安全标准化与信息化融合下的企业安全管理模式创新

吕昌现
云南云铝海鑫铝业有限公司　云南　昭通　657100

摘　要：安全标准化作为企业安全管理核心支撑，与信息化技术深度融合成为必然趋势。本文阐述二者融合的理论基础，从管理架构、流程再造、决策机制、风险防控、培训与文化等方面提出创新路径，分析数据治理、系统集成、智能算法应用等关键技术实现，剖析技术、管理、人员层面挑战并提出应对策略，为企业安全管理模式创新提供参考。

关键词：安全标准化；信息化融合；企业管理模式；创新路径；关键技术

引言：企业安全管理关乎生产经营稳定与员工生命安全。传统安全管理模式存在效率低、响应慢等问题，难以适应复杂多变的安全形势。安全标准化提供系统管理框架，信息化技术赋予高效数据支撑，二者融合可实现优势互补，推动安全管理向智能化、精准化转型，提升企业安全管理水平与风险防控能力。

1 安全标准化与信息化融合的理论基础

1.1 安全标准化的内涵与特征

安全标准化是企业安全管理的核心支撑，其内涵聚焦于通过建立健全安全生产责任制，制定完善的安全管理制度与操作规程，构建系统化、规范化的管理框架[1]。这一框架全面覆盖目标职责、制度管理、风险管控、现场管理、教育培训、应急管理等全要素，实现企业安全管理各环节的有序衔接与规范运行。安全标准化引入国际通用的PDCA动态循环管理模式，通过策划、实施、检查、改进的闭环流程，推动企业安全管理水平持续优化，契合现代安全管理的发展方向，是先进安全管理思想与企业实际管理需求的有机结合。

1.2 信息化的技术支撑体系

信息化技术为安全管理模式创新提供坚实技术支撑，形成多技术协同的支撑体系。物联网技术凭借泛在感知能力，实现安全管理相关数据的实时采集与设备运行状态的动态监控，搭建起安全管理的感知网络。大数据分析技术能够对海量安全数据进行深度挖掘与关联分析，实现安全风险的精准预测，为安全管理决策提供科学依据。人工智能技术通过算法优化实现安全风险的智能预警，搭配自动化响应机制，有效提升安全隐患处置效率。云计算与区块链技术协同发力，云计算提供高效的数据存储与运算能力，区块链则保障安全数据的不可篡改与可追溯，实现数据资源的安全共享与规范管理。

1.3 融合的理论逻辑

安全标准化与信息化的融合具备清晰的理论逻辑，二者相互支撑、协同共生。安全标准化为融合过程提供明确的管理框架与行为准则，界定安全管理的核心要素与执行标准，为信息化技术的应用划定方向与边界。信息化技术为安全标准化的落地注入高效技术动能，通过技术手段优化管理流程，提升标准化要求的执行效率。信息化技术能够有效规避安全标准化执行过程中因人为操作不当产生的偏差，通过自动化管控、数据化核查等方式，确保标准化要求落地见效。安全标准化的具体要求驱动信息化系统的功能设计，信息化系统的研发与优化需紧密围绕标准化的核心要素，实现管理需求与技术应用的精准匹配，推动二者深度融合。

2 融合背景下的企业安全管理模式创新路径

2.1 管理架构创新

管理架构创新聚焦打破传统部门壁垒，构建“标准化+信息化”双轮驱动的组织体系，依托组织协同理论优化安全管理组织架构。明确安全管理部门与信息技术部门的协同机制，规范双方职责分工与沟通流程，推动安全管理需求与信息技术应用精准对接。设立跨部门的安全数据治理委员会，统筹协调安全数据的采集、整理、分析与应用，保障安全数据的规范性与可用性，为融合背景下的安全管理创新提供组织保障。

2.2 流程再造创新

流程再造创新以安全标准化条款为核心依据，将标准化要求转化为可落地的数字化流程节点，遵循业务流程再造理论优化安全管理流程[2]。依托信息化技术实现风险识别、评估、管控的全流程线上化，简化传统流程中的繁琐环节，提升流程执行效率。搭建“隐患上报—任务分配—整改跟踪—验收闭环”的数字化链条，实现隐患管理各环节的可追溯、可管控，确保标准化流程落地不走样，推动安全管理流程的规范化与高效化。

2.3 决策机制创新

决策机制创新立足数据驱动理论，构建基于大数据的安全态势感知与决策支持系统，整合企业安全管理各类数据资源，实现安全态势的实时研判。搭建多维度安全绩效指标体系，涵盖风险管控、隐患整改、培训教育等核心环节，为安全决策提供量化依据。依托数据挖掘与分析技术，实现安全管理从经验决策向数据驱动决策的转变，提升安全决策的科学性与精准性，契合现代安全管理的智能化发展趋势。

2.4 风险防控创新

风险防控创新聚焦双重预防机制的数字化落地，结合风险管控理论与信息化技术，搭建动态风险数据库，实时更新风险信息，搭配智能预警模型，实现风险等级的动态更新与精准预警，提前防范各类安全隐患。针对特殊作业环节的高风险特征，引入AI视频监控与行为分析技术，对作业人员操作行为进行实时监测，精准识别违规操作行为，及时发出预警信号并联动相关负责人处置，降低特殊作业环节的安全风险，推动风险防控模式从被动处置向主动预防转变，筑牢企业安全防控防线。

2.5 培训与文化创新

培训与文化创新依托现代教育技术与组织文化理论，搭建AI知识库支持的个性化安全培训系统，根据不同岗位人员的安全职责与知识短板，推送针对性培训内容，提升培训的针对性与实效性。构建基于VR/AR的沉浸式安全演练平台，模拟各类复杂安全场景，让培训人员在沉浸式体验中熟悉应急处置流程、提升应急处置能力，打破传统培训模式的局限。通过信息化手段搭建安全文化传播平台，常态化推送安全知识、案例警示、合规要求等内容，引导员工树立安全意识、规范操作行为，培育“人人参与、人人负责”的安全文化，夯实企业安全管理的文化基础。

3 融合过程中的关键技术实现

3.1 数据治理技术

数据治理技术是安全标准化与信息化融合的核心技术支撑，核心围绕多源异构数据的规范管控与高效利用展开[3]。针对企业安全管理过程中不同系统产生的异构数据，采用专业数据清洗技术剔除冗余、错误及无效信息，通过标准化处理规范数据格式、统一数据口径，确保数据一致性与准确性。搭建安全数据仓库，整合风险管控、隐患整改、设备运行、培训教育等各类安全相关数据，建立常态化维护机制，定期开展数据更新与质量校验，保障数据时效性与完整性。基于数据安全理论与隐私保护规范，设计科学合理的数据隐私保护与共享机制，采用加密技术与精细化访问控制策略，在筑牢数据安全防线的基础上，实现安全数据在企业内部各相关部门的规范流转与高效共享，充分释放数据价值。

3.2 系统集成技术

系统集成技术聚焦打破各系统信息壁垒，推动安全管理与企业生产运营全流程协同，是融合落地的关键支撑。实现安全生产管理系统与ERP、MES等核心业务系统的无缝对接，打通安全管理与生产计划、物料管理、生产执行等环节的数据流通渠道，实现数据互联互通，避免数据孤岛现象。构建云边端协同的物联网架构，边缘端负责现场安全数据的实时采集与本地快速处理，降低数据传输压力，云端承担数据存储、深度分析与全局管控功能，优化数据处理效率与系统响应速度。采用微服务架构设计系统模块，将安全管理各项功能拆解为独立可扩展的微服务单元，实现系统功能的灵活升级与按需扩展，适配企业安全管理需求的动态变化与融合深度的持续推进。

3.3 智能算法应用

智能算法应用推动安全管理向智能化、精准化升级，为融合模式下的安全管理提供高效技术支撑。基于机器学习算法构建安全风险预测模型，通过对历史安全数据、实时运行数据的深度学习与训练，捕捉风险演变规律与潜在关联，实现安全风险的提前预判与精准管控。将计算机视觉技术应用于作业行为识别，通过图像识别与特征提取技术，对作业现场人员操作行为进行实时监测，精准识别违规操作行为，为风险防控提供及时技术支撑。引入自然语言处理技术实现安全文档的智能分析，对安全规章制度、操作规程、隐患报告等各类文档进行深度解析，提取核心信息并实现结构化呈现，提升安全文档的检索效率与利用价值，为安全管理决策与培训工作提供高效支持。

4 融合实施中的挑战与应对策略

4.1 技术层面挑战

4.1.1 技术层面核心挑战表现

技术层面挑战贯穿安全标准化与信息化融合全流程，聚焦设备适配、环境适配与算法性能三大核心维度。老旧设备与新系统的兼容性存在明显短板，部分企业存量安全设备服役周期较长，技术规格滞后于当前信息化发展水平，缺乏统一的标准化数据接口，无法与新型信息化管理系统形成高效联动，制约数据采集的全面性与传输的顺畅性[4]。复杂工业环境中存在的电磁干扰、信号遮挡、温湿度波动等客观因素，易导致数据传输稳定性不足，常出现数据丢失、传输延迟、信号中断等问

题，干扰融合系统的常态化运行。

4.1.2 技术层面挑战应对策略

应对策略需采用接口适配技术对老旧设备进行针对性改造，搭建标准化数据转换模块，打通新旧系统数据流通壁垒，实现二者高效兼容；优化工业环境数据传输链路，采用抗干扰传输技术与数据冗余备份方案，减少外部环境对数据传输的影响，提升传输稳定性；引入可解释性算法框架，结合工业安全场景特征优化模型训练过程，强化算法对复杂场景的适配能力，增强算法鲁棒性。

4.2 管理层面挑战

4.2.1 管理层面核心挑战表现

管理层面挑战聚焦协同效率、思维转型与投入产出三大维度，成为融合实施的重要制度性阻碍。部门间数据共享的权限管理缺乏科学规范的体系设计，各部门数据管理标准不一、统计口径各异，权限划分模糊且缺乏动态调整机制，易出现数据共享不及时、权限滥用、数据泄露等问题，阻碍安全数据资源的高效流转与深度利用。传统经验型管理思维向数字化管理思维的转变存在明显阻力，部分管理人员长期依赖过往工作经验开展安全管理，对数字化管理模式的价值认知不足，缺乏主动推动融合工作落地的意识与动力。

4.2.2 管理层面挑战应对策略

应对策略需建立统一的数据共享权限管理体系，明确各部门权限划分标准与动态调整机制，规范数据共享流程，实现数据资源高效安全流转；通过常态化管理培训与实践场景引导，强化管理人员数字化管理理念，推动管理思维从经验型向数字化转型；构建信息化投入分级管控与收益评估体系，合理规划投入节奏，聚焦核心管理环节精准投入，实现投入与收益的动态平衡。

4.3 人员层面挑战

4.3.1 人员层面核心挑战表现

人员层面挑战直接关联融合实施的落地效果，核心集中在接受意愿、人才储备与技能提升三大方面。部分员工长期习惯于传统手工操作与管理模式，对信息化系统、智能监控设备等新型工具的操作存在畏难情绪，主动学习与适应的意愿不强，直接导致新技术应用效果未能充分发挥。复合型安全-IT人才供给存在明显缺口，安全管理与信息技术的交叉融合不足，现有从业人员多专注单一领域，难以兼顾安全管理规范与信息化技术应用的双重需求，成为制约融合深度推进的人才瓶颈。数字化技能培训体系缺乏系统性与针对性，培训内容与岗位实际安全管理需求脱节，未形成分层分类的培训机制，难以有效提升不同岗位员工的数字化操作、数据解读与技术应用能力[5]。

4.3.2 人员层面挑战应对策略

应对策略需搭建新技术应用引导体系，通过直观操作演示、场景化适配训练，降低员工学习门槛，逐步提升员工对新技术的接受度；建立校企合作与内部培养相结合的人才培育机制，聚焦安全与IT知识的交叉融合，针对性开展人才培养，补齐复合型人才缺口；构建分层分类的数字化技能培训体系，结合不同岗位安全管理需求定制专属培训内容，强化培训实效，为融合实施提供坚实的人员支撑。

结束语

安全标准化与信息化融合下的企业安全管理模式创新，是顺应时代发展的必然选择。通过管理架构、流程、决策等多方面创新，以及关键技术的有效应用，虽面临技术、管理、人员等挑战，但采取针对性应对策略可逐步克服。这一融合模式将持续提升企业安全管理效能，为企业稳定发展筑牢安全根基。

参考文献

[1]张文显.冶金企业安全管理模式创新策略[J].金属制品,2025,51(5):63-66.

[2]文雁冰.新形势下工贸企业安全管理模式创新研究[J].中国公共安全,2025(6):68-70.

[3]贾赟.造纸企业建筑工程安全管理模式创新[J].华东纸业,2025,55(11):22-24.

[4]刘芳.安全管理模式创新护航冶金企业转型升级[J].南方金属,2025(3):77-79,84.

[5]邬秀兰.创新企业粮食质量安全管理模式探索[J].粮油仓储科技通讯,2023,39(3):9-11.