

T/WEA

团 体 标 准

T/WEA XXXX—2026

建筑工程安全风险智能预警系统建设规程

Code of practice for construction of intelligent safety risk early
warning systems for building engineering

(征求意见稿)

2026 - XX - XX 发布

2026 - XX - XX 实施

中国智慧工程研究会 发布

目 次

前言 III

引言 V

1 范围 1

2 规范性引用文件 1

3 术语和定义 1

4 总体要求 3

5 建设规划与需求分析 4

6 数据要求与接口规范 5

7 风险模型与阈值管理 8

8 预警发布与闭环管理 9

9 网络与信息安全要求 10

10 部署与运维 10

11 系统评价与验收要求 11

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。

本文件由中国智慧工程研究会提出并归口。

本文件起草单位：

本文件主要起草人：

全国团体标准信息平台

引 言

建筑工程具有参建主体多、工序交叉密集、作业环境动态变化快、现场不确定性强等特征，安全风险呈现“多源耦合、链式传导、突发性与隐蔽性并存”的典型规律。传统安全管理以人工巡查、经验判断与事后处置为主，容易受到人员能力、巡查频次、信息滞后与现场复杂条件的限制，难以及时识别高风险作业的临界状态与风险演化趋势，导致隐患发现不及时、预警不精准、处置不闭环等问题，最终影响工程安全生产目标的实现。

随着物联网、BIM、视频智能分析、边缘计算、云平台、机器学习与数字孪生等技术在施工现场的应用深化，建设“建筑工程安全风险智能预警系统”已成为提升工程安全治理能力的重要手段。该系统通过对人、机、料、法、环关键要素的多源数据采集与融合，结合风险模型、阈值规则与预测算法，实现隐患识别、风险分级、预警发布、联动处置与闭环核销，从而将安全管理的“事后处置”前移至“事前预警”与“过程控制”。

然而，现阶段不同项目在系统建设中普遍存在建设目标不清、数据标准不统一、风险模型口径不一致、预警阈值设置随意、联动机制缺失、权限与审计薄弱、与既有管理流程脱节等问题，导致系统“能看不能用、能报不能控、能控不能闭环”，难以形成可复制、可推广的工程化体系。为规范建筑工程安全风险智能预警系统的规划、设计、建设、部署、运行与评价，提升系统的适用性、可靠性与可持续运维能力，本文件从总体架构、功能与性能、数据与接口、安全与隐私、模型与阈值、预警分级与响应、运维与评价等方面提出统一要求，为建设单位、施工单位、监理单位、系统集成方与平台运维方提供可执行的技术依据。

本文件强调“业务牵引、风险导向、数据驱动、闭环治理”的建设理念，倡导以风险场景为单元构建“监测—识别—预警—处置—核验—复盘”的全流程机制，同时兼顾不同规模项目与不同数字化基础条件，提供可分级实施、可渐进迭代的建设路径，促进系统建设与施工安全管理体系深度融合。

建筑工程安全风险智能预警系统建设规程

1 范围

本文件规定了建筑工程安全风险智能预警系统的总体要求、建设规划与需求分析、数据要求与接口规范、风险模型与阈值管理、预警发布闭环管理、网络与信息安全要求、部署运维及系统评价与验收要求等内容。

本文件适用于房屋建筑工程、市政基础设施工程等施工阶段（含基坑、主体结构、装饰装修、机电安装等）安全风险智能预警系统的新建、改建、扩建与运维管理，也适用于以项目为单位的专项预警子系统（如高支模、深基坑、起重吊装、临电、消防等）的建设与集成。勘察设计阶段与运营维护阶段可参照执行。

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/T 2887 计算机场地通用规范
GB/T 22239 信息安全技术 网络安全等级保护基本要求
GB/T 25069 信息安全技术 术语
GB/T 26224—2010 信息技术 软件生存周期过程 重用过程
GB/T 31167 信息安全技术 云计算服务安全指南
GB/T 35273 信息安全技术 个人信息安全规范
GB/T 37988 信息安全技术 数据安全能力成熟度模型

3 术语和定义

下列术语和定义适用于本文件。

3.1

安全风险 safety risk

在一定条件下，危险源导致人员伤害、财产损失或环境破坏的可能性与后果严重性的组合。

3.2

智能预警 intelligent warning

基于多源数据与风险模型，对风险状态进行识别、预测或判定，并按预设规则输出分级预警信息的过程。

3.3

安全风险智能预警系统 smart safety risk early-warning system

以建筑工程施工现场为对象，综合采集、融合与分析安全相关数据，实现风险识别、分级预警、联动处置与闭环管理的信息系统。

3.4

风险场景 risk scenario

在特定工序、区域或作业活动中，危险源、触发条件与暴露对象组合形成的可描述、可监测、可评价的风险单元。

3.5

预警阈值 warning threshold

用于触发预警的指标边界值或规则集合，可为固定阈值、动态阈值或模型输出阈值。

3.6

事件 event

系统识别或外部上报的具有安全意义的客观发生或状态变化，如违规进入、倾角异常、荷载超限、烟火识别等。

3.7

告警 alarm

系统对异常指标或事件的即时提示信息，通常用于提示需关注的状态变化。

3.8

预警 warning

系统依据风险评估结果输出的分级风险提示信息，通常包含风险等级、影响范围、处置建议与响应时限。

3.9

闭环管理 closed-loop management

从发现问题到处置、核验、销项与复盘的全过程记录与追踪机制，确保问题“可追溯、可核验、可考核”。

3.10

边缘计算 edge computing

在靠近数据源侧进行数据处理、分析或推理的计算模式，用于降低时延、减轻网络负载并提升现场连续运行能力。

3.11

多源数据融合 multi-source data fusion

对传感器、视频、人员定位、设备运行、BIM、进度计划、气象等数据进行关联、对齐、融合与一致性处理的过程。

3.12

服务水平协议 service level agreement, SLA

是一种正式的协议或合同，定义了服务提供者与客户之间的服务标准、质量、可用性等指标。它明确了服务的性能要求、服务交付的时间框架、服务中断的响应方式等，以确保服务符合预期标准，并为双方提供明确的责任界定。

4 总体要求**4.1 建设原则**

系统建设应遵循以下原则：

- a) 风险导向：以高风险作业与事故易发环节为重点，优先覆盖深基坑、高支模、起重吊装、脚手架、临时用电、动火作业、有限空间等场景；
- b) 业务融合：与施工单位安全管理制度、监理旁站与验收流程、隐患排查治理体系相衔接，形成可执行的闭环流程；
- c) 数据驱动：明确数据口径、采集范围、采集频率、质量控制与主数据管理，保证模型与阈值可解释、可校准；
- d) 分级实施：按项目规模与数字化基础条件分阶段建设，先“可用”后“好用”，支持渐进迭代；
- e) 安全可信：落实网络安全、数据安全与个人信息保护要求，确保系统可用性、完整性与可审计性；
- f) 可运维：建立运维组织与制度，明确SLA、故障处置、备份恢复、版本管理与持续优化机制。

4.2 系统总体架构

系统总体架构宜采用“感知层—边缘层—平台层—应用层—集成与接口层”的分层设计，支持多项目、多标段、多参建单位的统一管理与分级授权。系统总体架构应与图1所示的分层结构相符，并支持多项目、多标段的分级授权管理。

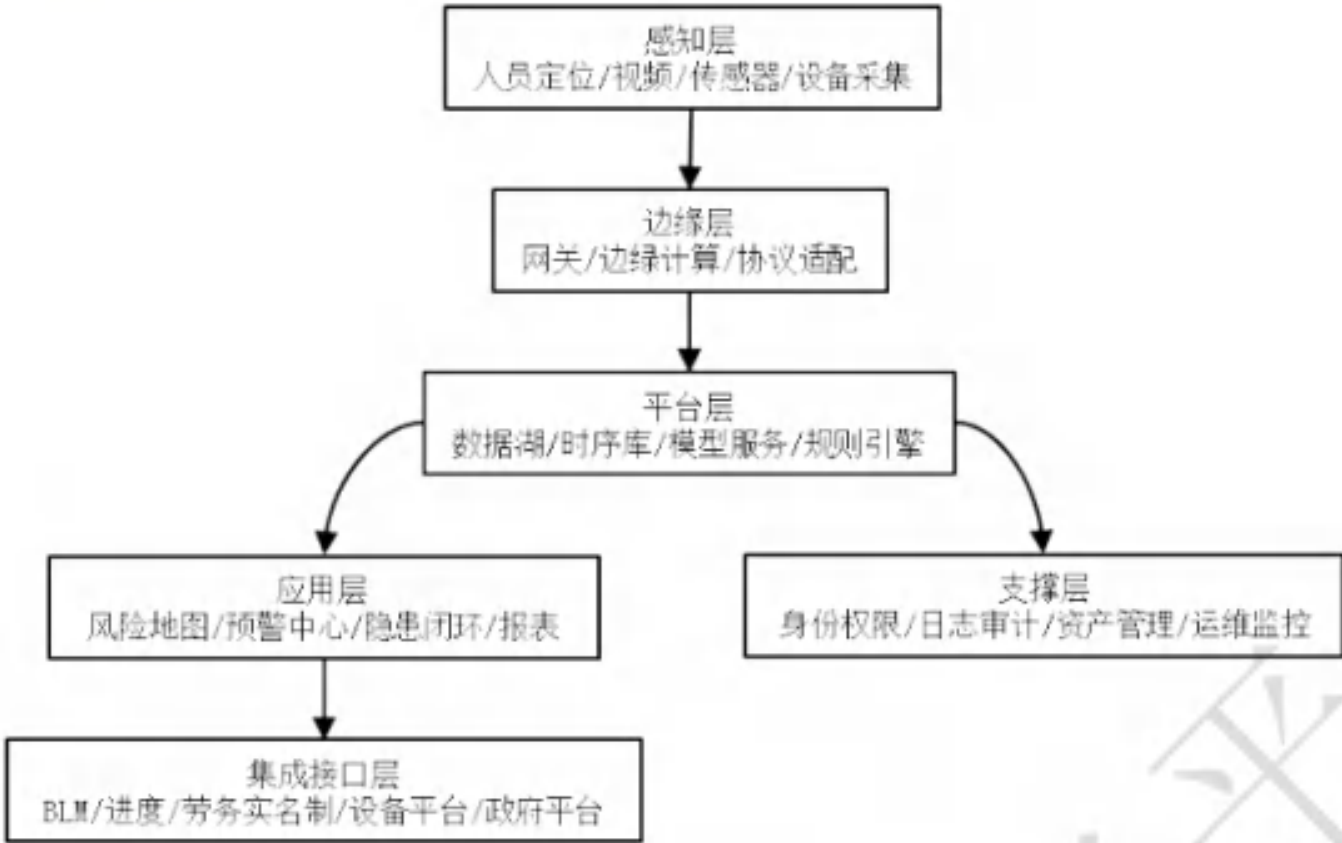


图1 系统总体架构

4.3 功能总体要求

系统应至少具备以下功能能力：

- a) 风险场景管理：风险库、场景库、指标库、阈值库、处置预案库的维护与版本控制；
- b) 数据采集与融合：多源数据接入、时间同步、空间关联、数据清洗与质量校验；
- c) 风险识别与评估：规则判定、模型推理、趋势分析与风险分级；
- d) 预警发布与联动：多渠道推送（平台、APP、短信/语音、广播等可选）、分级响应、联动处置；
- e) 闭环治理：工单派发、处置记录、现场核验、销项归档、统计分析与复盘；
- f) 可视化：风险地图、热力分布、视频联动、BIM联动（可选）与关键指标看板；
- g) 运维与审计：设备在线率、数据质量、模型健康度、告警/预警命中率、日志审计与报表。

系统应以风险场景为单元组织监测要素与预警输出，风险场景分类与典型监测要素应符合表1的要求，项目可结合实际扩展细化。

表1 风险场景分类与典型监测要素

场景类别	典型风险点	监测数据类型	预警输出
深基坑	围护变形、支撑轴力异常、渗漏水	位移/倾角/轴力/水位/视频	变形超限预警、趋势预警
起重吊装	超载、碰撞、风速过大、人员闯入	载荷/力矩/黑匣子/风速/定位/视频	超载预警、禁入预警
高支模	立杆沉降、水平位移、超载	沉降/位移/荷载/视频	稳定性预警、超载预警
临时用电	漏电、过载、私拉乱接	漏保状态/电流/温度/巡检	漏电预警、过载预警
动火作业	未审批动火、烟火异常、气体超限	作业票/视频/气体传感	违规动火预警、气体超限预警

5 建设规划与需求分析

5.1 需求调研

系统建设前应开展需求调研，至少包括 项目概况、施工组织与关键工序、重大危险源清单、现有安全管理流程、既有信息化系统与数据源、现场网络与供电条件、参建单位职责边界、预警响应组织与资源配置等。需求调研应输出可执行的需求说明书，包含功能需求、性能需求、数据需求、安全需求与运维需求。

5.2 风险场景建模要求

风险场景建模应以“危险源—触发条件—暴露对象—控制措施—预警阈值—处置动作”为主线，形成可配置的场景模板。场景模板应支持按工程部位、工期阶段、作业班组、设备台账与地理围栏等维度进行参数化配置，并支持版本升级与回滚。

5.3 指标体系与预警分级原则

系统应建立统一指标体系，指标宜包含：状态类指标（如位移、沉降、风速）、行为类指标（如闯入、未佩戴PPE）、设备类指标（如超载、故障码）、管理类指标（如未审批作业、未验收投入使用）与环境类指标（如高温、扬尘、气体浓度）。预警分级宜与项目安全管理响应机制匹配，做到“等级清晰、处置明确、时限可控、责任可追溯”。

预警等级划分、响应要求及处置时限应与表2相一致；项目可根据风险等级与管理资源配置进行收严，但不得降低响应要求。

表2 预警等级、处置要求与时限

预警等级	风险含义	响应要求	处置时限
一级	重大风险，可能导致群死群伤或重大事故	立即停工/停机，启动应急处置与现场管控	立即（≤10 min）
二级	较大风险，短期内可能演化为重大风险	立即整改与复核，必要时局部停工	≤30 min
三级	一般风险，需要及时纠正	限时整改、加强监测与复核	≤4 h
四级	关注提示，存在苗头或管理缺口	提醒与跟踪，纳入巡查与复盘	≤24 h

6 数据要求与接口规范

6.1 数据总体要求

系统数据体系应满足“可采集、可理解、可对齐、可追溯、可复用”的要求，支撑风险识别、预警分级、处置联动与闭环核验。数据应覆盖人员、设备、环境、结构与管理过程等关键要素，并满足以下要求：

- a) 一致性：数据口径、单位、精度、坐标系、时间基准应统一；
- b) 完整性：关键风险场景所需数据不得缺失，缺失应有补采或降级策略；
- c) 准确性：采集误差、漂移、异常值应受控，具备校准与纠偏机制；
- d) 及时性：满足预警业务的时效需求，关键场景应满足秒级或分钟级更新；
- e) 可追溯性：原始数据、处理过程、模型版本、阈值版本与处置记录应可追溯。

数据体系应以风险场景为牵引进行规划，风险场景所需数据类别、关键字段与质量指标应按表3执行。系统数据类别、关键字段与质量指标应符合表3的要求。

6.2 数据分类与主数据管理

6.2.1 数据分类

系统数据宜分为：

a) 感知数据：传感器（位移、沉降、倾角、应力、轴力、风速、气体等）、设备运行数据（起重设备黑匣子、功率/载荷/力矩等）、视频与图像、人员定位等；

b) 业务管理数据：作业票（动火、高处、有限空间等）、危大工程验收、教育培训、班组与人员资质、隐患整改工单等；

c) 工程基础数据：项目组织结构、标段/楼栋/区域、设备台账、人员实名制、施工进度计划、BIM模型（可选）；

d) 衍生数据：清洗对齐后的时序数据、特征数据、规则判定结果、模型推理结果、风险评分与预警记录等。

6.2.2 主数据对象

系统应建立主数据管理机制，主数据至少包括：项目、标段、区域/楼栋、工点、危险源/风险场景、设备、人员、作业票类型、预警类型、处置预案、阈值版本与模型版本。主数据应具备唯一编码与版本控制，并支持跨系统对齐。

6.3 数据编码、标识与字典

6.3.1 编码规则

系统应制定统一编码规则，至少满足唯一性、可扩展性与可读性要求。建议采用“项目—标段—区域—对象类型—序号—版本”的组合编码。与BIM联动时，构件编码与系统编码映射关系应维护在统一映射表中，并支持变更追踪。

6.3.2 数据字典

系统应建立数据字典，至少包含字段名称、含义、单位、精度、取值范围、缺失处理规则、采集频率、来源系统/设备、校准周期与责任单位。数据字典应纳入配置管理，并与接口文档保持一致。

6.4 时间同步与空间关联

6.4.1 时间同步

系统应采用统一时间基准，平台层、边缘层、采集终端应具备时间同步能力。对秒级预警场景（如人员闯入、吊装碰撞风险）应明确最大允许时钟偏差，并在数据接入时记录时间戳来源（设备时间/网关时间/平台时间）。

6.4.2 空间关联

系统应支持将数据与工程空间对象关联，包括：区域围栏（地理围栏）、楼层/轴线、工点、设备作业半径与危险区边界等。空间关联规则应与现场布设方案一致，并支持随施工阶段动态调整。

6.5 数据质量控制

系统应具备数据质量监控与治理能力，至少包括：

- a) 缺失监测：关键数据缺失报警与降级策略；
- b) 异常检测：突变、漂移、越界、噪声过大等自动识别；
- c) 校准管理：传感器校准计划、校准记录与校准到期提醒；
- d) 数据修复：可追溯的补采、插值或剔除策略（不得篡改原始数据）；
- e) 数据质量指标：在线率、有效率、延迟、丢包率、异常占比等。

6.6 接口与协议要求

6.6.1 接入方式

系统应支持设备直连、边缘网关接入与第三方平台对接等方式。对视频、时序传感与设备黑匣子数据应优先采用边缘接入以降低时延并提升现场连续运行能力。

6.6.2 协议与格式

接口应采用开放、可维护的协议与数据格式，接口文档应包含：认证方式、调用频率限制、错误码、重试策略与幂等要求。数据格式宜采用JSON/CSV/Protobuf等，时序数据应明确采样频率与聚合规则。

6.6.3 接口安全

接口应支持身份认证、访问控制、传输加密与调用审计。对涉及个人信息与敏感数据的接口，应进行最小化字段输出与脱敏处理，并提供授权与撤销机制。

表3 数据类别、关键字段与质量指标

数据类别	关键字段示例	采集/更新频率建议	质量指标建议	备注
人员定位	person_id、position、 zone_id、timestamp	1 - 5 s	在线率≥98%，时延 ≤3 s	关键用于禁入与聚集 风险
视频智能	camera_id、event_type、 confidence、snapshot、 timestamp	事件驱动	误报率可评估；事件 留痕可追溯	需记录算法版本
基坑监测	point_id、displacement、 rate、timestamp	1 - 10 min	有效率≥95%，漂移 可识别	支持趋势预警

表3 数据类别、关键字段与质量指标（续）

数据类别	关键字段示例	采集/更新频率建议	质量指标建议	备注
起重设备	device_id、load、moment、wind、alarm_code、timestamp	1 - 10 s	丢包率≤1%，时延≤2 s	吊装联动优先
临电监测	circuit_id、current、temp、leak_state、timestamp	10 - 60 s	异常可识别，缺失可告警	支持电气火灾预警
作业票/验收	permit_id、type、status、approver、valid_time	状态变更	完整性100%，可审计	管理类预警依据

7 风险模型与阈值管理

7.1 风险计算总体要求

系统应采用“规则判定+模型评估+趋势预测（可选）”的组合策略。对强监管、可明确量化阈值的场景（如基坑变形、风速、轴力）宜优先采用阈值规则；对行为识别与复杂耦合场景（如人员闯入、违规作业组合、工序交叉风险）可采用模型评估或知识图谱规则。风险计算过程应可解释、可追溯，并记录输入数据版本、阈值版本与模型版本。

7.2 规则引擎要求

规则引擎应支持：

- a) 多条件组合（AND/OR）、时间窗、频次、持续时间、空间围栏、设备状态联动；
- b) 多级触发（告警→预警→升级）、解除条件与迟滞机制（避免抖动）；
- c) 规则版本管理与灰度发布；
- d) 规则命中审计与回放（支持事后复盘）。

7.3 模型服务要求

采用机器学习/统计模型时，应满足：

- a) 模型训练数据来源合法合规，具备数据标注与质量说明；
- b) 模型评估指标明确（准确率、召回率、误报率、漏报率等），并与工程安全目标匹配；
- c) 模型上线前应进行离线验证与现场试运行验证；
- d) 模型应支持版本管理、回滚与健康度监测；
- e) 对关键安全决策输出应提供解释信息（关键特征、置信度、触发原因摘要等）。

7.4 阈值设定与校准

阈值应分为固定阈值、动态阈值与模型阈值：

- a) 固定阈值应基于规范标准、专项方案、设备说明书或经论证的控制指标；

b) 动态阈值可基于施工阶段、环境条件、设备工况与趋势特征进行自适应调整，但应保留上限/下限保护；

c) 模型阈值应通过现场数据进行校准，明确目标误报率/漏报率。

阈值调整应履行审批流程，并记录调整原因、调整人、调整时间、影响范围与生效版本。

8 预警发布与闭环管理

8.1 预警流程要求

系统应建立“识别—分级—发布—响应—处置—核验—销项—复盘”的闭环流程。预警流程与闭环机制见图2，预警闭环管理流程应符合图2的要求。

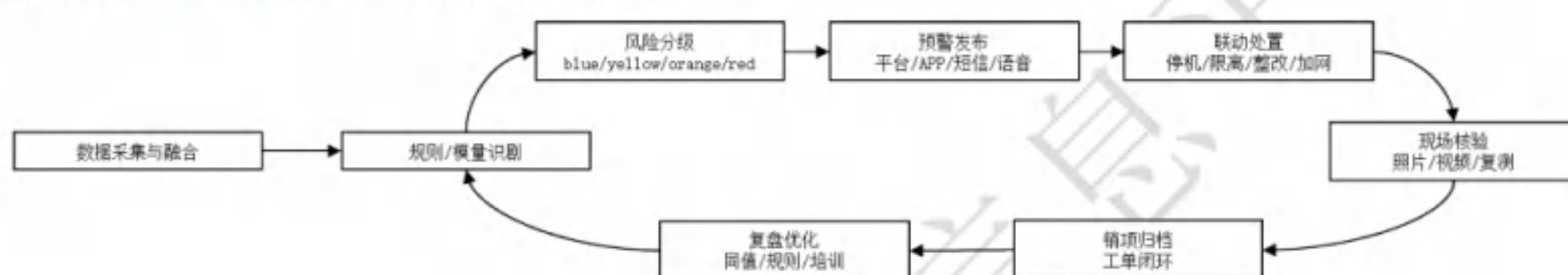


图2 预警闭环管理流程图

8.2 预警发布要求

8.2.1 发布渠道

系统应至少支持平台端与移动端发布；对一级、二级预警宜支持短信、语音或现场广播等强提醒方式，并支持多角色、多组织的分级推送。

8.2.2 发布内容

预警信息应包含：预警等级、预警类型、时间、位置/区域、关联对象（人员/设备/工点）、触发原因摘要、建议处置措施、响应时限与责任人/责任单位。对视频类预警宜附关键截图或短视频留痕。

8.2.3 去重与合并

系统应具备预警去重、合并与升级机制，避免同一风险重复刷屏；当风险持续或加剧时，应按规定升级预警等级，并记录升级链路。

8.3 联动处置要求

系统应支持与现场控制措施联动，如：设备停机/限位、电子围栏告警、门禁联动、广播提示等。联动动作应具备权限控制与审计，避免误触发造成生产损失或新的安全风险。对自动联动的高影响动作（如停机），应设置人工确认或双重确认机制，并规定异常情况下的手动解除流程。

8.4 闭环工单管理

系统应提供闭环工单能力：

- a) 工单生成：预警触发自动生成工单或由管理人员确认生成；
- b) 工单派发：按责任矩阵派发到责任人/班组/分包单位；
- c) 处置记录：处置过程与结果需上传文字说明、照片/视频、测量数据或第三方记录；
- d) 核验与销项：核验人独立确认后方可销项，销项需记录核验依据；
- e) 统计与考核：支持按标段、分包、场景、时间维度统计闭环率、超时率与重复发生率。

8.5 复盘与持续改进

系统应支持对典型预警事件进行复盘，包括 触发原因、响应效率、处置质量、阈值合理性、误报漏报分析与纠正措施，并形成可追溯的优化闭环（规则/阈值/模型/流程/培训）。

9 网络与信息安全要求

9.1 等级保护与合规要求

系统应满足网络安全等级保护相关要求，结合项目规模、数据敏感性与对外联通情况确定安全保护等级并落实建设与测评。涉及个人信息处理的，应遵循最小必要原则与合法合规要求，明确告知、授权与访问控制机制。

9.2 身份认证与权限管理

系统应采用统一身份认证与分级授权管理，至少支持 建设单位、总包、分包、监理、运维与监管接口等角色。权限应按最小权限原则配置，关键操作（阈值调整、规则发布、联动控制、数据导出、账号管理等）应采用双因素认证或等效强认证，并全量审计。

9.3 数据安全

系统应对数据进行分类分级管理，至少包括 采集数据、个人信息、视频图像、风险评估结果、工单记录与审计日志。应采取访问控制、传输加密、存储加密、脱敏与水印等措施 应建立数据备份、恢复与留存策略，并规定留存期限与销毁流程。

9.4 日志审计与安全监测

系统应记录登录、访问、配置变更、阈值调整、规则发布、模型版本切换、联动动作触发、数据导出等关键行为日志。日志应具备防篡改能力（可通过集中存储、签名或等效机制实现），并支持安全事件告警与追溯。

10 部署与运维

10.1 部署架构

系统部署可采用本地化部署、云部署或混合部署。涉及现场连续运行与低时延场景的，宜采用“边缘+平台”的混合部署方式，并明确断网/弱网情况下的降级策略。

10.2 运维组织与服务水平协议

应明确建设单位、总包、系统集成方与运维方的职责边界，建立SLA指标，至少包括：系统可用性、数据在线率、预警时延、故障响应时间、恢复时间目标、备份频率与演练频次等。运维应覆盖应用、平台、网络、终端设备与算法模型等全栈要素。

10.3 设备管理与巡检

系统应对摄像机、网关、传感器、定位基站、服务器与网络设备建立资产台账，包含型号、位置、责任人、校准周期、维护记录与寿命管理。应具备在线状态监测与离线告警能力，并规定现场巡检频次与备件策略。

10.4 版本管理与变更控制

系统应建立版本发布、灰度验证、回滚与变更审批机制。涉及阈值、规则、模型与联动策略的变更应纳入变更控制，变更后应开展回归测试与现场验证，并保留变更记录与影响评估结论。

11 系统评价与验收要求

11.1 验收总体原则

系统验收应以“可用、可信、可控、可闭环”为目标，覆盖功能、性能、数据质量、信息安全、运维能力与业务融合效果。验收应结合项目风险场景覆盖范围，采用“场景化验收”的方式进行，即以典型场景完成从识别到闭环的全流程验证。

11.2 验收内容

验收宜至少包括：

- a) 架构与部署符合性：与图1所述分层架构一致，满足现场网络与边缘部署要求；
- b) 场景覆盖：危大工程与高风险场景覆盖满足建设目标，场景配置与表1一致或经扩展论证；
- c) 预警分级与响应：预警等级与响应机制与表2一致；
- d) 数据质量：关键数据在线率、时延、有效率满足表3要求或项目约定指标；
- e) 闭环能力：按图2完成“触发—派单—处置—核验—销项—复盘”全流程演练；
- f) 安全合规：权限、审计、加密与备份恢复满足第9章要求；
- g) 运维能力：SLA、监控告警、巡检校准、备份演练与变更控制机制齐备。

11.3 验收方法

验收方法宜包含：文档审查、现场核查、联调测试、压力与稳定性测试、场景化演练、抽样核验与访谈评估。验收应形成报告，包含问题清单、整改闭环与最终结论。

11.4 运行评价与持续评估

系统上线后应开展运行评价，评价指标宜包括：预警命中率、误报率、漏报事件回溯、平均响应时长、闭环率、超时率、重复发生率、设备在线率、数据延迟等。运行评价结果应作为阈值/规则/模型优化与管理制度完善的依据。