电状态查询报文（01）: 查询充电状态，剩余电量等

BMS 回复报文 CONFIRM：0x0101

b、 充电属性查询报文（02）: 查询最大充电电压限值，电流限值等
BMS 回复报文 CONFIRM：0x0102 、0x0103
c、 充电要求查询报文（03）: 查询充电要求电压和充电要求电流-
BMS 回复报文 CONFIRM：0x0104
d、 充电过程查询报文（04）: 充电是否完成及充电剩余时间-
BMS 回复报文 CONFIRM：0x0105

EVCC 通知 BMS 充电桩的状态信息报文，根据通知的内容分为 5 种：

a、通知 SECC 的充电状态：充电状态、绝缘检测状态 MsgID：0x0201
b、通知 SECC 的充电属性 1：最大充电电流与最大充电电压限制 MsgID：0x0202
c、通知 SECC 的充电属性 2：最小充电电流与最小充电电压限制 MsgID：0x0203
d、通知 SECC 的充电属性 3：最大功充电功率限制等 MsgID：0x0204
e、通知 SECC 的充电过程：输出电压与电流等 MsgID：0x0205
f、BMS 在充电过程中发送的心跳报文通知 EVCC 的状态： MsgID：0x0300

12.3.2.1.1.4 充电流程介绍

充电流程控制大致可分为：电子锁上锁、充电配置、绝缘检测、预充电、充电开、循环充电、充电停止、粘连检测、解锁。欧标充电过程中应具备充电池插座温度检测功能，如果温度超过上限需降电流充电或停止充电；要求电池包允许进行快充的温度范围一般是 0-45℃，否则执行高压辅助模式进行电池包热管理，将电池包温度恢复到 5-40℃范围内；允许快充过程中进行电池包热管理，将电池包温度维持在 0-45℃范围内。

12.3.2.1.2 欧标双枪直流充电

直流双枪充电时，主桩与主充电口负责通讯，副桩和副充电口不通讯。主副充电回路的定义如下：充电插座和充电桩都不预先定义主副，先插的枪为主充电枪，先插入的座为主充电插座；先插枪的桩由用户通过充电桩接口定义为主桩，后插枪的桩由用户通过充电桩接口定义为副桩；两把枪的先后顺序时间差大于等于 2s；如果用户把先插入的枪设置为副桩则不能充电；如果用户没有设置主桩和副桩的属性，则只能单枪充电。

对 BMS 的要求如下：BMS 与先插入的枪正常建立通讯连接并进行正常的充电流程，过程中当检测到另一把枪插入时，后插入的充电插座定义为副座，副座电子锁上锁，上锁成功后即闭合副回路正负继电器。如果过程中没有检测第二把充电枪插入，按照正常单枪模式充电；BMS 确认副座回路正负极继电器后，根据充电桩充电能力的提升，提升充电请求电流；当充电完成后，BMS 同时断开主回路与副回路的充电继电器、粘黏检测与电子锁解锁。

12.3.2.2 美标直流充电

美国汽车工程协会 SAE 制定的 SAE J1772 对应 IEC61851，其中包含了 IEC 62196 的所有内容。美标直流充电最新标准为：SAE J1772-2017 电动汽车传导充电系统，该标准同样采用了 ISO15118/DIN70121 协议标准；

和欧洲一样，美国的直流充电系统采用系统 C（Combined Charging System,联合充电系统），不同于中国采用的系统 B，美国充电接口配置采用 EE 配置，也不同与欧洲采用的 FF 配置。

12.3.3 欧美地区交流充电

在交流充电方面，欧美地区的充电流程和国内交流充电相差不大，控制导引电路功能基本相同，交流充电占空比和电流限值的映射关系也与国标兼容，区别主要在于充电接口方面，通过转接线，基本上可以做到兼容。但是，交流充电由于受不同国家和地区电网系统的影响，在充电标准中对充电连接器电压和电流的要求也不尽相同。因此应严格按照销售国家的实际

情况进行设计。比如，SAE J1772-2017 对交流充电只定义了 5 芯的充电接口，因此采用此标准的电动汽车只能使用单相交流充电；比如，在德国三相电的使用比较普遍，即使个人用户在民宅中也可以使用，因此在 IEC 62196-2 标准中，定义了 480V 交流充电电压和 63A 充电电流，实际充电功率可以达到 40kW 以上。相比在国标 GB/T 20234.2 中虽然也定义了三相充电电压为 440V，但因为中国私人住宅及小区进户直接能使用三相电的情况很少，所以目前交流充电电流最大只有 32A，而实际多采用 220V，16A 进行充电。

13 热管理

13.1 几种热管理方式分析

电池热管理系统设计，是保证电池系统安全运行的重要因数，也是提升电池系统寿命、动力等性能指标的关键技术。在开展热管理设计之前，首先要了解电池系统热管理关键需求。

（1）系统运行环境区域：依据不同区域运行环境设计不同热管理方式和策略，如在中国南方，加热管理可以不予考虑。

（2）系统功率边界需求：整车动力性能需求取决于动力电池系统的功率性能，而热管理系统的控制能力也就决定了电池系统功率性能。

（3）系统运行寿命需求：系统寿命除了取决于电芯寿命、一致性以外，还取决于电芯的舒适性、均温性。一般来讲，锂离子电池温度控制在 15℃~35℃之间，系统温差控制在 5℃以内，终极目标控制在 2℃以内。除了从热结构、制冷介质、控制策略等来保证其系统均温性，还要考虑系统保温设计。高温环境降温时，避免受到外界环境影响；低温环境时避免温度下降过快。

（4）系统热安全性需求：系统过热或者局部过热会引起电池热失控风险；低温下进行充电可能会引起电池过充，造成电池析锂引发内部短路，从而引发热失控；热管理需要依据系统安全需求、电芯安全特性来进行设计，保证系统全生命周期的安全性要求。

目前热管理方式分为自然冷却、风冷、液冷、直冷等四种，其中自然冷却时被动式的热管理方式，其他三种属于主动式的热管理方式，区别主要在于换热介质的不同。

自然冷却无需额外装置进行换热，仅仅依靠自然风吹，自然冷却的优势是结构简单、成本低、占用空间较小，缺点是散热效率极低，系统温差大，无法适应大功率充放电的冷却需求，一般只用于运行工况缓和、对成本敏感的电动汽车。系统温差在 5℃~15℃。

BMS 控制策略：无；

风冷以空气为介质利用热的对流来降低电池以及动力电池的控制单元等部件温度。优点是系统结构简单，技术成熟可靠，成本低，安全无泄漏，便于维护。缺点是换热量小，响应慢，温度均匀性不易控制，电池箱的密封设计困难，防尘、防水效果较差。系统温差在 5℃~10℃。

BMS 控制策略：根据整车不同场景需求，依据热仿真和实验结果，当电池温度≥设定温度（建议值 30℃）控制风机开启，当电池温度≤设定温度（建议值 25℃）控制风机关闭。由于风冷换热效率低、响应速度慢，故需要在电池达到最高允许温度之前提前开启风机。当风机具备 PWM 调速功能时，依据电池温度、温升速率、系统温差等动态调整风机风量。建议选择自带转速检测风扇，通过转速来监测风扇运行状态，避免造成风扇停转发热燃烧事故。

液冷通过液体对流换热方式将电池产生的热量带走以达到降温目的。优点是液体介质的换热系数高、热容量大、冷却速度快，对降低最高温度、提升电池组温度场一致性的效果显著。缺点是系统更复杂，重量大，成本高，维修和保养难度大，并且存在漏液的可能。冷却液一般为 50%乙二醇和 50%水的混合液体，内部管道和连接器设计时需要考虑密封性要求，同时箱体内增加漏液检测功能，保证系统电气安全性。液冷的控制分为泵的控制、加热控制（水冷水热系统）和制冷控制。

BMS 控制策略：制冷策略---根据整车不同场景需求，依据热仿真和实验结果，当电池温度≥设定温度（建议值 36℃）控制压缩机和水泵开启，当电池温度≤设定温度（建议值 34℃）控制压缩机关闭。加热策略---根据整车不同场景需求，依据热仿真和实验结果，当电池温度≤设定温度（建议值 14℃）控制加热 PTC 和水泵开启，当电池温度≥设定温度（建议值 16℃）控制压缩机关闭。均温性控制---当系统温差≥3℃以上开启水泵，当系统温差≤2℃关闭水泵；均温性控制一般由整车来执行。BMS 通过整车 CAN 来通知整车控制器，由整车控制器来执行压缩机、水泵、加热 PTC 的开启和、关闭以及功率和泵速调整。

直冷是利用制冷剂蒸发潜热的原理，在整车或电池系统中建立空调系统，将空调系统的蒸发器安装在电池系统中，制冷剂在蒸发器中蒸发并快速高效地将电池系统的热量带走，从而完成对电池系统冷却。优点是系统复杂度低，换热效率非常高。缺点是它对系统的气密性要求非常高，对生产制造工艺提出了跟高的要求，另外系统均温性不易控制，电芯温差存在过大的风险，温度控制策略较为复杂。

BMS 控制策略：（无具体研究和应用，请其他公司协助编制）

13.2 低温充电过程中热管理设计

低温下大电流充电会导致电池析锂，为了保护电池，BMS 在监测到电池处在低温情况下会开启加热，即车辆充电前（处于辅助模式 HV_Assist），当电池温度低于某一阈值（低于阈值电池不允许充电）时，启动预加热功能，把电池加热到某一温度再进行充电。鉴于用户对快速充电的需求，热管理策略需要合理的设计以平衡保护电池的需求和快速充电的需求。低温充电过程中的热管理策略一般分为三个阶段，即电池只加热阶段、边加热边充电阶段以及关闭加热充电阶段。 通常设计为电池在低于某个温度阈值 T0 只进行加热；在温度高于 T0 而小于某个温度阈值 T1 边加热边充电；温度高于 T1 时关闭加热进行充电。每个阶段的温度阈值需要根据充电时间需求、电池系统热仿真以及实验结果来确定。

在只加热过程中电池系统从充电桩获取电能来进行加热，电池管理系统要实时检测流入电池的电流，并根据检测的电流值实时调整请求电流的大小，保证充电桩输出的电流只有用于加热，不用于充电。具体实现方法为当检测到流入系统的电流大于加热所需电流时，电池系统要及时请求充电桩减小电流输出，当检测到流入系统的电流过小时电池系统要请求充电桩增大电流输出。当检测到流入电池的系统电流超过一定阈值时，有可能是加热继电器故障没有闭合，电池管理系统要及时请求充电桩停止输出，保证大电流不会对电池系统充电。

另外基于安全的考虑，对于独立加热系统的控制回路通断需要做冗余设计，一般会安置两个继电器即加热正、负继电器。并且要对这些继电器进行粘连检测，一旦粘连发生要进行故障报警和故障处理。加热的启动条件和退出条件中的温度阈值选择要有一定的回差，比如如果选择 T＜15℃开启加热 T≥15℃关闭加热，因为采样的准确性和温度变化加热继电器可能会频繁开启和关闭，因此加热开启和关闭的阈值的回差建议值至少 2℃以上。

13.3 温度检测点的布置

（1）电池组温度采样点布置

通过不同工况、不同环境条件下的热仿真和实验对电池组多个温度采样点进行采集分析，统计出极耳-汇流排温升曲线与电池外壳中间温升曲线相接近的位置；再统计出极耳-汇流排温度典型值（最大值、最小值、平均值），最终确定能够代表电池组温度特征的采样点。

- 通常每个模组（1P12S）布置 2~3 个温度采样点；
- 模组间连接排应布置温度采样点，监测连接点松动引起的温升异常；
- 建议电芯温度和连接排温度采样设计均通过前端模拟采样来实现，避免高低压相互干扰，引起绝缘性能下降风险。

（2）其他温度采样点布置

从系统安全上考虑，还需要对其他关键部件进行温度采样，如极柱温度采样点，充电座温度采样点，进出水口温度采样点，功率继电器触点温度采样点，熔断器、MSD 温度采样点，均衡电路温度采样点，电路板运行温度采样点等。

（3）温度采样可靠性和准确性

由于温度实时性要求不高，可以通过降低更新周期来保证温度采样的可靠性和准确性，建议 500ms 更新一次。周期内进行多次采样后经过数字滤波，剔除因噪声干扰引起的异常值；温度采样线出现断线、短路情况下，温度值超出采样量程，应及时进行故障处理，因温度采样线出现虚短、虚断的情况下，温度值未超出采样量程，可以通过和环境温度、其他采样点温度、不同工况下的温度、电压进行数据比较分析，如低温条件下，温度过高异常；高温条件下，温度过低异常；充放电状态下，温度持续下降等。

硬件上可以采用冗余设计，通过对比温度采样的一致性来判定采集到温度是否可靠；通过将模拟参考电源进行采样，消除参考电源波动、环境温度变化带来的影响，提升采样的准确性；采用恒流源信号电路设计，降低超长采样线束对采样精度的影响。

（4）温度故障告警处理

BMS 具备温度异常报警分级报警功能，通常分为三级报警，故障严重程度越高级别越高。

一级报警处理方式：只发送报警信息，不进行限功率或者断电处理；

二级报警处理方式：充放电过程中进行限功率并发送报警信息；

三级报警处理方式：立即停止充电；通知 VCU 进行下电处理或 BMS 自行进行下电处理。

14 故障检测及处理

14.1 故障分级定义

典型的故障分级定义如下表所示：

表 14.1 典型故障分级定义

故障等级	故障处理	描述	
		充电模式	放电模式
Ⅰ	记录故障码	系统无故障，只记录故障码，系统性能不受影响	
Ⅱ	仪表报警	轻微故障，记录故障码，同时在仪表上提示，系统性能不受影响，或影响不可被驾驶人员察觉	
Ⅲ	限功率	限制到当前查表电流 60%（可标定）	60 秒内当前功率线性降至 5kW（可标定）
Ⅳ	延时下电	立即将功率限到 0kw，BMS 等待 VCU 下电指令，收到指令或故障产生后 10 秒（可标定），BMS 走正常流程下高压	60 秒内当前功率线性降至 0kw，BMS 等待 VCU 下电指令，收到指令或故障产生后 10 秒（可标定），BMS 走正常流程下高压
Ⅴ	紧急下电	立即将功率限到 0kw 并断开高压继电器	

发生故障时功率限制策略及动力切断的要求（除了严重影响人身安全的故障，其他故障切断动力需要考虑车况，比如车速；降功率速度需要考虑对驾驶安全的影响）；避免故障响应机制导致更严重的安全后果。

14.2 故障确认及清除的方法

故障确认及清除的两种方法：

1) 基于时间：
   a) 故障确认：在监控参数（如单体电压）达到故障阈值（如 4.3V）时启动计时，如果该异常现象持续一段时间（如 4 秒）则确认为故障（单体过压故障）。
   b) 故障清除：故障确认后，如果监控参数达到恢复阈值（如 4.2V）时启动计时，持续一段时间后可以清除故障；通常恢复阈值不等于故障阈值，这就是典型的滞回控制。
2) 基于次数：
   a) 故障确认：在监控到异常现象（如 VCU 报文丢失）时启动计数，下次再监测到同样的异常现象时将计数加上 δ1（如+5），如果计数器达到故障阈值（如 20 次）则确认为故障（VCU 报文丢失故障）。
   b) 故障清除：在故障确认过程中以及故障确认后，如果异常现象恢复正常（如 VCU 报文恢复），则将计数减去 δ2（如-3）。如果计数器达到恢复阈值（如 0 次）则可以清除故障。通常恢复阈值不等于故障阈值，这是另一种形式的滞回控制。

以上描述的是故障现象的确认和清除，对于故障码而言，轻微故障（如 SOC 过低）可以 key cycle 清除，中等故障（如内 CAN 通信故障）需要休眠/复位后清除，严重故障（如绝缘阻值过低）必须用诊断仪手动清除。

14.3 故障列表

典型的故障列表如下：

表 14.3 典型故障列表

参数项目	故障等级	处理方式
总电压过压故障一级	Ⅳ	延时下电
总电压过压故障二级	Ⅴ	紧急下电
总电压欠压故障一级	Ⅳ	延时下电
总电压欠压故障二级	Ⅴ	紧急下电
单体过压故障一级	Ⅲ	限功率
单体过压故障二级	Ⅳ	延时下电
单体过压故障三级	Ⅴ	紧急下电
单体欠压故障一级	Ⅱ	仪表报警
单体欠压故障二级	Ⅳ	延时下电
单体欠压故障三级	Ⅴ	紧急下电
单体压差过大	Ⅱ	仪表报警
放电过流一级	Ⅱ	仪表报警
放电过流二级	Ⅲ	限功率
充电（含制动能量回收）过流一级	Ⅲ	限功率
充电（含制动能量回收）过流二级	Ⅳ	延时下电
电池温度过高一级	Ⅱ	仪表报警
电池温度过高二级	Ⅳ	延时下电
电池温度过高三级	Ⅴ	紧急下电
电池温度过低	Ⅱ	仪表报警
电池温差过大	Ⅱ	仪表报警
低压供电电压过高	Ⅳ	延时下电

低压供电电压过低	Ⅳ	延时下电
热失控	Ⅴ	紧急下电
高压互锁故障	Ⅱ	仪表报警
高压继电器无法闭合	Ⅳ	延时下电
高压继电器粘连	Ⅴ	紧急下电
高压继电器带载切断次数过多	Ⅱ	仪表报警
高压继电器驱动电路故障	Ⅲ	限功率
电流传感器故障/采样故障	Ⅳ	延时下电
单体电压传感器故障/采样故障	Ⅳ	延时下电
温度传感器故障（单个）	Ⅱ	仪表报警
温度传感器故障（多个）	Ⅳ	延时下电
高压采样传感器故障/采样故障	Ⅱ	仪表报警
高压回路断路	Ⅴ	紧急下电
均衡区电路故障	Ⅱ	仪表报警
均衡区温度过高故障	Ⅱ	仪表报警
预充超时	Ⅳ	延时下电
预充过流	Ⅳ	延时下电
预充短路	Ⅴ	紧急下电
SOC 过高	Ⅱ	仪表报警
SOC 过低	Ⅱ	仪表报警
SOC 差异过大	Ⅱ	仪表报警
与 VCU 通信故障	Ⅳ	延时下电
与交流充电机通信故障	Ⅱ	仪表报警
与直流充电桩通信故障	Ⅱ	仪表报警
与电机控制器通信故障	Ⅱ	仪表报警
与网关通信故障	Ⅱ	仪表报警
内网通信故障	Ⅳ	延时下电
绝缘检测电路故障	Ⅳ	延时下电
绝缘阻值过低（继电器闭合前）	Ⅴ	紧急下电
绝缘阻值过低（继电器闭合后）	Ⅴ	紧急下电

14.4 国六排放标准与 BMS 相关的技术要求

国六排放标准对 BMS 的诊断要求分为基本诊断和排放相关的诊断：

14.4.1 基本诊断

基本诊断是指对输入部件和输出部件进行诊断，集成在 PCB 板上的传感器和执行器也同样属于基本诊断的范畴。

基本诊断涉及的名称及解释如下：

表 14.4-1 基本诊断列表

名称	解释
电路故障	短电源故障、短地故障、开路故障

超范围故障	超范围上限故障、超范围下限故障
合理性故障	输入信号在正常范围内，但并不准确，比如卡滞故障
功能响应故障	输出部件/执行器不能正常响应控制器的动作指令
通信故障	通信超时、通信丢失等与通信协议相关的故障

a） 对输入部件的基本诊断要求如下：

表 14.4-2 输入部件的基本诊断要求

接口类型	诊断要求
模拟量	电路故障、超范围故障、合理性故障
开关量（0/1）	合理性故障
PWM	电路故障、超范围故障、合理性故障
数字量（以通信方式输入的信号）	超范围故障、合理性故障
通信	通信故障

b) 对输出部件的基本诊断要求如下：

表 14.4-3 输出部件的基本诊断列表

接口类型	诊断要求
模拟量	电路故障、功能响应故障
开关量（0/1）	电路故障、功能响应故障
PWM	电路故障、功能响应故障
数字量（以通信方式输出的指令）	功能响应故障
通信	通信故障

14.4.2 排放相关的诊断

排放相关的诊断是指对导致排放超过阈值的故障进行诊断，包括影响制动能量回收的故障、影响发动机工作的故障等。

排放相关的故障与整车控制策略有关，一般而言 SOC、SOP 相关的故障会影响排放，但不同的企业、不同的车型可能存在差异，具体故障类别需要与 VCU、EMS 联合分析得出。

以 SOC 误差过大故障为例，需要根据实际采用的 SOC 估算方法（假设为安时积分法），采用 FTA 故障树分析在输入/处理/输出三个环节可能的影响因素，比如电流传感器故障、单片机最小系统故障、与 VCU/EMS 通信故障等（如下图所示），然后针对这些故障实施相应的诊断。与 14.4.1 节基本诊断内容重复的故障不需要在故障列表里重复两次。

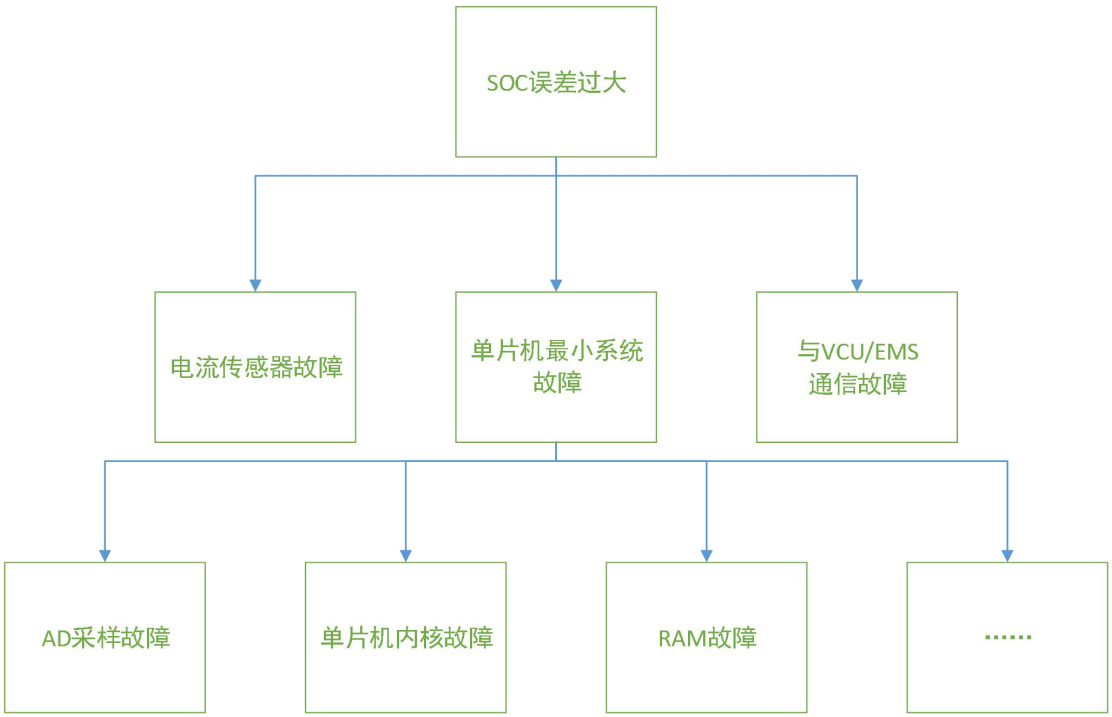


图 14.4 以 SOC 为例的故障树分析图

除此之外，可以根据特定工况对 SOC 进一步诊断，比如大电流充、放电一段时间后，SOC 估算值没有更新，可以认为是故障。这也和企业/车型的 SOC 算法策略有关，需要具体问题具体分析。

15 辅助功能

15.1 碰撞检测及处理

15.1.1 总体要求

在发生碰撞事故后，为保证驾驶舱内乘客安全，BMS 应具备自行判断碰撞故障是否发生的能力，在检测到碰撞事件的第一时间切断高压回路；为保证电池系统故障反应时间尽可能短，在碰撞确认后 BMS 应在 10ms 内做出故障反应。

15.1.2 故障等级定义

碰撞故障一般被认定为最高等级的故障，在未发生碰撞故障时，BMS 不应误报故障导致车辆高压异常断开，避免车辆行驶期间动力突然丢失导致的安全隐患。

15.1.3 碰撞信号种类

动力电池一般不会配备单独的碰撞传感器，所以 BMS 判断碰撞事件一般通过整车传递的碰撞检测信号。碰撞检测信号一般有以下几种：

(1) 由其他控制器（比如 ABM—Air Bag Manangement）通过 CAN 发送的碰撞信号（直接通知 BMS 是否发生碰撞）；

(2)高低电平信号；

(3)由其他控制器（比如 ABM）产生的 PWM 硬线信号；

除了以上几种不同的碰撞识别信号，针对不同的车辆配置 BMS 应能通过车辆其他控制器提供

的碰撞识别信号判断碰撞是否发生。

15.1.3.1 基于 CAN 碰撞信号的碰撞事件检测

整车相关控制器将其检测碰撞事件的结果以 CAN 信号的形式直接发送给 BMS，BMS 应接收并处理该碰撞信号，并结合其他检测条件，判断是否有碰撞事件发生。

15.1.3.2 基于 PWM 信号的碰撞事件检测

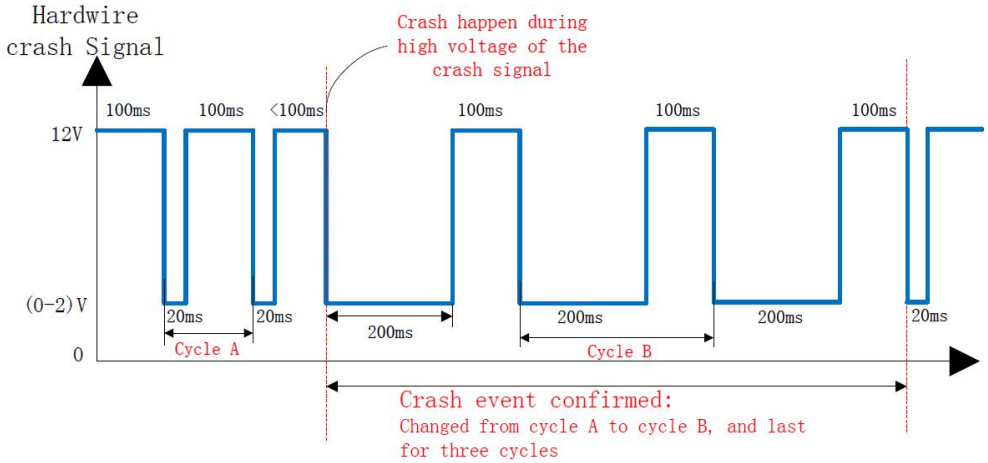


图 15.1　PWM 碰撞信号

整车其他相关控制器（比如 ABM），给 BMS 发送 PWM 信号，不同的占空比和周期代表不同的碰撞事件状态，如图 13-1 所示，整车未发生碰撞事件时，PWM 信号占空比为 5/6，周期为 120ms；车辆发生碰撞事故后，PWM 信号占空比变为 1/3，周期变为 300ms；为了避免误报，在连续检测到 3 个周期的碰撞波形，BMS 确认碰撞事件；当碰撞波形不属于两者中的任何一种，BMS 可认为碰撞检测电路出现故障。

BMS 应基于车辆碰撞信号发生器的实际情况进行设计，BMS 在解析波形时需要考虑占空比和周期的偏差。

15.1.3.3 基于高低电平信号的碰撞事件检测

车辆正常时，碰撞信号源持续输出 12V 的高电平信号，当碰撞发生后，12V 输出源被切断（比如通过电子爆炸管），BMS 端通过检测电平变化确定是否发生碰撞。

15.1.4 碰撞检测的冗余设计

碰撞检测应具备冗余的检测策略确保不出现误报；冗余设计应包含但不限于：

(1)碰撞检测电路的诊断：BMS 应具备碰撞检测电路自检功能，如碰撞检测电路开路、断路、短电源/地等故障场景；

(2)冗余的检测方案，在整车提供的硬线信号和 CAN 信号的基础上，BMS 应具备冗余的检测方案，比如通过车辆加速度的变化进行判断。

15.1.5　碰撞事件的故障反应

在确认碰撞事件发生后，BMS 应立即切断高压回路，且功率应降至零；

BMS 应存储故障发生时对应的车辆信息，并作为故障快照存储在 NVM 中，在需要时，故障快照应该可以通过 UDS 服务读取；

在碰撞事件发生后，碰撞故障的故障位应锁存，且只能通过 UDS 服务手动清除；在故障位清除之前，禁止所有高压上电操作。

15.2 高压互锁检测及处理

15.2.1 高压互锁功能定义

高压互锁（High Voltage Inter-lock， 简称 HVIL），用低压信号检查电动汽车上所有与高压母线相连的各分路的电气完整性。高压互锁功能的主要监控目标是需要通过机械安装实现高压连接的高压连接器比如 MSD，或者高压器件外部某些特殊的保护结构；一旦检测到高压回路的电气完整性存在异常，通过断开高压回路保障高压安全。

15.2.2 高压互锁的检测方法

BMS 在高压互锁电路的输入端注入一个低压电源信号，让低压信号延高压互锁回路传递，一旦存在某个高压连接器松动或脱落，接收端回检到的低压信号都会发生变化，根据回检的信号可以判定高压回路是否有故障；根据输入信号类型的不同，以下列举了两种典型的高压互锁回路检测方法。

15.2.2.1 恒流源检测方法

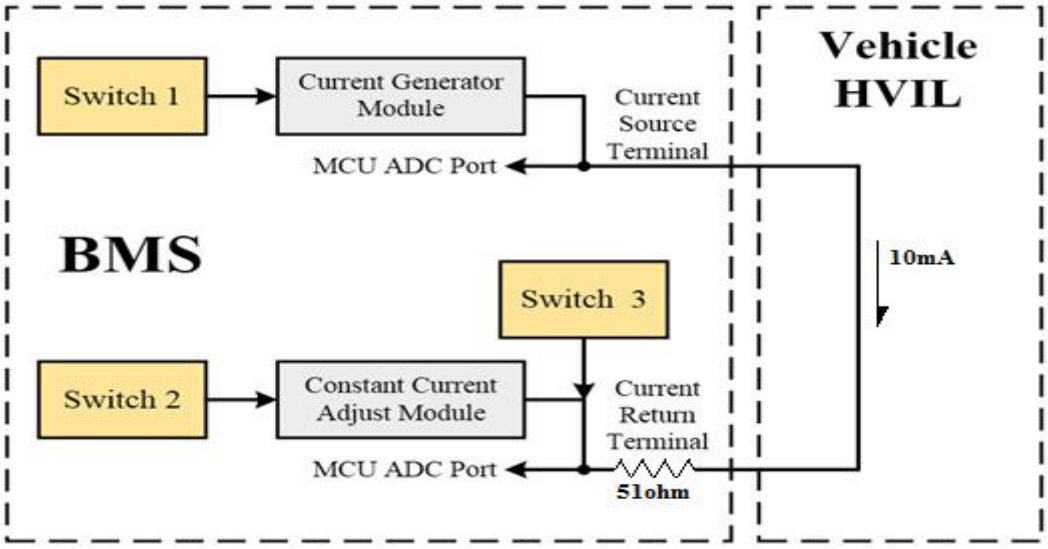


图 15.2-1 恒流源检测 HVIL 方法示意图

以上图为例输入端注入恒定的电流，在高压回路连接器等出现异常时会导致互锁回路的电阻发生变化，回采端的电压会由于回路中电阻变化而变化，基于回采电压可以判断高压回路是否异常。

15.2.2.2 PWM 检测方法

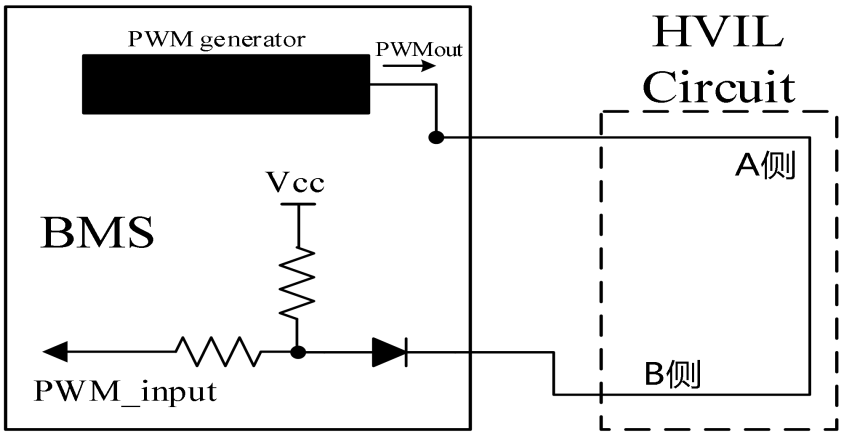


图 15.2-2　PWM 检测 HVIL 方法示意图

上图是使用 PWM 波检测高压互锁的方式，BMS 输出 PWM 波形，并进行回采。当采集端的 PWM 波形为正常占空比时，可认为高压回路是正常的；当回采的 PWM 波占空比为 100%时，有两种情况，一种是高压互锁回路断开，另一种为高压互锁回路与 LV 电源短路;当回采的 PWM 波占空比为 0%时，说明高压互锁回路出现与 GND 短路的故障。

15.2.3 高压互锁检测的其他要求

（1）具体的高压互锁实现形式，不同项目可能有不同设计。理论上，低压监测回路比高压先接通，后断开，中间保持必要的提前量，时间长短可以根据项目具体情形确定，比如 150ms；高压互锁回路必须能够有效、实时、连续地监控整个高压回路的通/断情况；

（2）当 BMS 检测到高压互锁回路断开或异常时，应禁止高压回路接通；在高压回路接通条件下，如果 BMS 检测到高压互锁回路断开或异常，综合车辆运行状态，在合适条件下应立即断开高压（比如车速低于 5km/h）；

（3）无论车辆在任何状态，BMS 在识别到高压互锁回路断开或异常时，必须对危险情况作出报警提示，比如仪表或者其他指示器以声或光报警的形式对驾驶员进行提醒。

15.3 大数据技术在 BMS 中的应用

15.3.1 开发大数据技术的目的

OEM（或者动力电池开发商）可以通过大数据平台查看动力电池当前状态数据、历史信息和变化趋势，依托后台计算机更强大的运算能力，通过多维分析、计算，提供动力电池最真实的状态信息，实现软件参数在线自动标定，车辆状态在线预测等功能。

15.3.2 大数据平台的基本架构搭建

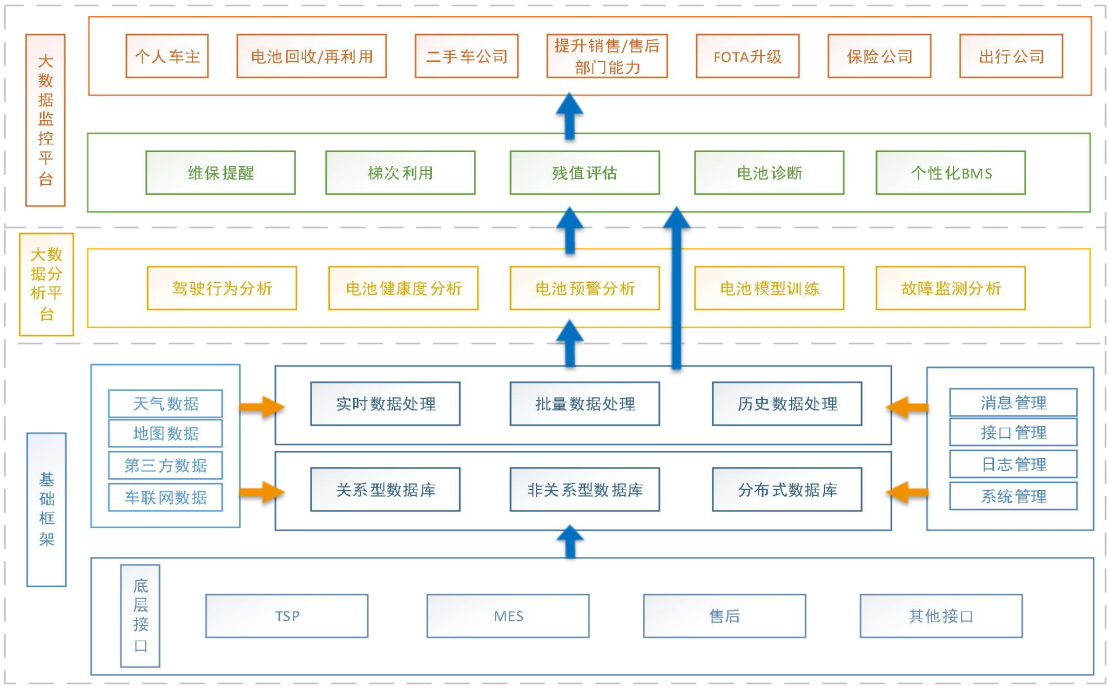


图 15.3 典型的大数据平台架构图

基于不同主机厂或电池厂的需求差异，大数据平台的架构定义和功能定义的范畴比较宽泛；上图中是大数据平台的示例架构，可用作大数据应用规划的参考。

15.3.3 数据及格式要求

BMS 远程数据传输应满足 GB/T 32960-2016 的要求，数据内容应覆盖但不限于标准要求的内容。

15.3.4 大数据功能

为了更方便的确认车辆状态和车辆数据的线上/线下分析，建议大数据实现以下功能：

——动力电池在线分布图，包括数量分布，动力电池 SOC 信息，SOH 分布统计信息；

——动力电池类型分布，包含电芯类型、容量以及供应商信息；

——动力电池累计使用信息，比如累计充放电容量；

——线下参数计算以及参数优化：通过平台的历史数据和实时数据推算电池状态参数（比如 SOH），推送至 BMS 用于数据修正；通过历史数据统计分析，更新、优化电池预置参数，推送至 BMS，确保电池与 BMS 软件实现最优匹配；

——通过历史数据分析功能，通过历史数据及算法模型，分析电池状态，提前发现安全隐患；

——信息推送，推送的方式可以包含邮箱、手机 APP 或者其他方式，推送的内容包含电池基本信息，电池维护信息，故障报警，驾驶建议，附近充电桩推荐等；

——电池残值评估，大数据平台分析电池各方面数据，可以快速生成电池参数评估的可视化报告。

15.4 非车载使用场景下对 BMS 的设计要求

15.4.1 产品检验及交付验收

15.4.1.1 EOL 测试

所有 BMS 交付前需要完成 EOL 测试，并出具含测试项目的书面文件。
EOL 测试应包含但不限制以下项目：
——基本功能测试；
——通讯检测；
——机械尺寸和外观检测；
——诊断检测和故障码清除（如果有故障码记录）。

15.4.1.2 合格检验

每套 BMS 产品经检验合格方可出厂，并应附有产品合格证或标记。

15.4.1.3 型式检验

有下列情况之一者，BMS 制造商应进行型式检验:
—— 新产品或老产品易地生产的试制定型鉴定;
—— 正式生产后，如结构、材料、工艺有较大改变而可能影响产品性能时;
—— 产品停产一年以上、恢复生产时;
—— 出厂检验结果与上次型式检验结果有较大差异时;
—— 国家监督机构提出进行型式检验的要求时;
产品的型式检验应全部符合规定的要求。如有一个项目不合格时，可重新抽取加倍数量的产品就该不合格项目进行复查，如仍有不合格时，则该批产品判为不合格，但对耐久性试验不合格时不应重新抽取，直接判为不合格。

15.4.2 产品包装、标识、贮存和保管

15.4.2.1 产品铭牌要求

每台产品应在其明显的部位固定产品铭牌，其基本内容包括：
——产品名称及商标；
——产品型号；
——生产日期或生产批号；
——生产企业名称代号；
——商品条码；
——软/硬件版本号；
其中商品条码应与 BMS 铭牌中的产品信息一一对应，以满足产品追溯性的要求。

15.4.2.2 包装要求

包装箱外部应有下列标志：
——产品名、产品型号、规格；
——生产企业名称、详细地址、邮政编码及电话号码；
——生产日期(或编号)或生产批号；
——包装储运图示标志(符合 GB 191-2008 的有关规定)，如防振”、“防潮”等；
——运输作业的文字:包装箱的体积(长 X 宽 X 高)尺寸；
——每箱内装产品数量;每箱产品总质量；
产品包装应满足以下要求：
——防潮、防振、防尘；
——适应公路、铁路、航空运输及叉车装卸；
——包装前产品的金属零件无防护层的配合部位，应有临时性的防锈保护措施；

——包装箱应牢固，产品在箱内不应窜动，以免运输途中损伤；
——包装箱中随同产品供应的技术文件应包括:①装箱单；②产品出厂合格证

15.4.2.3 贮存和保管

产品的贮存应符合 QC/T 238-1997 的有关规定。产品的贮存期通常为 2 年(从制造厂入库日期算起)。在贮存期满 2 年时，产品仍应符合本文档的规定。

15.5 电池系统快换对 BMS 产品的设计要求

15.5.1 电池系统快换的定义

新能源车辆在换电站使用电量充足的电池包更换电量低的电池包,在短时间内使车辆续驶里程增加的方法。

15.5.2 电池系统快换对 BMS 的要求

15.5.2.1 总则

BMS 在设计阶段要考虑电池系统快换的需求，并增加相应的信号接口，在电池包更换后通过与整车接口的信号交互，通过软件策略进行自动匹配，即 BMS 软件需要通过特殊设计具备一定的兼容性，在电池更换后不需要更新 BMS 软件即可直接匹配车辆使用。

15.5.2.2 同车型平台，同款电池系统快换

相同车型，同款电池包快换，因为电气系统完全兼容，BMS 软件在这种状态下不需要做任何调整；同电池系统快换（同一款车型平台，配有不同续航或者不同电芯的电池包）；相同车型，不同电池系统快换，BMS 软件需要将电池信息发送至整车，整车识别电池系统类型，并进行参数匹配（比如电机控制器基于不同电池系统的电压重新调整电机控制参数）。

15.5.2.4 不同车型平台，不同电池系统之间的快换

不同车型平台之间电池系统快换，需要充分评估不同平台之间软件的兼容性，若平台之间策略偏差很大，则不建议相互之间使用电池系统快换。若平台之间偏差不大，BMS 按照 15.5.2.1 节和 15.5.2.4 节要求的原则进行设计。
平台之间的偏差主要包含但不限于一下几个方面：

1）BMS 与整车的接口是否相同；
2）BMS 和其他 ECU 之间的信号交互逻辑是否相同；
3）整车的网络架构是否相同；
4）BMS 相关的功能策略（比如高压上下电流程）是否相同。

15.5.3 其他要求

不同车型平台之间要实现电池系统快换，在平台开发阶段，所有与 BMS 相关的功能策略及软硬件接口，建议全部采用平台化设计，包括但不限于：
——软件策略：高压上下电策略、状态机、充电策略、热管理策略等；
——硬件接口：所有 BMS 与整车对接的低压信号接口；
——软件接口：所有 BMS 与其他 ECU 交互的信号；

16 BMS 产品开发过程管理要求

BMS 的开发活动（包括但不限于产品的需求分析，设计，实现，集成，测试及验证，问题管理，配置管理）是否有规范的流程进行管控和约束，将直接影响到产品的安全与质量目标。为了规范开发过程中的活动，保证产品开发的质量，确保 BMS 可以达到电池系统全生命周期的安全目标,厂家必须建立一套符合道路车辆电子控制单元开发要求的流程以及相应的评价体系。厂家应当通过开发流程规范所有的开发活动，确保各活动符合相应的流程规范要求，并通过评价体系对开发流程和相应的活动进行评价，寻找流程体系及开发活动中不完善的地方，做到持续的改进。

厂家在进行 BMS 的开发流程及评价体系的建立时，建议参考如下标准：

ISO 26262 Road vehicles-Functional safety

ISO/IEC 15504

Automotive SPICE 3.1

附录 A
（资料性）
安全设计案例 — 预防高压采集回路间的串扰

A.1 问题背景及概述

电池系统中有多个高压回路需要 BMS 实时、准确的进行采集，例如电池包内部电压、外部电压，充电回路电压，绝缘检测回路电压等。由于采集的电压点数量多、采集的频率及时间点都不尽相同，因此很容易发生两路电压采集互相干扰的情况。从而造成了电压测量的失真，并且以此为基础做的其他的安全诊断项也会出现误判的情况，例如误判正极或负极接触器粘连，误判绝缘状态差等严重的故障。

本章节通过一个案例，分析由于正极电压检测回路与负极状态检测回路相互影响造成 BMS 误判负极接触器出现烧结的故障。详细分析该故障产生的原因，然后分享一种解决方案，最后总结提出设计注意事项。

A.2 案例分析

如下图 A.2 是某电池系统的部分高压检测回路示意图。其中电池包外部总电压的检测回路由图中 R1、K1 和 R2 构成，读取 AD2 值同时通过电阻分压计算可得总电压的实际值。另外一个检测高压回路即负极接触器状态检测回路由 R3 和 R4 构成，读取端口为 AD。

针对负极接触器检测回路，AD 读数大致等于 1/3 测量电压。设定测量电压在 3.9V 到 4.8V 之间，即 AD 读数为 1.3V 到 1.6V 之间判断负极接触器为有效的闭合状态，大于 1.6V 为无效值。

图 A.2 中的红色的回路是两路高压采集共同构成的回路，包含 R1、K1、R2、二极管、R3 和 R4。按照红色回路 AD 点的电压计算公式为 AD=(U-0.6)*100/(100+200+20+5000)。将上面分析的 1.3V 和 1.6V 两个 AD 电压点分别代入公式，可分别得到 U 为 70V 和 86V。即外部总电压在 70V 到 86V 的区间时，判断负极接触器为闭合状态。

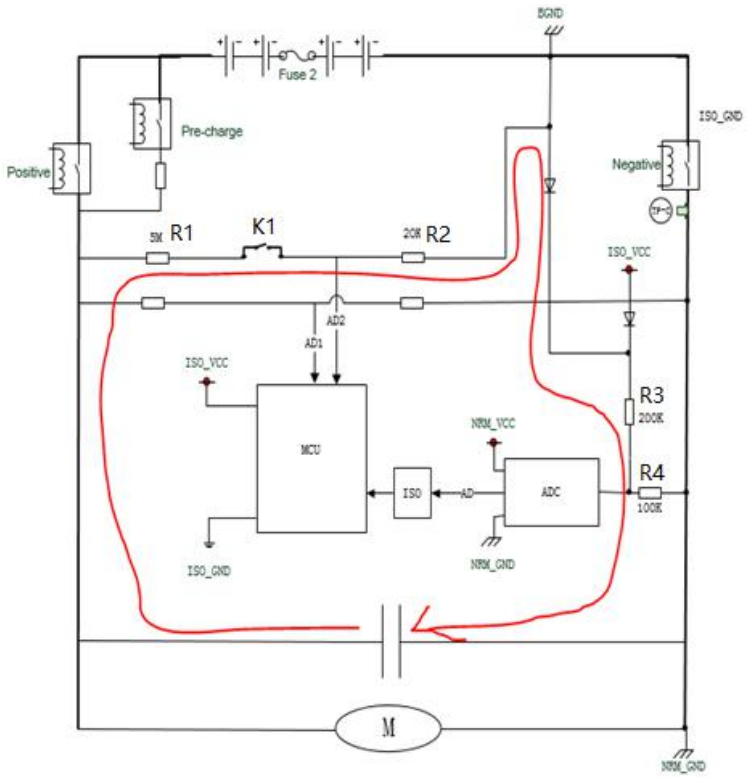


图 A.1 高压串扰案例电路示意图

最后再根据负极接触器烧结故障的判断逻辑，即发出负极接触器断开指令后检测到该接触器还是闭合状态。考虑一种情况，在高压下电后，接触器为断开状态，U 的电压逐渐下降，当降到 86V 到 70V 的区间的时候，BMS 判断负极接触器为闭合状态，根据控制策略判断负极接触器由烧结故障。在 BMS 的故障列表中该故障为等级较高的故障，有可能导致电池系统无法上高压电。

A.3 解决方案

根据以上分析，造成负极接触器烧结误报的原因是电池外部电压检测与负极状态检测电路构成回路的影响。解决方案的总体思路是：外部电压检测与负极状态检测分时进行，通过电子开关 K1 进行切换。在受影响的电压区域执行分时逻辑，该区域设定为 65V 到 90V（包含以上分析的 70V 到 86V 的区间）。分时检测的控制逻辑可参照图 A.3 两路串扰电压分时检测逻辑。

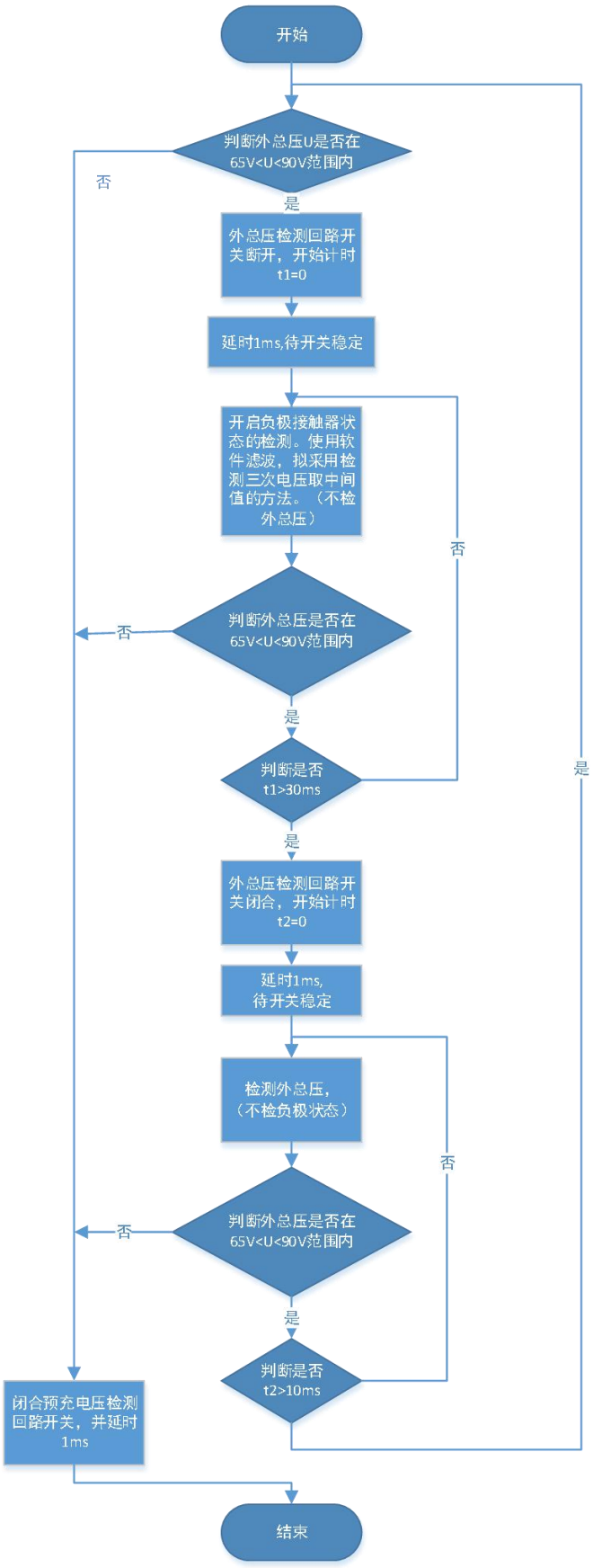


图 A.2 两路串扰电压分时检测逻辑图

A.4 安全设计提示

以上案例仅是两路高压检测间出现互相影响的案例，BMS 设计上有可能出现类似影响的电压回路还有很多，例如绝缘回路检测、充电回路检测等。如果要从根本上避免类似问题，必须在需求分析、系统设计、硬件设计和软件设计等各个环节都要注意。需求分析方面，要列出各个跟高压检测有关的功能并加以分析，不能有遗漏。系统设计方面，要合理设计高压控制及采集回路，尽量减少相互间的干扰。硬件设计上，要对各路高压采集做模拟仿真，再次找出由于硬件设计需要而引入的干扰项，尽量避免。实在无法避免的，建议在相关回路上加入电子开关，以便进行分时检测。软件设计上，合理安排检测时序，要同时保证单独检测功能的实时可靠性及各路检测间不受干扰。

附录 B
（资料性）
安全设计案例 — 接触器非预期切断导致烧结

B.1 问题背景及概述

某些 BMS 的功能安全设计上有一个目标为防止接触器的非预期切断。该功能可有效防止如 MCU 复位等原因引起的接触器非预期切断，从而提高了整车系统的安全性能。但是在某些情况下，该功能启动的同时如果接触器的供电电源断开又恢复的话，就会出现接触器没有进行预充过程从而发生接触器烧结的严重故障出现。

B.2 案例分析

为了实现防止接触器的非预期切断功能，需要借助一个信号锁存器来实现，下图 B.2 为信号锁存器相关电路图。包括输入信号引脚，功能引脚 OE 与 LE，及其输出引脚。

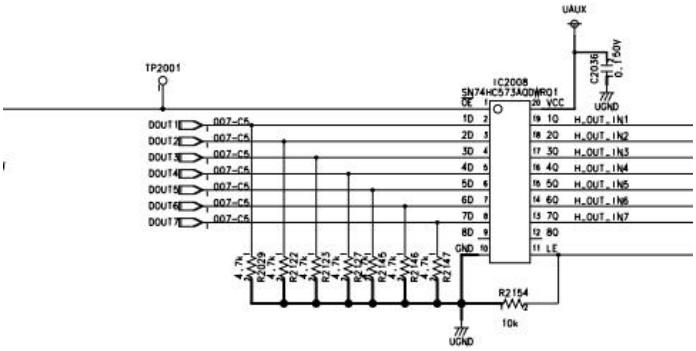


图 B.1 信号锁存器相关电路图

该锁存器的逻辑框图及真值表见图 B.2 及表 B.1。

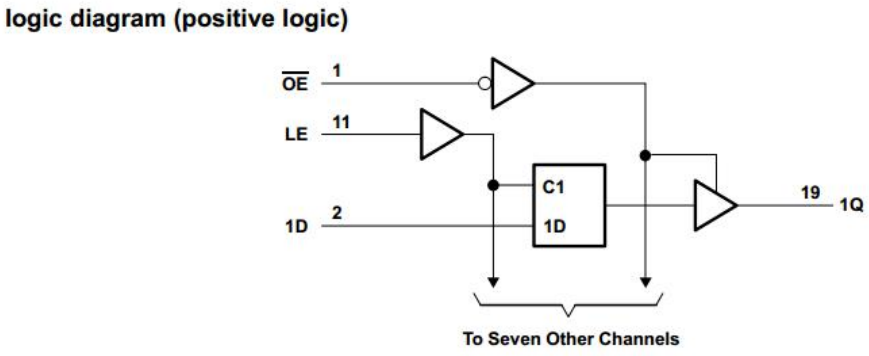


图 B.2 锁存器逻辑框图

表 B.1 锁存器真值表

FUNCTION TABLE
(each latch)

INPUTS			OUTPUT
$\overline{OE}$	LE	D	Q
L	H	H	H
L	H	L	L
L	L	X	Q_0
H	X	X	Z

该锁存器的逻辑框图及真值表见图 B.2-2 及表 B.2。锁存器内部是有一个 D 触发器与一个逻辑开关组成。锁存信号为 LE，使能信号为 OE。

当 OE=L,LE=H 时，输出的信号为前端输入信号 D

当 OE=L,LE=L 时，输出的信号为上一次的信号 QO

以上介绍清楚了锁存器的操作逻辑。现在来分析一下，在高压上电状态下进行软件程序刷写的情况。，此时主正接触器的驱动为 CLOSE,主负接触器的驱动为 CLOSE。刷程序时 MCU 复位，在初始化过程中时 OE 为 H。由于锁存器没有掉电，锁存器保持的主正与主负接触器还保持 CLOSE 状态，即 QO=CLOSE.OE 锁住输出，使驱动的输出一直保持 CLOSE 状态。同时接触器的供电电源由一个继电器控制，在程序刷写的过程中，该继电器先断开，再闭合。因此造成的主正和主负接触器没有经过预充过程而直接上高压电。最终导致两个接触器烧结，车辆无法正常行驶。

B.3 解决方案

在上高压状态进行 BMS 程序刷写，为避免出现烧结问题，在刷写程序时，要进行打开接触器的操作。在要进行刷写的时刻，底层软件要将接触器的控制状态由 CLOSE 状态切换至 OPEN 状态，此时锁存器将锁存 OPEN 的状态。然后 MCU 进行程序刷写，刷写完成后，MCU 完成初始化操作过程，直至应用层软件再次控制，其整个过程驱动的输出状态一直为 OPEN，不会出现烧结故障。

附录 C
（资料性）
安全设计案例 — 温度采集偏差的修正

C.1 问题背景及概述

电池系统中有多个温感线需要实时、准确采集温度数据，由于通道接口的限制和温感点安装的可操作性，实际整包中的温感点可能不超过 10 个且均布置在模组最外侧电芯表面，无法采集到模组内部最高温度，从而造成了温度测量的失真，而温度的准确度对整包的热管理策略，电芯的寿命、SOC、SOH 的估算至关重要。

本章节通过一个案例，分析由于温度采集偏差造成的整车功率使用限制。详细分析该故障产生的原因，然后分享一种解决方案，最后总结提出设计注意事项。

C.2 案例分析

如下图 C.1 是某电池系统整包常温充电热仿真结果，结果表明系统最高温度最低温度相差 5.7 ℃,其中前模组温度差异相对较小，后模组温度差异相对较大。实际模组表面温感不能准确测量模组中部最高温度点，整车在测试时，需要根据电池最高温度调整电池系统放电功率，防止电池发生过温情况。

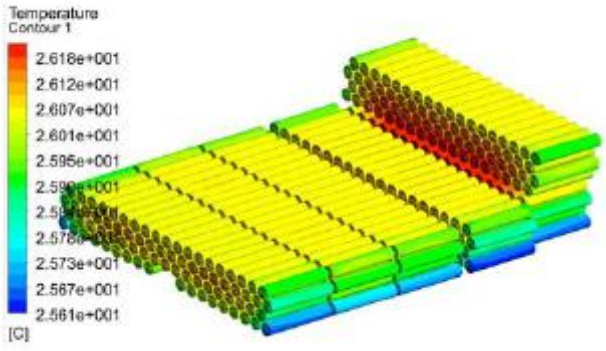


图 C.1 某电池系统常温充电热仿真

C.3 解决方案

根据以上分析，对整包温差较大的后部模组温度采集进行修正，从而估算最高点温度。

电池包静置时温感数据计算热阻 R1、R2，静置过程电芯发热功率 Q=0，T1 表示整包后模组实际温度最高值，T2 表示后模组温感点测量温度最高值。

$$\frac{T_a - T}{R} = \mathrm{C}\frac{dT}{dt}$$

$$\frac{dT}{dt} = \frac{T_a - T}{RC}$$

$$\frac{d(T - T_a)}{dt} = -\frac{T - T_a}{RC}$$

$$d\,ln(T - T_a) = -\frac{1}{RC}dt$$

1

$$C\left(\frac{dT_1}{dt}-\frac{dT_2}{dt}\right)=\frac{T_a-T_1}{R_1}-\frac{T_a-T_2}{R_2}$$

基于上述公式，通过整包环境温度和温感数据计算热阻 R1、R2 和 T1。

通过拟合公式，实际温度采集修正时，需 T1 进行约束：

(1) 当 T1-T2 大于设定温差 T0 时，需要对温度 T2 进行修正，使其接近实际整包最大值；

(2) 当 T1 小于 T2 时，无需对温度 T2 进行修正；

(3) 当 NTC 温感异时，不计算 T1。

C.4 安全设计提示

以上仅是温度采集偏差的案例，如果要从根本上避免类似问题，必须在需求分析、系统设计、硬件设计和软件设计等各个环节都要注意。需求分析方面，要结合整车实际使用需求和电芯性能参数并加以分析，不能有遗漏。系统设计方面，要合理设计温度采集点的位置，尽量覆盖到整包最高最低温度区域。硬件设计上，可设计用于模组内部测温的温感头，避免仅在模组表面位置进行测温。软件设计上，如温感点无法覆盖整包最高最低温度区域，应通过理论分析，对温度采集进行修正，保证温感点的数据能真实反应整包温度，防止对整车的使用产生影响。

附录 D
（资料性）
安全设计案例 — 烟雾热失控传感器漏报故障

D.1 问题背景及概述

基于国标GB 38031要求，电池包或系统在由于单个电池热失控引起热扩散、进而导致乘员舱发生危险之前5 min，应提供一个热事件报警信号（服务于整车热事件报警，提醒乘员疏散）。电池热失控时会喷出大量烟雾，电池系统中装有烟雾传感器，可以检测电池热失控时喷出的烟雾，当烟雾浓度达到一定标准时，传感器将发出热失控报警信号。由于成本和电池系统结构等因素，整包中可能仅一个烟雾传感器，放置在整包前部，中部或后部，整包中发生热失控的电池位置是随机的。当电池包成组使用电池容量小或失控产气量较少，且遇到烟雾传感器距离失效电芯较远情况时，由于结构件对喷出烟雾的绕流性，烟雾到达传感器时，浓度可能达不到传感器报警阈值，引起热失控故障无法报出而产生安全隐患。

本章节通过一个案例，分析由于整包结构设计和烟雾传感器安装位置对热失控故障的影响。详细分析该故障产生的原因，然后分享一种解决方案，最后总结提出设计注意事项。

D.2 案例分析

图D.1是某电池系统电芯热失控位置示意图。当电芯发生热失控时，如图D.1所示，失效电芯距离烟雾传感器较远，同时由于热管理需求，模组与周边环境密封相对较好，导致电芯喷出的烟雾在电池包内部扩散范围小，烟雾传感器检测的浓度值远低于报警阈值，传感器上报热失控故障码，而实际上电芯已经发生热失控，此种情况下存在严重的安全隐患。

图 D.1 某电池系统电芯热失控和烟雾传感器位置示意图

D.3 解决方案

根据以上分析，对烟雾热失控传感器报警策略进行修改，结合电压数据，避免热失控故障漏报。

图D.2和D.3分别是某电池系统优化后烟雾传感器位置示意图和模组开孔示意图，将传感器位置从整包边角移动到整包中间，同时在保证热管理性能需求的基础上，在模组侧板位置进行开孔，增加模组与外界进行气流传递的通道，使电芯热失控喷出的烟雾能够大量扩散到电池包烟雾传感器所在位置，同时传感器安装位置调整到电池包的中部。

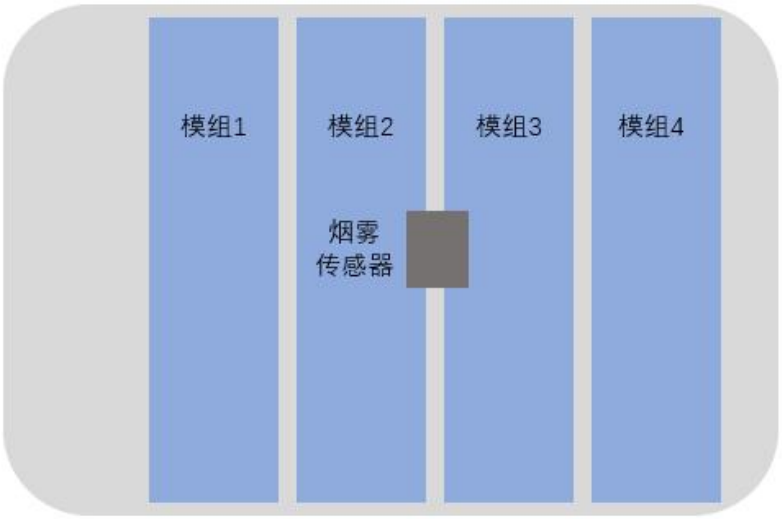


图 D.2 某电池系统优化后烟雾传感器位置示意图

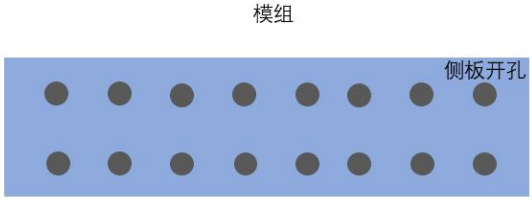


图 D.3 某电池系统模组开孔示意图

将烟雾传感器的热失控判断条件进行修改，传感器烟雾报警浓度为C0，当浓度低于C0时，增加电压判断条件，具体判断条件如下：

热失控烟雾传感器检测浓度达到C0时，则进行热失控报警；

2、当热失控烟雾传感器浓度达到较低浓度C1 时，在后续的10min内，对各串电压做如下判断：某一时刻出现某一串电压值U比所有串电压平均值Uavg之差： Uavg －U>特定压差U0，则进行热失控报警；

3、当检测到某一时刻某一串电压值U比所有串电压平均值Uavg之差： Uavg －U>特定压差U0时，在后续的10min内，如热失控烟雾传感器浓度达到较低浓度C1时 ，则进行热失控报警。

当上述条件任意一个满足均触发热失控报警。

D.4 安全设计提示

以上仅是烟雾热失控传感器漏报的案例，如果要从根本上避免类似问题，必须在需求分析、系统设计、硬件设计和软件设计等各个环节都要注意。需求分析方面，要结合整车客户的实际需求和电芯热失控特征表现综合分析，不能有遗漏。系统设计方面，要合理布置类似热失控传感器的位置，尽量覆盖到整包任一电芯热失控均能检测到。硬件设计上，可设计用高灵敏、抗干扰、响应快的热失控传感器，避免单一方面性能好的热失控传感器。软件设计上，不仅通过传感器浓度进行热失控判断，应通过电芯热失控特征表现分析，结合电压，压力，温度等数据，综合判断电芯热失控的发生，防止对整车的安全使用产生影响。

附录 E
（资料性）
安全设计案例 — 快充流程控制避免继电器粘连

E.1 问题背景及概述

电动汽车在大功率插枪充电时，在外部充电桩进行绝缘检测后，但是充电桩的电压还没有完全泄放时，闭合快充继电器，会导致快充继电器粘连。充电时，在继电器控制阶段，会因外部充电桩带异常高压导致继电器粘连。

E.2 案例分析

电动汽车在大功率充电枪上进行充电时，在 CHM 和 BHM 报文交互之后，CRM 和 BRM 交互之前，充电桩需要先进行绝缘检测。充电桩先闭合内部的 K1 和 K2 继电器，开启绝缘检测电路，并输出高压。如果充电桩检测绝缘正常，则停止电压输出，关闭绝缘检测电路。同时，开启泄放电路。通常情况下，快充桩输出电压可以下降到 60V 以下。但是市场上的充电桩良莠不齐，会出现有些充电桩没有严格按照国标的规定实现，导致泄放时电压未达到 60V 以下。如果在充电桩外侧有异常高压时，闭合快充继电器，会导致快充继电器粘连。

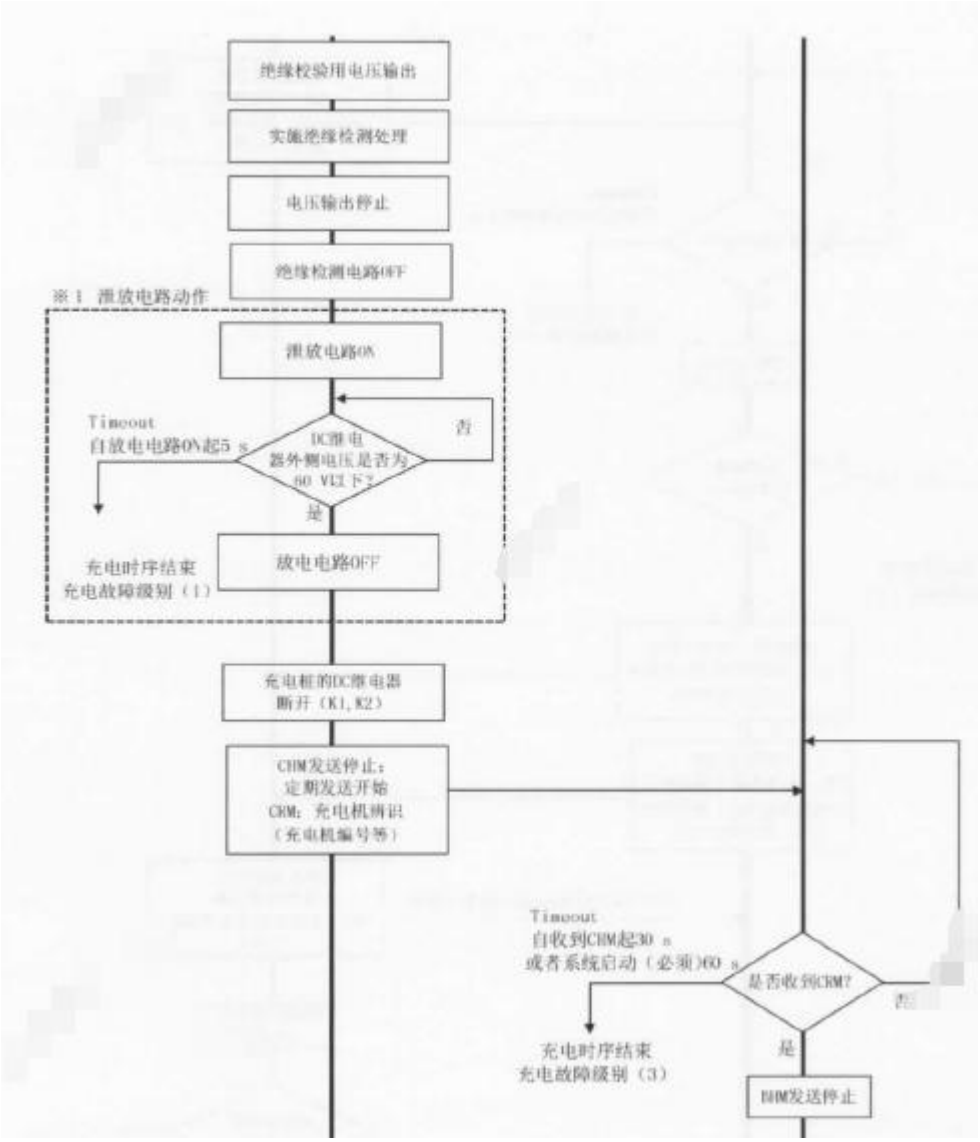


图 E.1 快充控制住部分流程图

E.3 解决方案

为了防止在充电桩外侧带高压时，BMS 控制快充继电器闭合导致继电器粘连，需要先检测快充继电器外侧电压。如果 BMS 检测到快充继电器外侧电压值相对较高，应等待充电桩外侧电压下降后，再闭合快充继电器。如果等待超时，应停止闭合继电器，退出充电。如果 BMS 检测到快充继电器外侧电压值相对较低，应可以正常闭合继电器。

附录 F
（资料性）
安全设计案例 —对于 AFE 芯片复位机制要求

F.1 问题背景及概述

BMS 需要实时对电池的单体电压和温度信号进行监控。基于电压和温度的基础数据，进行 SOX 的估算、故障的判断，特别是热失控报警，更加严重依赖于单体电压和温度信号。目前，采集单体电压和温度所用的 AFE 芯片，在板间都采用菊花链的通讯方式，一旦一个 AFE 采样芯片发生复位，后续芯片的数据都无法正常上传到 BMC。因此，需要对 AFE 芯片的复位机制进行规范和要求，以便于满足功能需求。

F.2 案例分析

有电池包热失控实验案例，菊花链不更新会一直尝试复位，由于一直在复位所有的单体电压和温度均无法获取，这样无法判断出热失控。

F.3 解决方案

菊花链不更后，不一直尝试复位。建议复位 3 次之后，不再执行复位，保证采样正常的芯片能够正常上报温度和电压值;这样当热失控发生时候触发菊花链异常仍能保证在出现异常的前面的采样芯片链路能够正常上报采集电压和温度，从而增加热失控报出的可能。

附录 G
（资料性）
安全设计案例 — 误报高压互锁故障导致异常下电

G.1 问题背景及概述

高压互锁（High Voltage Inter-lock， 简称 HVIL），用低压信号检查电动汽车上所有与高压母线相连的各分路的电气完整性。高压互锁功能的主要监控目标是需要通过机械安装实现高压连接的高压连接器比如 MSD，或者高压器件外部某些特殊的保护结构；一旦检测到高压回路的电气完整性存在异常，通过断开高压回路保障高压安全。

本章节通过一个案例，分析由于整车 EMC 干扰，误判高压互锁误报的故障。详细分析该该故障产生的原因，然后分享一种解决方案。

G.2 案例分析

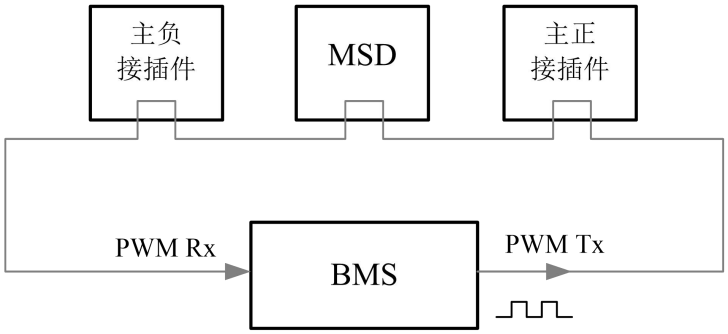


图 G.1 PWM 检测 HVIL 方法示意图

上图是使用 PWM 波检测高压互锁的方式，在高压互锁线路的始端注入 1KHz 频率 50%占空比的 PWM 信号，让 PWM 信号高压互锁回路传递。一旦存在某个高压连接器松动或脱落，接收端回检到的 PWM 信号周期和频率都会发生变化，根据高压互锁线路接收端的周期和频率可以判定高压回路是否有故障。

实际使用过程中，整车 EMC 干扰严重时，高压互锁线接收端检测到的 PWM 频率会远远偏离 1KHz，若处理不当，将导致 BMS 误报高压互锁连接异常，引起紧急停车。

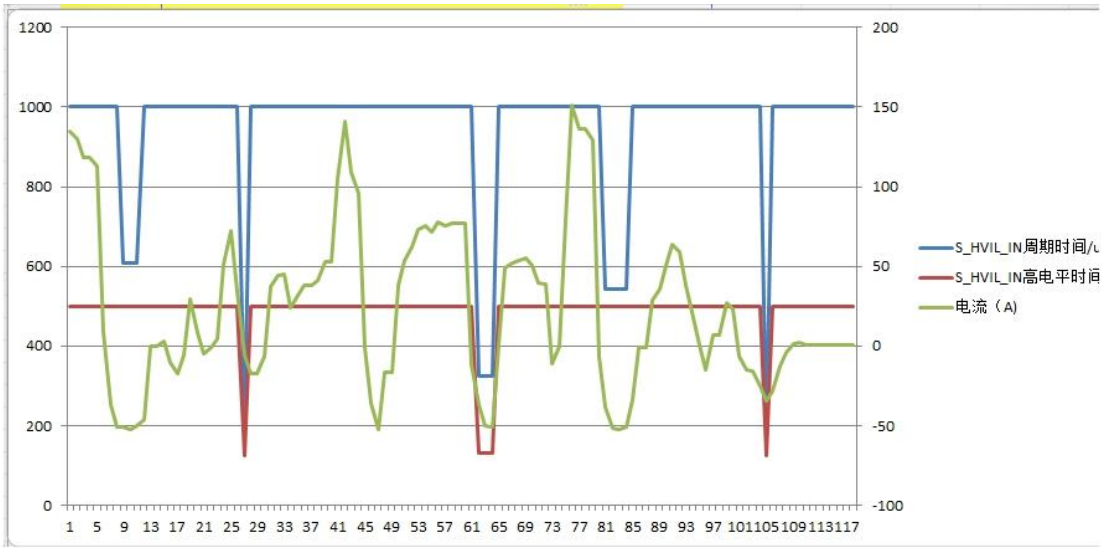


图 G.2 实际项目检测到的 PWM 输入信号

上图所示是实际项目，行车过程中，在接收端采集到的 PWM 信号：

蓝色的折线是 PWM 的周期，没有干扰时，周期为 1000us（单位为 us）

红色的折线是 PWM 的高电平时间，没有干扰时，高电平时间为 500us

黄绿色的折线是整车实时电流。

当驾驶员踩刹车时，电流下降，引起整车 EMC 干扰，导致 BMS 检测到的 PWM 信号出现偏差，PWM 输入信号周期降低到 300us，远远偏离了 1KHz 的输出频率，占空比也远远偏离 50%。若处理不当，将导致 BMS 误报高压互锁连接异常。

G.3 解决方案

从功能安全角度考虑，需要优化高压互锁 PWM 输入检测的判断逻辑，确保整车 EMC 干扰时，BMS 不误报高压互锁连接异常，引发行车安全事故。

同时，为了区分动力接插件松动故障和高压互锁检测线自身故障，将高压互锁相关的故障分为两个：

1） 高压互锁开路故障（表征动力接插件发生松动故障，影响行车安全）

2） 高压互锁检测线故障（表征高压互锁线自身发生故障，不影响行车安全）

下文给出了判断高压互锁相关故障的一个参考案例：

1） 高压互锁线的源端注入 1KHz@50%占空比的 PWM 信号。

2） 根据高压互锁接收端 PWM 频率和占空比，BMS 判断是否存在如下故障：

高压互锁开路故障

检测高压互锁接收端 PWM 的频率和占空比，若

a）频率在(20Hz[1],+∞)，BMS 不上报高压互锁开路故障。

b）频率在（0Hz，20Hz]，持续 1s[2]，BMS 上报高压互锁开路故障。

c）频率在 0Hz，且为低电平（占空比为 0%），持续 1s，BMS 上报高压互锁开路故障（高压互锁输入检测线默认下拉，当高压互锁线连接断开时，PWM 接收端将检测到低电平）。

高压互锁检测线故障

检测高压互锁接收端 PWM 的频率和占空比，若频率在 0Hz，且为高电平（占空比为 100%），持续 1s，说明高压互锁检测线和整车 KL30 电粘连，BMS 上报高压互锁检测线故障。一般而言，高压互锁检测线故障属于轻微故障，不影响行车安全，可以提示驾驶员行驶至服务站维修。

[1] 经验值，需实车标定。

[2] 实际故障触发时间，取决于客户需求。为防止误报，不宜低于 1s

附录 H
（资料性）
安全设计案例 — 预防主负接触器诊断电路击穿

H.1 问题背景及概述

在动力电池系统中，BMS 需要对主负接触器的开闭状态进行监测，各 BMS 设计厂商对主负接触器诊断有不同的方案，其中通过外搭有源电路辅助主负接触器诊断是比较常用的解决方案。图 H.1 展示的是一种典型的主负接触器状态监测的电路设计方案。该方案主要是设置一个以 PACK 负极为参考地的基准电源，通过高阻值分压电阻形成一个分压电路，当主负接触器闭合时，基准电源、分压电阻和 PACK 负极形成回路，在采样点 AD1 处采集的即为基准电源分压后的采集电压，当主负接触器打开时，在采样点 AD1 处采集的为基准电源的电压，这样通过 AD1 处不同的采集电压，可以区分主负接触器的开闭状态。

当动力电池处于高压连接状态，且高压负载处于运行状态，此时若主负接触器若因故障突然断开，同时高压负载未关闭或关闭延时，动力电池电压将通过主正接触器、整车高压负载、主负诊断电路、高压采集芯片和 PACK 负极形成回路，从而导致采集芯片基准电源电路两端产生高压，导致芯片损坏。

H.2 案例分析

如下图 附 H.1 是某电池系统主负接触器状态检测回路示意图。主负接触器的开闭状态的不同，AD 值也不同，根据图 H.1 中分压电路计算得知，当 BMS 主负诊断采样电压<=2.5V 认为接触器闭合，>2.5V 认为接触器断开。但是当主负接触器突然断开时，从电池包的高压会通过整车负载、R2 和 R3 施加到采集芯片，导致芯片损坏。

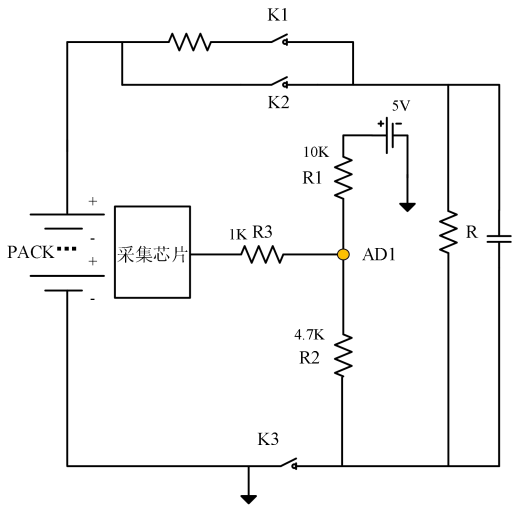


图 H.1 主负接触器检测回路

H.3 解决方案

根据以上分析，在主负接触器断开时采集芯片被击穿原因是电池包电压通过主负接触器检测回路施加至采集芯片。解决方案的主题思路：在主负接触器断开时，避免动力电池高压通过主负接触器检测电路形成回路，可以在主负接触器检测回路加入防反二极管，如图 H.2，该二极管的耐压值应该大于电池包总压，加入二极管后，即使在高压连接状态下主负接触器突然断开，由于防反二极管的阻隔作用，动力电池高压也不会通过整车负载和主负诊断电路形成回路，从而避免了采集芯片被击穿。

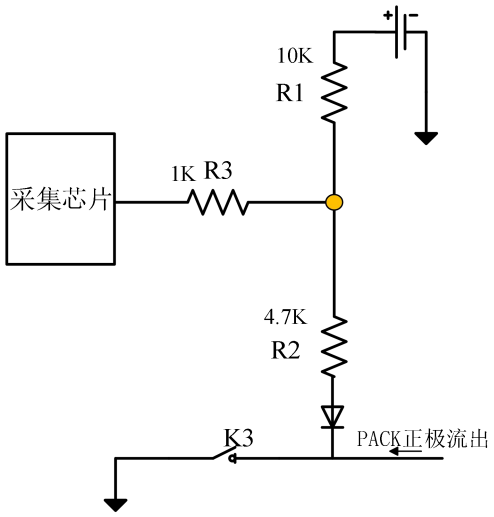


图 H.2 改进后的主负接触器检测回路