ICS 35.240
CCS L70

团　　体　　标　　准

T/ISC XXX—XXXX

智能门锁 门前主动安防通用技术要求

Smart lock: General technical specifications for proactive security in front of the door

在提交反馈意见时，请将您知道的相关专利与支持性文件一并附上。

（征求意见稿）

XXXX－XX－XX 发布　　XXXX－XX－XX 实施

中 国 互 联 网 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。

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。

本文件由中国互联网协会提出并归口。

本文件起草单位：

本文件主要起草人：

本文件及其所代替文件的历次版本发布情况为：

——

引　　言

随着智能家居与视觉AI技术的快速发展，智能门锁正从被动身份识别向门前全域主动安防升级，门前感知、AI 行为分析、主动预警告警、事件回溯与多设备协同联动等能力已成为新一代家用入户智能门锁的核心标配，为家庭出入口安全带来了更前置、更主动、更全面的防护体验。

但当前智能门锁门前主动安防相关技术缺乏统一的行业规范，不同产品在感知范围、AI识别可靠性、预警触发逻辑、事件记录管理及策略管控配置等方面实现方式差异较大，功能边界不清晰、告警机制不可控、策略配置僵化等问题日益显现，既影响用户使用安全感与体验一致性，也制约行业向规范化、标准化、高质量方向发展。

为规范智能门锁门前主动安防的技术实现与功能配置要求，引导行业良性发展，特制定本文件。本文件结合当前家用智能门锁产品技术现状与主动安防场景特点，构建了以“事前监测、事中预警、现场干预、事后回溯、全程可控”为核心的全流程技术体系，可为相关产品的设计、研发、生产、测试及行业监管提供统一技术依据。

智能门锁 门前主动安防通用技术要求

1 范围

本文件规定了智能门锁门前主动安防系统的感知监测、识别验证、预警处置、事件回溯、联动协同策略管控、通信能力的通用技术要求。

本文件适用于具备门前主动安防能力的家用入户智能门锁及其配套组件的设计、开发与部署，可为产品制造商、系统集成商及服务运营方提供技术指引。

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 44602-2024 网络安全技术 智能门锁网络安全技术规范

3 术语和定义

下列术语和定义适用于本文件。

3.1

智能门锁 smart lock

以生物特征、电子标签、无线遥控编码、电子口令或远程控制指令等作为鉴别凭证控制门锁开启或关闭，由门锁终端、接入网关、管理平台以及控制端等部分组成的门锁系统。

3.2

门前主动安防 proactive security in front of the door

通过智能门锁及其配套感知设备，在用户未与门锁发生直接物理交互前，在入户门前必要安防与交互范围内自动探测门前区域目标及行为，以保护居家安全为核心目标的技术体系。

3.3

异常行为 abnormal behavior

在门前区域发生的、可能威胁居家安全或违背正常访客逻辑的动作模式，如长时间逗留、反复徘徊、刻意遮挡等。

3.4

逗留抓拍 loitering capture

当监测到人员在门前区域内停留时间超过预设阈值时，系统自动触发拍照或录像的功能。

3.5

人像过滤 face filtering

在感知监测过程中，利用算法区分家庭成员、已授权访客与陌生人，并对不同类型人员采取差异化处理策略的技术。

3.6

主动威慑 active deterrence

在识别到潜在安全威胁时，系统自动采取的旨在阻止或驱离威胁目标的现场干预措施。

4 概述

门前主动安防以保护居家安全为核心目标，构建“事前监测、事中预警、现场干预、事后回溯、全程可控”的全流程体系，确保智能门锁的门前主动安防能力，核心技术能力主要包括：

a) 感知监测：实现门前区域实时监测，及时捕捉人员、物体及环境变化；
b) 识别验证：识别可疑行为与入侵风险，完成身份验证，保障出入安全；
c) 预警处置：快速响应风险，主动威慑入侵，及时发送预警信息；
d) 事件回溯：留存安全事件数据，支持事后核查与责任认定；
e) 联动协同：扩展防护范围，覆盖延伸场景，提升整体安防能力；
f) 策略管控：支持自定义防护策略，灵活适配不同居家场景的主动安防需求。
g) 通信能力：保障感知数据、控制指令的稳定可靠传输。

5 感知监测

5.1 区域检测

应具备对入户门前近景区域的实时有效监测能力，覆盖门锁交互区及门前必要安防区域易。宜支持多传感协同监测（如视觉与雷达融合）。

5.2 目标捕捉

应能够及时捕捉进入监测区域的动态目标，区分人员、车辆及宠物等不同类型。宜具备对静止目标的感知能力，识别门前区域的异常遗留物体。

5.3 环境感知

应具备门前环境安全状态的主动感知能力，能够实时监测并识别监测区域内的异常情况，包括但不限于烟雾、明火、大面积积水等安全隐患。

5.4 环境适应

在门外强光逆光、夜间无光或微光等环境下，应能有效捕捉与识别门前人员面部及行为特征。

6 识别验证

6.1 行为风险识别

应具备异常行为分析能力，能够识别以下风险行为：

a) 非授权人员在门前规定时间阈值内的持续停留或来回走动；

b）针对门锁、门体或感知设备的敲击、撬动、异常拆卸等破坏行为；

c）针对感知设备进行的遮挡或破坏行为；

6.2 身份验证辅助

应支持在人员靠近时，配合门锁完成身份验证（如人脸识别等），区分授权人员、常访客与陌生人。

7 预警处置

7.1 风险响应

7.1.1 快速响应

系统识别风险后应立即启动预警与处置流程。

7.1.2 分级预警

应根据6.1中识别到的风险行为类型及威胁程度，建立分级预警机制，并触发对应级别的处置策略。风险分级及对应类型宜包括：

a）高级别风险（紧急威胁）：针对门锁、门体或感知设备的破坏行为（如敲击、撬动、异常拆卸），触发声光威慑、远程紧急告警及锁定保护等应急联动处置；

b）中级别风险（可疑威胁）：陌生人较长时间逗留、刻意遮挡感知设备，触发远程告警信息推送与语音劝离；

c）低级别风险（一般异常）：陌生人在门前短时逗留或徘徊，触发常规抓拍与远程提示。

7.1.3 主动威慑干预

应具备主动威慑干预能力。在触发预警时，宜自动执行声光警报以震慑和驱离目标，声光报警强度应具备有效的现场震慑作用。应具备语音干预能力，支持在预警状态下向门前区域播放预置警告语音。应对多次试探、暴力破坏等行为执行锁定保护。宜支持用户通过终端设备与门外进行实时语音对讲，实现远程喊话干预。

7.2 预警信息推送

系统在触发预警时，应将告警事件、风险等级及现场记录（如抓拍图片或短视频片段）及时推送至用户关联终端。

7.3 安防低电量保障

应具备电量监测与低电量预警能力。当电量低于安防保障阈值时，应向用户终端推送充电提醒告警。当电量低于安防保障阈值时，宜自动调整功耗策略（如降低非敏感期逗留抓拍频率）。

8 事件回溯

8.1 事件数据留存

应对触发预警的安全事件进行数据留存，留存内容应包含事件发生时间、事件类型、风险等级及对应的感知数据（如音视频、图片）。留存的结构化事件记录应具备可靠的时间基准，确保记录时序的准确性。系统宜对未触发预警的常规监测数据进行一定周期的留存，作为事后分析的补充。

针对包含音视频、图片等涉及个人隐私的感知数据，系统应采取安全存储措施，包括但不限于数据加密存储、严格的访问权限控制及防泄露机制，确保感知数据的保密性与完整性。

8.2 检索与回放

应支持用户按时间、事件类型等条件对留存的门前安防事件进行检索。系统应支持对留存的事件感知数据进行回放，还原事件发生过程。

8.3 责任认定支撑

留存的事件数据在关键特征上应具备可辨识性，能够为居家安全事故的事后核查、纠纷处理或责任认定提供有效依据。

8.4 记录完整性

事件记录应防篡改、防删除，保证真实有效。记录应连续完整，不缺失关键安全事件信息。

9 联动协同

9.1 室内设备联动

应支持与室内智能设备进行联动。在触发主动安防预警时，宜联动室内安防设备（如室内摄像机、智能音箱、智能灯光）以增强室内外的整体防御效果。系统宜支持与室内智能屏等终端的跨屏联动，实现门外异常情况在室内的实时展示与提醒。

9.2 外部系统协同

宜支持与社区安防系统或云端服务平台进行协同，扩展防护边界。系统宜支持在极端威胁情况下，向紧急联系人或物业管理端发送协同求助信息。

9.3 应急联动处置

如遇高危事件，系统应自动进入应急联动状态，快速处置。

10 策略管控

10.1 策略自定义

应支持用户根据实际居住环境自定义防护策略，包括但不限于：设置布防或撤防时段、调整监测区域与灵敏度、配置不同风险等级的预警与威慑方式、调整逗留抓拍的触发时间阈值。

10.2 场景模式切换

宜支持根据用户日常作息提供“居家模式”、“外出模式”、“睡眠模式”等一键安防场景切换，不同模式下自动应用预设的感知、预警及联动策略。

11 通信能力

11.1 本地通信

宜具备与室内配套组件的本地通信能力，确保在断网等极端情况下，门前的感知数据与告警信息仍能在室内端进行实时展示与提醒。

11.2 远程数据传输

应具备将抓拍图片、短视频片段及结构化告警数据实时上传至云端或用户终端的广域网通信能力。从触发高级别预警到用户终端接收到告警信息的端到端通信时延宜满足远程实时干预的要求。

11.3 协同通信

宜具备与社区安防系统、物业管理平台或云端服务平台进行数据对接的通信协议与接口能力。

11.4 抗干扰与通信异常应对

应具备对恶意通信干扰（如Wi-Fi屏蔽、射频干扰等）的检测能力。当检测到远程通信被强行中断或屏蔽时，应自动提升本地主动安防等级（如立即触发本地声光警报震慑）。

当检测到远程通信被强行中断或屏蔽时，宜通过本地短距通信向室内关联设备推送安全警示。