锂离子电池储能系统功能安全规范

|  |
| --- |
| Functional safety specification for lithium ion battery energy storage system |
|  |
|  |
| （征求意见稿） |

2025-XX-XX发布

2025-XX-XX实施

深圳市市场监督管理局   发布

深圳市地方标准

DB4403/T XXX—2025

|  |
| --- |
|  |

ICS 29.220

CCS F19

|  |
| --- |
|  |

**DB4403**

目次

[前言 II](#_Toc188293686)

[1 范围 1](#_Toc188293687)

[2 规范性引用文件 1](#_Toc188293688)

[3 术语和定义 1](#_Toc188293689)

[4 功能安全目标 2](#_Toc188293690)

[5 功能安全设计验证 3](#_Toc188293691)

[6 风险分析 5](#_Toc188293692)

[7 功能安全保障措施 6](#_Toc188293693)

[8 安全信息提示 8](#_Toc188293694)

[附录A（资料性） 功能安全目标确认示例 9](#_Toc188293695)

[附录B（资料性） 串并联电路模型计算可靠性示例 10](#_Toc188293696)

[附录C（资料性） 安全测试项目 11](#_Toc188293697)

[附录D（资料性） 故障树分析示例 12](#_Toc188293698)

[附录E（资料性） 消防风水法 13](#_Toc188293699)

1. 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这些专利的责任。

本文件由深圳市科技创新局提出并归口。

本文件起草单位：。

本文件主要起草人：。

锂离子电池储能系统功能安全规范

* 1. 范围

本文件规定了锂离子电池储能系统的功能安全目标、功能安全设计验证、风险分析、功能安全保障措施和安全信息提示的要求。

本文件适用于家用储能、集装箱式移动储能、电力储能等锂离子电池储能系统的功能安全验证。

* 1. 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 4888 故障树名词术语和符号

GB/T 7829 故障树分析程序

GB/T 16855.1 机械安全 控制系统安全相关部件 第1部分：设计通则

GB/T 20438（所有部分） 电气/电子/可编程电子安全相关系统的功能安全

DL/T 2528 电力储能基本术语

* 1. 术语和定义

DL/T 2528和GB/T 20438.4界定的以及下列术语和定义适用于本文件。

锂离子电池储能系统 lithium ion battery energy storage system

由锂离子电池组、电池管理系统（BMS）、能量管理系统（EMS）、储能变流器（PCS）、监控系统、继电保护和安全自动装置、计量系统以及相关辅助系统等设备构成，能够独立实现电能存储、转换及释放功能的系统。

交叉审核 cross verification

在功能安全设计与验证过程中，对硬件、软件、系统等项目采取由不同人员或两种诊断方法进行验证的活动。

安全完整性等级 safty integrity level（SIL）

一种离散的等级(四个可能等级之一),对应安全完整性量值的范围。安全完整性等级4是最高的，安全完整性等级1是最低的。

1. 四个安全完整性等级对应的目标失效量在GB/T 20438.1-2017的表2和表3中规定。
2. 安全完整性等级用于规定分配给E/E/PE安全相关系统安全功能的安全完整性要求。
3. 安全完整性等级(SIL)并非系统、子系统,组件或元器件的属性。对“SILn安全相关系统”(n=1、2、3、4)的正确解释是系统具有支持安全功能的安全完整性等级达到”的潜在能力。

[来源：GB/T 20438.4—2017，3.5.8]

所需性能等级 required performance level;PL

每种安全功能为达到所需的风险减小所采用的用于规定控制系统安全相关部件在预期条件下执行安全功能的离散等级。

[来源：GB/T 16855.1—2018，3.1.24，有修改]

* 1. 功能安全目标
		1. 一般要求

锂离子电池储能系统供需双方应根据储能系统的类型、使用环境、装机容量、设计寿命及事故后果严重程度等要素确定系统的功能安全目标，参见附件A。

功能安全目标的设定宜由安全完整性等级或所需性能等级表征。

由安全完整性等级表征的锂离子电池储能系统目标应符合GB/T 20438（所有部分）的要求，由所需性能等级表征的锂离子电池储能系统目标应符合GB/T 16855.1的要求。

* + 1. 残余风险失效概率

应按照表1将功能安全目标转换为残余风险的失效概率。

1. 功能安全目标与残余风险失效概率的对应关系

|  |  |
| --- | --- |
| 功能安全目标 | 残余风险的失效概率（F/h） |
| 安全完整性等级a | 所需性能等级b | 最小值 | 最大值 |
| —— | a | 10-5 | ——c |
| 1 | b，c | 10-6 | 10-5 |
| 2 | d | 10-7 | 10-6 |
| 3 | e | 10-8 | 10-7 |
| 4 | ——c | 10-9 | 10-8 |
| 1. 安全完整性等级按GB/T 20438.1分类。
2. 所需性能等级按GB/T 16855.1分类。
3. 代表没有要求。
 |

* + 1. 特定要求

锂离子电池储能系统功能安全目标的确定不应低于以下特定要求：

——安全完整性等级1级目标：品质级别的异常缺陷；

——安全完整性等级2级目标：集装箱式移动储能遇到撞车等异常断电时间小于0.1s；

——安全完整性等级3级目标：储能系统表面温度不超过100℃；

——安全完整性等级4级目标：储能系统释放到环境的蒸汽不超过爆炸下限的10%。

* + 1. 确定方法

确定功能安全目标时，应基于电路类型和安全冗余情况，参见附录B选择合适的串联电路或并联电路模型计算可靠性和失效率。通过转变单点失效为多点失效实现安全冗余，以满足功能安全目标要求。

应使用交叉审核方式确保安全冗余。进行交叉审核时，应保证每项设计方案都配备相应的验证方案，每份测试计划制定配套的验证计划。

* 1. 功能安全设计验证
		1. 一般要求

应制定锂离子电池储能系统在设计阶段、制造阶段及售后服务阶段的功能安全设计验证方案和计划。

锂离子电池储能系统功能安全的设计验证流程见图1。



图1 锂离子电池储能系统功能安全设计验证流程图

* + 1. 设计阶段

设计阶段功能安全验证工作应至少包括以下内容：

1. 验证资料收集与分析：收集锂离子电池储能系统需要遵循的安全法规、标准，分析整理成功能安全验证要点清单；
2. 确定功能安全目标：具体见第4章；
3. 修订功能安全目标：根据特定系统运行环境、装机规模和使用频繁程度等修订功能安全目标；
4. 确定安全相关系统：明确受控设备（EUC）和EUC控制系统，确定安全相关系统；
5. 确定系统分析的故障树模型：分析系统结构、外部事件、事件类型和其他设备系统等，确定顶事件、中间事件、底事件、基本事件及事件概率，见6.2；
6. 确定售后服务内容，通过开展检测、保养、更换服务，实现质保期内的功能安全目标和售后服务清单（项目、频次、价格），见5.4；
7. 对a）～f）设计开展交叉评审，验证试验数据开展交叉稽核。

设计阶段的功能安全验证工作应平衡商业秘密和产品品质安全，验证工作应确保产品规格说明书、售后服务说明书的相关内容能达到功能安全目标。

对于电力用储能系统、公共交通工具储能系统，应设置具备监测和预警功能的远程监控系统确保功能安全的有效性；对于小型储能系统，宜设置具备监测和预警功能的远程监控系统。

* + 1. 制造阶段

制造阶段功能安全验证工作应至少包括以下内容：

1. 系统原型的验证和修改，更新故障树分析模型和验证测试报告；
2. 组织内审或客户审核，形成冻结的设计结果；
3. 开展首批量产产品验证的故障树分析，分析未来售后服务阶段的故障树分析的可实现性；
4. 交叉审核故障树分析和验证测试结果；
5. 量产品质的持续监督。若出现影响功能安全的产品品质波动和管理变更，立即更新故障树分析模型，并开展新的分析和验证测试工作；
6. 产品生产的中止或召回。如果产品不能满足功能安全目标，应中止生产，必要时产品召回；
7. 产品的重新优化设计，重新优化设计的产品，应按照5.2.1和5.3中a）～f）重新开展验证工作；
8. 完成产品出货前的安全检验报告；
9. 发布功能安全报告、产品说明书，产品说明书应包含售后服务内容，以及开展用户安全沟通的必要内容。
	* 1. 售后服务阶段

功能安全设计验证应考虑以下售后服务：

——系统售后涉及的可检测、可维修、可更换部件的非整体报废服务；

——预设的售后服务计划，包括检测、保养、更换的易耗品部件频次和价格等；

——售后服务的不适宜项目：优化拆装点、检测点；

——低寿命部件的更换方式，必要时纳入易耗品清单；

——持续量产出货期间，持续分析品质表现和售后服务内容，优化售后服务计划。

售后服务阶段功能安全验证工作应至少包括以下内容：

1. 宣传沟通售后服务内容；
2. 执行售后服务，包括检测、保养、更换服务；
3. 利用监控数据提供安全服务，如安装远程监控系统；
4. 故障树模型的更新。收集售后服务信息，结合最新技术、行业案例，判断是否变更故障树模型；
5. 开展故障树分析，验证是否符合功能安全目标，通过交叉审核确保分析到位。

必要时，锂离子电池储能系统供应商可决策和执行召回行动，对召回产品进行部件更换以达到重新安全使用的功能安全目标。

* 1. 风险分析
		1. 数据获取

应通过开展锂离子电池单体、电池模组、电池簇、电池储能系统安全测试获得风险分析的数据，对于功能安全分析涉及的安全测试项目，应保证测试数据的有效性。安全测试的项目参见附录C。

制造商提供的数据，应要求制造商提供数据来源并分析数据的有效性。

制造商开发的测试项目，用于预计使用场景的风险分析前，应获得系统使用方认可，可邀请第三方专业机构论证测试数据的适用性。

来自同类案例、第三方数据库或行业专家经验的数据，应验证数据的适用性、有效性，并获得系统使用方认可。

* + 1. 失效模式分析

应辨识系统起火、爆炸、触电等事故场景及失效模式，确定故障树分析模型。

典型的事故场景及失效模式包括但不限于以下：

1. 电池火焰或高温气体喷溅，点燃环境可燃物；
2. 热失控电池释放的气体在设备密封容器或密封房间堆积发生气体爆炸；
3. 泡水后，残留水分引发电极电解金属膜，逆变器短路引发触电；
4. 因温度剧烈变化产生冷凝水或电池本身有泄露电解液风险，造成电池内部电解金属膜短路，从而搭接电池外壳和极柱形成电池电解液破损泄露或产生气体；
5. 电网谐波造成电路板控制逻辑失效错误动作，造成MOS管导通不关闭等失效现象。

失效模式的分析应找出基础事件和/或底事件，并获取相关数据。所获取的数据宜形成关联，便于风险的评估。

* + 1. 残余风险计算

通过应用故障树分析顶事件的残余风险验证功能安全目标。

故障树分析应符合GB/T 7829的要求。在故障树分析的顶事件下，中间事件宜分为出厂验证阶段、售后服务阶段事件；中间事件宜分解为风险发生事件、诊断连锁抑制事件、扑灭事件等至少三方面的安全冗余，并依次向下分解中间事件直到基础事件。

故障树分析示例见附录D，所用符号应符合GB/T 4888的要求。

利用布尔运算等工具简化故障树分析模型，分析影响功能安全目标的主要失效事件，通过增加安全诊断覆盖率，降低失效率。

注：对失效率极低，如低几个数量级的事件，不进行展开分析。

利用获取的数据，通过故障树分析模型计算残余风险，必要时可邀请第三方专家参与计算。

* + 1. 补充安全措施

按6.3计算出的残余风险级别不满足功能安全目标时，应补充安全措施直到残余风险级别满足功能安全目标为止。

补充安全措施，宜结合底事件概率重要度、失效率、经济性等因素综合确定。宜优先使用软件逻辑控制等方法降低残余风险。

如有补充安全措施，应按第5章要求重新进行功能安全验证设计，并应重新开展故障树分析，并应确定故障树分析模型及验证测试方案/计划。在补充安全措施后，应再次开展故障树分析。

* + 1. 残余风险再次核算

应根据更新后的故障树分析模型验证测试方案/计划、补充安全措施等，按照6.3的要求再次核算残余风险。

* + 1. 文档管理

在冻结设计前的各阶段节点，应开展交叉审核，保存变更记录。

在小试、中试、首批量产阶段，应开展验证测试、交叉审核，并符合功能安全目标。

在各阶段的事件节点，应开展验证测试，记录结果，针对结果开展交叉审核。

应进行多次交叉审核，以判断是否满足功能安全目标。必要时，应与客户沟通并达成一致后，冻结设计方案，确定量产安排。

应保存验证测试数据及测试方案。

* + 1. 风险确认

风险分析结束后，宜将风险分析资料汇总，并通过备案或公证等方式，声明风险辨识全面，风险控制措施控制风险到可接受水平。

注：公证方式包括制造厂和客户达成的交叉审核确认，或制造厂聘用专业第三方评估认可等。

* 1. 功能安全保障措施
		1. 一般要求

应建立包括设计、制造、运输、存储、运行、维护的功能安全保障技术措施体系，并明确功能各阶段安全保障措施。

* + 1. 设计阶段

在设计冻结时，应形成系统制造工艺文件，明确系统设计功能安全保障措施及重点工艺控制标准、制造要求等内容。

在设计冻结时，应评估功能安全保障的重要安全内容，对经销商、运输商、最终用户及专业安装人员开展配套的说明、培训及要求。

在设计冻结时，应形成产品说明书，包括系统的介绍、运行、存储、安全环保警示、需要的培训、售后服务等内容。

* + 1. 制造阶段

制造阶段应选择合理的工艺路线，确保系统功能与安全匹配，达到设计功能安全目标。

制造阶段应建立全面的质量管控体系，不合格产品不应进入流通环节。

建立可追溯的产品返修、报废控制流程。

产品质量验证应符合功能安全验证需要，通过测试项目和测试数据跟踪产品安全风险水平，安全风险升高时，应及时查找原因，并采取控制措施。

* + 1. 运输阶段

应分析运输中存在的风险及控制措施，采用合规的包装方式。

电池单体宜采用的包装方式如下：

——少量电池用结实的木箱或胶箱运输；

——非专车运输的堆垛，使用泡沫、空纸箱等填充物充满堆垛上方至车辆顶部的空间，堆垛四周用纸皮等材料防护并固定。不应混放其他货物在堆垛上；

——运输的专车设置海关锁，超过800km的长途运输在堆垛间加防护气袋进行固定。

电池储能系统宜采用的包装方式如下：

——宜采用纸箱或木箱包装，依靠电池储能系统结实的外壳，并辅以缓冲材料；

——非专车运输的少量堆垛使用纸箱外壳，使用泡沫、空纸箱等填充物充满堆垛上方至车辆顶部的空间，堆垛四周用纸皮等材料防护并固定。不应混放其他货物在堆垛上。

应使用厢式车辆运输，不应使用平板车、敞篷车运输。

出货资料中应包含安全培训内容，货物外包装应设置安全提示，宜具备扫码在线学习功能。

运输人员应经电池消防灭火培训合格后方可上岗。运输车辆宜携带水桶、喷雾器、水基灭火器、灭火毯等消防器材。

* + 1. 存储阶段

应使用合理的低剩余电量（SOC）状态保存锂离子电池和电池储能系统，宜使用实验室安全滥用测试不易起火的SOC值。

1. 航空运输存储用30%×SOC。
2. 一般存储运输用70%×SOC。

仓库存放锂离子电池、锂离子电池储能系统时，应专库储存，不和其他危险化学品混放。

正常的锂离子电池、锂离子电池储能系统应在丙类仓库存放。存在安全缺陷的锂离子电池、锂离子电池储能系统应在甲类仓库存放。

仓库的电线应穿管布线，不应乱拉电线和超负荷使用排插，并应设置防鼠设备。

存储仓库应计算电池燃烧的产烟量、需要的抽风量、爆炸半径，来配置、核算风机的抽风量、房间间隔距离、样本存储容器尺寸等。抽风量、爆炸半径的计算方式参见附录E.3。

参见附录E在仓库安装抽风排烟措施，作用区域的风速应不低于0.5m/s。

应保持足够的通风量和适当的抽风排烟距离，计算通风稀释能力，减低释放燃气浓度。燃气浓度不超过气体爆炸下限的10%的区域为安全区域，可选择普通风机排烟。

仓库应配置以水为主的灭火器材，包括但不限于：泡水桶和坩埚钳、泡水池、喷雾器、洗车器、橡胶水管、消防软管卷盘、消防水带、消防水枪、水基灭火器。

仓库外非正在装卸的车辆，宜保持与仓库至少6m的安全间距。

锂离子电池搬运作业时不应损坏电池。作业人员应掌握水基灭火器等消防器材扑灭锂离子电池火灾的技能。

* + 1. 运行阶段

使用阶段应定期开展功能安全验证。

应按照系统的设计要求开展使用，不应过度放电和过度充电。

* + 1. 维护阶段

对于不能维护或维护风险较高的锂离子电池和电池储能系统，应进行报废处理。

选用泡水惰化处理方式的，应在与客户沟通同意后进行。泡水惰化处理操作如下：使用重量比例为5%的盐水浸泡锂离子电池4h、锂离子电池储能系统24h。泡水时，宜依次刺破电池，使水尽可能进入电池内部。放电完成后，应进行验电、沥干处理，交由专业回收单位处理。

* 1. 安全信息提示

锂离子电池储能系统应配备产品说明书。产品说明书中应写明使用和维护内容、用户应做事项、禁止事项，明确应由专业售后服务团队完成的工作事项。

应用说明书、网页、微信、在线培训考试、现场培训考试等多种沟通途径，向相关方传递使用、维护信息。

应向物流运输、存储的人员传递简易版的安全信息，宜用二维码扫描开展在线培训、在线考试。

1.
2. （资料性）
功能安全目标确认示例
	1. 基于销售规模与质保要求的电池储能系统功能安全目标确定示例

销售40万台电池储能系统，合同质保期为十五年不出现起火事故，不考虑中途加速损坏阶段，计算出厂前每台电池储能系统的失效率＝1次/（40万台×15年×365天/年×24h/天）＝1.9×10-11次/h。若希望电池储能系统在全生命周期发生0.1次失效，则计算的失效率＝1.9×10-12次/h。

销售20万台电池储能系统，合同质保期为十年不出现起火事故，不考虑中途加速损坏阶段，计算出厂前每台电池储能系统的失效率＝1次/（20万台×10年×365天/年×24h/天）＝5.7×10-10次/h。若希望电池储能系统在全生命周期发生0.1次失效，则计算的失效率＝5.7×10-11次/h。

1. （资料性）
串并联电路模型计算可靠性示例
	1. 原理

串联、并联电路模型是用来理解可靠性的方法，将串联系统改为并联系统能提升系统可靠度和降低系统失效率。

 

（a）串联电路模型 （b）并联电路模型

* 1. 串联电路和并联电路可靠性模型
	2. 示例分析

图B.1两个电路元件，每个元件可靠度R1＝R2＝0.9，则每个元件失效率F1＝F2＝1-0.9＝0.1；如图B.1（a）所示两个部件串联，系统可靠度Rs＝R1×R2＝0.81，系统失效率Fs＝1-Rs＝0.19；如图B.1（b）所示两个部件构成并联系统，系统可靠度Rs＝1-Fs＝0.99，系统失效率Fs＝F1×F2＝0.01；计算看出并联系统显著改善可靠性，降低失效率。

1. （资料性）
安全测试项目

锂离子电池或电池组的单个因素安全测试类型主要包括：

——机械安全滥用测试项目：碰撞、挤压、跌落、翻滚、振动、个别有穿刺等测试；

——环境安全滥用测试项目：高温、低温、高低温、高温高湿、盐雾、泡水、火烧等测试；

——电气安全滥用测试项目：短路、过充电、过放电、电路板抗静电或者电磁干扰等测试。

综合安全滥用测试项目通常包括将C.1所述因素组合测试，如高低温环境振动台上的充放电测试等。

1. （资料性）
故障树分析示例

家用电池储能系统故障树分析模型如图D.1。



注：辨识典型的符号为：顶事件、中间事件为矩形文本框图，基础事件为圆圈框图，或运算为“＋”号（OR单词）、与运算为“×”号（AND单词），在文本框里面加概率计算，可以在文本框外补充说明计算过程文本框，当页写不完时，分页画图用带箭头的线条和文字备注跳转或链接。

* 1. 家用电池储能系统故障树分析模型
1. （资料性）
消防风水法
	1. 原理

利用通风、机械排烟等方式将烟雾燃气浓度稀释至不超过爆炸下限的10%，可降低锂离子电池燃烧速度。同时，将低电导率的水溶剂注入破损锂离子电池，可将活泼的LiCx惰化为碳酸锂陶瓷，从而控制LiCx与其他物质发生反应。

* 1. 参数

消防风水法中，通风的参数如下：

——鼓风、抽风相互结合，打开门窗形成风道；

——作用区域风速不低于0.5m/s；

——典型作用距离为墙壁抽风5m，汽油鼓风机室内30m，伸缩管移动风机随管道长度宜60m；

——事故抽风为12次/h换气次数，所需要的抽风量计算见E.3。

消防风水法中，水的参数如下：

——宜用低电导率的清水、自来水、5%稀盐水、含水饮料灭火。不应用高电导率的饱和盐水、泥浆水、化雪盐水灭火；

——单位泡水量从大到小灭火方式，依次为泡水、定点射水、定点水雾、消防栓射水、喷淋系统喷水；

——用水量为每5万Ah配9L水或每500m2配60L水。

注：灭火过程中，应防范用水触电。设备应提前断电、接地，安装漏电开关。

* 1. 计算方法

锂离子电池和电池组燃烧的产烟量计算公式如下：

 $V\_{gas}=800×N×V\_{ele}×K$ (E.1)

式中：

$V\_{gas}$——产烟量，单位为立方米（m3）；

$N$——燃烧电池数量，单位为个；

$V\_{ele}$——单个电池电解液体积，单位为立方米（m3）；

$K$——电池电解液燃烧比例，按快速灭火（3min以内）、中速灭火（3min～10min）、慢速灭火（超过10min）的需求分别取0.2、0.5、0.8。

锂离子电池和电池组燃烧的需要的抽风量计算公式如下：

 $V\_{fan}=160000×N×V\_{ele}×K$ (E.2)

式中：

$V\_{fan}$——需要的抽风量，单位为立方米（m3）；

$N$——燃烧电池数量，单位为个；

$V\_{ele}$——单个电池电解液体积，单位为立方米（m3）；

$K$——电池电解液燃烧比例，按快速灭火（3min以内）、中速灭火（3min～10min）、慢速灭火（超过10min）的需求分别取0.2、0.5、0.8。

锂离子电池和电池组燃烧的爆炸半径计算公式如下：

 $R=2.9×W^{1/3}$ (E.3)

式中：

$R$——爆炸半径，单位为米（m）；

$W$——燃烧电池的电解液质量，单位为千克（kg）。

