非标搬运夹具防误释放与负载落位确认方法研究

——基于负载状态机与多重互锁安全控制的工程实现

夹具安全不仅是"夹得住"，更要确保夹具不能在错误时间松开。

出品单位 **江苏安睿克智能科技有限公司 · 工程研究中心**
文档类别 **企业工程研究白皮书**
版本 **V1.1（优化发布版）**
发布 **2026 年 6 月**

释放状态控制：仅在 S6 执行释放，其余状态封锁释放通道

S0 S1 S2 S3 S4 S5 → ✓ S6 · 允许释放 → S7 · 完成

⚠ S8 · 异常锁定　任意状态检测到异常即转入，禁止释放

发布说明

本文面向非标搬运夹具的工程设计、方案评审与验收验证。文中阈值与示例参数用于说明方法，不构成对所有项目或所有工况的通用性能承诺；实际项目应结合工件、工况、风险评估与验证记录确定。

摘要

在非标自动化搬运系统中，夹具承担工件的抓取、提升、搬运、定位与释放等关键动作。夹具安全不仅取决于"需要夹住时夹得住"，也取决于"尚未满足安全条件时不能松开"。在工件悬空、未落稳、负载尚未转移、操作人员误触按钮、气路或真空状态异常等场景中，非预期释放可能直接导致负载坠落或设备损伤。

本文以非标搬运夹具的释放安全为对象，建立负载状态模型，提出由高度确认、位置确认、支撑接触确认和负载转移确认组成的释放许可逻辑，并将该逻辑与气动互锁、真空保压、断气保护、双按钮释放、长按确认、异常锁定和多传感器融合判断相结合，形成"非允许状态不释放"的工程控制方法。

本文同时给出公式变量说明、不同夹具类型的设计要点、FMEA 风险分析、测试方法、验收项目和工程设计检查表。相关阈值、次数和合格判据均应在项目风险评估和实测验证基础上确定；文中示例用于说明方法，不替代项目级安全评估。

关键词

非标夹具；防误释放；负载落位确认；负载转移；气动互锁；真空保压；断气保护；状态机；FMEA。

1 引言

1.1 研究背景

非标搬运夹具广泛应用于机械加工上下料、汽车零部件搬运、电池模组转运、钣金件搬运和重载物流等场景。与标准夹具相比，非标夹具通常根据工件形状、质量、表面状态、搬运节拍和设备边界条件进行定制，因此其结构形式、传感器配置和控制逻辑差异较大。

在工程实践中，夹具安全常被简化为夹持力、吸附力或磁力是否足够。但释放阶段同样是高风险阶段：如果负载仍处于悬空状态，或虽接触支撑面但尚未完成负载转移，释放动作就可能把"已夹住"的工件转化为"失去支撑"的工件。因此，释放条件的确认应被纳入夹具安全设计的核心范围。

1.2 "夹得住"不等于"安全"

夹具安全包含两个相互独立的命题：第一，需要夹住时必须夹得住；第二，不满足安全释放条件时不能松开。前者属于夹持能力与保持能力问题，后者属于释放许可与状态控制问题。两者任何一项失效，都可能造成负载失控。

核心观点

夹具安全不是"夹得住"就够，还要确保夹具不能在错误时间松开。释放动作应被设计为受状态机、传感确认、安全链和硬件互锁共同约束的安全动作，而不是由单一按钮或单一软件位直接触发的普通动作。

1.3 研究范围与边界

本文讨论的对象为非标搬运夹具的防误释放与负载落位确认方法，重点覆盖机械夹爪、真空吸附、电永磁夹具及其组合形式。本文不替代项目安全评估、设备风险评估、功能安全计算或第三方认证；在具体项目中，应结合工件失效后果、搬运动作、人员可达区域、控制系统架构和相关标准要求进行验证。

2 误释放风险定义与控制目标

2.1 误释放定义

本文将误释放定义为：在未满足安全释放条件时，夹具发生松夹、泄压、破真空、退磁、吹气释放或其他导致保持力下降的动作。误释放与夹持失败不同：夹持失败是"抓不住"，误释放是"在不该松的时候松了"。

防误释放控制目标可概括为三点：不在空中释放、不在未落稳时释放、不在异常状态下释放。为满足该目标，系统需要同时确认负载状态、释放许可、操作意图和安全链状态。

2.2 误释放风险分类

表 2-1　误释放风险分类与主要控制措施

编号	风险类型	典型情形	主要控制措施
R1	空中释放	负载仍悬空，释放阀或松夹机构收到释放请求	状态机封锁、落位/转移确认、气动或电气释放互锁
R2	未落稳释放	负载已接触支撑面，但支撑不足或重量尚未转移	接触力确认、负载转移确认、稳定时间判定
R3	误触释放	单个按钮误按、HMI 误操作或维护误操作	双按钮、长按确认、权限管理、操作日志
R4	断气松夹	气源中断、压力低于阈值导致夹持力下降	常闭/自锁、单向阀、保压阀、储气罐、压力开关
R5	真空失压释放	真空泄漏、吸盘失效、气源中断导致真空度下降	真空罐、真空开关、单向阀、独立回路、失压锁定
R6	传感器误判	高度、位置、接触或负载传感器受污染、漂移、冲击影响	多源融合、2oo3 表决、自诊断、异常锁定

2.3 顶事件逻辑

以"负载意外失去支撑"为顶事件 T，可用下式描述主要致因路径：

$$T = E_{air} \vee E_{unstable} \vee E_{pressure} \vee E_{control}$$

式中，E_{air} 表示空中释放事件，$E_{unstable}$ 表示未落稳释放事件，$E_{pressure}$ 表示气压或真空异常导致的保持力下降事件，$E_{control}$ 表示控制误动作或人为误操作事件。该式为风险分析示意，实际项目应进一步展开至具体部件、信号和操作模式。

由于顶事件通常呈"或门"关系，任一关键失效路径都可能导致危险后果，因此防护不能依赖单一措施。合理的工程方法应采用状态约束、传感确认、硬件互锁和失效保护的组合。

3 负载状态模型

3.1 状态模型的必要性

误释放常发生于控制系统未准确区分负载状态的情况下。若释放阀只响应"按钮按下"或"释放位为真"，而不确认负载是否已落位、是否稳定、是否已完成负载转移，则释放动作可能在任意阶段发生。负载状态模型的作用，是把释放动作约束为"只有在允许释放状态下才能执行"的受控行为。

3.2 状态定义

表 3-1　负载状态定义与释放约束

状态	名称	含义	释放约束
S0	空载	夹具未保持工件	无负载释放动作；仍需防止误动作
S1	夹持确认	夹具已夹紧/吸附/磁保持，尚未提升	禁止释放，除非处于受控取放或维护流程
S2	提升	工件离开取料面并进入提升过程	禁止释放
S3	搬运	工件随夹具移动，处于悬挂或受夹具保持状态	禁止释放
S4	接近落位	工件下降至目标支撑区域附近	禁止释放
S5	负载转移	工件接触支撑面，载荷从夹具向支撑面转移	禁止释放，直至转移完成且稳定
S6	允许释放	落位、支撑、负载转移和安全链条件均满足	唯一常规释放许可状态
S7	释放完成	夹具已解除保持，负载由支撑结构承担	释放动作结束，进入退出或复位流程
S8	异常锁定	检测到失压、真空异常、传感器不一致、急停或逻辑异常	禁止释放；保持或安全处置后受控复位

3.3 状态转移原则

> **State(t+1) = f (State(t), Sensor(t), Logic(t), Safety(t))**

式中，State(t) 为当前状态，Sensor(t) 为传感器信号集合，Logic(t) 为状态机与释放许可逻辑，Safety(t) 为急停、安全门、安全 PLC 或安全继电器等安全链信号。

正常作业可沿 S0→S1→S2→S3→S4→S5→S6→S7 推进。任意状态下，如检测到压力异常、真空异常、传感器矛盾、通信异常、急停或安全链断开，应转入 S8 异常锁定。状态推进应依赖充分的传感证据；证据不足时应停留在当前状态或进入安全侧状态。

4 释放许可逻辑与控制架构

4.1 多条件"与"逻辑

安全释放的基本原则是多条件"与"逻辑：高度、位置、接触、负载转移、操作请求、安全链和无故障状态必须同时满足。任何单一传感器、单一按钮或单一软件变量都不应具备独立触发释放的能力。

4.2 四要素释放许可

$$R = H_s \wedge L_s \wedge P_s \wedge O_s$$

式中，R 为释放许可；H_s 为高度确认；L_s 为水平/姿态位置确认；P_s 为支撑接触确认；O_s 为负载转移确认。四项均为真时，释放许可才成立。

该判据强调"不可替代性"：高度到位不能替代负载转移，位置到位不能替代支撑接触，操作请求不能替代安全确认。

4.3 最终释放命令合成

$$Release = Operator\_Request \wedge R \wedge Safety\_OK \wedge No\_Fault$$

式中，Operator_Request 为经防误操作处理后的释放请求；Safety_OK 为安全链有效状态；No_Fault 表示未处于异常锁定、传感器故障、压力不足、真空不足或维护旁路未授权等状态。

在工程实现中，Release 不应直接驱动释放阀，而应通过安全输出、先导许可或硬件互锁链路间接使能。这样即使上位机或普通 PLC 出现单点逻辑错误，也难以绕过硬件层释放约束。

4.4 双通道与多样性

$$R = R_{sensor} \wedge R_{logic}$$

式中，R_{sensor} 为来自物理传感通道的判定结果，R_{logic} 为状态机和控制逻辑通道的判定结果。两个通道应尽量采用不同原理，降低共因失效风险。

例如，传感器通道可由高度传感器、支撑侧称重模块和压力/真空开关组成；逻辑通道则由状态机、动作顺序、时间窗和安全链状态构成。若两个通道结论不一致，系统应禁止释放并提示诊断。

4.5 软件与硬件职责分离

软件适合完成状态机、信号融合、诊断和记录；硬件互锁适合承担"即使软件误发释放请求也不能释放"的最后防线。建议将释放动作分解为"软件许可、硬件使能、阀件动作、动作反馈确认"四个环节，并分别设置诊断。

5 落位确认与负载转移确认

5.1 高度确认

$$\Delta H = | H - H_{set} | \leqslant E_H$$

式中，H 为实测高度，H_{set} 为设定落位高度，ΔH 为高度偏差，E_H 为高度允许误差。E_H 可根据定位精度、支撑结构和传感器重复性确定，不宜作为通用固定值。

高度确认只能说明负载已接近目标高度，不能单独证明负载已被支撑面承重。

5.2 位置与姿态确认

$$| X - X_0 | \leqslant E_X \quad , \quad | Y - Y_0 | \leqslant E_Y \quad , \quad | \theta - \theta_0 | \leqslant E_\theta$$

式中，X、Y、θ 为实测水平位置和姿态角；X_0、Y_0、θ_0 为目标位置和姿态；E_X、E_Y、E_θ 为允许误差。必要时还应确认 Z 向位置、定位销进入状态或托盘格位状态。

位置确认的目标是确保负载落在有效支撑区域内，避免总重量已经接触但局部悬空、偏载或倾覆风险。

5.3 支撑接触确认

$$F_c \geqslant F_{min}$$

式中，F_c 为接触力或支撑侧检测到的有效接触信号，F_{min} 为最小有效接触阈值。F_{min} 应大于传感器噪声、振动扰动和空载漂移，并通过空载/带载试验确定。

5.4 负载转移确认（核心判据）

落位确认的核心不是"高度够低"，而是"重量是否已经交给支撑结构"。负载转移确认直接对应"松开后不会坠落"的安全目标。

$$W = m\,(g + a_z)$$

$$W = F_g + F_s$$

$$O_s = 1，当\ F_s / W \geqslant \eta\ 且持续时间 \geqslant \tau$$

式中，W 为设计载荷，m 为工件质量，g 为重力加速度，a_z 为落位或搬运需考虑的垂向设计加速度（静态计算时可取 0，存在冲击、快速下降或急停时应计入动态载荷）；F_g 为夹具仍承担的载荷，F_s 为支撑面承担的载荷，随负载落稳 F_s 增大、F_g 减小；O_s 为负载转移确认结果，η 为负载转移比例阈值（常以 0.85～0.95 作为工程起点并经验证确定），τ 为稳定确认时间，用于过滤短时冲击或抖动。

对于多点支撑或长大工件，仅判断总支撑力可能不足，还应检查各支撑点载荷分布和倾覆风险。例如，可增加"任一关键支撑点 $F_{si} \geqslant F_{si,min}$""支撑力矩 $|M_x|$、$|M_y|$ 不超过限值"等条件。

5.5 多源融合与可信度

负载转移可由支撑侧称重模块、夹具侧压力/力传感器、升降轴电流变化、吸盘真空变化或接触开关共同佐证。对关键判定，建议至少包含两类不同物理原理。

$$Vote = 2oo3$$

$$C = \Sigma\,(w_i \cdot S_i)\ ，\ \Sigma\, w_i = 1\ ，\ C \geqslant C_{th}$$

式中，2oo3 表示三取二表决，即三个独立判定信号中至少两个确认有效时才采纳该结论（可容忍一个传感器偶发失效，但不替代传感器诊断和项目风险评估）；S_i 为第 i 个传感器或判定通道的归一化结果，w_i 为权重，C 为综合可信度，C_{th} 为可信度阈值。权重和阈值应通过试验确定，并记录其依据。

5.6 综合落位判据

$$Placement\_OK = Height\_OK \wedge Position\_OK \wedge Contact\_OK \wedge Transfer\_OK$$

该式表明，高度、位置、接触和负载转移必须全部满足。Transfer_OK 是不可被替代的必要条件；若转移证据不足，应拒绝释放，而不是以高度或按钮请求补偿。

6 气动、真空与失效保护设计

6.1 互锁层级

防误释放建议采用机械、电气/安全控制、气动/真空回路三个层级的纵深防御。机械层用于自锁或限位，电气层用于状态判定和安全输出，气动/真空层用于在执行回路中阻断未经许可的释放动作。

6.2 气动释放互锁

$$R \wedge Safety\_OK \wedge No\_Fault \rightarrow Pilot\_Enable \rightarrow Release\_Valve\_Enable$$

> 该逻辑表示：只有完整释放许可、安全链有效且无故障时，释放阀先导或使能回路才可动作。互锁条件不应简化为 Position_OK，因为位置到位不能代表负载已转移。

推荐采用"失电/失气保持夹持或封锁释放"的阀组设计。若普通 PLC 输出与安全输出并存，释放阀的能量通道应由安全输出或安全继电器控制，普通输出仅作为操作请求或动作命令。

6.3 断气保护与保压

断气保护的目标不是允许设备继续正常搬运，而是在气源异常时保持负载处于受控状态，并使系统进入安全停机、受控下降或异常锁定流程。

- ◇ 夹爪宜采用常闭、自锁或机械楔紧结构，使失气、失电时不主动松开。
- ◇ 对夹持腔或真空腔设置单向阀、保压阀或锁紧阀，降低异常泄放速度。
- ◇ 必要时配置储气罐或蓄能单元，但应明确保持时间、最低压力和处置策略。
- ◇ 压力开关应作为独立硬件条件接入释放封锁链；压力低于阈值时禁止释放并报警。
- ◇ 保压能力应通过泄漏、保持时间和最小夹持力试验验证，不能默认阀件存在即可满足安全要求。

6.4 真空保压与真空释放控制

真空夹具应同时考虑两类风险：一是真空不足导致保持力下降，二是在未满足落位条件时执行破真空或吹气释放。真空释放、吹气、排气阀动作应与机械松夹一样纳入 S6 释放许可。

- ◇ 配置真空开关或真空传感器，监测真空度是否达到夹持许可和搬运保持阈值。
- ◇ 采用真空罐、单向阀和分区回路，降低单点泄漏对全部吸盘的影响。

◇ 泄漏检测应覆盖静态保持、搬运加速度、吸盘老化和工件表面变化等工况。

◇ 破真空/吹气释放阀必须由 Release 许可控制，禁止维护或调试状态下无授权旁路。

◇ 真空保持时间、真空下降率和报警阈值应项目化确定；如采用"30 s 内下降率不超过 10%"等指标，应有测试记录支持。

6.5 异常锁定与复位

异常锁定 S8 应同时包含动作封锁、报警提示、状态记录和受控复位。复位不应直接恢复释放能力，而应重新完成状态确认、压力/真空确认、传感器一致性确认和操作权限确认。

7 不同夹具类型的防误释放方法

7.1 机械夹爪夹具

机械夹爪主要依靠形状配合、夹紧力和摩擦力保持工件。对于依赖摩擦保持的垂直搬运工况，可按下式进行夹持力校核：

$$n \cdot \mu \cdot F_N \geqslant K \cdot m(g + a_z)$$

式中，n 为有效摩擦接触面数量，μ 为最不利工况摩擦系数，F_N 为单个接触面的法向夹紧力，K 为安全系数，m、g、a_z 含义同前。若存在水平加速度、偏载或冲击，还应单独校核防滑和倾覆。

防误释放要点包括：常闭/自锁结构、夹紧到位与开度反馈、夹持压力监测、断气保持、释放阀互锁、异常状态禁止松夹。对形状配合夹具，应确认插入深度、定位销到位和锁止件到位，而不仅是气缸已到位。

7.2 真空吸附夹具

$$F_{vac} = \Delta P \cdot A_{eff} \cdot \lambda$$

$$S = F_{available} / F_{required} \geqslant S_{min}$$

式中，F_{vac} 为可用吸附力，ΔP 为真空压差，A_{eff} 为有效吸附面积，λ 为考虑吸盘压缩、表面粗糙度、泄漏和姿态影响后的修正系数；S 为吸附安全裕度，$F_{available}$ 为最不利真空度和有效面积下的可用吸附力，$F_{required}$ 为考虑工件重量、加速度、姿态和扰动后的需求力，S_{min} 由项目风险评估确定。

防误释放要点包括：真空达到阈值才允许提升，搬运中实时监测真空度，真空不足进入保持/报警/安全处置流程，破真空释放仅在 S6 允许释放状态执行。多吸盘系统应评估单吸盘、单支路或单真空源失效后的剩余保持能力。

7.3 磁力夹具（电永磁）

电永磁夹具通电完成充磁或退磁动作，断电后通常可保持磁力，适用于可被磁化材料的搬运。其安全关注点不只是断电释放，还包括贴合不良、气隙变化、材料差异、剩磁误判和退磁动作误触发。

$$F_{mag} \geqslant K \cdot m(g + a_z)$$

式中，F_{mag} 为在最不利气隙、材料和贴合条件下的有效磁保持力。磁力参数应通过样件测试或供应商有效数据确认，不能只采用理想吸力值。

防误释放要点包括：充磁完成反馈、吸力或贴合状态确认、退磁动作纳入释放许可、维护退磁权限管理、异常断电后的负载处置流程。

7.4 不同夹具类型对比

表 7-1　各类夹具保持原理、失效模式与防误释放重点

夹具类型	主要保持原理	主要失效模式	防误释放重点
机械夹爪	夹紧力、摩擦、形状配合	断气松夹、夹紧不足、滑移、锁止不到位	常闭/自锁、压力监测、开度反馈、释放阀互锁
真空吸附	吸盘内外压差	泄漏、吸盘老化、破真空误动作、表面不良	真空监测、真空罐、单向阀、分区回路、破真空许可
电永磁	磁路保持力	贴合不良、材料差异、退磁误触发、剩磁误判	充/退磁状态约束、吸力确认、退磁权限管理
组合夹具	多保持原理叠加	单一保持方式失效、逻辑切换错误	明确主/辅保持关系，切换时维持至少一种有效保持

8 人机工程与误操作防护

人机工程措施用于降低人为误触和误操作概率，但不应替代状态机、传感确认和硬件互锁。即便操作员发出释放请求，只要释放许可不成立，系统仍应拒绝释放。

8.1 双按钮与长按确认

$$Button\_OK = B_1 \wedge B_2 \wedge (|t_{B1} - t_{B2}| \leqslant T_{sync}) \wedge (T_{press} \geqslant T_{hold})$$

式中，B_1、B_2 为两个独立按钮信号，T_{sync} 为同步窗口，T_{press} 为持续按压时间，T_{hold} 为长按阈值。T_{sync} 和 T_{hold} 应结合操作节拍、人机工效和风险评估确定。

双按钮和长按可降低单点误触概率，但若需要达到安全等级要求，应选用相应安全等级的输入器件和安全控制架构，而不是仅在普通 PLC 中编写逻辑。

8.2 HMI 二次确认与状态指示

HMI 可用于显示"禁止释放、接近落位、负载转移中、允许释放、异常锁定"等状态，并在关键工位提供二次确认。HMI 确认的作用是增强操作可见性和可追溯性，不能绕过 R、Safety_OK 和 No_Fault。

8.3 维护模式与权限管理

维护释放、手动破真空、手动退磁等旁路操作应通过权限、钥匙开关、低速/点动、区域清空和操作日志进行约束。维护模式下的释放仍应尽可能保留负载支撑确认或人工工装支撑确认，避免"维护旁路"成为新的误释放路径。

9 FMEA 风险分析

下表为非标搬运夹具防误释放的 FMEA 示例。评分仅用于说明方法，项目实施时应根据工件质量、人员暴露、节拍、历史故障、诊断覆盖率和实际试验数据重新评定。

表 9-1　防误释放失效模式与影响分析（示例）

失效模式	主要原因	后果	示例 S/O/D/RPN	控制措施	验证要点
空中释放	状态机错误、释放阀误动作、旁路未受控	负载坠落、设备损伤、人员风险	10/3/4/**120**	S1～S5 封锁释放；释放阀安全互锁；S6 唯一许可	在悬空状态注入释放请求，确认阀不动作且记录报警
未落稳释放	高度到位但支撑不足；偏载；转移未完成	倾倒、滑落、夹具或工件损坏	9/4/4/**144**	接触确认、负载转移确认、稳定时间、偏载监测	制造边界落位、偏载和部分支撑工况，确认危险侧不许可
断气松夹	主气源中断、管路泄漏、阀件泄放	保持力下降、负载失控	10/2/5/100	常闭/自锁、单向阀、保压阀、压力开关、储气罐	切断气源并测量保持时间、最低压力和夹持力
真空失压	吸盘泄漏、真空源异常、表面污染	吸附力下降、负载掉落	10/3/4/**120**	真空罐、单向阀、真空监测、分区回路、失压锁定	模拟不同泄漏率，验证报警、保持和释放封锁
误触释放	单按钮误碰、HMI 误点、维护误操作	非预期释放请求进入系统	8/5/3/**120**	双按钮、长按、二次确认、权限管理	单按钮、短按、非授权操作均不得触发 Release
传感器误判	污染、漂移、线缆故障、反光或振动	错误认为已落位或已转移	8/4/4/**128**	多源融合、2oo3、自诊断、信号一致性检查	断开/短接/漂移注入，确认进入禁止释放或异常锁定
软件或通信异常	程序缺陷、通信延迟、变量错写	释放许可错误或状态错乱	10/2/5/100	安全 PLC、看门狗、双通道许可、版本管理	通信中断、看门狗超时和版本回归测试

对 RPN 较高或严重度为 9～10 的项目，应优先落实硬件互锁和试验验证。即使 RPN 经措施降低，严重度较高的失效仍应保留周期性验证和维护检查。

10 测试方法与验收项目

10.1 验证原则

验证应围绕"不误释放、不危险侧误判、异常可诊断"展开。建议采用边界工况、故障注入、重复性试验和记录追溯相结合的方式。所有"100% 抑制""零误释放""十万次无故障"等表述，只有在存在完整测试报告、样本定义和统计口径时才可作为项目结果发布。

10.2 功能与互锁测试矩阵

表 10-1　功能与互锁测试矩阵

测试类别	测试方法	期望结果	验收记录
状态封锁	在 S1～S5 逐一发送释放请求	Release 不成立，释放阀不动作，系统给出禁止原因	记录状态、请求、阀输出、报警信息
允许释放	在 S6 条件全部满足时发送释放请求	释放动作按顺序执行，释放完成后进入 S7	记录 H_S/L_S/P_S/O_S、安全链、动作反馈
气动互锁	断开先导许可或安全输出后发送普通释放命令	释放阀无动作，气路保持封锁	记录先导压力或阀位反馈
安全链	触发急停、安全门或安全继电器断开	立即禁止释放；必要时保持夹持或执行安全处置	记录安全链输入和状态机转移
异常复位	制造传感器矛盾或压力不足后复位	复位需重新满足诊断和许可条件，不得直接释放	记录故障码、复位人和复位条件

10.3 落位与负载转移测试

表 10-2　落位与负载转移测试

项目	测试方法	合格判据建议
高度确认	在目标高度、边界高度和超差高度分别测试	高度在阈值内才允许 Height_OK；超差时拒绝
位置确认	设置 X/Y/姿态偏差、定位销未进入、托盘偏移等工况	偏差超限或定位不到位时 Position_OK 为假
接触确认	设置有接触、轻微接触、无接触和传感器噪声工况	接触力低于 F_{min} 或信号不可信时拒绝释放
负载转移	使用称重、夹具侧力或电流趋势测量转移比例	F_s/W 达到 η 且持续 τ 后才置 Transfer_OK
偏载/多点支撑	制造单点悬空、单侧承载过高或支撑点异常	总支撑力满足但偏载超限时仍拒绝释放
危险侧误判	对所有应拒绝工况统计误许可次数	危险侧误许可应为 0；保守拒绝应记录并优化

10.4 断气、失压与保持测试

表 10-3　断气、失压与保持测试

项目	测试方法	记录内容	验收关注点
断气保持	在额定负载下切断气源	压力曲线、夹持力、保持时间、状态转移	保持时间满足安全处置需要；不发生松夹
缓慢泄漏	人为设置小泄漏并持续监测	压力/真空下降率、报警时间、锁定时间	报警阈值合理，趋势可诊断
快速失压	断开主气源或真空源	阀位、压力、负载状态、报警	系统进入保持/锁定，不允许释放
恢复气源	异常后恢复气源并尝试操作	是否需要复位、是否重新确认状态	恢复不应自动释放或自动清故障

10.5 人机误操作测试

表 10-4　人机误操作测试

测试项	测试方法	期望结果
单按钮	仅按 B_1 或 B_2	Release 不成立
不同步按下	两个按钮超过 T_{sync} 按下	Release 不成立
短按	持续时间小于 T_{hold}	Release 不成立
无权限维护释放	非授权用户执行手动释放或破真空	拒绝操作并记录
允许释放提示	S6 时操作员执行释放	状态指示清晰，动作顺序正确

10.6 资料与验收输出

◇ 风险评估与 FMEA 记录；

◇ 夹持力、吸附力或磁保持力计算书；

◇ 释放许可逻辑图、状态机图和安全 I/O 清单；

◇ 气动/真空/电气原理图及互锁说明；

◇ 测试记录表、故障注入记录、异常复位记录；

◇ 维护检查项、保压/泄漏周期性验证计划；

◇ 操作说明与维护模式权限说明。

11 工程设计检查表

表 11-1　非标搬运夹具防误释放工程设计检查表

类别	检查项	验收判据
夹持能力	夹持/吸附/磁力计算	采用最不利工况参数，安全系数与依据明确
夹持能力	动态载荷考虑	考虑提升、下降、急停、摆动或冲击导致的附加载荷
落位确认	高度与位置确认	阈值依据清楚，边界测试通过
落位确认	支撑接触确认	接触信号大于噪声与漂移，失效可诊断
负载转移	转移比例确认	F_S/W 达到项目阈值 η 并保持 τ；多点支撑偏载受控
释放逻辑	四要素许可	$R = H_S \wedge L_S \wedge P_S \wedge O_S$，不允许单点替代
释放逻辑	最终命令合成	Operator_Request、R、Safety_OK、No_Fault 同时成立
气动互锁	先导许可	释放阀由完整许可链使能，失电/失气导向禁止释放
断气保护	保压与保持	切断气源后保持时间满足安全处置要求，有测试记录
真空系统	真空监测与防泄放	真空开关/传感器、真空罐、单向阀和泄漏测试齐全
人机工程	双按钮/长按/权限	单点误触、短按、非授权操作均不能触发释放
异常处理	异常锁定与复位	S8 锁定、故障码、受控复位和操作记录完整
验证资料	测试与追溯	测试方法、样本量、合格判据、原始记录和问题闭环齐全

12 工程结论

非标搬运夹具的安全设计应同时覆盖"夹得住"和"不能在错误时间松开"两个命题。前者是保持能力问题，后者是释放许可和状态安全问题。

释放动作应由负载状态机约束，仅在 S6 允许释放状态执行。S1～S5 和 S8 等状态应在软件与硬件层同时封锁释放通道。

落位确认不应只依赖高度或位置。高度、位置、支撑接触和负载转移必须共同成立，其中负载转移确认最接近"释放后不坠落"的安全本质。

气动互锁、真空保压、断气保持、压力/真空监测、双按钮、长按确认和异常锁定不是重复配置，而是覆盖不同失效路径的纵深防御。

文中涉及的阈值、同步窗口、保持时间、转移比例和安全系数应通过项目级风险评估、样件试验和验收记录确定。未经验证的数据不宜作为官网资料中的通用结论。

将夹具控制从单纯"动作控制"升级为"状态安全控制"，有助于降低空中释放、未落稳释放、失压释放和人为误操作引起的风险，为非标搬运夹具的工程设计、方案评审和验收提供可执行框架。

出品单位：江苏安睿克智能科技有限公司 · 工程研究中心。本文为企业工程研究资料，用于方法说明与工程交流，不替代具体项目的安全评估、试验验证或认证要求。