ICS 13.100
CCS C78

中华人民共和国国家标准

GB/T XXXXX—XXXX

实验室安全监测与智能管控通用要求

General requirements for laboratory safety monitoring and intelligent control

（征求意见稿）

XXXX－XX－XX 发布　　XXXX－XX－XX 实施

国家市场监督管理总局
国家标准化管理委员会　发布

目　　次

前　言

本文件按照GB/T 1.1—2020《标准化工作导则　第1部分：标准化文件的结构和起草规则》的规定起草。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别专利的责任。

本文件由中华人民共和国应急管理部提出。

本文件由全国安全生产标准化技术委员会（SAC/TC288）归口。

本文件起草单位：中国安全生产科学研究院、中国矿业大学、中国合格评定国家认可中心、中国海关科学技术研究中心、北京东土科技股份有限公司、北京芯盾时代科技有限公司、中矿检测（辽宁）有限公司、上海交通大学、雅砻江流域水电开发有限公司、中检集团公信安全科技有限公司、南京诺飞尔信息科技有限公司、抚顺中煤科工检测中心有限公司、中国石油天然气股份有限公司西南油气田分公司、西北农林科技大学、扬州大学、贵州省生态环境监测中心

本文件主要起草人：周福宝、田军、白向玉、潘锋、时训先、桑海泉、张晓龙、程远、季文东、李国、曾明荣、梁昕、熊开智、宋宪旺、豆梓文、钱小东、曹轩、王艳、张金娥、王义保、黄昌忠、吕欢、吴北平、黄洪发、王思、李彦、徐书杰、李亚松、顾永琴、李珊、滕丽霞、杜会芳、黄海燕、郝雄飞、陈小雨、李论、蔡四堂、袁伟斌、周骥平、胡佳佳、李卓柯

引　言

0.1 背景

实验室是科学研究、技术开发、成果转化和检验检测的重要场所，其安全管理直接关系到人员健康、环境安全和实验活动的可持续性。随着实验室规模的扩大、设备复杂性的提升以及智能化技术的快速发展，传统安全管理模式已难以满足现代实验室的风险防控需求。通过构建标准化、智能化的安全监测与智能管控体系，实现实验室安全风险的实时感知、动态预警和高效处置，已成为行业发展的必然趋势。

0.2 目的

本文件旨在规范实验室安全监测与智能管控的设计、建设和运行，提升实验室安全管理的科学性、精准性和主动性。本文件结合物联网、大数据、人工智能等新一代信息技术，围绕实验室环境、设备、危险化学品、人员等要素，提出安全监测、数据分析、智能预警和应急响应的通用技术要求，旨在为各类实验室的安全管理提供统一的技术框架和实施指南。

0.3 原则

本文件的制定参考了国内外相关法规、标准及最佳实践，兼顾技术先进性与适用性，适用于新建、改建或扩建实验室的安全监测与智能管控建设。通过本文件的实施，期望推动实验室安全管理向数字化、信息化、智能化转型，为教学、科研、检测活动的安全高效开展提供基础保障。

0.4 本文件内容

本文件第1章至第3章阐述了适用范围、规范性引用文件及术语定义，第4章至第9章规范了实验室安全监测与智能管控6个要素的核心要求。实验室应对人的不安全行为、物的不安全状态、环境的不安全因素、管理的薄弱环节等进行风险评估，根据风险评估结果，运用信息技术，有针对性地引导高风险实验室构建安全管控长效机制，提升安全生产风险智能化管控能力。

实验室安全监测与智能管控通用要求

1 范围

本文件规定了实验室安全监测与智能管控的总体要求、安全监测、智能管控、集成、运行管理要求以及评价与改进。

本文件适用于安全生产领域高风险实验室的安全监测、智能管控的设计、建设、验收和智能管控平台的开发与集成。可作为第三方评估与认证的依据。其他实验室可参照使用。

2 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件；不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

GB 20815 视频安防监控数字录像设备

GB/T 25069 信息安全技术术语

GB/T 28181 公共安全视频监控联网系统信息传输、交换、控制技术要求

GB/T 35273 信息安全技术 个人信息安全规范

GB 37300 公共安全重点区域视频图像信息采集规范

GB/T 39555 智能实验室 仪器设备 气候、环境试验设备的数据接口

GB/T 39556 智能实验室 仪器设备 通信要求

GA/T 1216 安全防范视频监控网络视音频编解码设备

GA/T 1325 安全防范 人脸识别应用 视频图像采集规范

3 术语和定义

下列术语和定义适用于本文件。

3.1

高风险实验室 high-risk laboratory

实验操作存在较大意外风险的、容易引发严重事故的，经风险评估，须采取严格的安全控制和防护措施的实验室。

3.2

危险源 hazards

实验室内可能导致人身伤害和（或）健康损伤、财产损失的根源、状态或行为，或其组合。

[来源：GB/T 27476.1-2014，3.4，有修改]

3.3

安全监测 safety monitoring

通过传感器、视频等终端设备对实验室环境、设备、危险化学品、人员操作及潜在危险源进行实时监测，并利用相关技术，根据一定策略实现自动监测、诊断、预警等的一种自动化的工作行为，能及时将监测数据反馈给管理者。

[来源：GB/T 36342-2018，3.9，有修改]

3.4

智能管控 intelligent management and control

利用人工智能（AI）、物联网（IoT）、大数据分析、自动化控制等信息技术，对实验室的设施、设备、环境、能源、安全及实验流程等的安全监测结果，进行动态优化与自主决策的智能化管理，实现实验室安全态势感知、风险评估和自动控制。

4 总体要求

4.1 基本原则

4.1.1 人机协同原则

通过明确人与人工智能的能力边界，建立动态互补的决策机制，使人的主观判断力与机器的客观计算力形成闭环，最终实现风险控制效率最大化、人为失误最小化的目标。

4.1.2 事前预防原则

通过系统性风险评估、前瞻性技术防控和全过程管理干预，在事故发生前主动识别、消除或控制危险源，最大限度降低风险发生概率及后果严重度的根本性指导。

4.1.3 全生命周期管理原则

通过对人员、设备、危险化学品、环境及数据等要素从规划、建设、运行到终止的全过程实施动态化、系统化安全管理，利用标准化技术手段和持续化管理措施，确保每个阶段的安全风险可控。

4.2 总体架构

实验室安全监测与智能管控通常应由感知层、传输层、平台层、应用层和用户端构成，见图1。

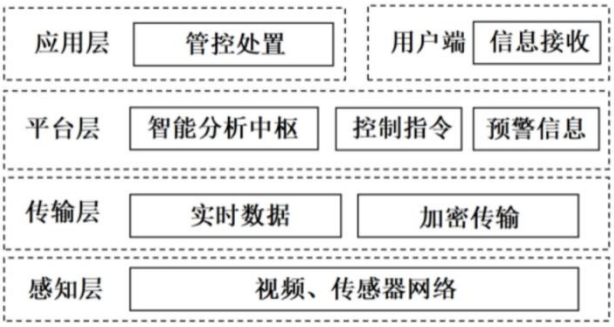

图 1 总体架构图

5 安全监测要求

5.1 监测范围

5.1.1 环境安全

根据实验室特性，重点监测实验室环境温湿度、压差、气体浓度、VOCs、颗粒物等，发现异常，及时报警。

5.1.2 设备状态

实验室应对高温、高压、强辐射、强磁、激光以及储存易燃、易爆、有毒、有害物质等危险性较大的设备设施的运行状态参数进行监测、监控、预警、跟踪分析和处理。

5.1.3 危险化学品

监测实验室使用的危险化学品采购、入库、储存、领用、使用、废弃处置等情况，发生意外状况，应及时感知并报警。

5.1.4 安全准入

监测实验区域内人员、高温、高压、强辐射、强磁、激光等危险性较大的设备设施出入。高风险实验项目实施实验活动前审批授权。

5.1.5 行为安全

监测实验区域内人员行为状态，如防护装备穿戴、违规操作、高危区域停留等情况。

5.2 监测设备

5.2.1 实验室应配备符合规定要求的传感器，如温度、湿度、氧含量传感器，VOCs、有毒有害气体传感器，粉尘浓度传感器等，其量程、精度以及安装位置应满足标准要求，并定期维护。

5.2.2 实验室应按规定配备符合 GB/T 28181、GB 37300、GA/T 1216 标准要求的视频设备。高风险区域视频设备数量与安装位置应确保监控无盲区。

5.2.3 实验室应按规定配备符合 GA/T 1325 标准要求的门禁系统，对管理人员、实验人员、外来人员等进行身份鉴别和访问控制。身份鉴别应符合 GB/T 25069 标准要求，并支持多因素鉴别（MFA）。

5.2.4 实验室应配备声光报警装置，必要时，应具有防爆功能。报警装置抗电磁干扰能力应符合相关标准要求。

5.2.5 实验室应配备语音播报或广播对讲设备、应急疏散指示设备。

5.2.6 实验室应为安全监测与智能管控系统配备 UPS 应急电源。

5.3 智能分析

5.3.1 视频 AI 异常行为检测

视频分析系统应具备实时监测能力，包括但不限于：

——事故监测：火焰、烟雾等；

——人员行为：跌倒、睡觉、饮食等；

——个体防护：未佩戴个体防护用品；

——操作合规：危险品违规取用、设备误操作、气瓶未固定及违规混放、通风橱可视窗过高等；

——入侵监测：非授权区域闯入；

——环境监测：摄像头被遮挡、未关门窗、逃生通道堵塞等。

5.3.2 算法性能要求

算法性能包括但不限于：

——目标检测准确率≥95%；

——响应延迟≤3s；

——支持多人场景下的行为语义分析。

5.3.3 多参数耦合分析

系统应具备多源传感器数据融合分析能力，实现环境参数与设备状态、化学品存储等数据的动态关联分析。针对易挥发化学品，需建立温湿度变化与挥发浓度的数学模型，阈值超标时触发分级预警。支持历史数据回溯与趋势推演，生成关联性分析报告，辅助事故溯源。

5.3.4 基于数字孪生的风险预测

应构建实验室三维数字孪生模型，实时映射物理空间的设备布局、人员动线及环境状态。

通过仿真引擎模拟风险场景，包括但不限于：

——化学品泄漏扩散路径预测；

——设备连锁故障影响范围模拟；

——应急疏散通道动态评估。

风险预测结果应以可视化形式呈现，预测准确率不低于90%。

5.4 数据管理

5.4.1 采集频率与存储周期

无特殊规定的，环境参数采集频率通常1次/10s，存储频率至少1次/min，最低存储周期1年；设备运行状态采集频率通常1次/1s（关键设备），存储频率至少1次/min，最低存储周期3年；视频监控数据单路记录速度≥25帧/s，最低存储周期90天，报警事件触发回溯视频存储，依据GB 20815实验室事故触发前预录≥5s，事故触发后延录≥3min，最低存储周期3年。

存储周期届满后，敏感数据需进行不可恢复式擦除，非敏感数据可转为冷存储。

宜建立数据备份与容灾恢复机制，保护关键数据。

5.4.2 数据加密与完整性校验

应采用国密SM4或AES-256算法对实时传输数据加密，SSL/TLS协议版本不低于1.2；无线传输信道需额外启用WPA3-Enterprise认证。

静态数据使用SM9或RSA-2048进行非对称加密；密钥管理符合GB/T 39786三级要求，硬件加密模块需满足GM/T 0028要求。

每批次数据附加SHA-256哈希值，校验失败时触发数据重传机制；建立区块链存证系统（可选），对关键操作日志进行上链固化。加密策略变更、密钥轮换等操作需留存审计日志，日志文件防篡改时间戳精度≤1ms。

6 智能管控要求

6.1 风险预警

6.1.1 预警分级与多级阈值设定

实验室应按照表1所示的四级预警体系，设置各类传感器的预警阈值、预警通知方式和预警时的应急处置方式。

表 1 预警体系

等级	颜色标识	触发条件	响应要求
Ⅰ级	红色	可能造成人员伤亡/重大财产损失	立即停机+紧急疏散+联动 119
Ⅱ级	橙色	可能造成设备严重损坏	自动停机+负责人现场处置
Ⅲ级	黄色	潜在风险累积	声光提示+值班人员核查
Ⅳ级	蓝色	一般性违规	语音提醒+日志记录

6.1.2 多模态预警发布

发布渠道包括但不限于：

——声光报警：现场蜂鸣器与LED屏同步显示预警点位；

——移动端推送：通过多渠道发送定位图片与处置指引；

——广播系统：自动播报预制应急语音。

发布预警信息内容包括但不限于：

——风险类型、发生位置、建议措施、倒计时（如“Ⅱ级预警：XXX实验室东侧氢气泄漏，剩余安全处置时间08:23”）等；

——疏散路线图、应急联系人一键呼叫。

系统应在预警发布后3min内未收到人工确认时，自动升级预警等级；通过视频AI识别人员是否抵达处置位置，否则触发二次报警。

应分析历史误报数据，对重复误报点位启动智能过滤，并应经人工复核解除。月度统计误报率应控制在≤5%。

每起Ⅰ/Ⅱ级预警事件需生成根因分析报告，包含传感器数据异常时间轴、处置过程视频片段、类似风险防范措施建议等。

系统发布预警后，应能根据预警等级、类型和预设规则，自动生成预警信息核查与处置任务单。

6.1.3 报警规则配置

视频分析算法配置：应根据不同实验室安全管理需求配置不同的识别算法种类和识别区域。

视频分析报警规则设置：针对不同算法进行报警规则设置，包括采集频率、报警逻辑（检测帧率）、报警周期、报警阈值、视频分析时间段。

6.2 智能决策

6.2.1 决策层级

决策层级见表2所示。

表 2 决策层级列表

决策层级	适用场景	技术实现	人工干预要求
L1 自动执行	明确规则的紧急处置（如灭火）	规则引擎+硬联动设备	无需批准，事后报备
L2 人机协同	复杂风险研判(如气体扩散路径)	数字孪生仿真+AI 建议方案	需责任人电子签名确认
L3 专家会商	系统性风险（如建筑结构安全）	多专家视频会诊+虚拟白板协同	需 3 人以上专家共识

6.2.2 决策模型要求

决策模型的核心算法库应至少包含贝叶斯网络（用于概率风险评估）、LSTM时序预测（设备故障预警）和知识图谱（化学品相容性推理）。算法更新周期≤6个月。决策有效性指标应符合表3要求。

表 3 决策有效性指标

指标项	阈值要求	检测方法
应急决策准确率	≥95%(历史数据验证)	混淆矩阵分析
方案生成时效	L1≤10s，L2≤30s	压力测试
可解释性	符合标准要求	决策路径可视化追溯
AI 视频分析预警置信度	≥0.6	混淆矩阵分析

6.3 应急响应

6.3.1 响应等级与处置流程

响应等级与处置流程见表4所示。

表 4 响应等级与处置流程

触发条件	响应主体	处置时限	关键动作
Ⅰ级预警+多系统连锁报警	实验室负责人+外部救援	立即响应	1. 全员紧急疏散 2. 启动抑爆系统 3. 联动 119/120

Ⅱ级预警+单系统失效	安全管理员+技术团队	≤5min	1. 隔离危险区 2. 启用备用系统 3. 医疗组待命
Ⅲ级预警	值班人员	≤15min	1. 风险源排查 2. 受影响设备停机
Ⅳ级预警	现场操作人员	≤30min	1. 纠正违规行为 2. 系统确认复位

6.3.2 智能处置系统

在Ⅰ/Ⅱ级事件中，系统应自动执行包括但不限于以下动作：

——切断相关区域电源（通过智能断路器）

——关闭气路电磁阀（响应时间≤10s）

——启动应急通风（换气次数≥12次/h）

可通过辅助决策，如调用数字孪生模型生成三维处置方案、自动推送MSDS数据库中的化学品处置卡片、提供最近应急物资柜的AR导航路径（精度为±0.5m）等支持。

6.4 控制执行

6.4.1 响应等级与处置流程

执行设备分级管理见表5所示。

表5 执行设备分级管控表

类别	响应时间	控制精度	冗余要求
安全关键设备	≤100ms	±0.5%FS	双CPU+双通信通道
过程控制设备	≤10s	±1%FS	热备份模块
辅助执行设备	≤30s	离散量控制	无

6.4.2 通信协议

传感器设备应支持Modbus RTU等标准开放协议，过程控制设备应支持Modbus TCP/RTU、OPC UA等开放标准协议，视频监控设备应符合 GB/T 28181协议要求，实现视频流传输与控制，门禁设备应兼容韦根协议（WG26/WG34），通讯类执行设备应支持Modbus TCP/RTU、OPC UA、MQTT等多种开放标准协议，广播对讲设备应支持VoIP，无线设备应支持LoRaWAN 1.0.3或Wi-Fi6（802.11ax）及以上版本。

系统应配置支持异质协议之间的无缝转换的标准化协议转换网关，转换延迟≤50ms，协议转换过程中需保留原始数据标识与时间戳；网关应具备协议异常识别能力，当检测到协议帧错误、传输乱序时，立即触发本地告警并向平台层上报。

6.4.3 安全验证机制

应通过闭环反馈验证，执行结果应满足设备状态反馈与指令一致性（如阀门开度误差≤2%），环境参数变化符合预期（如排风启动后VOC浓度5分钟内下降30%）。

硬件应有容错机制，关键设备采用“三取二”表决机制（3个控制信号需至少2个一致）。

6.4.4 特殊情况的处理

针对毫秒级响应的极高危事件（如爆炸前兆、有毒气体瞬时泄漏），应启用独立、与常规控制网络物理隔离的应急通信链路，宜采用硬接线+无线备用的双链路模式，确保即使常规网络中断，紧急控制指令仍可无延迟传输；事后智能决策系统补发的分析报告，应同步记录应急通信链路的运行状态与指令传输日志。

6.5 智能复审

预警信息经核查与处置后，系统应自动对预警信息整改情况进行智能复审。

7 集成要求

7.1 硬件兼容性

应至少支持以下物理接口：

——RS-485/Modbus RTU（工业设备）

——PoE+（IEEE 802.3at，监控设备）

——M12防水连接器（危险区域设备）

——千兆以太网口（RJ45 高速数据交互）

——光纤接入口（传输距离≥10km）

无线通信需同时支持：

——LoRaWAN（Class C，传输距离≥1km）

——Wi-Fi 6（5GHz频段，MU-MIMO）

7.2 软件开放性

微服务架构应基于Docker容器化部署（Kubernetes编排）。

开放API：

——RESTful API（符合OpenAPI 3.0规范）

——GraphQL（用于知识图谱查询）

SDK支持：提供Python/Java/C#语言工具包

中间件应兼容：

——Kafka（消息队列）

——Redis（实时数据缓存）

——PostgreSQL（时序数据库）

推荐支持：Apache Spark（大数据分析）

8 运行管理要求

8.1 责任体系

8.1.1 实验室责任体系宜采用三级责任架构，见表 6 所示。

表 6 责任体系架构表

责任层级	角色定义	典型职责	技术权限
决策层	实验室负责人	应急预案审批/资源调配决策	系统最高权限(SYS_ADMIN)
执行层	实验室安全负责人	日常运维/异常处置	操作权限(OPERATOR)
操作层	设备责任人	分管设备点检/数据确认	受限权限(USER_RESTRICTED)
特殊角色	AI 监督员	负责机器学习模型的效果审计	无

8.1.2 可根据实际配置责任体系，展示框架式责任体系构架，清晰显示各级责任人、联系方式及其安全职责。应根据责任人角色配置责任清单，各级责任人可查询责任清单、执行期限等相关信息，可通过系统实现责任书签订。实时监控各责任人的责任落实情况，生成责任落实进度报告，对未按时限和内容要求落实安全责任的人员可自动提醒。

8.2 安全准入管理

8.2.1 人员准入管理

实验室应对出入实验区域的各类人员设定全权限、区域权限或临时权限，并根据岗位、风险进行动态调整。

出入实验区域的人员在授权前应经理论、实践培训考核。理论知识学习可通过创建多种类型题库，利用线上、线下及手机、PC机等终端开展，实践技能培训可采用实际操作、沉浸式体验等方式开展。题库内容还应覆盖风险识别、应急处置等核心内容。考核合格方可准入，培训考核记录留存应不少于2年。

实验室应对人员出入身份识别、权限验证、禁区闯入等情况进行监测，出入记录留存不少于90天，异常情况及时预警处置。

实验人员进入实验室前应签署安全承诺；外来人员实行报备审批、专人陪同、临时标识管理，严禁擅自进入高风险区域。

8.2.2 设备准入管理

实验室应建立设备准入清单及审批流程，审核重点包括设备合规证明、安全校验报告、操作人员资质等，未通过准入审核的设备不应放行。

高温、高压、强辐射等危险性较大的设备，严格出入管控及台账管理，必要时进行全流程轨迹智能监控，监控记录留存不少于90天。

危险性较大设备准入后应定期校验维护，建立安全档案。

8.2.3 项目准入管理

高风险实验项目立项前，应对项目方案、风险评估、危险源等安全内容进行逐级审批。

高风险实验项目实施前，应明确风险管控措施、应急处置方案、检测人员等，经授权方可在指定区域、时限内开展实验。

项目实施过程中加强过程监控与现场核查，发现违规或存在隐患时立即暂停；项目变更需重新审批授权，结束后及时注销并清理实验现场。

交叉学科、复合型项目，联合相关部门开展准入审核，明确安全责任及综合防控措施。

8.3 应急预案数字化管理

8.3.1 预案数字化实现

实验室宜采用数字化实现应急预案相关内容，可采用 BPMN 2.0 流程建模标准构建应急流程，包括事件触发器（传感器阈值/视频 AI 识别）、响应动作（设备控制/人员调度）、决策节点（人工确认/AI 自动判断）等。

应急预案宜建立知识图谱集成，包括构建预案-设备-人员关系图谱。

8.3.2 动态预案管理

宜及时记录预案详情、预案执行时间轴、触发原因、通知人、执行动作等信息，保留每次修订的对比、修订人数字签名、生效时间等记录。

宜基于历史处置数据自动推荐优化方案。

8.3.3 数字化演练

实验室宜采用数字化开展演练，演练应覆盖危化品泄漏、火灾、爆炸、人员中毒、仪器设备故障、辐射泄漏等典型应急场景，采用专业物理引擎实现灾害过程动态仿真（如火灾蔓延速度模拟误差≤0.5m/s）；支持多人协同实战化演练（满足≥5 人同时在线交互演练)。应自动记录并生成结构化处置报告，包含事件时间轴、处置过程视频片段、资源消耗清单等信息。

8.3.4 性能要求

预案加载时间≤10s，具备并发处理能力，本地缓存支持离线运行≥4h。

8.4 信息安全管理

8.4.1 信息网络应进行分域、分级设计，根据用户角色和业务需求合理划分安全域。各安全域之间应实施路由控制和带宽管理，保障网络资源的可用性和可靠性。应具备鉴权管理机制，通过 OAuth 、JWT 等方式，保证接口调用安全。

8.4.2 系统网络应按感知层、传输层、平台层、应用层等划分核心域，域间部署物理防火墙（支持状态检测、应用层过滤、VPN）。域内依据风险等级划分子域，子域间通过 VLAN 逻辑隔离，独立分配 VLAN ID，禁止跨 VLAN 二层互通。

8.4.3 传输层带宽预留≥50%，平台层带宽预留≥30%，避免高峰拥塞。域间数据流执行单向控制策略，仅允许下级域向上级域上传数据、上级域向下级域下发指令，禁止反向无规则访问。

8.4.4 实验室网络边界防护需部署下一代防火墙和入侵检测/防护系统（IDS/IPS），支持 Modbus、OPC UA、LoRaWAN 等工业协议对第三方终端进行接口集成，具备实时终端准入控制功能，能够识别、报警并实时阻断未经授权的终端设备，确保系统边界完整性。

8.4.5 应具备异常流量检测及实验室专用攻击特征库，检测准确率≥99%、攻击响应≤1s；外部访问实验室内部系统必须通过 VPN 专用通道，接入须采用多因素鉴别(MFA)并按用户角色精细化控制权限。基于应用层的入侵检测与防护能力，对攻击流量进行深度特征分析，支持对攻击源头、类型进行快速、精准的识别，并自动执行阻断、告警等安全响应措施。

8.4.6 应采用 VPN（虚拟专用网络）技术，确保远程访问过程中的数据机密性和完整性，对数据流实施加密传输，防止数据在传输过程中被监听、截获或篡改。

8.4.7 系统运行环境宜符合国产化及信创适配要求。

8.4.8 数据隐私保护应符合 GB/T 35273 规定，数据脱敏处理后存储。

8.5 通讯管理

8.5.1 实验室通讯应采用多层级网络部署，并留有冗余设计；

8.5.2 应具备与实验室内外部 ERP、MES、CRMS 等系统进行数据通信的功能；数据通信 API 接口应具备鉴权管理机制。跨系统数据通信应建立数据交互接口清单，内容至少包括接口名称、协议类型、数据格式、访问权限、传输频率、审计日志、异常告警等信息。

8.5.3 与实验室中仪器设备通信的总体要求、网络通信模式和命令格式应符合 GB/T 39556 的规定；与气候环境试验设备实现数据通信，其通信数据接口应符合 GB/T 39555 的规定。

8.5.4 通讯协议应适用于设备控制、应急广播、移动终端等应用场景。应急通讯应支持数字集群对讲、声光报警等多模态通信和全断电、电磁干扰、网络攻击等极端场景通讯。

8.6 运维管理

8.6.1 实验室安全监测与智能管控系统中所涉及的各类传感器应定期核查。

8.6.2 实验室安全监测与智能管控系统的数据传输、通讯和信息推送等功能应定期进行测试。

9 评价与改进

9.1 系统效能评估指标

核心评估指标体系应包括监测能力、响应效能、系统可靠性、安全防护（漏洞修复率）、能效表现等。通过自评、第三方评估、事件触发评估等进行定期评估。

9.2 持续改进机制

应形成“效果监控-问题发现-根本原因分析-改进方案制定-方案验证-应用”闭环改进流程。

每项改进措施宜形成标准化操作、故障代码库更新、案例教学视频（适用时）等。

参 考 文 献

[1] GB/T 3836.1—2021 爆炸性环境 第1部分：设备 通用要求
[2] GB/T 22117—2018 信用基础术语
[3] GB/T 23792—2009 信用标准化工作指南
[4] GB/T 27476.1-2014 检测实验室安全 第1部分：总则
[5] GB/T 27025-2019 检测和校准实验室能力的通用要求
[6] GB/T 36342-2018 智慧校园总体框架
[7] GB/T 37092 信息安全技术 密码模块安全要求
[5] DB 51/T 3106—2023 化学实验室安全应急智慧系统建设指南