

T/EJCCCSE

团 体 标 准

T/EJCCCSE XXXX-XXXX

锂电启动电池设计安全规范

Lithium battery starter battery design safety specification

（征求意见稿）

20XX-XX-XX 发布

20XX-XX-XX 实施

中国商业股份制企业经济联合会 发布

目 次

前言 II

1 范围 1

2 规范性引用文件 1

3 术语和定义 1

4 基本要求 1

5 电芯选择与设计 1

6 电池管理系统（BMS） 2

7 机械结构设计 5

8 电气系统设计 5

9 安全防护设计 6

前 言

本文件按照GB/T 1.1—2020《标准化工作导则 第1部分：标准化文件的结构和起草规则》的规定起草。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别专利的责任。

本文件由苏州妙益科技股份有限公司提出。

本文件由中国商业股份制企业经济联合会归口。

本文件起草单位：苏州妙益科技股份有限公司、.....。

本文件主要起草人：XXX、XXX、XXX.....。

锂电启动电池设计安全规范

1 范围

本文件规定了锂电启动电池设计安全规范的术语和定义、基本要求、电芯选择与设计、电池管理系统（BMS）、机械结构设计、电气系统设计、安全防护设计。

本文件适用于汽车启动、点火、照明及驻车用锂离子蓄电池系统的设计。

2 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件；不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

- GB/T 5013.1 额定电压450/750V及以下橡皮绝缘电缆 第1部分：一般要求
- GB/T 5023.1 额定电压450/750V及以下聚氯乙烯绝缘电缆 第1部分：一般要求
- GB 18384 电动汽车安全要求
- GB/T 19666 阻燃和耐火电线电缆或光缆通则
- GB/T 31486 电动汽车用动力蓄电池电性能要求及试验方法
- GB/T 34590.5 道路车辆 功能安全 第5部分：产品开发：硬件层面
- GB/T 34590.6 道路车辆 功能安全 第6部分：产品开发：软件层面
- GB 38031 电动汽车用动力蓄电池安全要求
- GB/T 38661 电动汽车用电池管理系统技术条件
- QC/T 989 电动汽车用动力蓄电池箱通用要求
- QC/T 1023 电动汽车用动力蓄电池系统通用要求
- QC/T 1067.1 汽车电线束和电气设备用连接器 第1部分：定义、试验方法和一般性能要求
- QC/T 1067.2 汽车电线束和电气设备用连接器 第2部分：插头端子的型式和尺寸

3 术语和定义

GB/T 31486、GB 38031 界定的以及下列术语和定义适用于本文件。

3.1

测试态 test state

为满足容量测试，根据电池组充放电特性制定的控制策略。

注：因运行态放电策略内预留了启动电量，放电时会先达到SOC放电停止条件，达不到容量测试电压下限条件。

4 基本要求

应符合QC/T 989、QC/T 1023的规定，电池系统在各种工况下应安全、可靠运行，实现预期功能，且在整个生命周期内对人员、车辆及环境无危害。

5 电芯选择与设计

5.1 电芯性能要求

电芯应具有高能量密度、良好的充放电性能和循环寿命，在不同温度和充放电倍率下性能稳定。其容量、内阻等参数应满足电池系统启动、辅助供电及车辆运行要求，且在正常使用条件下，容量衰减应符合规定。

5.2 电芯安全特性

电芯应具备过充、过放、短路、过热保护功能或能与 BMS 配合实现上述保护。在过充、过放、针刺、挤压、高温等试验中，应能有效防止起火、爆炸等危险情况。

6 电池管理系统（BMS）

6.1 BMS 功能要求

6.1.1 一般要求

BMS 应具有数据采集、通信、报警和保护、控制、状态估算、参数设置、数据存储、计算和统计等功能，宜具有显示功能，锂离子电池、钠离子电池管理系统还应具有均衡功能。电池管理系统工作条件应满足GB/T 28046的规定。

6.1.2 数据采集

采集电池单体电压、电池单体温度、电池模块正负极端子温度、电池包总电压、电池包总电流等参数，采集误差及采样周期应符合表1的要求。

表 1 数据采集误差及周期

项目	采样误差	采样周期
单体电池电压	<0.3%	100 ms
电池总电压	<0.5%	100 ms
电池电流	<2	50 ms
单体电池温度	<2	1 s
加热膜温度	<2	1 s
极柱温度	<2	1 s

6.1.3 电池状态估算

应实时估算电池能量状态（SOC）和电池健康度（SOH），估算最大允许误差应为±5%。

6.1.4 报警与保护

6.1.4.1 报警信息分为一级、二级和三级，各级报警应按严重程度触发相应处理措施：

- a) 一级报警信息：应立即停机或停电处理的报警信息；
- b) 二级报警信息：应立即采取应急处理措施的报警信息；
- c) 三级报警信息：应加强监视及一、二级报警复归的报警信息。

6.1.4.2 应具备短路、过流、温度、过充、过放保护及充电限流功能：

- a) 短路保护：整车电气出现短路情况时，应在规定时间内及时切断功率回路，电池管理系统功能不受影响，测试完成后，所有电池管理系统保护功能都应处于正常运行状态；

- b) 过流保护：检测持续过载时，应在规定时间内断开电池输出，保护电池包功能不受影响；
- c) 温度保护：应监测电池组、极柱、功率器件的温度，检测温度超出限定值，应立即采取措施，如切断电池与负载的连接及输出告警信号；
- d) 过充电保护：当电池组的电压超过安全范围时，应及时切断电池组与充电设备之间的连接，避免电池内部发生化学副反应，测试完成后，所有电池管理系统保护功能都应处于正常运行状态；
- e) 过放电保护：当电池组的电压降低到安全范围以下时，应及时切断电池组与负载之间的连接，测试完成后，所有电池管理系统保护功能都应该处于正常运行状态；
- f) 充电限流：当电池包电量较低时，充电机或汽车发电机为电池充电时电流较大，在低 SOC 充电时，电池管理系统应具备主动限流充电功能，在适当情况下对充电过程进行电流限制。

6.1.5 计算与统计

应具有对累计充放电量、单次充放电量、电压越限次数、温度越限次数、故障保护事件次数等数据统计功能。

6.1.6 均衡

应具备均衡功能，修正串联电池组中单体电池电压或能量离散性，使电池单体压差小于 ± 30 mV，防止个别单体过充或过放。

6.1.7 休眠与唤醒

6.1.7.1 电池管理系统应具备锁电功能，在驻车等持续放电场景时，应自动预留足够的电量，通常不低于 10%。

6.1.7.2 当车辆熄火后，BMS 系统应进入低功耗状态。在低功耗状态下，应对其功耗电流加以限制，以防止因长时间停车造成电池亏电。

6.1.7.3 电池管理系统在进入低功耗模式时，应支持多种方式唤醒，包括但不限于充电唤醒、放电唤醒、KL15 信号唤醒、外部信号唤醒、报警唤醒、CAN 网络唤醒。

6.1.8 通信

6.1.8.1 电池管理系统应具备与整车通信能力，宜使用汽车电子电气架构中常见 CAN、LIN 等通信接口。

6.1.8.2 电池管理系统应具备告警功能，可通过通信接口对外发送电池系统时候信息，如电压、电流、SOC、告警等状态，为整车仪表盘或其他可视化设备提供数据源。

6.1.9 远程监控与预警

BMS 应具备远程监控功能，对异常电池包工作状态进行监控，对异常情况进行预警。

6.2 BMS 硬件设计

6.2.1 硬件开发流程

按 GB/T 34590.5 的规定，进行硬件层面产品开发，包括硬件安全要求定义、设计、架构度量评估、硬件集成和验证等，硬件设计应满足功能安全目标。

6.2.2 硬件安全要求

相关项硬件要素的硬件安全需求规范应从分配给硬件的技术安全要求中导出，涵盖控制内部和外部失效、符合其他安全要求、探测和发送失效信息等方面的硬件要求，以及不定义安全机制的硬件安全要求。硬件安全要求应符合相应的故障容错时间间隔和诊断覆盖率要求，并进行验证。

6.2.3 硬件架构设计

硬件架构应实现定义的硬件安全要求，将安全要求分配到对应的硬件要素，遵循 ASIL 等级分解规则。设计应具有模块化、适当粒度和简单性等特性，考虑硬件组件失效的非功能性原因，硬件架构应具有可靠性和可维护性。

6.2.4 详细硬件设计

应考虑安全相关硬件元器件失效的非功能性原因和任务剖面、运行条件，遵循鲁棒性设计原则，选择合适的元器件和设计电路，硬件在各种工况下应稳定运行。

6.2.5 安全分析与验证

应进行硬件设计的安全分析，识别失效原因和故障影响，对安全机制的有效性进行评估，包括对单点故障、多点故障和潜伏故障的分析。通过多种验证方法验证硬件设计满足安全要求，与软硬件接口规范兼容。

6.3 BMS 软件设计

6.3.1 软件开发流程

按GB/T 34590.6的规定进行软件层面产品开发，进行生命周期剪裁，选择合适的方法、语言和工具，软件开发各阶段应与系统和硬件开发协调一致，符合安全要求和相应的 ASIL 等级。

6.3.2 软件安全要求定义

定义软件安全要求，细化软硬件接口要求，软件安全要求应与技术安全概念和系统设计规范一致。考虑硬件约束、时间约束、外部接口和运行模式等因素，对软件安全要求和接口规范进行验证。

6.3.3 软件架构设计

开发实现软件安全要求的软件架构设计，进行验证。采用合适的标记法描述架构，具备可验证性、可配置性、可维护性等特性，遵循模块化、封装性和简单性原则。将软件安全要求分配到软件组件，对不同类型组件按规定开发或鉴定，分析相关失效，定义安全机制，预估资源需求，软件架构设计应合理。

6.3.4 软件单元设计和实现

按照软件架构和安全要求定义软件单元，实现并静态验证。选择合适的标记法和设计原则，软件单元功能应正确、接口一致、数据流和控制流正确，符合软硬件接口规范和安全要求，与目标硬件兼容。

6.3.5 软件单元测试

对软件单元进行测试，证明其满足设计规范且无非期望功能。按照规定计划、定义和执行测试，采用多种测试方法和案例生成方法，测定要求覆盖率和结构覆盖率，测试应充分性，测试环境应接近目标环境。

6.3.6 软件集成和测试

应集成软件要素，证明软件架构设计已实现。计划软件集成步骤，执行集成测试，采用多种测试方法和案例生成方法，测定覆盖率，验证嵌入式软件功能和资源，软件集成质量应符合要求，测试环境应接近目标环境。

6.3.7 软件安全要求验证

应证明嵌入式软件满足软件安全要求，在规定测试环境中执行测试，在目标硬件上测试，评估测试结果，软件在目标环境下应符合安全要求。

6.4 BMS 安全认证与测试

BMS 应通过相关安全认证，进行全面测试，包括功能测试、环境测试、可靠性测试、电磁兼容测试等，BMS 在各种工况下应性能稳定、功能可靠，符合安全要求。

7 机械结构设计

7.1 外壳设计

应满足GB 38031及QC/T 989的要求，通过振动、机械冲击、模拟碰撞、挤压、湿热循环、浸水、温度冲击、盐雾、高海拔、过温保护、过流保护、外部短路保护、过充电保护、过放电保护等试验，应无泄漏、外壳破裂、起火或爆炸现象，试验后绝缘电阻不小于100 Ω/V 。

7.2 内部结构布局

应根据电池包典型结构，合理布局电池单体、部件、高压电路、过流保护装置及接口等，满足 QC/T 989对安装空间和防护的要求，内部结构应紧凑、连接可靠、便于维护，防止部件间相互干扰和损坏。

7.3 机械固定与连接

应满足QC/T 989和QC/T 1023的要求，蓄电池箱在车上应可靠定位和锁止，具有锁止提示功能，采用双重锁止机构，在异常情况下不影响快速分离，电池安装和更换应具有安全性与便捷性。

8 电气系统设计

8.1 电气连接与布线

8.1.1 动力线路要求

8.1.1.1 按电池系统最大限流值选择动力线导线和母排，载流面积应满足最大电流要求，动力线缆应符合 GB/T 5013.1 和 GB/T 5023.1 的要求。

8.1.1.2 动力线缆阻燃和耐火性能应满足 GB/T 19666 的要求，安装和绑扎牢固，具有抗振功能。

8.1.1.3 动力线连接器应输电可靠，接触电阻应符合 GB 18384 的规定，工作温度范围为-40℃~80℃，并采用插拔型式的动力线连接器，单个接插器插拔力应不小于 50 N。

8.1.2 控制线路要求

线束材料应符合QC/T 413的规定，线束应符合QC/T 1067.1的规定，其阻燃和耐火性能应满足GB/T 19666的要求。低压控制线路、采集线路连接器应满足QC/T 1067.1、QC/T 1067.2的要求。

8.2 绝缘设计

动力蓄电池系统的电气绝缘性能应满足GB 18384的要求，具有保险控制功能，快速熔断器应适用于直流分断时可靠断弧、外壳完好、无拉弧现象。

8.3 电气保护装置

电压高于60 V的动力蓄电池系统应具有自动断电装置，宜有手动断电装置。过流时应能限制放电功率或向车辆控制 ECU 发送信号并报警，有效保护电气系统，防止过流损坏设备和引发危险。

9 安全防护设计

9.1 热管理系统设计

应遵循QC/T 1023的要求，宜具有热管理系统，维持电池系统在正常工作温度范围内，保证温度场均匀性，热管理接口应符合GB/T 38661的要求，防止电池过热或过冷影响性能和寿命。

9.2 防火与防爆设计

应满足GB 38031规定的相关试验要求，通过振动、冲击、碰撞、挤压等机械试验和环境试验后，无泄漏、破裂、起火或爆炸现象，电池系统在各种恶劣工况下防火防爆性能应达标。

9.3 防泄漏设计

动力蓄电池包防护等级在规定试验后不应低于IP55，防止电解液、气体等泄漏对环境及设备造成损害。
