ICS 35.240.01
CCS L67

T/ACCEM

团　　体　　标　　准

T/ACCEM XXXX—2025

基于视觉 AI 的异常行为实时预警技术规范

Technical specification for real-time early warning of abnormal behavior based on visual AI

（征求意见稿）

在提交反馈意见时，请将您知道的相关专利连同支持性文件一并附上。

2025－XX－XX 发布　　2025－XX－XX 实施

中国商业企业管理协会　　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。

本文件由宁波甬想科技有限公司提出。

本文件由中国商业企业管理协会归口。

本文件起草单位：

本文件主要起草人：

基于视觉 AI 的异常行为实时预警技术规范

1 范围

本文件规定了基于视觉 AI 的异常行为实时预警系统的术语和定义、系统架构、功能要求、性能指标、数据处理、模型管理、安全要求、测试方法以及评估与认证。

本文件适用于基于视觉 AI 技术，对人员、物体或场景的异常行为进行实时监测、分析和预警的系统的设计、开发、实施、测试和评估。

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 22239-2019 信息安全技术 网络安全等级保护基本要求

GB/T 35273-2020 信息安全技术 个人信息安全规范

3 术语和定义

下列术语和定义适用于本文件。

3.1

视觉 AI Visual AI

利用人工智能技术对视觉数据（如图像、视频）进行处理、分析和理解，以实现目标检测、识别、行为分析等功能的技术集合。

3.2

异常行为 abnormal behavior

偏离正常行为模式或不符合预设规则、场景要求的人员、物体或场景的行为状态。

3.3

实时预警 real-time early warning

在异常行为发生的同时或极短时间内，通过特定方式向相关人员或系统发出警报信息，提示异常情况发生的过程。

3.4

行为模型 behavior model

通过对大量正常和异常行为数据的学习和分析，建立的用于描述和预测行为模式的数学模型或算法模型。

3.5

误报 false alarm

系统将正常行为错误判断为异常行为并发出的警报。

3.6

漏报 missed alarm

系统未能检测到实际发生的异常行为，未发出相应警报的情况。

4 系统架构

4.1 总体架构

基于视觉 AI 的异常行为实时预警系统应至少包括数据采集层、数据传输层、数据处理与分析层、预警输出层以及用户管理层，各层之间应协同工作，实现异常行为的实时监测与预警功能。

4.2 数据采集层

4.2.1 视觉采集设备

应根据应用场景和监测需求，合理选择摄像头等视觉采集设备，如高清摄像机、红外摄像机等。设备应具备良好的图像采集性能，包括分辨率、帧率、感光度等指标应满足实际应用需求。例如，在人员密集场所，应选用分辨率不低于 1080P、帧率不低于 25fps 的摄像机，以确保清晰捕捉人员行为。

4.2.2 其他辅助传感器

可根据需要配备如声音传感器、温度传感器等辅助传感器，用于采集与异常行为相关的其他环境信息，提升异常行为判断的准确性。

4.3 数据传输层

4.3.1 传输方式应支持有线传输（如以太网、光纤等）和无线传输（如 Wi-Fi、4G/5G 等）两种方式。应根据实际应用场景的网络条件、数据传输量和实时性要求，选择合适的传输方式或多种方式结合。在网络稳定、数据量较大的室内环境，优先采用有线以太网传输；在布线困难或移动场景下，可选用 4G/5G 无线传输确保数据及时上传。

4.3.2 传输协议应采用成熟稳定的数据传输协议，如 TCP/IP 协议，确保数据传输的可靠性和稳定性。同时，应具备数据加密传输机制，防止数据在传输过程中被窃取或篡改。

4.4 数据处理与分析层

4.4.1 应对采集到的原始视觉数据和其他传感器数据进行去噪、增强、归一化等预处理操作，提高数据质量，为后续分析提供可靠数据基础。

4.4.2 利用先进的目标检测与识别算法，对视频中的人员、物体等目标进行检测和识别，确定目标的类别、位置和姿态等信息。

4.4.3 应通过对目标的运动轨迹、动作特征、行为模式等进行分析，结合历史数据和领域知识，建立行为模型。利用长短期记忆网络（LSTM）等算法，学习人员在不同场景下的正常行为模式，从而识别出异常行为。

4.5 预警输出层

4.5.1 系统应支持多种预警方式，包括但不限于声光报警、短信通知、邮件推送、系统弹窗提示等。可根据不同的应用场景和用户需求，灵活配置预警方式和预警级别。如在工厂车间，采用声光报警及时提醒现场人员；对于管理人员，同时发送短信通知和邮件详细说明异常情况。

4.5.2 预警信息应包含异常行为的类型、发生时间、发生地点、相关目标信息（如人员身份、物体特征等）以及预警级别等关键信息，以便相关人员快速了解异常情况并采取相应措施。

4.6 用户管理层

4.6.1 应具备完善的用户权限管理功能，可根据用户角色（如管理员、普通用户等）设置不同的操作权限和数据访问权限。管理员拥有系统的最高权限，可进行系统配置、用户管理等操作；普通用户仅能查看授权范围内的监测数据和预警信息。

4.6.2 应支持对系统的各种参数进行配置，包括摄像头参数、行为模型参数、预警规则参数等，以适应不同应用场景和需求的变化。

5 功能要求

5.1 异常行为检测功能

5.1.1 系统应能实时检测人员的跌倒、奔跑、打架、长时间滞留、闯入禁区等常见异常行为，并准确识别异常行为的类型和发生位置。

5.1.2 对于物体的异常移动、掉落、异常摆放等行为，系统应具备检测能力。在物流仓库场景中，能检测货物是否出现异常位移或堆叠倒塌风险。

5.1.3 应能对场景中的异常情况进行检测，如火灾烟雾、爆炸火光、环境光线异常变化等。在室内公共场所，能根据光线变化异常检测是否有灯光故障引发的安全隐患。

5.2 实时预警功能

系统应在检测到异常行为后的规定时间内（如不超过 1 秒）发出预警信号，确保相关人员能及时响应。同时，预警信号应明显且易于识别，不会与正常提示信息混淆。

5.3 历史数据查询与分析功能

5.3.1 应具备可靠的数据存储功能，能够存储至少 30 天的原始视频数据和经过分析处理的行为数据。数据存储格式应便于后续查询和分析。

5.3.2 应支持用户根据时间、地点、异常行为类型等条件对历史数据进行查询，快速定位到相关事件的视频记录和分析报告。用户可通过输入具体时间段，查询该时段内特定区域发生的所有人员跌倒事件。

5.3.3 应能够对历史数据进行统计分析，生成异常行为发生频率、趋势图等分析报表，为用户提供决策支持。通过分析报表，用户可了解某区域在不同季节人员异常行为的发生规律，提前制定防范措施。

5.4 系统自诊断与维护功能

5.4.1 系统应具备实时自诊断能力，定期对硬件设备和软件系统进行检测，及时发现故障或异常情况，并生成自诊断报告。

5.4.2 应提供方便的系统维护接口和工具，支持远程维护和升级。维护人员可通过网络远程对系统进行参数调整、软件更新、故障修复等操作，确保系统的正常运行和性能优化。

6 性能指标

6.1 异常行为检测准确率

系统对各类异常行为的检测准确率应不低于 90%。检测准确率计算公式为：检测准确的异常行为数量 / 实际发生的异常行为数量 ×100%。

6.2 误报率

系统的误报率应不高于 5%。误报率计算公式为：误报的次数 /（误报次数 + 正确报警次数）×100%。

6.3 漏报率

系统的漏报率应不高于 3%。漏报率计算公式为：漏报的次数 / 实际发生的异常行为次数 ×100%。

6.4 预警响应时间

从系统检测到异常行为到发出预警信号的时间间隔应不超过 1 秒。

6.5 数据存储容量与时长

系统应具备足够的数据存储容量，满足至少 30 天的原始视频数据和行为分析数据的存储需求。存储设备应具备数据备份和恢复功能，确保数据的安全性和完整性。

7 数据处理

7.1 数据采集与标注

7.1.1 应采集丰富多样的视觉数据和相关环境数据，覆盖不同场景、不同时间段、不同人员和物体类型，以满足行为模型训练和优化的需求。在采集数据时，应遵守相关法律法规，保护个人隐私和数据安全。

7.1.2 对采集到的数据进行准确标注，标注内容应包括目标类别、行为类型、发生时间、地点等关键信息。数据标注应采用统一的标准和规范，确保标注的一致性和准确性。可采用人工标注与半自动标注相结合的方式，提高标注效率。

7.2 数据清洗与预处理

对采集到的原始数据应进行清洗，去除噪声数据、重复数据和错误数据。同时，进行数据增强操作，如对图像进行旋转、缩放、裁剪等变换，增加数据的多样性，提高行为模型的泛化能力。

7.3 数据存储与管理

应采用可靠的数据存储技术和管理系统，对数据进行分类存储和管理。数据应存储在安全可靠的存储设备中，如磁盘阵列、云存储等，并定期进行数据备份。建立数据访问权限控制机制，确保只有授权人员能够访问和使用数据。

7.4 数据使用与共享

在使用数据进行行为模型训练和系统优化时，应遵循数据使用的目的和范围，不得超出授权范围使用数据。如需与第三方共享数据，应签订数据共享协议，明确数据使用的权利和义务，确保数据的安全和合规使用。

8 模型管理

8.1 模型训练

8.1.1 训练数据选择

应选择具有代表性和多样性的训练数据，包括正常行为数据和各类异常行为数据。训练数据的质量和数量应满足模型训练的需求，以确保训练出的行为模型具有较高的准确性和泛化能力。

8.1.2 训练算法选择

应采用先进的机器学习和深度学习算法进行模型训练，如卷积神经网络（CNN）、循环神经网络（RNN）、长短时记忆网络（LSTM）等。根据不同的应用场景和异常行为类型，选择合适的算法模型和网络结构，并对算法参数进行优化。

8.1.3 训练过程监控

在模型训练过程中，应实时监控训练指标（如损失函数、准确率等）的变化情况，及时调整训练参数，确保训练过程的稳定性和收敛性。同时，记录训练过程中的相关信息，如训练时间、训练数据量等，以便后续分析和优化。

8.2 模型评估与优化

8.2.1 评估指标设定

应建立科学合理的模型评估指标体系，包括准确率、召回率、F1 值等，全面评估模型对异常行为的检测性能。同时，根据不同的应用场景和需求，设置相应的评估指标权重，突出重点评估指标。

8.2.2 模型优化方法

应根据模型评估结果，采用调整模型结构、增加训练数据、优化训练算法等方法对模型进行优化，提高模型的性能和稳定性。定期对模型进行重新训练和优化，以适应场景变化和数据分布的变化。

8.3 模型更新与部署

8.3.1 更新机制建立

应建立模型更新机制，根据新采集的数据、应用场景的变化以及用户反馈，及时对模型进行更新。模型更新应经过严格的测试和验证，确保更新后的模型性能不低于原有模型。

8.3.2 部署流程规范

应制定规范的模型部署流程，确保更新后的模型能够安全、稳定地部署到实际运行环境中。在部署过程中，应进行充分的测试和调试，确保模型与系统其他组件的兼容性和协同工作能力。

9 安全要求

9.1 数据安全

9.1.1 数据加密

应对采集到的原始数据、经过处理的中间数据以及存储的数据进行加密，确保数据在传输和存储过程中的安全性。采用行业标准的加密算法，如 AES 加密算法，对数据进行加密保护。

9.1.2 访问控制

应建立严格的数据访问控制机制，根据用户角色和权限，对数据的访问进行授权管理。只有经过授权的用户才能访问和使用相关数据，防止数据泄露和滥用。

9.1.3 数据备份与恢复

应定期对重要数据进行备份，并将备份数据存储在安全可靠的位置。制定数据恢复计划，确保在数据丢失或损坏时能够及时恢复数据，保障系统的正常运行。

9.2 网络安全

9.2.1 网络隔离

将基于视觉 AI 的异常行为实时预警系统与外部网络进行隔离，采用防火墙、入侵检测系统（IDS）、入侵防御系统（IPS）等网络安全设备，防止外部网络攻击和恶意软件入侵。

9.2.2 安全漏洞管理

定期对系统进行安全漏洞扫描和检测，及时发现并修复系统存在的安全漏洞。关注软件供应商发布的安全补丁，及时对系统软件和应用程序进行更新，提高系统的安全性。

9.3 隐私保护

9.3.1 个人信息保护

在数据采集和使用过程中，严格遵守相关法律法规，保护个人隐私信息。对于涉及个人身份、敏感信息的数据，应进行匿名化处理，确保个人信息不被泄露和滥用。

9.3.2 隐私政策声明

向用户明确告知系统的数据采集、使用和共享政策，取得用户的同意和授权。在系统界面或相关文档中，清晰说明隐私保护措施和用户的权利，保障用户的知情权和选择权。

10 测试方法

10.1 功能测试

10.1.1 测试用例设计应根据系统的功能要求，设计全面、详细的测试用例，覆盖异常行为检测、实时预警、历史数据查询与分析、系统自诊断与维护等各个功能模块。测试用例应包括正常情况和异常情况的测试场景，以充分验证系统的功能正确性。

10.1.2 测试执行应按照测试用例，使用模拟数据或实际采集的数据对系统进行测试。在测试过程中，观察系统的运行状态和输出结果，检查系统是否满足各项功能要求。对于发现的问题，及时记录并进行分析和解决。

10.2 性能测试

10.2.1 应搭建与实际应用场景相似的性能测试环境，包括硬件设备、网络环境、数据量等。确保测试环境能够真实反映系统在实际运行中的性能表现。

10.2.2 宜采用专业的性能测试工具，如 LoadRunner、JMeter 等，对系统的异常行为检测准确率、误报率、漏报率、预警响应时间、数据存储容量与时长等性能指标进行测试。

10.2.3 根据性能测试结果，分析系统的性能瓶颈和不足之处，提出针对性的优化建议。对优化后的系统再次进行性能测试，验证优化效果，确保系统性能满足设计要求。

10.3 安全测试

10.3.1 宜使用漏洞扫描工具，如 Nessus、OpenVAS 等，对系统进行安全漏洞扫描，检测系统是否存在常见的安全漏洞，如 SQL 注入、跨站脚本攻击（XSS）、文件上传漏洞等。

10.3.2 应委托专业的安全测试机构或团队对系统进行渗透测试，模拟黑客攻击手段，尝试突破系统的安全防线，检测系统的安全性和防护能力。对于渗透测试发现的安全问题，及时进行修复和加固。

10.3.3 应对系统的数据加密、访问控制、数据备份与恢复等数据安全功能进行测试，验证数据在传输、

存储和使用过程中的安全性。检查系统是否符合相关数据安全标准和规范的要求。

11 评估与认证

11.1 评估机构与流程

应由具备相关资质和专业能力的第三方评估机构对基于视觉 AI 的异常行为实时预警系统进行评估。评估流程包括系统提交申请、评估机构资料审核、现场测试与检查、评估报告出具等环节。

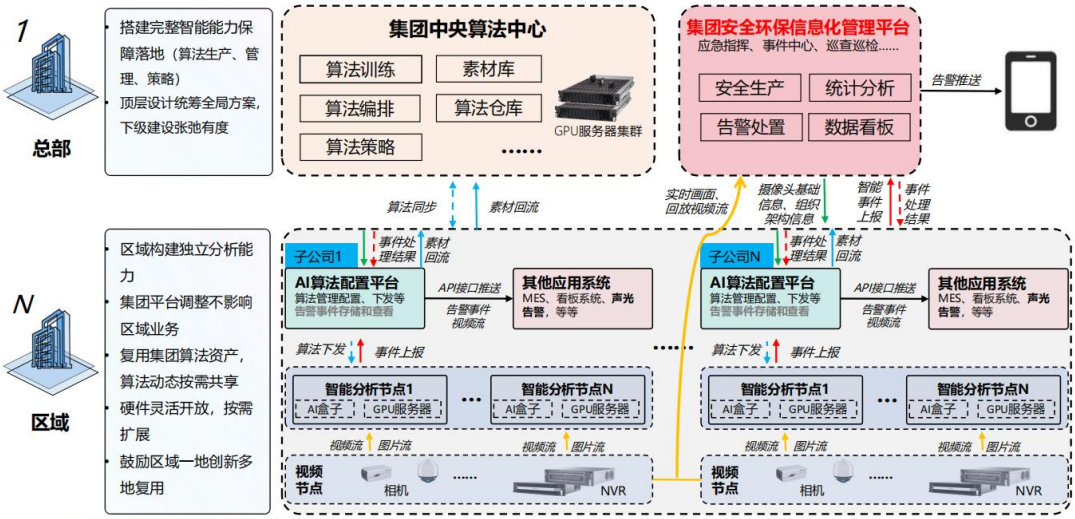
11.2 评估内容与标准

应评估内容应涵盖系统的功能要求、性能指标、数据处理、模型管理、安全要求等方面。评估标准应依据本文件以及相关的国家、行业标准和规范进行制定，确保评估结果的科学性和公正性。

11.3 认证与标识

对于通过评估的系统，应由评估机构颁发相应的认证证书和标识。认证证书和标识应明确系统的认证范围、有效期等信息，以证明系统符合基于视觉 AI 的异常行为实时预警技术规范的要求。

附 录 A
（资料性）
示例



一、集团安全环保信息化管理平台（安环平台）：
1、接收AI平台推送的告警信息（摄像头IP、位置和告警的事件、图片、短视频）
2、对AI识别的告警事件进行统计分析、报表分析、大屏看板
3、接收到的告警信息，按流程推送相关人员进行处理
3、返回告警事件的处理结果给AI平台
4、推送告警信息到移动终端，如企业微信、钉钉，这只是提醒消息

二、子公司视频AI平台（AI平台）：
1、实时推送告警信息到安环平台
2、从安环平台同步组织机构、人员基本信息（可选择）
3、从安环平台同步摄像头信息（可选择）
4、接收安环平台返回的事件处理结果，并在AI平台消除对应的告警