基于物联网的智能安全设计理论与方法研究

杨 帆[1]，王军强[1]，张 磊[1]，薛虎林[1]，任卫华[2]，米 超[2]，鲁 斌[2]

[1]陕西新能选煤技术有限公司 陕西西安
[2]山西汇永青峰选煤工程技术有限公司 山西朔州

【摘要】围绕选煤厂供配电系统接入工业物联网后安全边界扩大、信息侧异常可能传导至物理执行端的问题，结合智能安全供配电工程实践，对物联网条件下的安全设计对象与实施方法进行了重新梳理。研究把人员、设备、环境、管理以及网络/数据纳入同一风险链，以本质安全、纵深防御、失效安全、过程可追溯和故障恢复为约束，形成从危险场景识别、需求分解、多源感知、可信判断到安全联锁、物理隔离和运行复核的设计流程。工程系统采用规则判断与随机森林复验相结合的方式，并通过软闭锁、硬联锁和物理隔离限制高风险操作。现场应用中，身份识别精度达到 100%，巡检机器人识别精度不低于 96%，系统无故障运行时间不低于 99.9%，停送电操作耗时缩短 40%以上；非计划停电识别准确率为 92.5%，平均响应时间不超过 4.2min，次生故障率下降 70%。结果显示，物联网智能安全设计的关键并非增加监测设备数量，而是使风险识别、数据校验、决策、执行和恢复形成可验证的闭环。相关思路可为能源与矿山工业智能化系统的安全设计及工程验收提供参考。

【关键词】工业物联网；智能安全设计；本质安全；风险分级；安全联锁；韧性恢复；选煤厂
【收稿日期】2026 年 3 月 5 日 【出刊日期】2026 年 9 月 1 日 【DOI】10.12208/j.sdr.20260069

Theory and method of intelligent safety design based on the Internet Of Things

Fan Yang[1], Junqiang Wang[1], Lei Zhang[1], Hulin Xue[1], Weihua Ren[2], Chao Mi[2], Bin Lu[2]

[1]Shaanxi Xinneng Coal Preparation Technology Co., Ltd., Xi'an, Shaanxi
[2]Shanxi Huiyong Qingfeng Coal Preparation Engineering Technology Co., Ltd., Shuozhou, Shanxi

【**Abstract**】To address the limitations of conventional safety design when industrial Internet of Things (IIoT) extends safety objects from individual equipment to a coupled human-machine-environment-management-network/data system, a five-domain collaborative theory and a lifecycle design method are proposed based on an intelligent safe power-distribution project in a coal preparation plant. Inherent safety, defense in depth, fail-safe behavior, traceability and resilience are taken as fundamental principles. A design chain of hazard identification, safety-requirement mapping, multi-source sensing, trusted decision-making, safety interlocking, physical isolation, recovery validation and iterative optimization is established. Hierarchical decision-making combining rule engines and machine learning, coordination of software blocking and hardware interlocking, and a dual closed loop between the information and physical domains are introduced. Evaluation dimensions include sensing integrity, diagnostic accuracy, control reliability, response timeliness, environmental adaptability, traceability and system resilience. Engineering results show 100% identity-recognition accuracy, robot-recognition accuracy not lower than 96%, system availability not lower than 99.9%, and more than 40% reduction in power-switching operation time. The accuracy of unplanned-outage identification reached 92.5%, the average response time was within 4.2 min, and secondary faults decreased by 70%. The results indicate that IIoT-based intelligent safety design should shift from adding monitoring devices to integrated risk-data-decision-control-recovery design, with authorization, interlocking, physical isolation and fail-safe degradation implemented together with network connectivity.

第一作者简介：杨帆（1993-）男，本科，助理工程师，研究方向：煤炭洗选。

【**Keywords**】Industrial Internet of Things; Intelligent safety design; Inherent safety; Risk grading; Safety interlock; Resilience; Coal preparation plant

引言

工业物联网通过传感器、通信网络、边缘计算与控制系统的深度互联，将工业现场从封闭的机电系统转化为信息空间与物理空间双向耦合的工业信息物理系统。其优势是实现设备状态实时感知、远程控制、预测维护与资源优化，但同时改变了传统安全设计的边界：安全问题不再只来源于机械、电气或作业行为，还可能由数据错误、通信中断、权限越界、算法误判以及信息域故障向物理域传播所触发[1-3]。

矿山和能源工业具有设备连续运行、环境复杂、高危操作多和安全联锁要求严格等特征，是工业物联网安全设计的典型场景。相关研究已从矿山 IIoT 参考架构、人员安全监测扩展到矿山信息物理系统韧性与安全—网络安全联合风险分析[2-5]。这些研究说明，智能化程度提升并不会自动带来安全水平同步提高，只有在系统架构和控制逻辑中预先嵌入安全约束，才能避免连接性和自主性增强形成新的风险耦合。

用户提供的项目研究报告和总结报告以选煤厂低压供配电系统为对象，融合物联网、PLC(Programmable Logic Controller)控制、身份识别和机器人巡检，实现配电状态监测、远程停送电、抽屉柜自动物理隔离、故障预警与无人巡检。工程实践形成了较完整的感知、决策、联锁、执行和反馈链条，为提炼智能安全设计的一般方法提供了案例基础。

本文不将项目中已有的“智能安全评估体系”简单改写，而是从安全设计前移的角度，重点回答 3 个问题：物联网条件下安全设计对象如何重新定义；如何把风险识别转化为可执行的感知、决策、联锁与隔离要求；如何通过验证和运行反馈保证安全功能在全生命周期持续有效。在此基础上构建五域协同理论模型和方法流程，并以智能供配电系统进行工程验证。

1 物联网智能安全设计理论基础

1.1 智能安全设计的内涵

传统安全设计通常以危险源识别、结构防护、安全联锁和操作规程为核心，其基本逻辑是控制物理系统失效及人员误操作。工业物联网加入后，安全控制链增加了传感、通信、数据、模型和远程指令等环节，安全系统本身具有更强的动态性和软件依赖。因此，本文将物联网智能安全设计定义为：面向信息—物理耦合工业系统，在全生命周期内把危险场景转化为可感知、可判定、可约束、可隔离、可恢复的技术与管理要求，并利用运行数据持续验证和优化安全功能的系统化设计活动。

该定义强调 3 点。第一，智能安全设计的核心仍是安全，而不是算法复杂度；第二，安全功能必须覆盖从风险识别到物理执行的完整链路；第三，系统上线不是设计终点，现场数据、故障和变更应反向驱动阈值、规则和模型更新。

1.2 “人—机—环—管—网/数”五域协同模型

项目资料提出面向供配电安全构建“人—机—环—管”全维度体系。结合工业物联网的信息物理特征，本文在此基础上增加“网/数”域，形成五域协同对象模型。人域包括身份、资质、权限与操作行为；机域包括设备状态、执行机构、联锁和物理隔离；环境域包括温度、湿度、粉尘及其他影响设备可靠性的条件；管理域包括工作票、操作票、挂牌、审批和应急流程；网/数域包括通信、数据完整性、访问控制、模型和日志。

五个域并非相互独立。例如越权远程送电同时涉及人域权限、管理域流程、网/数域认证、机域联锁和现场环境状态；设备温升异常则需要环境与设备传感、数据可信传输、算法识别和维护流程共同处置。智能安全设计的对象因此应从单个设备转变为跨域风险链，五域协同理论模型如图 1 所示。

1.3 基本设计原则

基于项目实践和工业信息物理系统安全研究[4-6]，本文归纳 5 项基本原则：①本质安全优先，即优先通过物理隔离、结构防护和减少人员暴露消除风险，而非依赖报警后处置；②纵深防御，即身份、流程、软件闭锁、硬件联锁和物理隔离形成多层防线；③失效安全，即通信、模型或平台异常时系统进入预定义安全状态，不因智能功能失效破坏原有保护；④全程可追溯，即操作、报警、授权和恢复全过程记录；⑤韧性恢复，即系统不仅能识别故障，还应具备隔离、人工接管、恢复和经验学习能力，各域典型风险与设计要求见表 1。

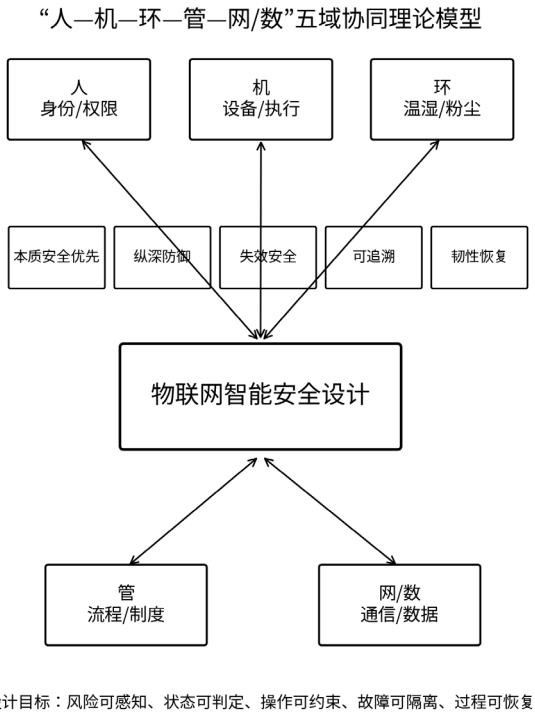


图 1　“人—机—环—管—网/数”五域协同理论模型

表 1　五域安全对象、典型风险及设计要求

安全域	典型对象	主要风险	设计要求
人	运行与检修人员	越权访问、误操作、身份冒用	多因素认证、按角色授权、操作留痕
机	配电柜、断路器及执行机构	拒动、误动、位置状态不确定	独立状态反馈、硬联锁、物理隔离、故障安全
环	温度、湿度、粉尘等环境条件	过热、积尘、绝缘下降或机构失效	环境监测、防尘散热、越限联动
管	两票、挂牌、审批及检修流程	流程被绕过、信息不同步	流程约束、电子挂牌、责任可追溯
网/数	网络、数据库、模型与日志	通信中断、数据失真或篡改、模型误判	通信冗余、数据校验、访问控制、降级运行

2 基于物联网的智能安全设计方法

2.1 危险场景识别与风险分级

安全设计不宜从设备清单直接展开，而应先还原具体作业过程，把可能发生的危险事件、触发条件、现场能够观测到的变量、需要执行的安全动作以及恢复条件逐项对应。以非计划停电为例，短路、电缆异常、设备故障或未经授权的操作均可能成为触发因素；电压、电流、断路器状态、抽屉位置、温度和操作记录则可作为识别依据。发现异常后，系统需要根据场景进入报警、故障定位、回路隔离或人工复核等处置环节。

对后果和处置要求差异较大的事件，还需要进行风险分级。项目中以影响范围 A、设备重要性 B 和环境风险 C 作为评分因素，非计划停电场景采用：

$$L = 0.3A + 0.4B + 0.3C$$

式中 L 表示该场景的风险等级得分。0.3、0.4、0.3 的权重取值来自本项目的现场设定，不能直接视为其他工业系统的固定参数。实际应用时，应结合事故后果、人员暴露频率、设备关键程度和现场环境重新校准。分级的用途在于确定不同事件采用何种报警方式、由谁取得控制权限、需要在多长时间内响应，以及故障消除后按什么条件恢复运行。

2.2 安全需求映射与多源感知设计

完成场景识别后，下一步是把安全要求落到可以实施和验收的功能上。本文将每个危险场景拆分为监测、核验、动作和反馈几个环节，并据此建立安

全需求矩阵。一个完整场景至少应配置主要监测量和独立的辅助核验量，同时明确对应的安全动作及动作后的状态反馈。若系统只能下发指令，却无法确认现场是否真正完成执行，则该控制链仍存在断点。

项目供配电系统的数据来源并不局限于电气量。PLC 和现场传感器记录电流、电压、温度及设备位置，门禁系统保存人员身份和出入信息，巡检机器人提供可见光、红外等现场观测数据。不同来源的数据用于相互印证：例如电流变化需要结合温升和开关状态判断，抽屉退出动作除保留控制记录外，还要以位置限位信号确认执行结果。这样做可降低单一测点异常直接引起误判的概率。

2.3 可信决策：规则引擎与数据模型分层组合

对于直接关系停送电和设备隔离的场景，判断逻辑不能完全交给单一黑箱模型，涉及安全相关功能的软硬件设计参照 IEC 61508：2010[7]的功能安全要求。项目将确定性规则和数据模型分开使用：法规要求、联锁条件以及明确的禁止项由规则引擎处理；缓慢漏电、电压暂降等边界不清、特征组合复杂的异常，再由随机森林进行复核。计划停电数据库先用于排除已知操作，剩余疑似事件进入规则筛选和模型二次判断，置信度不足的情况转由人员确认。

这种配置的重点不是算法叠加，而是给不同判断手段安排不同职责。规则承担不可突破的安全约束，数据模型用于提高复杂异常的识别能力，人工复核负责处理低置信度和训练样本未覆盖的工况。因而，模型结果在进入控制环节前还需经过阈值、动作范围及权限校验，防止识别偏差直接被放大为执行风险。

2.4 纵深防御：软闭锁、硬联锁与物理隔离

远程控制把操作地点从配电室延伸到集控端，但“能够远程操作”并不等同于“当前条件允许操作”。在工程实施中，身份认证、电子挂牌、操作流程校核、安全联锁和往复式物理隔离被布置在同一操作链上，相关作业流程遵循 GB 26860—2011[8]和 AQ 1010—2005[9]的要求。权限和流程先由软件侧核对，设备侧再由硬联锁限制不允许的动作；进入检修状态后，还需通过实际电气断口完成物理隔离。

从控制过程看，可将这一结构理解为信息侧和物理侧相互校验的闭环。信息侧完成数据汇集、风险判断和操作授权，只有满足安全边界的指令才允许下发；物理机构动作后，再利用位置、电气状态或其他独立反馈确认结果，并把确认信息返回系统记录。若指令与反馈不一致，后续顺控立即中止，转入异常处置而不是继续执行，信息—物理双闭环结构如图 2 所示。

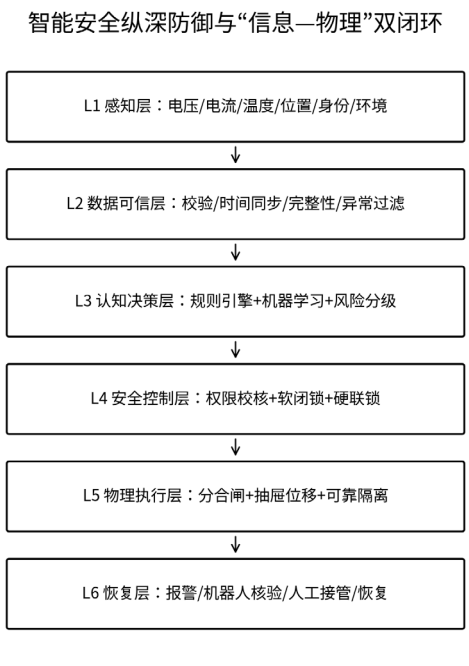


图 2　智能安全纵深防御与信息—物理双闭环

2.5 失效安全与韧性恢复设计

物联网系统的安全性还取决于异常情况下会怎样工作。除正常功能测试外，设计阶段需要事先考虑传感失真、通信中断、数据库不可访问、算法服务退出以及执行机构卡涩等情况，并为不同故障给出可接受的安全状态、降级方式、人工接管条件和恢复判据。

在供配电场景中，远程平台出现故障时，原有保护和本地急停仍应保持有效；算法服务中断后可以退回确定性规则；失去通信且无法获得远程确认时，不继续执行高风险操作；位置反馈与控制结果不一致时禁止送电。故障被隔离以后，还要结合路径重构、机器人复核、人工处置和服务恢复，使系统不仅能够停止在安全状态，也能够按照明确条件恢复运行。

2.6 全生命周期验证与持续迭代

智能安全功能投入运行后，原先的设计条件并

不是永久不变的。设备更换、工艺调整、人员变化以及算法版本更新，都可能使既有阈值或控制逻辑失去适用性。项目运行中采用月度参数调整、季度全量更新和现场问题反馈，对预警偏差、权限设置不便及定位误差等问题进行记录，经过整改和测试后再上线。

因此，全生命周期验证应与系统版本管理同步进行。除需求追溯和单元功能测试外，还应检查联锁逻辑、异常注入、通信故障下的降级行为、系统性能与压力、现场试运行结果以及版本变更后的回归情况。重要修改是否可接受，不以功能增加多少为判断依据，而要确认原有安全约束没有被削弱，整体设计方法流程如图 3 所示。

3 智能安全设计评价方法

3.1 多维评价指标

评价智能安全设计时，单看某一项识别精度不足以说明系统是否可靠。结合项目验收内容，本文从感知是否完整、诊断是否准确、控制是否可靠、响应是否及时、复杂环境下能否稳定工作、操作过程能否追溯以及故障后能否恢复等方面进行检查，对应记为 I_s、I_d、I_c、I_t、I_e、I_r 和 I_q。若某一应用场景确需形成综合量化结果，可采用加权形式：

$$S = \Sigma\, w_i\, I_i,\ \Sigma\, w_i = 1$$

各指标的权重应随危险场景而调整。例如涉及停送电和隔离的高风险操作，控制可靠性和系统韧性显然比界面便利性更重要。本文没有用项目数据强行计算一个统一的安全总分，原因在于平均值可能掩盖某个关键环节不合格。工程验收时，更适合先设置不可突破的门槛，再对非关键性能进行加权比较，各评价维度与验证方式见表 2。

图 3　基于物联网的智能安全设计方法流程

表 2　智能安全设计评价维度与验证方式

维度	典型指标	验证方式	未达标时处理
感知完整性	关键测点覆盖、反馈一致性	断点及异常数据试验	增加测点或引入独立核验
诊断准确性	准确率、误报率、漏报率	历史数据与现场故障试验	调整规则、补充样本并人工复核
控制可靠性	联锁正确率、执行成功率	顺控及异常注入试验	不允许进入自动闭环
响应及时性	响应时延、故障定位时间	端到端时延测试	下沉处理或优化处置路径
环境适应性	粉尘、湿度、温升条件下稳定性	环境试验与长期运行记录	加强防护、散热或冗余
追溯与韧性	日志完整性、降级与恢复时间	断网及故障恢复演练	完善备份、人工接管和恢复流程

3.2 门槛指标与风险加权并用

对于身份、联锁和隔离确认等直接决定安全边界的功能，项目采用的是“必须达标”而不是“平均得分较高”的判定方式。例如身份识别精度和联锁逻辑正确率均要求达到 100%，系统响应时间控制在 1.5 s 以内。故障诊断属于概率性判断，则可结合准确率、召回率、F1 值以及响应耗时进行评价。

评价结果还要能够反馈到系统调整。项目资料规定，故障识别准确率低于 90%时，应先检查规则阈值并补充训练样本；平均故障响应超过 5 min 时，需要重新优化机器人行走路径。也就是说，指标不是验收表中的静态数字，而应成为触发整改和复测的条件。当关键数据缺失、模型置信度下降或响应超限时，系统首先进入安全降级，而不是维持原有自动执行。

4 选煤厂智能安全供配电工程验证

4.1 系统构成与应用场景

工程示范部署在选煤厂多个配电室，项目依据《煤矿智能化建设指南（2021 年版）》[10]的总体要求开展智能化供配电改造。现场系统仍采用分层结构，但各层承担的任务有所区别：基础设施侧布置 PLC、传感器、门禁、隔离机构和巡检机器人；数据与平台侧负责数据保存、通信、算法运行及安全联锁；业务应用侧则面向停送电管理、设备状态、智能巡检、身份认证和故障预警等实际工作。

从五域模型看，这些设备和功能分别落在不同风险对象上。人员身份和权限属于人域，配电柜、断路器、隔离机构及其状态反馈属于机域；温度、粉尘等现场条件归入环境域；电子挂牌、操作流程及审计记录属于管理域；工业网络、数据库、算法服务和访问控制构成网/数域。工程应用的意义在于把五类对象放到同一作业链中检查，而不是分别建设、彼此独立运行，工程应用场景如图 4 所示。

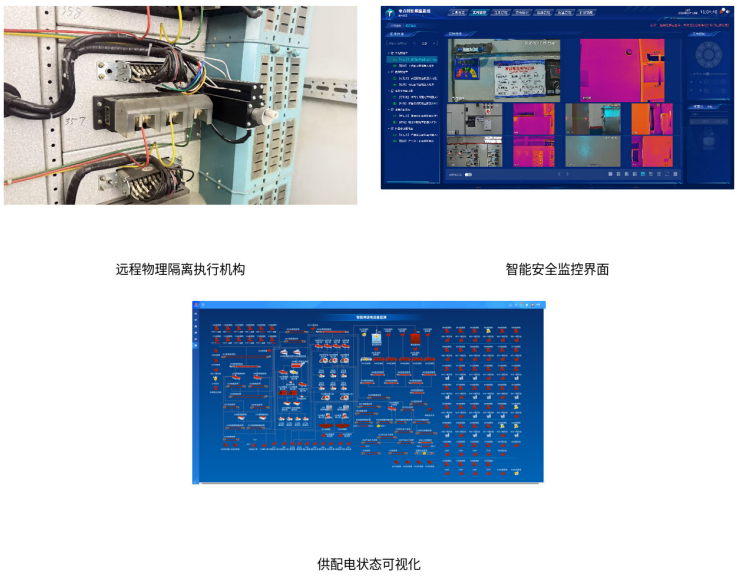


图 4　智能安全设计工程应用场景

注：照片来自项目研究报告，展示远程物理隔离执行机构及智能安全监控界面。

4.2 人员与操作安全验证

配电室入口通过人脸识别与门禁权限联动，联网和脱网状态下均可完成身份校验，项目记录的识别精度为 100%。电子挂牌同时与操作流程关联，挂牌人与摘牌人受到规则约束，权限不匹配时不能继续完成相关操作，从流程入口减少无授权作业。

远程停送电减少了人员进入带电间隔进行现场操作的次数。电动执行机构完成抽屉推拉后，再通过物理隔离状态进行确认。项目统计显示，停送电操作总耗时比改造前缩短 40%以上；单次抽屉推拉由人工约 90s 降至远程自动 15s 以内，测试中的操作成功率为 100%。这些结果反映出人员暴露时间、操作权限和物理隔离三者协同控制后带来的安全改善。

4.3 智能巡检与环境适应性验证

轨道式巡检机器人同时配置可见光、红外测温和环境监测模块，可识别仪表读数、开关位置及温升异常，现场记录的识别精度不低于 96%。在粉尘和湿度较高的配电环境中，项目另行配置了防尘和智能散热措施。研究报告显示，相关装置投入后设备内部积尘量降低 95%以上，高温告警次数减少 80%。

这组结果提示，智能安全系统的可靠性并不只由识别算法决定。传感器、执行机构和电气元件长期处于粉尘、湿度和温升影响下，其性能变化会直接影响控制结果。因此，环境适应性既要作为设备选型和防护设计的依据，也应纳入后续运行评价。

4.4 非计划停电识别与应急响应验证

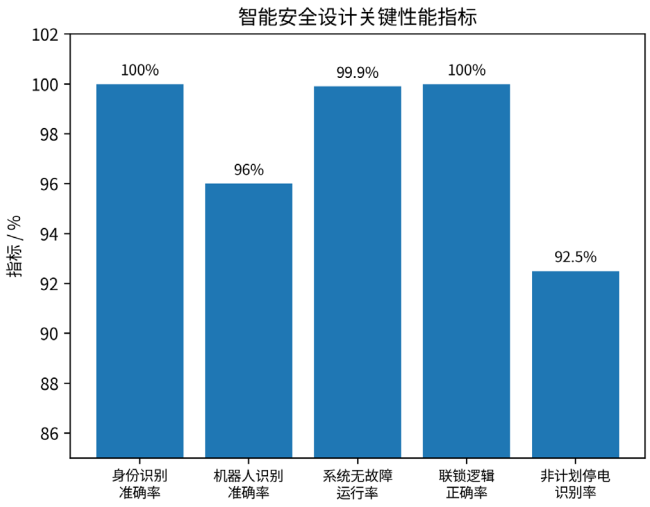
非计划停电的识别按多阶段完成。系统先与计划停电数据库比对，再由规则引擎筛出异常事件，随机森林负责对复杂特征进行复验。确认存在风险后，按照影响范围、设备重要性和环境条件确定报警级别，并调度巡检机器人到疑似故障位置进行可见光和红外复核。

试运行期间，非计划停电识别准确率达到 92.5%，平均响应时间控制在 4.2 min 以内；原来依靠人工排查时约 30 min 的故障定位过程缩短到 5 min 以内，相关次生故障率下降 70%。与单阈值报警相比，该流程把数据库、规则、模型和现场核验串联起来，减少了单一信号误报造成的无效处置，也缩短了从发现异常到隔离故障的时间。

4.5 系统可靠性与综合效益

从连续运行结果看，系统无故障运行时间达到 99.9%以上，数据查询响应时间不超过 1.5 s。与改造前相比，设备故障停机时间减少 50%，维护效率提高 30%。同期吨煤电耗由 2.96 kW·h/t 降至 2.51 kW·h/t，按项目最终应用口径计算，年节约电费 184.25 万元，工程验证关键指标如图 5 所示。

上述能耗数据并不是用于直接证明安全设计水平，但可以从侧面反映系统运行方式的变化。故障定位加快后，无效停机和重复启停减少；巡检和部分操作转到远程后，现场人员进入频次下降；设备状态数据的持续积累也为节能运行提供了依据。因此，安全改造与运行效率改善在工程上存在一定协同效应，主要指标与对应设计机制的关联见表 3。



另：停送电操作耗时缩短>40%，非计划停电平均响应≤4.2 min，次生故障率下降70%。

图 5　智能安全设计工程验证关键指标

表 3　工程验证主要指标及其对应设计机制

工程指标	验证结果	关联设计措施
身份识别精度	100%	身份与权限校验
机器人识别精度	≥96%	移动多模态感知
系统无故障运行	≥99.9%	可靠性与故障恢复
停送电操作耗时	缩短>40%	远程顺控与多重安全约束
非计划停电识别	92.5%	规则筛查与随机森林复验
平均响应时间	≤4.2 min	分级报警与机器人现场核验
次生故障率	下降 70%	快速定位及故障隔离

5 讨论

5.1 从“安全功能叠加”转向“安全设计前移”

工业物联网建设中，如果先完成联网和控制功能，再单独补充门禁、报警或权限模块，安全要求往往难以真正进入控制逻辑。本文案例采取相反的顺序：先依据作业过程识别危险场景，再把安全要求拆解到测点、数据字段、网络接口、操作权限和执行机构。这样，安全不再是系统上线后的附加功能，而是在方案阶段就决定系统如何感知、如何判断以及哪些动作可以执行的约束条件。

5.2 安全与网络安全应协同而非相互替代

IIoT 把传统生产安全与网络安全放到了同一条控制链上。通信中断、账号越权或数据被篡改可能改变设备动作，而错误的远程指令又可能把信息侧故障转化为物理危险。已有工业信息物理系统研究也强调两类风险需要联合分析[4]，工业网络的系统安全要求可参照 IEC 62443-3-3：2013[11]。因此，五域模型单独设置网/数域，用于检查通信、数据、模型和访问控制是否会影响现场安全。

不过，信息侧安全不能取代现场的物理安全措施。即使远程控制已经采用身份认证和加密通信，检修回路仍需要形成可靠断口；反过来，硬联锁和机械隔离完备，也不能忽略账号权限、数据完整性和通信劫持问题。更合理的做法是把网络身份、业务流程、设备联锁和物理状态连续校验，使其中任一环节异常时都不能直接进入高风险执行。

5.3 智能算法的安全边界

机器学习适合从多变量中识别传统阈值难以描述的异常，但其输出会受到样本覆盖、模型漂移和可解释性不足等因素影响。因此，在高风险保护中，数据模型更适合作为增强判断手段，而不是替代确定性规则和硬联锁。涉及安全边界的最终许可条件仍应由可验证、可复现的逻辑给出。

这一原则对后续大模型和智能体应用同样适用。规程检索、故障原因解释和任务编排可以借助生成式模型提高信息处理效率；但停送电、物理隔离、急停等动作不宜由生成式模型直接决定。此类动作应调用已经经过验证的控制逻辑，并继续受权限、联锁和现场反馈约束。

5.4 面向环境与能源系统的扩展

尽管工程验证对象是选煤厂供配电系统，五域划分并不依赖某一种具体设备。在能源环境监测、污水处理、通风、储运或危险作业中，也可以按人员、设备、环境、管理和网络/数据重新梳理风险，类似思路也出现在地下开采数字化参考架构[12]和基于 IIoT 的矿井爆炸性气氛监测[13]等应用中。例如环境治理系统既要看污染物浓度，也要同时掌握设备状态、气象条件、人员权限和控制网络状态；若关键传感失效或通信中断，应转入较保守的运行方式，并保留人工接管渠道。

因此，将该方法扩展到能源与环境系统时，评价内容也不能只剩生产效率。环境适应性、能源消耗、人员暴露程度以及异常情况下的恢复能力，都应作为工程运行效果的一部分进行记录和比较。

5.5 后续研究方向

后续工作可沿三条路线继续完善。第一，积累典型危险事件及其触发条件、监测量和处置规则，逐步形成可复用的场景库和安全需求知识组织；第二，利用数字孪生先在虚拟环境中进行故障注入和联锁策略验证，补足现场难以重复测试的极端工况；第三，针对工业大模型和多智能体应用，进一步明确其调用权限、任务边界、继承关系及行为审计要求。

目前的评价框架主要依据单个工程的技术指标建立，跨行业、跨工况的大样本验证仍然不足。下一阶段需要比较不同能源工业场景下指标权重、门槛值和故障类型的差异，确认哪些指标可以通用、哪些必须现场标定，再据此形成更稳定的智能安全设计成熟度评价方法。

6 结论

1）工业物联网接入后，选煤厂安全对象不再局限于单台设备。本文把人员、设备、环境、管理和网络/数据纳入同一分析框架，并以本质安全、纵深防御、失效安全、过程可追溯和韧性恢复约束各环节设计。

2）围绕实际危险场景，形成了由风险分级、需求分解、多源感知、分层判断、安全联锁、物理隔离到运行复核和持续更新的实施路径。工程中，规则引擎、机器学习和人工复核分别承担确定性约束、复杂异常识别和低置信度处置，软闭锁、硬联锁及物理隔离共同限制高风险操作。

3）评价时采用“门槛+多维指标”的思路，重点检查感知完整性、诊断准确性、控制可靠性、响应及时性、环境适应性、可追溯性和系统韧性。对联锁、身份和隔离确认等关键功能，单项不达标不能由其他指标的高分抵消。

4）现场验证结果显示，身份识别精度为 100%，巡检机器人识别精度不低于 96%，系统无故障运行时间不低于 99.9%，停送电操作耗时缩短 40%以上；非计划停电识别准确率达到 92.5%，平均响应时间不超过 4.2 min，次生故障率下降 70%。这些数据说明，只有把数据采集、判断、联锁、物理执行和反馈确认连成完整链路，物联网连接能力才能转化为可验证的安全控制效果。

参考文献

[1] Kiziroglou M E, et al. A robust end-to-end IoT system for supporting workers in mining industries[J]. Sensors, 2024, 24(11): 3317.

[2] Khan W Z, et al. A study on industrial IoT for the mining industry: synthesized architecture and open research directions[J]. Internet of Things, 2020, 1(2): 29.

[3] On the impact of Industrial Internet of Things (IIoT)—mining sector perspectives[J]. Mining Technology, 2024.

[4] Sun Z, Chen G, Ding Y, et al. Joint safety and security risk analysis in industrial cyber-physical systems: a survey[J]. IET Cyber-Physical Systems: Theory & Applications, 2024, 9(4): 334-349.

[5] Cascade failure modeling and resilience analysis of mine cyber physical systems under deliberate attacks[J]. Journal of Safety Science and Resilience, 2024, 5(3): 266-280.

[6] Amiri A, Steindl G, Hollerer S. Integrated safety and security by design in the IT/OT convergence of industrial cyber-physical systems[C]//2024 IEEE 7th International Conference on Industrial Cyber-Physical Systems. 2024: 1-2.

[7] IEC 61508:2010 Functional safety of electrical/electronic/programmable electronic safety-related systems[S].

[8] GB 26860—2011 电力安全工作规程 发电厂和变电站电气部分[S].

[9] AQ 1010—2005 选煤厂安全规程[S].

[10] 国家能源局. 煤矿智能化建设指南（2021 年版）[S/OL]. 2021.

[11] EC 62443-3-3:2013 Industrial communication networks—Network and system security—System security requirements and security levels[S].

[12] Reference architecture design and evaluation for digitalization of underground mining[J]. Internet of Things, 2024, 26: 101238.

[13] Medina F, Ruiz H, Espíndola J, et al. Deploying IIoT systems for long-term planning in underground mining: a focus on the monitoring of explosive atmospheres[J]. Applied Sciences, 2024, 14(3): 1116.