ENGINEERING RESEARCH REPORT · 工程研究报告

动力电池包搬运夹具失效安全设计与故障注入验证研究

面向汽车行业助力搬运与非标夹具的公开资料研究、工程推导与验证方法

文件编号 AUREK-RC-AR-039

版本 V1.0

发布日期 2026-07-13

发布单位 江苏安睿克智能科技有限公司

研究与验证方法文件 · 非产品认证 / 非客户验收证明

报告结构

> **研究边界** 正文中的标准、论文与供应商资料用于支持方法框架；示例计算均带有假设。项目应用必须补充真实工件、夹具、动作曲线、风险评估与原始测试证据。

> **研究边界** 文档属性：方法研究与验证方案。本文未执行某一具体电池包夹具的故障注入，也不提供合格证书；示例载荷和响应要求必须由项目风险评估、真实载荷试验和客户技术条件确认。

00 执行摘要

动力电池包质量大、重心分布复杂、壳体和密封面敏感，并可能带有高压连接、冷却接口和受损电芯风险。搬运夹具一旦发生断气、断电、锁止不到位、传感器失真或误释放，后果不仅是工件坠落，还可能引发壳体变形、绝缘/冷却系统损伤和后续安全隐患。GB 38031-2025 已于 2026 年 7 月 1 日实施，规定了电动汽车用动力蓄电池安全要求[1]；该标准面向电池产品安全，并不直接替代搬运夹具的机械安全设计，但说明电池包属于需要严格避免机械损伤和异常能量事件的对象。

本研究提出“几何承托优先、危险释放受控、单故障可诊断、异常可安全落位”的失效安全架构。夹具不应主要依赖摩擦或持续气压保持重载；应优先建立明确的机械承力路径、闭合后自保持的锁止、受托确认后才能释放的联锁，以及对压力、位置、锁止和负载状态的多信号诊断。控制系统相关安全功能可依据 ISO 13849-1:2023 设计，并按 ISO 13849-2:2012 通过分析和测试验证[2][3]，所需性能等级由具体风险评估确定。

核心结论

- 重载电池包应以几何托承和机械自保持为主要承载路径，不把单一气压、真空或摩擦作为唯一防坠措施。
- “失效安全”不是所有故障后继续生产，而是故障后保持载荷、停止危险动作、禁止释放并进入可诊断的恢复状态。
- 故障注入必须覆盖传感器卡死、信号短路/断路、阀卡滞、管路破裂、压力渐降、通信中断、配方错配和误释放命令。
- 测试应遵循低能量到高能量、替代载荷到真实电池包、单故障到合理组合故障的递进原则。
- 验证证据要能追溯到安全需求、故障假设、试验步骤、原始信号、判定和整改闭环。

01 研究范围与安全目标

研究对象包括电池模组、下壳体、电池托盘和完整动力电池包在装配、检测、返修和线边转运中的专用搬运夹具，载体可以是助力机械臂、起重装置、机器人或专机。本文重点研究夹具与控制接口，不覆盖电芯电化学设计、BMS 算法认证或运输法规。

安全目标分为四类：人员不暴露于坠落和挤压危险；电池包不因搬运产生超出产品允许的壳体、密封面或接口损伤；夹具单一故障不会直接导致危险释放；异常状态能够通过明确步骤把载荷转移到安全支撑。ISO 12100 要求在机械全生命周期内识别危险并进行风险降低[4]，ISO/TR 20218-1 则为机器人末端执行器的设计与集成提供安全指导[5]。

安全功能	触发条件	目标反应	必须保留的证据
夹持/托承确认	取件前	未确认则禁止提升	位置、压力/力、锁止状态
载荷保持	断气、断电、阀故障	不危险释放，停止运动	保持时间、位移、结构状态
受托释放	工件已落位且姿态允许	才允许解锁/松夹	支撑信号、位置和命令记录
错配抑制	电池型号/夹具/配方不一致	禁止夹持或提升	ID、配方版本、联锁日志
异常恢复	任一安全相关故障	进入受控落位或维修状态	恢复步骤与授权记录

02 承载架构与失效安全原则

02.1 几何承托优先

电池包质量大且底部通常存在结构允许区和禁触区。优先使用托臂、叉形支承、承力孔/边梁定位或经产品方确认的机械抓取点，让重力通过明确结构路径传递。气缸或电机主要用于闭合、定位与锁止，不应在能源消失后立即失去全部承载。

若必须使用夹紧摩擦传力，应取得最低摩擦系数、接触材料、表面状态和夹紧力的可验证数据，并评估夹紧对壳体、冷却板、密封面和涂层的影响。对重载安全功能，几何托承通常比单纯提高夹紧力更稳健。

02.2 载荷工况与示例计算

$$F_{eq} = m \cdot (g + a_z) + F_{shock}$$
$$F_{design} = S_L \cdot F_{eq}$$

假设电池包质量 650 kg，最大向上加速度 0.25g，暂不计额外冲击，则等效竖向载荷约为 7.97 kN。若示例安全系数 S_L=2.0，设计竖向载荷约为 15.9 kN；四个理想均匀支点平均约 4.0 kN/点。实际必须再考虑重心偏移、支点刚度不一致、制造公差、倾斜、制动和单支点失效。该示例不代表项目额定载荷或推荐系数。

对于偏心重心，应通过静力平衡或有限元计算每个支点反力。不能把总载荷简单平均分配。若电池包存在不同长度、质量或附件配置，应将“最大单点反力”而非“最大总质量”作为支点设计输入之一。

02.3 锁止与释放

锁止机构应在闭合到位后形成可验证的机械状态；失去驱动能源时，应保持载荷或至少防止危险释放。释放必须满足工件受托、夹具处于允许位置、运动停止、人员区域安全和操作命令有效等条件。任何传感矛盾应进入保守状态，而不是用软件默认值代替真实反馈。

03 气动、电气与控制安全架构

ISO 4414:2010 适用于机械上的气动系统和部件，覆盖与预期使用相关的重要危险[6]。在电池包夹具中，气路设计要考虑管路破裂、接头脱落、阀芯卡滞、压力源波动、残余能量和维护隔离。储气或保压元件只能延缓能力下降，不能自动等同于安全保持。

推荐的诊断层包括：源压力、执行器两腔或关键回路压力、锁止位置、夹爪/托臂位置、工件存在、受托状态、载荷/重量合理性和控制通信健康。不同信号应尽量具有物理多样性，避免两个“冗余”信号实际来自同一个机械靶标或同一根电缆。

$$Lift\_Enable = Load\_Present \land Clamp\_Closed \land Lock\_Confirmed \land Pressure\_OK \land Recipe\_Match$$
$$Release\_Enable = Supported \land Safe\_Position \land Motion\_Stopped \land Operator\_Command \land Diagnostics\_OK$$

逻辑表达式只描述功能关系，不等同于已满足某一性能等级。安全相关控制系统的结构、诊断覆盖、共因失效、软件和验证应按项目选定标准实施[2][3]。

04 危险分析与 FMEA

失效模式	局部原因	潜在后果	设计控制	验证方式
气源突然丢失	总管断气、接头脱落	夹紧力下降、载荷滑移	机械托承、自保持锁、止回与监测	断气故障注入
单支路破裂	软管磨损、接头损坏	单夹爪失效、偏载	分区隔离、支点冗余、压力监测	指定位置开漏
阀芯卡在释放位	污染、机械故障	非预期松夹	释放隔离、双条件许可、机械保持	模拟阀卡滞
锁止未完全到位	公差、异物、错位	承载时脱开	独立锁止反馈、几何防脱	半锁状态试验
传感器卡常开	线路短路、软件冻结	未夹紧却允许提升	互补信号、时序/合理性诊断	信号强制为 1
传感器卡常闭	断路、靶标偏移	无法释放或误判故障	断线诊断、维护状态	信号强制为 0
型号配方错误	扫码/网络/人工错误	受力点错误、干涉	机械防错、ID 一致性、版本控制	错配注入
误释放命令	人机界面或程序错误	悬空坠落	受托联锁、受限位置、双动作	悬空发释放命令
通信中断	总线故障、PLC 重启	状态未知	保持载荷、停止运动、禁止释放	断网/重启注入
负载异常	双包、异物、重心异常	结构或起重装置过载	重量合理性、取件位防双取	替代载荷测试

FMEA 需与故障树或安全需求矩阵配合。对坠落顶事件，应寻找最小割集，例如“无几何承托 + 锁止失效 + 释放误命令”或“传感器共因失效 + 软件未诊断”。若某个单故障即可触发顶事件，应优先修改结构，而不是仅降低发生概率评分。

05 故障注入验证策略

ISO 13849-2:2012 规定通过分析和测试验证安全功能、实现类别和性能等级的程序与条件[3]。故障注入是验证的一部分，不能替代完整的设计审查、元件数据、计算和软件验证。测试前必须完成风险评估、试验区隔离、替代载荷设计、紧急支撑和恢复方案。

05.1 分级顺序

1. **模型与逻辑级**：在控制仿真或离线逻辑中强制输入，确认状态机和报警。
2. **低能量台架级**：使用空夹具或轻质假件注入断线、短路、阀和压力故障。
3. **额定替代载荷级**：使用几何和质量等效的非电池载荷验证保持、位移与结构。
4. **真实电池包级**：只对前三级无法覆盖的界面和产品保护项目测试，风险受控且经授权。
5. **现场集成级**：确认与机械臂、起重装置、输送线、工装和安全系统的联锁。

05.2 故障注入矩阵

编号	注入故障	注入时刻	预期系统状态	关键记录
FI-01	总气源切断	提升后静止/运动中	保持载荷，停止危险运动，禁止释放	压力、位移、停止时间
FI-02	单支路快速泄漏	最不利姿态	隔离故障，报警，维持可落位状态	分区压力、支点反力
FI-03	锁止反馈卡常开	闭合前	不允许提升	输入/输出与报警日志
FI-04	锁止反馈卡常闭	半锁状态	合理性诊断触发，不允许提升	位置、压力、信号矛盾
FI-05	释放阀命令粘连	悬空状态	物理或控制层阻止危险释放	阀电流、压力、锁状态
FI-06	受托信号虚假	未落位	双重/多样性检查拒绝释放	支撑、位置、负载变化

编号	注入故障	注入时刻	预期系统状态	关键记录
FI-07	控制器重启/总线丢失	运输中	输出进入定义安全状态，载荷保持	重启时间、输出状态
FI-08	错误电池型号/配方	取件前	配方不一致，禁止动作	ID、配方版本、CRC/签名
FI-09	急停	最大合理速度	停止且载荷不释放	峰值加速度、结构/载荷位移
FI-10	维护释放误操作	未支撑	受权限和机械条件限制	权限、步骤、锁具状态

每个用例应定义“通过、失败、需工程评审”三种结果。不能只记录最终是否掉落，还应检查峰值位移、锁止变化、报警可见性、恢复是否需要绕过安全功能，以及是否产生电池包隐藏损伤。

06 验收指标与证据链

项目指标应从风险评估和技术协议导出。常见类别包括额定与最不利载荷、单支点反力、允许壳体变形、保持时间、最大滑移、停止加速度、故障检测时间、报警与复位、释放许可和维护隔离。本文不为这些指标给出通用数值，因为不同电池包、载体和人员暴露条件差异很大。

证据层	典型文件	质量要求
需求	安全需求规范、客户接口、产品禁限区	唯一编号、版本和来源
分析	载荷计算、有限元、FMEA/FTA、PL 评估	假设明确、最不利工况可追溯
设计	图纸、BOM、气路/电气图、软件版本	与分析和实物一致
验证	测试计划、原始曲线、照片、日志	注入故障、时间基准和判据完整
放行	偏差清单、整改闭环、签字与维护要求	未关闭问题有明确限制

测试信号应使用统一时间基准，以便分析命令、阀动作、压力变化、锁止位移和载体停止之间的因果关系。只保存 HMI 截图不足以支持故障响应验证。

07 安全恢复、维护与变更管理

异常恢复必须在设计阶段定义。典型步骤包括：停止载体、确认载荷保持、建立临时支撑、隔离能源、消除故障、重新确认锁止、低速落位和复位审批。人员不得站在电池包下方或依靠手动持续托举。若需要人工释放机械锁，应具备工具、权限和受托条件限制。

维护项目包括锁止件磨损、托臂变形、紧固件、软管磨损、阀污染、传感器靶标、线缆弯折、接触垫材料和校准状态。任何电池包质量、重心、壳体结构、允许支撑点、夹具模块、软件配方或载体加速度变化，都应触发影响分析和必要的再验证。

08 结论与适用限制

动力电池包搬运夹具的失效安全设计，应从结构承力路径开始，再由气动、电气和控制系统提供状态确认、故障诊断和受控释放。安全目标不是故障后维持节拍，而是防止危险释放并把系统带入可安全恢复的状态。故障注入验证必须与需求、FMEA/FTA、控制逻辑和真实结构对应，形成可审计证据链。

本文是工程研究和验证方案，不构成 GB 38031 产品符合性证明、ISO 13849 性能等级认证、第三方检验或客户验收报告。具体项目需由具备能力的专业人员依据适用法规、标准、客户规范和实际风险完成设计与签署。

参考文献

1. GB 38031-2025 电动汽车用动力蓄电池安全要求. https://openstd.samr.gov.cn/bzgk/std/newGbInfo?hcno=3AB693FAFF5D9716DF61C61D6FD2187A
2. ISO 13849-1:2023. Safety of machinery - Safety-related parts of control systems - Part 1: General principles for design. https://www.iso.org/standard/73481.html
3. ISO 13849-2:2012. Safety of machinery - Safety-related parts of control systems - Part 2: Validation. https://www.iso.org/standard/53640.html
4. ISO 12100:2010. Safety of machinery - General principles for design - Risk assessment and risk reduction. https://www.iso.org/standard/51528.html
5. ISO/TR 20218-1:2018. Robotics - Safety design for industrial robot systems - Part 1: End-effectors. https://www.iso.org/standard/69488.html
6. ISO 4414:2010. Pneumatic fluid power - General rules and safety requirements for systems and their components. https://www.iso.org/standard/44790.html
7. ISO/TR 14121-2:2012. Safety of machinery - Risk assessment - Part 2: Practical guidance and examples of methods. https://www.iso.org/standard/57180.html
8. U.S. Department of Transportation / NHTSA. Safety Management of Automotive Rechargeable Energy Storage Systems. https://rosap.ntl.bts.gov/view/dot/38221/dot_38221_DS1.pdf
9. Held, M.; Bronnimann, R. Safe cell, safe battery? Battery fire investigation using FMEA, FTA and practical experiments. Microelectronics Reliability 64, 2016. https://doi.org/10.1016/j.microrel.2016.07.051