机械自动化系统中的人机协作安全控制技术研究

张琦

西安永瑞杰能源科技有限公司，陕西省西安市，710000；

摘要：聚焦机械自动化系统中的人机协作场景，构建兼顾可解释与可实施的安全控制框架。方法以风险机理、感知评估、控制约束与组织治理四条主线展开，在系统层定义边界与角色，在控制层固化互锁与限幅，在感知层强化近场识别与姿态判断，在运行层引入动态授权与行为约束。围绕触达距离、速度能量与注意负荷等关键变量，提出可度量的阈值与留量设置方法，并给出面向异常的分级处置流程。通过模型与数据的双向校准，实现从设计到运维的闭环验证，在不牺牲节拍的前提下降低暴露风险与误停代价。在多工位协同时引入分级权限与错峰策略，以温和的节拍调度减少争用与拥塞，让安全与效率在同一度量体系内共同优化。

关键词：人机协作；安全控制；机械自动化；风险评估；功能安全

DOI：10.69979/3060-8767.25.05.058

引言

人机协作将人的感知判断与设备的稳定执行结合在一起，能在复杂、定制与小批量任务中提升柔性与效率。协作并非简单并置，而是共享空间与时间的组织方式，触发新的危险源与连锁影响，包括近距相对运动、意图分歧、界面误导与注意耗竭。若缺乏成体系的安全控制，要么以过度保护换来频繁停机，要么在追求产能时扩大暴露风险。为在安全与效率之间找到稳定解，需要把风险机理、感知能力与控制策略统一到同一口径，以场景为单位给出阈值、留量与处置规则，并以验证与记录支撑长期收敛。协作安全并非只依赖单一技术，还依赖可执行的组织与文化，需要对培训、演练与记录形成稳定机制。有效的系统应在规则、工具与行为三方面同时落地，把抽象原则转化为岗位动作，并以度量与复盘促进持续改进。

1 协作场景与安全风险机理

1.1 协作模式与危险源刻画

协作模式可按空间重叠程度、任务耦合强度与角色主导权划分。空间重叠体现人员与设备在同域行动的比例，任务耦合体现传感与执行之间的依赖链条，主导权体现指令与节拍的发起侧[1]。不同组合映射出不同危险源，高重叠配合高耦合容易形成意外接触与力能聚集，低重叠但频繁交接易出现误解读与路径冲突。危险源并非孤立，会通过注意转移与节拍波动形成放大效应，例如人员在等待中注意力下降导致迟缓回避，又进一步拉长设备减速路径。刻画危险源需要把相对速度、相对距离、可见度与力量阈值纳入统一变量，以便在设计与运行阶段被一致地调用与验证。

为了避免经验化与口号化，可基于场景单元建立事件图谱，以进入、靠近、交互、离开等关键时刻组织证据。每一时刻记录主体位置、姿态、速度与意图，并把界面提示与信号反馈作为可观测量。在此基础上定义可达域与禁入域，在可达域内分级设置留量，把安全边界转化为可执行的几何与时序条件。对存在携带工具与夹具的场景，把额外质量与突出部分纳入边界估算，防止误判人员包络。事件图谱还能支撑回放与复盘，帮助团队追踪从轻微异常到接触事故的变化路径，从而修正阈值与交互信息。协作强度还受环境与组织因素调制，照明、噪声与地面状态会改变感知与制动性能，排班与培训会改变注意曲线与沟通效率。将这些因素映射为权重，在风险计算中形成加权系数，即可把环境变化转化为阈值的动态偏移，避免一刀切的静态设定。由此可在多班组与多班次条件下维持一致的安全体验。最终把危险源映射为结构留边、速度曲线与界面提示的组合，在设计评审与现场验收中使用同一口径完成确认与复核。

1.2 风险传播路径与度量方法

风险在协作过程中的传播常见三类路径，从物理量出发的直接路径，从信息不对称出发的间接路径，从组织规则缺陷出发的隐性路径。直接路径来源于速度、能量与接触几何，间接路径来源于意图误解与界面误导，隐性路径来源于职责划分模糊与交接程序缺失[2]。为把三类路径纳入统一框架，可以事件为节点以因果为连边，通过影响强度与触达时间两个指标形成可计算的网络。

网络的关键边对应高敏感环节，一旦出现波动就会迅速传导到接触风险。治理思路是在关键边上增设缓冲，在弱边上提升可观测度，并在节点处设置复核与确认，将错误阻断在低成本位置。

度量方法应服务于决策与执行，不仅给出分数还要映射到动作。可将风险分解为概率、暴露与后果三项，分别由任务频度、空间重叠与能量限幅给出量化。概率来自负载与节拍，暴露来自可达域与可视线，后果来自质量与速度的组合。在此基础上定义阈值与留量并绑定处置规则，达到阈值即减速或进入安全模式，持续超限则触发停机与复位。度量结果与调试记录一并沉淀，在版本迭代中修正权重，让系统逐步接近稳定区域。为了兼顾效率，计算应尽量依托在线可得的信号，如位置、速度与界面交互日志，用增量更新替代全量重算。当出现黑天鹅事件时，先以高置信度的简约模型给出安全动作，再在复盘环节用更精细的模型复现细节，防止复杂工具在关键时刻拖慢响应。环境扰动与个体差异会改变风险网络的拓扑，应通过标签与分层管理维护多个场景版本，在切换班次与工艺时同步切换。多版本管理不追求繁多，而是以覆盖常见边界为目标，每个版本限定适用范围与复核要点，确保切换过程清晰可控。风险图谱对应到工程接口与操作步骤，每一条边都能找到责任人与数据来源，一旦触发即可快速对齐证据与处置。

2 安全控制架构与关键技术

2.1 安全感知体系与评估闭环

安全感知的核心在于稳定识别人的存在与意图，并在靠近与交互的关键时刻保持高置信度。感知链路以多模融合提高稳健性，把距离、姿态、速度与视线方向融合为统一表述，同时暴露估计的置信区间，让控制策略能够按置信度分配动作强度[3]。为了抑制误报与漏报，在模型之外配置简单而可靠的物理边界，例如固定障碍与软限制，把极端场景交由硬约束兜底。感知输出不直接等于动作，还需通过评估层完成场景解释，例如判断人员是路过还是参与协作，判断举手是求助还是正常手势。

评估闭环通过先验模板与在线证据共同驱动，既利用长期积累的常见模式，也接受现场数据的差异。证据不足时采取保守动作并记录为待确认事件，在事后复核时更新模板与阈值。评估层须暴露可读的中间量，例如相对轨迹与行动意图，便于值守与工程人员理解与优化。为降低系统负担，把高频小动作在边缘侧处理，把低频大决策交由中心侧处理，两侧以节拍与留量协商，确保响应不失序也不迟缓。长期运行中，感知与评估会受到光照、粉尘与遮挡的影响，需要周期校准与快速自检。可在换班或停线时执行短程标定与回放，用对照片段校核阈值与融合权重，把漂移控制在可管理范围。在群组场景，以集中管理的方式下发感知策略与阈值，结合本地统计进行微调，既保证口径一致又兼顾差异。所有变更都绑定版本与时间，一旦出现异常可迅速回滚到稳定档，减少反复试探带来的额外风险与停机损失。这样即可在不同工位与不同班次维持一致的安全体验与响应边界。感知与评估的输出采用分级标签与短语说明，让不同岗位在同一画面获得可执行的信息与明确的下一步动作。

2.2 控制逻辑与执行链的安全约束与容错

控制逻辑承担把风险度量映射为动作的职责，需要在速度、力矩与路径等维度设置硬约束与软约束。硬约束不可破例，用于防止灾难性后果，软约束用于平衡节拍与舒适度，允许在留量内动态调整。执行链包含驱动、制动与传动等环节，每一环节都要暴露健康度与响应时延，让上层在决策时掌握真实边界。当健康度下降或时延上升，控制逻辑应自动收紧速度与距离，并提示维修安排与风险级别。

容错机制以分层思路构建，边缘层负责快速介入，系统层负责状态重置与协同恢复。当感知置信度骤降或执行时延超限，边缘层直接降速或停机，系统层完成路径重规划与互锁复位，并在恢复后以渐进方式回到正常节拍。为减少误停，可引入短时确认窗口，在不降低防护强度的前提下过滤抖动。对反复触发的告警，自动进入根因定位流程，从传感、通信与执行三条链路逐一排查，把软错误与硬故障区分开来。为保障一致性，控制参数与阈值在上线前必须经过虚拟环境的覆盖性验证，把典型工况与极端场景都走一遍。上线后依据运行档案滚动更新，每次变更先影子运行再灰度发布，在有限范围内确认收益与风险后再全面推广。执行链的维护以健康度趋势为依据，用温度、振动与电流等信号估计退化速度，在合适窗口实施维护，避免在高负载时被动停机。界面与提示也是控制的一部分，提示语需简洁可执行，把动作与理由同时呈现，减少沟通误差与反复确认，并在事后复盘时提供清晰证据。对多设备协同的工位，在互锁之上增设仲裁与优先级，避免同时争用同一空间或资源，把队列与让步转化为显式规则。当设备构型变化或工艺

升级时，控制逻辑沿用原有模板并以标签描述差异，减少从零开始的代价并保证规则可追溯。

3 运行组织与协同优化

3.1 人机协作过程的动态授权与交互设计

动态授权把权限与风险水平绑定，在低风险阶段授予更高自由度，在高风险阶段收紧控制。授权对象不仅包含设备，还包含人员与团队，例如允许经过训练的人员临时接管近场操作，同时把速度与力限制在更严格范围。授权过程需要明确入口、持续与退出三个环节，入口阶段校验身份与意图，持续阶段监控行为与边界，退出阶段恢复默认状态并记录轨迹。若在持续阶段出现偏离，系统立即收回权限并引导进入安全姿态，避免在含糊状态停留。

交互设计以清晰与连贯为目标，把状态、边界与意图通过多通道呈现，包括视觉、听觉与触觉反馈。界面不堆砌信息，而是围绕关键变量组织，用趋势与阈值带引导关注，让操作者在短时间内做出一致判断。对需要协同的动作，在界面上标注接力点与接触点，避免人员与设备对同一物体采取相反操作。对新手模式与专家模式给出分档，在早期以更强引导降低学习成本，在成熟期以更大自由度释放效率。为了降低长时任务中的注意流失，引入节拍与提示的节律化设计，把重复动作与确认操作编排成顺畅流程。重要提示的颜色与音调固定且稀缺，避免过度提醒导致麻木。针对多语言与多文化团队，界面符号与手势采用通用图形与短句，减少语义差异，并提供演练场景让团队在无风险环境熟悉协作节奏。交互日志与决策路径自动归档，在复盘时与风险事件对齐，找出误解读与误操作的高发位置，据此优化图标与提示。当工艺发生变化时，以可视化清单提示差异点与新增风险，保证团队在同一认知上开展协作。对高压力与高节拍的岗位，引入节奏化休整与轮换，配合界面提示的强弱变换，延缓疲劳积累并降低误操作概率。

3.2 全生命周期的安全管理与持续改进机制

全生命周期管理把设计、建设、调试、运行与退役置于同一链条，用一致的口径组织数据与责任。在设计阶段定义场景清单与边界参数，在建设阶段核对接口与互锁，在调试阶段验证阈值与留量，在运行阶段滚动修订与归档，在退役阶段回收经验与资产。每一阶段都有明确输入与输出，通过交接包的方式把事实移交给下一阶段，减少口口相传导致的信息损失。群组化部署时共享模板与基线，把差异以标签表达，既维持一致性又允许合理变通。

持续改进依赖指标与案例，指标提供趋势与优先级，案例提供语境与细节。指标体系覆盖风险水平、误停比例、产能与人因负荷，案例库记录成功与失败的关键片段，二者共同推动规则与阈值更新。改进要遵循小步与可回退原则，在虚拟环境先验证，再在小范围影子运行，确认收益后再推广。当制度与技术出现冲突时，以风险最小化为原则做出取舍，并在组织层面定期复盘，让改进不被短期压力带偏。为确保知识可传承，将图纸、参数与运行曲线统一存放与检索，以标准化字段与可视化看板呈现事实，新成员能在短时间复现上下文。在供应链侧建立共同语言与一致验收，外部部件进入系统前完成兼容性与安全性核验，减少集成阶段的反复。面对环境与业务的不确定性，建立应急演练与红蓝对抗，以模拟异常挑战规则与边界。演练结果转化为可执行任务单并纳入周期计划，让改进成为惯性而非突发活动。通过这一闭环，系统能在长期内维持稳定的安全水平与可预期的产能，同时把新风险纳入早期识别与快速响应。通过跨岗位的共创与评审，把经验性表达沉淀为可执行条目与可测量指标，让改进从个体技能升级为组织能力。

4 结语

研究围绕人机协作的风险机理、感知评估、控制约束与组织治理构建了可落地的方法。通过场景化建模与阈值留量设计，把抽象原则转化为可执行规则，以虚实结合的验证与档案沉淀支撑长期收敛。实施路径强调小步迭代与可回退，在不放松底线的前提下释放效率潜力，为机械自动化系统提供可复制的安全控制范式。未来可继续把人因负荷与认知状态纳入在线评估，强化群组协同与跨场景迁移，让安全与产能在多变量约束下取得更稳定的平衡。

参考文献

[1]郝智.制造业机械自动化生产中机器人协作应用与效率优化研究[J].时代汽车,2025,(10):16-18.
[2]牙韩情.现代机械自动化技术应用与发展前景[J].河北农机,2025,(05):67-69.DOI:10.15989/j.cnki.hbnjzzs.2025.05.048.
[3]睢雪亮,马兆宾.机械自动化技术在机械制造业中的应用[J].造纸装备及材料,2023,52(10):73-75.