

T/CASME

中国中小商业企业协会团体标准

T/CASME XXX—2023

民用建筑智能化安全技术防范系统工程设计规范

Code for design of intelligent safety technology prevention system engineering in
civil buildings

（征求意见稿）

2023 – XX – XX 发布

2023 – XX – XX 实施

中国中小商业企业协会 发布

目 次

前言 II

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 1

5 系统设计 2

6 入侵报警系统 3

7 视频安防监控系统 4

8 出入口控制系统 6

9 电子巡查管理系统 7

10 汽车库（场）管理系统 7

11 住宅（小区）访客对讲系统 8

12 安防监控室 8

13 网络信息安全 8

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。

本文件由陕西新创工程设计有限公司提出。

本文件由中国中小商业企业协会归口。

本文件起草单位：陕西新创工程设计有限公司、中誉设计有限公司、中骏设计集团有限公司、新疆时代城乡设计研究院有限公司、新疆通艺市政规划设计院有限公司、新疆正塔建筑安装有限公司、伽师县振鑫建筑安装有限责任公司、新疆华星盛世建筑安装工程有限责任公司、中地寅岗建设集团有限公司、新疆华信建设工程有限公司、新疆及地建设工程有限公司、新疆泰然建设工程有限公司、皓泰工程建设集团有限公司、新疆汇和鑫建设工程有限公司、新疆轩达伟业工程建设有限公司、新疆鑫马天成建设工程有限公司。

本文件主要起草人：韩贞、亢增军、张利峰、王耀、樊梓汶、杨嗣明、智彪、高红玲、刘金龙、王飞、张勐、陆新华、刘珊、庞逸飞、单雨晨、钟文江、方四明、李叶、高钰钰、冉运达。

民用建筑智能化安全技术防范系统工程设计规范

1 范围

本文件规定了民用建筑智能化安全技术防范系统工程设计的总体要求、系统设计、入侵报警系统、视频安防监控系统、出入口控制系统、电子巡音管理系统、汽车库(场)管理系统、住宅(小区)访客对讲系统、安防监控室、网络信息安全。

本文件适用于民用建筑智能化安全技术防范系统工程设计。

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 12663 入侵和紧急报警系统 控制指示设备
GB/T 15408 安全防范系统供电技术要求
GB 20815—2006 视频安防监控数字录像设备
GB/T 21050 信息安全技术 网络交换机安全技术要求
GB/T 21741 住宅小区安全防范系统通用技术要求
GB/T 22239 信息安全技术 网络安全等级保护基本要求
GB/T 31000 社会治安综合治理基础数据规范
GB 50198—2011 民用闭路监视电视系统工程技术规范
GB 50348 安全防范工程技术标准
GB 50394 入侵报警系统工程设计规范
GB 50395 视频安防监控系统工程设计规范
GB 50396 出入口控制系统工程设计规范
GA/T 367 视频安防监控系统技术要求
GA/T 543 (所有部分) 公安数据元
GA/T 751 视频图像文字标注规范
GA/T 1127—2013 安全防范视频监控摄像机通用技术要求
GA/T 1211 安全防范高清视频监控系统技术要求
GA/T 1400.3 公安视频图像信息应用系统 第3部分:数据库技术要求

3 术语和定义

本文件没有需要界定的术语和定义。

4 总体要求

4.1 设计原则

- 4.1.1 应符合国家法规和国家现行工程建设标准及有关技术标准、规范和规定的要求。
- 4.1.2 应纳入工程建设总体规划，并综合设计、同步施工、独立验收。
- 4.1.3 安全技术防范系统的设计原则、设计要素、系统传输与布线及供电、防雷与接地设计应符合 GB 50348 的相关规定。
- 4.1.4 应采用先进而成熟的技术、可而适用的设备。
- 4.1.5 安全技术防范系统的信息存储与管理根据实际需要，合理规划数据存储及管理模式。
- 4.1.6 安全技术防范系统应按照信息安全相关要求，整体规划安全防范系统的安全策略，选择适宜的传输网络安全措施、接入设备安全措施、系统安全措施、数据安全措施、以及不同网络的边界安全隔离措施等。

4.2 管理平台建设要求

- 4.2.1 应建设管理平台，管理平台应根据各安全技术防范子系统、设备互联互通以及信息共享应用的具体要求，统筹规划设计系统的各类接口以及信息传输、交换、控制协议。
- 4.2.2 管理平台应按照 GB/T 22239，通过配备必要的网络安全设备，采取必要的网络安全措施，确保系统自身安全和数据安全。
- 4.2.3 应根据安全技术防范系统集成、联网与管理的实际需要，合理规划设计管理平台的具体功能，符合 GB 50348 要求。

4.3 数据采集要求

安全技术防范系统采集的数据项应符合 GB/T 31000、GA/T 543、GA/T 1400.3 的规定。

5 系统设计

- 5.1 设计应根据被保护对象的风险等级确定相应的防范级别，满足整体纵深防护和局部纵深防护的设计要求，以达到所要求的安全防范水平。
- 5.2 安全技术防范系统宜由以下几个子系统构成：
 - 入侵报警系统；
 - 视频安防监控系统；
 - 出入口控制系统；
 - 电子巡查管理系统；
 - 汽车库（场）管理系统；
 - 住宅（小区）访客对讲系统。
- 5.3 安全技术防范系统的集成应符合下列规定：
 - 应通过统一的通信平台和管理软件将安防监控室的设备与安全防范子系统设备联网，实现由安防监控室对安全技术防范系统进行信息集成的自动化管理；
 - 系统集成管理时，应能对各安全防范子系统的运行状态进行监测和控制，应能对系统运行状况和报警信息数据等进行记录和显示；
 - 系统的应用软件应是成熟可靠的；
 - 网络结构应具有可扩展性，宜采用总线型、星型或两者相结合的拓扑结构；
 - 应设置必要的数据库，数据库应为开放式的；
 - 应采用用户登录操作管理，实行分级的操作权限；
 - 重要防护目标安全技术防范系统的服务器及网络核心交换设备宜采用双机热切换互为备用的冗余方式；

- 系统应提供离线分析用的报表功能，包括报警记录、事件记录和人员档案，操作人员可选择和过滤报表数据；
- 系统可提供动态报表书写器模块，允许用户创建自定义报表；
- 重要部门应建立以有线传输为主、无线传输为辅的信息传输系统，安防监控室应能对信息传输系统进行检测，并能与所有重要部位进行专用通信联络；
- 应预留多个数据输入输出接口，应能连接安全防范子系统管理计算机；
- 应留有向外部公安报警中心联网的通信接口；
- 可连接上位管理计算机，以实现更大规模的智能化系统集成。

6 入侵报警系统

6.1 根据各类建筑安全防范部位的具体要求和环境条件，应分别或综合设置周界防护建筑物内区域或空间防护、重点实物目标防护系统。

6.2 入侵报警系统应符合下列要求：

- 无漏报警，少误报警；
- 采用纵深防护；
- 具有防拆及防破坏功能；
- 系统可以自检；
- 探测无盲区；
- 具有模式鉴别功能；
- 与实体防护系统有机结合；
- 适应当地的物理与环境条件。

6.3 入侵报警系统应包括前端设备、传输设备和控制显示、处理、记录设备。前端设备包括一个或多个探测器，当采用多个探测器探测同一区域时，探测器应具有不同的探测原理：传输设备包括电缆或数据采集和处理器（或地址编解码器/发射接收装置）；控制设备包括控制器或中央控制台，控制器/中央控制台应包含控制主板、电源、声光指示、编程、记录装置以及信号通信接口等。

6.4 入侵报警系统应对下列可能的入侵行为进行准确、实时的探测并产生报警状态：

- 打开门、窗、空调百叶窗等；
- 用暴力通过门、窗、天花板、墙及其它建筑结构；
- 破碎玻璃；
- 在建筑物内部移动；
- 接触或接近保险柜或重要物品；
- 紧急报警装置的触发。

6.5 入侵探测器的设置应远离影响探测器工作的电磁辐射、声能、热辐射、光辐射气象条件等环境，或采取防护措施。

6.6 影响室外探测器工作的地形地貌、植被、土壤与铺装地面、野生动物、本底噪声、天气与气候等环境，应在布点时采取措施减少其影响。

6.7 室内入侵探测器的选择应符合下列规定：

- 用于周界防护的探测器宜选用：机电探测器、红外探测器、震动探测器、电容型探测器、光纤探测器、玻璃破碎探测器等类型；
- 用于室内运动的探测器宜选用：微波探测器、微波—红外双鉴探测器、视频移动探测器、超声探测器、声控探测器、被动红外探测器等类型；
- 用于接近实物目标的探测器宜选用：电容型探测器、压力探测器、光纤探测器等类型；

- 用于出入口部位的探测器宜选用：微波探测器、红外探测器、复合探测器、磁开关探测器等类型。
- 6.8 室外入侵探测器的选择应符合下列规定：
- 用于地下埋设的探测器宜选用：压力探测器、震动探测器、碰场探测器、泄漏电缆探测器、光纤探测器等类型；
 - 用于与屏障有关的探测器宜选用：栅栏扰动探测器、机械压力探测器、张力探测器、电场探测器等类型；
 - 独立设置的探测器宜选用：主动红外探测器、被动红外探测器、微波探测器、复合探测器、视频移动探测器等类型。
- 6.9 探测器的设置应符合下列规定：
- 每个/对探测器应设为一个独立防区；
 - 周界的每个独立防区长度不应大于 200 m；
 - 防护对象应在入侵探测器的有效探测范围内。探测器覆盖范围边缘与防护对象间的距离宜大于 5 m；
 - 当多个探测器的探测范围交叉覆盖时，应避免相互干扰。
- 6.10 控制器除应符合 GB 12663 有关规定外，应具有如下功能：
- 应能按时间、区域、部位任意编程撤布防；
 - 应能对设备运行状态和信号传输线路进行检测，及时发出故障报警并指示故障位置；
 - 应具有防破坏功能，当探测器被拆或线路被切断时，系统应发出报警；
 - 应能显示和记录报警部位和有关警情数据，并提供与其它子系统联动的控制接口信号；
 - 在重要区域和部位发出报警时，应能对报警现场的情况进行复核；
 - 应自成网络，可独立运行，有输出接口，可用手动、自动方式向外报警；
 - 根据需要，系统除应具有本地报警功能外，还宜具有异地报警功能。
- 6.11 入侵报警系统应与安全技术防范系统的视频安防监控系统、出入口控制系统联动。
- 6.12 入侵报警系统应与安全技术防范系统的安防监控室联网，满足安防监控室对该系统进行集中管理与控制的有关要求。
- 6.13 入侵报警系统设计除按照本文件规定外，应符合 GB 50394 及其它现行国家规范的规定。

7 视频安防监控系统

- 7.1 根据各类建筑物安全技术防范管理的需要，视频安防监控系统应对现场情况进行有效的监视和记录，并可提供对各类报警信号及时、迅速和可靠的复核手段。
- 7.2 视频安防监控系统可由下列部分组成：
- 摄像机及镜头；
 - 照明系统；
 - 信号传输系统；
 - 同步系统；
 - 画面处理系统；
 - 视频切换控制系统；
 - 视频监视器；
 - 视频记录系统。
- 7.3 视频安防监控系统的技术要求应符合相关规定。
- 7.4 摄像机安装应符合以下要求：

- 出入口安装的摄像机应固定焦距和方向，且朝向一致。建筑与外界相通的出入口安装的摄像机应一致向外；
- 摄像机监视区域应无遮挡，监视图像应避免出现逆光现象；
- 摄像机安装支架应稳定、牢固，安装位置应不易受外界干扰、破坏；
- 固定摄像机的安装指向与监控目标形成的垂直夹角宜不大于 30°，与监控目标形成的水平夹角宜不大于 45°；
- 摄像机工作时，环境照度应能满足摄像机获取清晰有效图像的要求，必要时应设置与摄像机指向一致的辅助照明光源；
- 带有云台、变焦镜头控制的摄像机，在停止云台、变焦操作 2 min±0.5 min 后，应自动恢复至预置设定状态；
- 电梯轿厢摄像机监控图像应能覆盖轿厢、避免逆光，系统应具有楼层显示功能；
- 室外摄像机应采取有效防雷击保护措施。

7.5 摄像机监视图像基本要求应符合表 1 的规定。

表1 摄像机监视图像基本要求

范围	要求
室外周边	应能清晰显示出入口外15 m范围街面过往人员的往来情况、体貌特征和机动车辆的车型、颜色、行驶等情况（存在环境遮挡情况的除外）。
出入口	应能清晰显示出入人员面部特征、活动情况，车辆出入口还应清晰显示车辆牌号。
通道楼道	应能清晰显示过往人员的体貌特征，室外通道还应看清机动车辆、非机动车颜色、车型、行驶等情况。
区域范围	应能清晰显示过往人员的行为特征和机动车辆、非机动车的行驶情况，以及以摄像机为基准5 m~10 m范围监视区域内人员的面部特征和车辆牌号。
楼梯口	应能清晰显示人员的面部特征及活动情况。
电梯厅	应能清晰显示人员的体貌特征及活动情况。
电梯轿厢	应能清晰显示电梯轿厢内全景。
设备机房	应能清晰显示出入人员的面部特征及活动情况。
设备操作	应能清晰显示工作人员对设备操作、维护的活动情况

7.6 摄像机的水平分辨力应不低于 700 TVL。在环境照度不低于 300 lx 的条件下，系统图像质量主观评价应符合 GB 50198—2011 中规定的评分等级 4 分的要求相应的系统技术指标除满足 GA/T 1211 的规定外，还应符合表 2 的要求。

7.7 视频图像应有日期、时间、监视画面位置等的字符叠加显示功能，字符叠加应不影响对图像的监视和记录回放效果。字符设置应符合 GA/T 751 和相关标准要求的规定，字符时间与标准时间的误差应在±30 s 以内。

表2 数字视频安防监控系统主要技术指标

图像尺寸	系统水平分辨力	像面灰度	图像帧率	网络型系统延时	非网络系统延时	视音频记录失步
GA/T 1127—2013中4.1.2的B类	≥600 TVL	≥10级	≥25帧/s	≤400 ms	≤250 ms	≤1 s
GA/T 1127—2013中4.1.2的C类	≥800 TVL					

7.8 视频安防监控系统应与出入口控制系统、停车库（场）管理系统、入侵和紧急报警系统联动，当触发报警时，安防中心控制室的图像显示终端应能自动联动切换出所对应和/或关联部位、区域的视频

图像,并根据联动视频图像的数量,自动调整显示窗口、显示终端。触发报警的响应时间应不大于 2 s,单个触发报警联动对应视频图像的能力应不小于 4 个。

7.9 图像显示终端最低配置数量应不小于 4 台,显示尺寸应不小于 30 英寸,应采用窄边框或无边框显示终端,并具有拼接显示功能:系统具有 128 路以上多路视频图像时,还应按不小于摄像机总数 1/64 (含)的比例另行配置图像显示终端。系统切换或轮巡显示的同步时间应不大于 1 s,画面停留时间应在 5 s 至 30 s 之间。视频图像单画面全屏显示时,显示图像的清晰度应与摄像机的清晰度相适配。

7.10 视频安防监控系统应配置数字录像设备对所有图像进行实时记录。数字录像机设备应符合 GB 20815—2006 中 II、II 类 A 级的要求,图像信息应以大于等于 25 frame/s 的速保存,图像信息保存时间和系统运行、系统备电应同时符合以下要求:

- 视频监控图像保存时间除特殊规定外,应不少于 30 d;
- 系统应保持 24 h 开启状态;
- 系统应有备用电源,应能保证在市电断电后系统供电时间不小于 1 h。

7.11 视频安防监控系统应配置统一时钟源对所有系统设备进行自动校时和时钟同步。

7.12 网络型数字视频安防监控系统,应采用数据结构独立的专用网络(允许采用 VLAN 的独立网段),应对系统中所有接入设备的网络端口予以管理和绑定,单层设备之间的铜缆传输距离应不大于 75 m。

7.13 应具有视频安防监控数据导出防泄密功能,对数字录像设备的 USB 端口采用可通过出入口控制系统授权刷卡认证的防泄密 USB 防插拔设备予以绑定管理,并应将 USB 插拔报警传送至本市技防工程监督管理系统。

7.14 视频安防监控系统的其他要求应符合 GB/T 15408、GB/T 21741、GB 50198—2011、GB 50395 和 GA/T 367 的相关规定。

8 出入口控制系统

8.1 建筑物的主要出入口、通道、财务室、金库、重要办公室等处宜设置出入口控制装置。

8.2 出入口控制系统宜由出入口对象识别装置,出入口信息处理、控制、通信装置和出入口控制执行机构等三部分组成。

8.3 出入口人员识别装置应具有核实个人识别卡号的功能。重要部门和设施的特殊部位还应具备人员身份识别功能。

8.4 根据特殊需要,可在出入口设置金属探测器、X 射线包裹检查仪、爆炸物探测器等特殊检查装置。

8.5 出入口识别装置应与执行机构联锁。控制主机应监视执行机构的状态(开启、关闭闭锁、解锁)。执行机构控制应满足紧急撤离功能要求。

8.6 系统应对被设防区域的位置、通过对象和通过时间等进行实时记录。

8.7 系统的信息处理装置应能对系统中的有关信息自动记录、打印、贮存,并应有防篡改和防销毁等措施。

8.8 系统应具有下列管理功能:

- 路径管理;
- 人员管理;
- 时间管理;
- 权限管理;
- 执行机构模式管理;
- 统计管理;
- 所有操作的记录和跟踪;
- 报警管理;

——自诊断功能。

- 8.9 系统应具有防反传和防重入的功能。
- 8.10 系统软件应界面友好，操作方便，易于扩展。
- 8.11 出入口控制系统应与电视监控系统、入侵报警系统联动：当与火灾自动报警系统联动时，在有火警时应能自动打开公共通道上的安全门。
- 8.12 当供电不正常、断电时，系统地密钥（钥匙）信息及各记录信息不得丢失。
- 8.13 识读设备与控制器之间的通信用信号线宜采用多芯屏蔽双绞线。
- 8.14 门磁开关及出门按钮与控制其之间的通信用信号线，线芯最小截面积不宜小于 0.50 mm^2 。
- 8.15 控制器与执行机构之间的绝缘导线，线芯最小截面积不宜小于 0.75 mm^2 。
- 8.16 控制器与管理主机之间的通信用信号线宜采用双绞铜芯绝缘导线，其线径根据传输距离而定，线芯最小截面积不宜小于 0.50 mm^2 。
- 8.17 执行部分的输入电缆应在该出口的对应受控区、同级别受控区或高级别受控区外的部分，应封闭保护，其保护结构的抗拉伸、抗弯折强度应不低于镀锌钢管。
- 8.18 出入口控制系统设计除按照本规范规定外，应符合 GB 50396 及其它现行国家规范的规定。

9 电子巡查管理系统

- 9.1 巡查点应设置在巡更路线上，宜设在主要出入口、主要通道、紧急出入口和各主要部门。
- 9.2 保安人员的巡查报告方式可以采用在线或离线方式。对实时性要求高的项目宜采用在线方式。
- 9.3 巡查软件应在预先设定的巡查图中，对保安人员的巡查活动状态进行监督和记录，并应在发生意外情况时及时报警。
- 9.4 巡查记录应包括日期、时间、巡查编号、巡查人员档案等。
- 9.5 巡查软件应根据巡查计划的更改进行修改。
- 9.6 巡查系统宜独立设置，也可以与出入口控制系统、入侵报警系统或无线通信系统联合设置。
- 9.7 独立设置的保安人员巡查系统应与安防监控室联网，满足安防监控室对该系统进行集中管理与控制的有关要求。

10 汽车库（场）管理系统

10.1 系统应具有下列功能：

- 入口处车位显示（适用于公共停车场）；
- 出入口及场内通道的行车指示；
- 自动控制出入栅栏门；
- 自动计费与收费金额的显示，并可语音提示，票据打印；
- 多个出入口组的联网与监控管理；
- 整个停车场收费的统计与管理；
- 分层车辆统计与车位实时显示；
- 车辆号牌拍照自动识别；
- 意外发生时应有报警功能。

10.2 出、验票机或读卡器配置的选择应视汽车库（场）的性质确定。短期或临时用户可采用出、验票机或智能车牌识别的管理方式。长期或固定用户宜采用读卡器或智能车牌识别的管理方式。

10.3 在汽车库（场）的入口区应设置出票机、读卡器或智能车牌识别设备；并应在汽车库（场）的出口区设置验票机、读卡器或智能车牌识别设备。

- 10.4 车辆出入口两侧应设置地感线圈，与挡车器联动，并设防砸车装置以防车辆被砸损伤。
- 10.5 安全技术防范等级高的场所，应选用防冲撞装置（防冲撞挡车器、液压路障器等）。
- 10.6 宜独立设置电视监控系统或报警系统，当条件不允许时可采取与安全技术防范系统的视频安防监控系统、入侵报警系统联动的方式。
- 10.7 应与安全技术防范系统的安防监控室联网，满足安防监控室对该系统进行集中管理与控制的有关要求。

11 住宅（小区）访客对讲系统

- 11.1 住宅楼入口或单元入口应设置访客对讲装置，住户应设置对讲分机，并附有紧急报警按钮。当投资允许时，宜采用可视对讲装置。住户对讲分机应可对所对应入口位置的人员出入管控系统进行远程开门操作。
- 11.2 所有通往住宅楼内部的通道口，包括地下车库直接通向楼内的通道均应安装与楼门相同的访客对讲装置。
- 11.3 访客对讲系统应于小区安防监控室内设置管理主机，并能与所辖区域内住户对讲机进行双向通讯。

12 安防监控室

- 12.1 安防监控室应设置为禁区。
- 12.2 安防监控室的门应采用防盗门，窗应采取防止入侵的物理隔挡措施。
- 12.3 安防监控室的出入口应设置出入口控制装置，自动或由安防监控室内人员手动控制门的开启。
- 12.4 安防监控室应能在接收报警信号的同时立即识别报警的部位和性质，并在屏幕上显示；打印记录及存储报警的时间、部位、性质及处置预案。
- 12.5 安防监控室内应设置紧急报警装置。
- 12.6 进行住宅建筑规划总图设计时，应以独立管理的小区、独立管理的楼群为单位设置面积不小于 20 m²（含卫生间）的报警值班室（安防监控室），并应有保证值班人员正常工作的响应辅助设施。
- 12.7 安防监控室宜与消防控制室设置在相同楼层，满足环境噪声小，电磁干扰弱的要求并有安全防范和消防措施；安防监控室可与消防、建筑设备监控室等管理用房合用，但操作区域应相对独立。
- 12.8 安防监控室应设置直拨报警中心的外线电话，重要目标的安防监控室宜设置经由 2 个不同路由的直拨报警中心的外线电话。

13 网络信息安全

13.1 网络安全

- 13.1.1 保证关键网络设备性能、网络带宽满足基本业务需要，并绘制网络拓扑结构图。
- 13.1.2 网络设备具备身份鉴别、登陆失败处理等功能，远程管理时，要采取必要措施防止鉴别信息在网络传输过程中被窃取。
- 13.1.3 在网络边界部署访问控制设备，启用访问控制功能。

13.2 系统安全

- 13.2.1 设备操作系统遵循最小化安装原则，仅安装需要的组件和应用程序，并保持系统补丁及时得到更新。

- 13.2.2 安装防恶意代码软件，并及时更新防恶意代码软件版本和恶意代码库。
- 13.2.3 对设备操作系统、应用系统和数据库的用户进行身份标识和鉴别。
- 13.2.4 配置访问控制策略，分级授权管理，严格限定信息的访问、下载权限和使用范围限制默认账户的访问权限，修改账户默认用户及口令。
- 13.2.5 及时删除多余、过期账户，避免共享账户的存在。
- 13.2.6 对人员操作日志进行记录并保存，采取技术措施确保日志不可修改、删除。

13.3 信息安全

充分保护用户信息和公民个人隐私，除配合国家机关依法行使监督检查权、刑事侦查权和其他依法行使的国家权力外，不得向任何第三方提供小区车辆、居民、访客个人信息，不得泄露涉及社会公共安全的敏感信息。
