|  |  |
| --- | --- |
| ICS | 35.240.99 |
| CCS | |  | | --- | | D:\000000部门项目\09标准化插件开发\程序源代码\StandardEditor_ShanDongKeXieYuan\团标首页面字母T.pngD:\000000部门项目\09标准化插件开发\程序源代码\StandardEditor_ShanDongKeXieYuan\团标首页面字母T后面的反斜杠.png XJBX |   P 09 |

西安市计量标准检测认证协会团体标准

T/XJBX 0037—2025

道路桥梁施工安全隐患智能识别

与大数据风险防控规范

Specification for intelligent identification of safety hazards and big data-based risk prevention and control in road and bridge construction

2025 - XX - XX发布

2025 - XX - XX实施

西安市计量标准检测认证协会  发布

目次

[前言 III](#_Toc200377646)

[引言 V](#_Toc200377647)

[1 范围 1](#_Toc200377648)

[2 规范性引用文件 1](#_Toc200377649)

[3 术语和定义 1](#_Toc200377650)

[4 总体要求 2](#_Toc200377651)

[5 安全隐患智能识别 3](#_Toc200377652)

[6 风险等级划分与分级响应 3](#_Toc200377653)

[7 安全隐患智能识别 4](#_Toc200377654)

[8 大数据风险分析与预警 5](#_Toc200377655)

[9 安全处置与应急联动 6](#_Toc200377656)

[10 系统运行与运维管理 7](#_Toc200377657)

[11 测试与验收方法 8](#_Toc200377658)

[12 应用推广与后续维护 9](#_Toc200377659)

1. 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。

本文件由西安市计量标准检测认证协会提出并归口。

本文件起草单位：绍兴市轨道交通集团有限公司、山东省威海市公路事业发展中心、宁波景业建设有限公司、山东黄河工程集团有限公司、邹城市交通运输局、绍兴市交通运输行政执法队、浙江绍金高速公路有限公司、瑞金市宏都检测技术开发有限公司、承德公路工程监理有限责任公司、辽宁省交通建设管理有限责任公司、平泉市交通运输局、河北锐驰交通工程咨询有限公司、葛洲坝集团交通投资有限公司。

本文件主要起草人：方建华、黄鲁明、陈友富、赵忠举、李红焱、张博文、冯鸣、陈步榕、孙志龙、李雨衡、刘一晖、武晓琳、李阳阳、李培培、王军。

1. 引言

随着交通基础设施建设的持续推进，道路桥梁施工规模和复杂性不断提高，施工现场的安全管理面临诸多挑战。传统的安全隐患识别与处理手段存在滞后性和主观性，难以有效应对多源异构数据、高风险作业场景及复杂作业流程带来的不确定性。近年来，人工智能、物联网与大数据技术在工程管理领域的快速发展，为施工安全管控提供了新的手段和思路。

本文件旨在推动智能识别技术与大数据风险防控体系在道路桥梁施工过程中的标准化应用，通过构建集感知、识别、预警、处置于一体的智能化安全管理框架，实现对施工现场人员行为、机械运行、结构状态及环境条件等关键风险因素的实时监测与分析。同时，通过大数据技术手段，构建多维度、动态化的风险评估模型，提升安全管理的前瞻性和科学性。

本文件的制定适应了智能建造的发展趋势，有助于提升道路桥梁施工阶段的本质安全水平，促进风险防控模式由“事后处置”向“事前预警”转变。规范内容既具有可操作性，也为行业智能化转型提供了技术基础和标准支持。

道路桥梁施工安全隐患智能识别

与大数据风险防控规范

* 1. 范围

本文件规定了道路桥梁施工过程中应用智能识别与大数据技术开展安全隐患排查与风险防控的总体要求、安全隐患智能识别、风险等级划分与分级响应、安全隐患智能识别、大数据风险分析与预警、安全处置与应急联动、系统运行与运维管理、测试与验收方法及应用推广与后续维护等内容。

本文件适用于新建、改建和扩建等各类道路桥梁工程施工阶段，涉及施工单位、监理单位、安全管理部门及信息化技术服务单位在实施智能安全管理与数据风险分析时的工作流程和技术应用。也可为其他交通基础设施项目的施工安全智能化管理提供参考。

* 1. 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 35484—2021 土方机械和移动式道路施工机械 工地数据交换

GB/T 39559—2020 城市轨道交通设施运营监测技术规范

GB/T 36074—2019 信息技术服务 服务管理

* 1. 术语和定义

下列术语和定义适用于本文件。

智能识别 intelligent recognition

基于人工智能算法，利用图像识别、语音识别、行为分析等技术手段，对施工现场人员、设备、环境等要素进行自动化感知、分析与识别的过程。

安全隐患 safety hazard

在施工过程中可能导致人身伤害、设备损坏或环境破坏的潜在不安全状态、行为或管理缺陷。

风险预警 risk early warning

通过数据模型和算法对潜在安全风险进行提前识别和等级划分，并触发相应响应机制的技术手段。

安全行为识别 safety behavior recognition

通过视频监控、传感器等方式，对施工人员的不规范作业行为进行实时识别与判断的过程。

多源异构数据 multi—source heterogeneous data

来源不同、格式不一的数据集合，如图像、视频、传感器数据、日志信息、结构监测数据等，用于构建施工安全风险分析的基础数据库。

* 1. 总体要求
     1. 系统构建原则

系统应按照“感知全面、识别精准、响应迅速、闭环可控”的理念进行设计，具备全场景覆盖、多模块集成、多源数据融合能力。建设过程中应遵循以下原则：

1. 兼容性与开放性：系统结构应具备良好的接口兼容性，便于与现有监控平台、安全管理系统、工程信息模型（BIM）等集成；
2. 实时性与可追溯性：应确保隐患识别与预警具有足够的时效性，关键环节全流程数据可回溯；
3. 安全性与稳定性：在数据通信、访问控制、故障容错等方面，系统应具备严密的安全防护和持续运行能力。
   * 1. 功能模块配置

系统应配置以下核心功能模块，以支撑施工安全管理需求：

1. 现场感知模块：实现对人员、设备、材料、环境等实时采集；
2. 图像与行为识别模块：具备图像识别、安全帽识别、越线行为识别等功能；
3. 风险评估与预警模块：融合模型算法，对安全隐患进行自动识别、等级划分并发出预警；
4. 大数据分析模块：对历史数据进行分析建模，为管理决策提供依据；
5. 可视化展示模块：以图表、地图、视频联动等方式展现风险状态和应急响应。
   * 1. 数据集成与管理要求

系统应建设统一数据平台，实现感知数据、监测数据、业务数据的融合集成，重点满足以下要求：

1. 数据标准统一，具备清晰的数据结构与标签体系；
2. 建立权限分级机制，保障数据存储、使用与共享的规范性；
3. 支持与外部监管、工程信息化平台的数据互通。
   1. 安全隐患智能识别
      1. 识别对象与范围

安全隐患识别应覆盖施工全周期的关键要素，包括但不限于：

1. 作业人员违规行为；
2. 机械设备异常运行；
3. 材料堆放与临边防护不规范；
4. 特殊作业区域（深基坑、高支模、隧道、桥梁高墩）危险源监测；
5. 气象、地质等外部环境因素诱发的潜在安全风险。
   * 1. 技术路径

智能识别可结合多种技术路径展开，常见方式包括：

1. 视频图像识别技术：通过部署AI摄像头，利用目标检测、行为识别等算法对人员行为与现场状态进行监测；
2. 物联网感知技术：基于传感器实时采集温度、湿度、位移、倾角、气体浓度等数据，识别异常状态；
3. 边缘计算设备部署：在现场设置边缘计算网关，实现本地快速分析与初级预警；
4. 大数据模型训练：基于历史隐患案例库训练识别模型，提升模型在新场景下的泛化能力；
5. 多源信息融合分析：结合视频、传感器、位置与作业信息，实现跨维度风险评估。
   * 1. 识别准确率评估与优化

为确保识别结果可靠，系统应定期开展识别准确率评估，评估内容包括：

* 1. 检出率与误报率；
  2. 典型场景识别成功率；
  3. 模型迭代周期与优化算法响应速度。

在评估基础上，持续迭代模型参数，优化特征提取策略，提高系统稳定性与适应性。

* 1. 风险等级划分与分级响应
     1. 风险等级划分原则

风险等级划分应综合考虑风险事件发生的可能性、影响程度与可控性，采用定性与定量相结合的方法，设定多级风险区分标准。典型划分具体内容见表1。

1. 风险等级划分表

| 风险等级 | 风险描述 | 主要特征 | 响应措施概述 |
| --- | --- | --- | --- |
| Ⅰ级（重大风险） | 极易导致人员伤亡、重大财产损失或社会影响，需立即处置 | 现场存在高能设备失控、高空坠落、基坑失稳等典型高危情形 | 启动紧急预案，立即停工，封闭区域，上报主管单位并启动问责机制 |
| Ⅱ级（较大风险） | 可能引发人员受伤、设备损毁，或对工程进度产生显著干扰 | 如支护失效趋势明显、吊装作业指令异常、监测预警频繁触发等 | 限期整改，调整作业工艺，实施专人专岗盯控，汇报整改进展 |
| Ⅲ级（一般风险） | 存在一定不规范施工行为，尚未造成实际损害，但具有积累演化风险 | 如脚手架搭设偏差、警示缺失、人员作业未穿戴防护装备等 | 记录隐患，通报责任班组，纳入现场日常管理体系 |
| Ⅳ级（低风险） | 影响较轻，短期内不会造成不良后果，管理手段成熟可控 | 多为可预见、可控的常规问题，如轻微堆料超标、文档不完整等 | 例行巡检跟踪，纳入教育培训，视情况优化现场管理流程 |

* + 1. 分级响应机制设定

系统在识别隐患后，应自动匹配风险等级并启动分级响应流程：

1. 重大风险响应机制：一旦识别为Ⅰ级风险，系统立即推送红色预警，施工单位需立刻停止相关作业，由安全管理人员第一时间赶赴现场处理，相关责任单位需在2小时内完成情况上报与初步整改措施实施；
2. 较大风险响应机制：Ⅱ级风险触发橙色预警，要求在12小时内制定整改计划，并安排专人跟踪闭环整改进度，同时向主管部门汇报整改进展；
3. 一般风险响应机制：Ⅲ级风险对应黄色提醒，纳入日常问题库，施工单位在24小时内完成现场处理并录入整改结果；
4. 低风险响应机制：Ⅳ级风险对应蓝色记录，作为施工行为数据积累与安全教育案例使用。
   * 1. 风险等级动态调整机制

随着施工阶段推进与环境变化，系统应具备风险等级动态调整能力。通过实时数据监测、现场视频分析与历史事故对比，对相同隐患场景进行再评估，并更新等级标注与响应规则，确保管理的前瞻性与灵活性。

* 1. 安全隐患智能识别
     1. 视频图像识别要求

系统应通过部署智能摄像头及图像识别算法，对以下关键隐患行为实现自动识别：

* 1. 高空作业人员未佩戴安全带；
  2. 人员擅自进入危险区域；
  3. 吊装作业过程中人员靠近吊物；
  4. 临边防护缺失、脚手架倾斜或异常荷载；
  5. 火源、电缆乱接、物料堆放混乱等场景。

识别算法应具备目标检测、行为分析、场景分割等能力，并支持边缘计算部署，以减少延迟。

* + 1. 传感器数据识别要求

通过位移、倾角、应力、振动、气体等多种传感器采集数据，系统应实现以下识别功能：

1. 检测基坑、边坡、支护结构的变形趋势；
2. 分析结构构件受力异常或临界状态；
3. 识别高温、可燃气体泄漏等危险环境因子；
4. 监测大型机械运行异常、失稳或碰撞风险。

多传感融合分析应结合历史数据，构建隐患识别模型，支持实时报警机制。

* + 1. 施工行为识别要求

结合施工计划、作业记录及现场调度信息，系统应识别以下非规范行为：

* 1. 未授权作业；
  2. 关键工序未按规范进行交底和检查；
  3. 工序超前或延误带来的安全隐患；
  4. 多工种交叉作业中的冲突风险。

此类识别需依赖于BIM模型、计划数据与日志行为的深度融合。

* + 1. 安全隐患分级识别机制

系统应对识别出的安全隐患进行自动分级，参考第6章中风险等级划分，依据以下指标进行综合评估：

1. 危害程度；
2. 影响范围；
3. 可控性；
4. 历史发生频率；
5. 应对资源需求。
   1. 大数据风险分析与预警
      1. 风险数据整合与建模

为实现科学预判和动态评估，系统应构建包括以下数据维度的综合分析模型：

1. 时序类数据：如监测传感数据、视频识别输出、环境指标等；
2. 结构类数据：包括施工工序流程、组织架构、作业分区等；
3. 事件类数据：如安全事故记录、隐患整改记录、报警日志等；
4. 空间类数据：结合BIM/GIS信息对风险分布进行空间映射。

基于上述数据，应采用分类模型、回归分析、聚类算法等方法构建多维风险预测模型，实现隐患趋势评估与关键区域识别。

* + 1. 风险等级评估与动态分析

系统应基于风险模型输出结果，综合评估当前施工现场的整体安全风险等级，具体包括：

1. 风险指标自动打分与等级划分；
2. 风险时空变化趋势分析；
3. 不同工序、施工区域与设备关联风险的比较分析；
4. 高频预警点识别及异常模式分析。

通过动态可视化图表、热力图等手段展示风险分布与演变趋势，辅助现场安全管理人员做出精准决策。

* + 1. 预警触发与响应机制

系统应具备多级预警能力，按风险等级设定分级响应机制，主要包括：

1. 预警分级设置：例如黄色预警（轻度异常）、橙色预警（中度风险）、红色预警（重大隐患）；
2. 自动通知机制：通过短信、App推送、语音广播等多通道通知相关责任人员；
3. 响应流程联动：自动启动整改任务派发、作业暂停指令、人员撤离提示等联动机制；
4. 预警日志管理：记录预警发生、响应处置、关闭流程等全过程信息，形成可追溯链条。

预警机制应支持人工干预与算法优化，增强系统的灵活性与实效性。

* 1. 安全处置与应急联动
     1. 安全隐患处置流程

系统应自动触发隐患处置流程，并支持全过程信息闭环管理。关键环节包括：

1. 识别确认：系统检测到风险事件后，自动生成隐患事件编号，定位发生位置与类别，生成待办任务；
2. 责任分配：根据隐患等级和类别，自动分派至对应责任人或班组；
3. 现场处置：责任人按规定流程完成隐患消除，并通过移动端上传现场处理图片、处理说明等佐证材料；
4. 复查验证：系统或管理人员对处理结果进行复核，判断隐患是否整改闭环；
5. 结果归档：处置过程及结果信息自动归档入库，形成完整的隐患处置链条。
   * 1. 应急响应机制

系统应与应急预案体系联动，建立多级响应机制，在突发情况下实现迅速联动处置。具体包括：

1. 应急预案数字化建模：将已有应急方案以模块化形式嵌入系统，可按风险类型（如坍塌、高空坠物、火灾等）快速调用；
2. 多方联动通道：支持与施工总包、监理、属地监管、医疗机构等实现数据互联、信息互通；
3. 现场应急调度：通过可视化地图、监控联动等手段快速掌握事故现场情况，调度应急物资与人员；
4. 实时通信保障：系统应具备应急通信保障机制，优先保证险情信息及时送达。
   * 1. 应急演练与智能优化

强调隐患与突发风险处置的智能化、流程化和协同化要求，构建从识别、处理、验证到优化的完整闭环机制，提升施工安全治理的响应效率与实效性：

1. 演练支持：系统应提供应急演练模块，支持虚拟演练、脚本推演及结果评估，提升施工人员的协同处置能力；
2. 数据分析反馈：基于应急处置过程数据，可分析响应时间、资源调度效率、协同完成度等指标；
3. 持续优化：借助AI分析技术对历史事件和处置过程进行优化建议生成，不断完善应急响应模型。
   1. 系统运行与运维管理
      1. 平台运行管理机制

平台应由专门的运营维护机构负责运行，需明确以下管理要求：

1. 运行策略制定：制定运行管理制度，涵盖系统启停规则、运行巡检计划、数据管理流程等；
2. 角色权限划分：建立分级分权的账户权限体系，区分数据上传、审核、调度、分析、导出等功能权限；
3. 日志记录与分析：平台应自动记录操作日志、访问日志、告警日志等，并提供日志检索与追溯功能。
   * 1. 数据维护与质量控制

系统应设有数据全生命周期管理流程，保障信息的准确性、完整性与可追溯性：

1. 数据校验机制：设置多重自动校验策略，包括格式规范检查、逻辑一致性校验、数值范围约束等；
2. 数据清洗与更新：对冗余、失效、冲突数据定期清洗，支持增量更新、批量修复等操作；
3. 数据备份与恢复：系统应具备每日定时备份与多副本冗余存储能力，并能在数据损坏时快速恢复。
   * 1. 运维保障机制

系统运维需涵盖软硬件全链条，并加强自动化、智能化程度，提升效率与安全水平。运维保障机制主要内容见表2。

1. 运维保障机制主要内容

| 运维项 | 具体内容说明 |
| --- | --- |
| 硬件运维 | 包括服务器、摄像头、传感器、通信设备的定期检测、故障处理与设备更换记录管理 |
| 软件运维 | 包括操作系统、数据库、中间件、应用系统的补丁升级、漏洞修复与性能优化 |
| 网络保障 | 包括带宽管理、防火墙配置、VPN接入管理、网络冗余与入侵检测系统（IDS）部署 |
| 安全监测 | 设置防病毒策略、安全事件监控、异常行为识别、攻击预警和安全加固 |
| 服务响应机制 | 建立7×24小时运维值守机制，设置分级告警响应时间标准，配备应急处置预案 |

* 1. 测试与验收方法
     1. 功能性测试

功能测试应覆盖系统的核心模块与主要应用场景，确保所有功能正常运行。具体包括：

1. 安全隐患识别功能：测试图像识别、视频分析、传感器联动等模块是否能识别典型隐患；
2. 风险评估模型：验证风险等级输出的准确性、逻辑合理性及其与实景匹配度；
3. 报警推送功能：测试告警触发条件是否灵敏准确，通知是否及时可靠；
4. 平台交互功能：测试系统中信息录入、查询、反馈、分析、统计等交互模块是否流畅；
5. 多端适配：验证系统在移动端、Web端、控制终端等设备上的兼容性与一致性。
   * 1. 性能测试

性能测试侧重于系统稳定性和响应能力，参考指标值范围见表3。

1. 性能测试关键指标

| 测试项目 | 参考指标值范围或要求 |
| --- | --- |
| 图像识别准确率 | ≥ 90%（根据典型工况测试集） |
| 实时识别响应时延 | ≤ 3秒（从隐患出现到报警推送） |
| 并发处理能力 | 支持≥ 50路视频/数据源同时接入 |
| 数据传输延迟 | ≤ 1秒（局域网环境下） |
| 平均无故障运行时间 | ≥ 500小时 |

* + 1. 安全性测试

应对系统在面对恶意攻击、数据泄露、越权访问等威胁时的防护能力进行全面测试，内容包括：

1. 权限控制测试：验证系统各类账户的访问权限设置是否合理，权限边界是否清晰；
2. 加密机制测试：检查传输数据与存储数据的加密手段是否有效，如是否采用标准加密协议；
3. 攻击模拟测试：通过模拟SQL注入、跨站脚本（XSS）、拒绝服务（DoS）等常见攻击方式，评估系统抵御能力；
4. 日志审计测试：验证日志系统是否完整记录用户行为、安全事件，且具备追溯能力；
5. 数据恢复测试：测试断电、误删等情况下，系统是否能快速恢复至正常运行状态。
   * 1. 验收流程

系统验收应遵循“技术检查—实际演示—指标比对—报告评估”的流程，需包括以下步骤：

1. 组织测试团队按标准方案进行功能与性能测试；
2. 撰写完整测试报告，列明各项指标达标情况；
3. 邀请第三方或用户单位代表参与系统实地演示；
4. 汇总评估结果，形成验收结论；
5. 验收合格后，签署交付使用确认文件。

通过规范测试与验收流程，可确保系统投入使用后达到预期功能与质量要求，为道路桥梁施工期间的隐患识别与风险防控提供可靠技术保障。

* 1. 应用推广与后续维护
     1. 推广应用策略

推广本系统的应用应因地制宜、分类施策。通过政策推动和项目试点，鼓励施工单位、监理机构主动采用智能识别技术，逐步形成行业普及机制。优先在风险较高的高墩大跨、深基坑、高边坡等桥隧重点施工区域试点部署系统，积累应用案例后向普通桥梁、普通路段扩展。可结合系统上线同步开展岗位培训和操作演示，提升一线管理人员对系统的理解与使用能力。

* + 1. 运维保障机制

为确保系统长期有效运行，应建立规范的运行维护机制，制定巡检计划，定期对图像识别设备、传感器、通信网络等进行检查与保养。

应对后台风险数据库进行动态更新，清除冗余数据、补充新类型隐患样本，提升系统学习能力。

应根据新技术发展和现场需求适时进行软件功能优化、补丁修复与算法模型升级，保持系统先进性。

建议记录日常运维操作与系统异常处理过程，构建“故障定位—预警通知—技术支撑”闭环体系，并制定关键数据和识别模型的定期备份计划，建设异地容灾系统，以应对突发事件。

