ICS
CCS 点击此处添加 CCS 号

T/

团 体 标 准

T/XXX XXXX—XXXX

安全防范 主动配合式人脸识别系统 技术要求

Security protection—Technical requirements for collaborative face recognition system

（征求意见稿）

20241212

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。

XXXX－XX－XX 发布 XXXX－XX－XX 实施

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。

本文件由上海安全防范报警协会提出并组织实施,上海安全防范报警协会标准化专业委员会归口。

本文件起草单位：

本文件主要起草人：

引　言

为更好地规范人脸识别技术在安全技术防范系统中实施应用，本标准针对安全防范领域应用的主动配合式人脸识别系统提出安全等级划分原则和方法。并按不同的安全等级，提出功能、性能和信息安全要求。本文件适用于包括但不限于DB 31/T 329系列标准覆盖的重点单位重点部位的人脸识别应用。

安全防范 主动配合式人脸识别系统技术要求

1 范围

本文件提出了安全防范领域主动配合式人脸识别系统的安全等级，规定了系统的功能、性能、信息安全和重点单位重点部位的安全等级要求。

本文件适用于安全技术防范系统中（包括但不限于出入口控制系统、人脸身份认证系统、实时电子巡检系统等）的主动配合式人脸识别系统产品和工程的设计、检测和验收，其他系统可参照执行。

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 38671—2020 信息安全技术 远程人脸识别系统技术要求

GB/T 41772—2022 信息技术 生物特征识别 人脸识别系统技术要求

GB/T 41786—2022 公共安全 生物特征识别 术语

GB/T 41819—2022信息安全技术 人脸识别数据安全要求

GB/T 41987—2022公共安全 人脸识别应用 防假体呈现攻击测试方法

GA/T 1093—2023 安全防范 人脸识别应用 出入口控制人脸识别技术要求

3 术语、定义和缩略语

3.1 术语和定义

GB/T 41787—2022界定的以及下列术语和定义适用于本文件。

3.1.1

用户 user

主动与系统进行交互，并需要系统对其身份权限进行验证的自然人。

[参考：GB/T 41772—2022: 3.3]

3.1.2

主动配合式人脸识别系统 collaborative face recognition systems

通过人脸识别技术对用户身份权限进行验证的系统。

3.1.3

人脸识别数据主体 face recognition data subject

人脸识别数据所标识或关联的自然人。

[参考：GB/T 41819—2022: 3.4]

3.1.4

呈现攻击 presentation attack

试图通过将假体呈现在采集设备前，达到干扰生物特征识别系统识别结果的目的。

[来源：GB/T 41786—2022: 3.13.4]

3.1.5

人脸关联数据 data associated with face

人脸数据所标识个体的相关信息。

注： 包含但不限于身份数据、活动轨迹数据和档案数据。

3.1.6

现场图像 on-site image

系统于出入口现场采集的原始图像。

3.1.7

响应时间 response time

系统从采集现场图像开始，到完成人脸识别，输出识别结果的时间。

注：在人脸确认模式中，响应时间不包含通过协作输入单元（如：证卡读取设备）读取或调用人脸图像/模板的时间。

3.1.8

协作输入单元 collaborative input unit

系统中接收辅助信息的单元。

注： 辅助信息一般来自身份证件读取设备。

3.2 缩略语

下列缩略语适用于本文件。

FAR：错误接受率（False Acceptance Rate）

FER：注册失败率（Failure to Enroll Rate）

FRR：错误拒绝率（False Rejection Rate）

4 系统说明

4.1 系统组成

主动配合式人脸识别系统（以下简称系统）主要由人脸图像采集部分、人脸图像解析部分、人脸识别部分、数据存储部分、决策部分、管理部分以及接口部分组成。各部分主要功能如下：

a) 人脸图像采集部分：用于采集原生人脸图像，通常有可见光采集方式、近红外采集方式等。

b) 人脸图像解析部分：用于处理解析人脸图像，包括图像预处理、人脸检测、质量判断、活体

检测、人脸特征提取等功能。

c） 人脸识别部分：用于人脸确认和/或人脸辨认。

d） 数据存储部分：用于存储人脸数据、人脸关联数据、识别记录等。

e） 识别决策部分：用于对人脸识别结果进行决策，如授权、拒绝、放行等

f） 管理部分：用于管理系统的总体策略、执行和应用，包括但不限于阈值设置、日志管理、记录管理、权限管理、安全管理等等

g） 接口部分：用户系统与其他外部系统或设备进行数据通信。

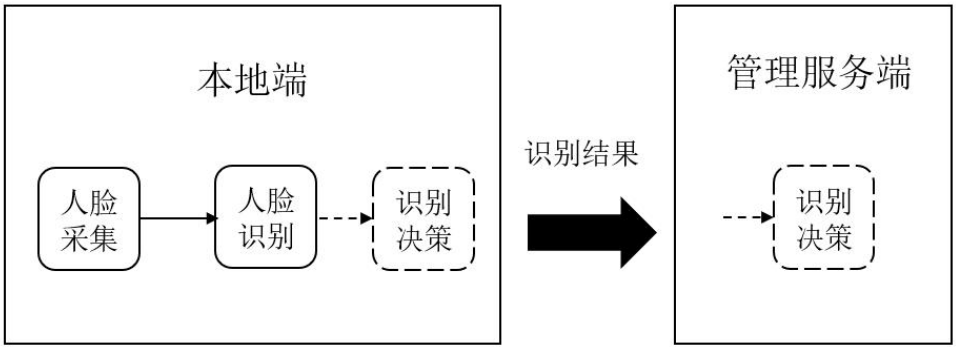
注： 系统的各组成部分仅表示其实现的功能，并不说明其部署在系统的具体位置。如人脸图像解析部分，即可能部署于本地端，也可能同时部署于管理服务端；数据存储部分即存在本地端也存在于管理服务端。

4.2 系统分类

4.2.1 按识别位置分类

根据系统的人脸识别部分所在位置不同，分为本地识别系统和远程识别系统。本地识别系统的人脸识别部分部署于本地端，远程识别系统的人脸识别部分部署在管理服务端。

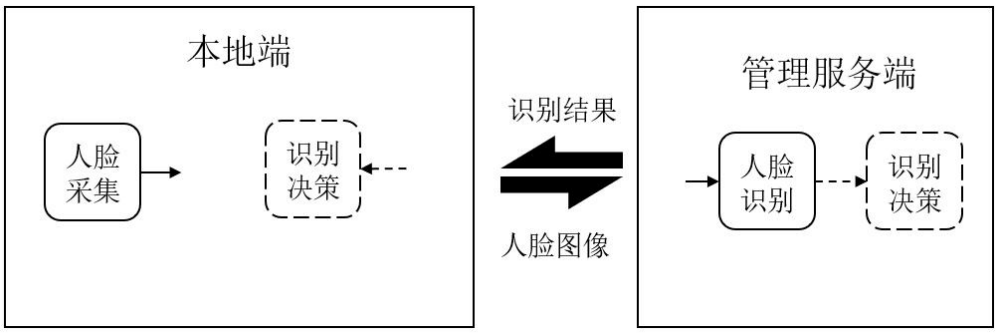
本地识别系统的人脸采集、人脸识别均在本地端完成，流程如图 1 所示。



注： 本地识别系统的识别决策部分可能在本地端，也可能在管理服务端。当识别决策部分在管理服务端时，管理服务端通过本地端传输的识别结果进行决策，如考勤。

图 1 本地识别系统

远程识别系统在本地端完成人脸采集后，将相关人脸数据传输至管理服务端进行人脸识别，流程如图 2 所示。

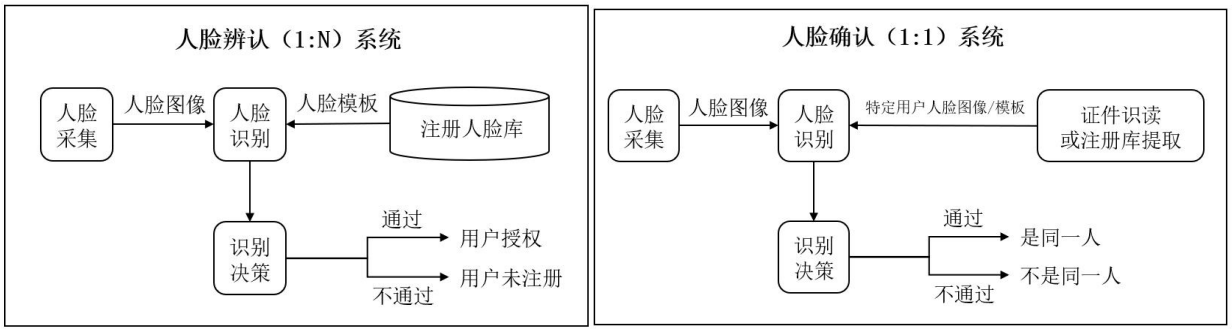


注： 远程识别系统的识别决策部分可能在本地端，也可能在管理服务端。当识别决策部分在本地时，管理服务端将识别结果传输至本地决策，如通过远程人脸验证后进入应用程序。

图 2 远程识别系统

4.2.2 按识别模式分类

根据系统的人脸识别模式不同，分为人脸辨认（1:N）系统和人脸确认（1:1）系统。人脸辨认系统采集现场人脸图像后，与系统的注册人脸库（人脸模板）进行人脸比对，辨认用户在系统中已注册的身份或该用户未注册，如图 3a)所示。人脸确认系统采集现场人脸图像后，与特定用户的本地读取证件人脸图像或系统中已有该特定用户的人脸图像或模板进行人脸比对，用以验证现场人脸图像与特定用户人脸图像为属于同一数据主体，如图 3b)所示。



a） 人脸辨认（1:N）系统　　b） 人脸确认（1:1）系统

图 3 人脸辨认系统和人脸确认系统

5 安全等级

5.1 一般要求

5.1.1 系统按照保护对象面临的风险程度和对防护能力差异化的需求，通过对系统中防呈现攻击能力、识别率等、信息安全等进行区分，构建对应的安全等级。

5.1.2 系统防护能力分为四个安全等级，安全等级 1 位最低等级，安全等级 4 位最高等级。

5.2 安全等级的划分

5.2.1 等级 1：低安全等级

防范对象为基本不具备主动配合式人脸识别知识，且仅使用常见、有限的工具试试破坏的攻击者。

注： 安全等级1的系统具有基本信息安全保护要求，满足最基本需求的识别率性能，能够抵御照片或视频等简易假体人脸呈现攻击。当出现错误识别、错误拒绝、防攻击失败等现象时，几乎不会对安全技术防范系统保护的对象造成损失。

5.2.2 等级 2：中低安全等级

防范对象为仅具有少量主动配合式人脸识别知识，懂得使用常规工具和便携式工具的攻击者。

注： 安全等级2的系统具有基本信息安全保护要求，满足较高的识别率性能，能够抵御照片和视频等简易假体人脸呈现攻击。当出现错误识别、错误拒绝、防攻击失败等现象时，不会对安全技术防范系统保护的对象造成较大损失。

5.2.3 等级 3：中高安全等级

防范对象为熟悉主动配合式人脸识别系统，可以使用复杂工具和便携式电子设备的攻击者。

注： 安全等级3的系统具有较高信息安全保护要求，满足最较高的识别率性能，能够抵御照片、视频以及面具等假体人脸呈现攻击。当出现错误识别、错误拒绝、防攻击失败等现象时，将会对安全技术防范系统保护的对象造成重大损失。

5.2.4 等级 4：高安全等级

防范对象为熟悉主动配合式人脸识别系统，具备实施攻击的详细计划和所需的能力或资源，具有所有可获得的设备，且懂得替换主动配合式人脸识别系统的部件方法的攻击者。

注： 安全等级4的系统具有较高信息安全保护要求，满足最高的识别率性能，能够抵御照片、视频、面具、头模等复杂精细工艺的假体人脸呈现攻击。当出现错误识别、错误拒绝、防攻击失败等现象时，将会对安全技术防范系统保护的对象造成特别重大损失。

6 功能要求

6.1 明示告知/同意

明示告知/同意应符合表1中A的要求。

6.2 图像质量判断

图像质量判断应符合表1中B的要求。

6.3 呈现攻击检测

呈现攻击检测应符合表1中C的要求。

6.4 人脸注册

人脸注册应符合表1中D的要求。

6.5 人脸识别

人脸识别应符合表1中E的要求。

6.6 管理功能

人脸查重应符合表1中F的要求。

表1 系统功能要求

项目	序号	要求	安全等级			
			1	2	3	4
A 明示告知 /同意	1	人脸数据及人脸关联数据采集应经数据主体授权同意，系统应具有向数据主体明示告知数据用途，提供数据应用范围和存储方式的选择项，提供确认、取消等操作选项，获得数据主同意体授权后进行采集	M	M	M	M
	2	采用导入或其他方式进行批量人脸注册的系统，批量注册的人脸数据及人脸关联数据应经数据主体授权同意，并具有确认、取消等操作选项	M	M	M	M
	3	对人脸数据进行导出操作时，需经过系统管理员授权同意，并具有确认、取消等操作选项。	M	M	M	M
B 图像质量 判断	4	当注册图像的图像质量不符合系统注册要求时，拒绝注册后应给出质量判断结果	OP	OP	M	M

表1（续）

项目	序号	要求	安全等级			
			1	2	3	4
B 图像质量判断	5	当现场采集的人脸图像不满足系统人脸识别要求时，本地端应给出可听/可视的提示	OP	OP	M	M
	6	当人脸有效面积遮挡过大时，应不能进行人脸识别，并给出给出可听/可视的提示	OP	OP	M	M
C 呈现攻击检测	7	具有呈现攻击检测能力，能够抵御不同类型假体人脸的呈现攻击。假体人脸符合GB/T 41987—2022中附录A的要求。根据不同抵御能力，分为以下四个级别： ● 级别I：应能检测人脸照片、人脸视频等2类人脸假体中的至少一种。 ● 级别II：应能检测人脸照片、人脸视频等2类人脸假体。 ● 级别III：应能检测人脸照片、人脸视频、人脸仿真面具等3类人脸假体 ● 级别IV：应能检测包括人脸照片、人脸视频、仿真人脸面具、仿真人脸头模等在内的至少4类人脸假体	级别I或以上	级别II或以上	级别III或以上	级别IV
	8	检测到呈现攻击时，宜给出可听/可视的受攻击提示	OP	OP	M	M
D 人脸注册	9	应符合GA/T 1093-2023中5.7的要求。	M	M	M	M
E 人脸识别	10	具有人脸确认识别模式的系统，用户证件信息读取方式应至少包含身份证读取	OP	OP	M	M
	11	多人脸识别：同一画面中检测并识别多张人脸	OP	OP	OP	OP
	12	戴口罩人脸识别：当用户佩戴口罩时，应能进行人脸识别	OP	OP	OP	OP
	13	佩戴口罩识别：应能检测用户是否佩戴口罩，并给出响应的提示	OP	OP	OP	OP
	14	远程人脸识别系统的功能符合GB/T 38671—2020中第6章的相关要求	OP	OP	OP	OP
F 管理功能	15	应符合GA/T 1093-2023中5.6的要求。	M	M	M	M
注：M表示必选项，OP表示可选项。						

7 性能要求

7.1 图像采集性能

图像采集性能应符合表2中A的要求。

7.2 距离与角度

距离与角度应符合表2中B的要求。

7.3 环境照度适应性

环境照度适应性应符合表2中C的要求。

7.4 防呈现攻击失败率

防呈现攻击失败率应符合表2中D的要求。

7.5 存储容量

存储容量应符合表2中E的要求。

7.6 注册失败率

注册失败率应符合表2中F的要求。

7.7 识别准确率

识别准确率应符合表2中G的要求。

7.8 响应时间

响应时间应符合表2中H的要求。

表2 系统性能要求

项目	序号	要求	安全等级			
			1	2	3	4
A 图像采集	1	采集图像的水平分辨力	≥ 720TVL	≥ 720TVL	≥ 720TVL	≥ 720TVL
	2	采集图像的灰度等级	10级	10级	11级	11级
B 距离与角度	3	人员人脸与图像采集设备采集点中心位置水平对齐后，能进行人脸识别的距离范围	0.3m ～ 1.2m	0.3m～ 1.2m	0.3m～ 1.2m	0.3m～ 1.0 m
	4	能够进行人脸识别的水平角度转动范围	±30°	±30°	±30°	±30°
	5	能够进行人脸识别的倾斜角转动范围	±30°	±30°	±30°	±30°
	6	能够进行人脸识别的俯仰角转动范围	±20°	±20°	±20°	±20°
C 环境照度适应性	7	在侧光、逆光、顺光条件下，系统满载（注册人数=系统系统声明容量）条件下，环境照度为暗光(10Lux～10000Lux)时能进行人脸识别	M	M	M	M

表2（续）

项目	序号	要求	安全等级			
			1	2	3	4
C 环境照度适应性	8	在侧光、逆光、顺光条件下，系统满载（注册人数=系统系统声明容量）条件下，环境照度为暗光(10Lux及以下)时能进行人脸识别	OP	OP	OP	OP
	9	在侧光、逆光、顺光条件下，系统满载（注册人数=系统系统声明容量）条件下，环境照度为强光(10000Lux～100000Lux)时能进行人脸识别	OP	OP	OP	OP
	10	在侧光、逆光、顺光条件下，系统满载（注册人数=系统系统声明容量）条件下，环境照度为超强光(100000Lux～200000Lux及以上)时能进行人脸识别	OP	OP	OP	OP
D 防呈现攻击失败率	11	防人脸照片攻击失败率	5%[1]	5%	5%	5%
	12	防人脸视频攻击失败率	5%[1]	5%	5%	5%
	13	防仿真人脸面具攻击失败率	OP	OP	10%	5%
	14	防仿真人脸头模攻击失败率	OP	OP	OP	10%
E 系统容量	15	系统注册人脸库（人脸模板）数量	根据实际应用声明	根据实际应用声明	根据实际应用声明	根据实际应用声明
	16	人脸识别记录数量是系统注册人脸库（人脸模板）数量的倍数	5倍或以上	5倍或以上	5倍或以上	5倍或以上
F 注册失败率	17	人脸辨认模式下的注册失败率	≤0.5%	≤0.1%	≤0.05%	≤0.03%
G 识别准确率	18	系统满载（注册人数=系统系统声明容量）条件下，人脸辨认模式下的识别准确率	FAR≤5%且FRR≤5%	FAR≤3%且FRR≤5%	FAR≤2%且FRR≤2%	FAR≤1%且FRR≤2%
	19	人脸确认模式下的识别准确率	FAR≤1%且FRR≤2%	FAR≤0.1%且FRR≤2%	FAR≤0.03%且FRR≤2%	FAR≤0.01%且FRR≤2%

表2（续）

项目	序号	要求	安全等级			
			1	2	3	4
H 响应时间	21	系统满载（注册人数=系统系统声明容量）条件下，呈现攻击检测关闭条件下，人脸识别响应时间	≤1s	≤1s	≤1s	≤1s
	22	系统满载（注册人数=系统系统声明容量）条件下，呈现攻击检测开启条件下，人脸识别响应时间	≤3s	≤3s	≤2s	≤2s
注1：M表示必选项，OP表示可选项。 注2：5%[1]表示有相同编号的数字指标至少被选择一项。						

8 信息安全要求

8.1 设备身份验证

图像采集性能应符合表3中A的要求。

8.2 用户身份验证

用户身份认证应符合表3中B的要求。

8.3 数据传输

数据传输应符合表3中C的要求。

8.4 访问控制

访问控制应符合表3中D的要求。

8.5 数据存储

数据存储应符合表3中E的要求。

8.6 数据脱敏

数据脱敏应符合表3中F的要求。

8.7 用户权限

用户权限应符合表3中G的要求。

8.8 操作日志

操作日志应符合表3中H的要求。

表3 系统信息安全要求

项目	序号	要求	安全等级			
			1	2	3	4
A 设备身份验证	1	基本级：基于设备身份ID号、MAC地址等的合法性验证 增强级：基于数字证书的双向身份验证机制，并对证书集中管理	基本级	基本级	增强级	增强级

表3（续）

项目	序号	要求	安全等级			
			1	2	3	4
B 用户身份验证	2	基本级：设备或系统的登录密码应具备不低于8位的复杂度，包含数字、字母或特殊字符中的2种； 增强级：设备或系统的登录密码应具备不低于10位的复杂度，密码不含用户名等，包含数字、字母和特殊字符，并要求定期更换。	基本级	基本级	增强级	增强级
	3	基本级：登录不成功尝试次数超过设定最大次数时，应对非法身份仿冒连续攻击行为进行限制； 增强级：1.满足基本级要求2.配置当登录连接超时自动退出等措施。	基本级	基本级	增强级	增强级
	4	基本级：采用口令技术对用户进行身份验证 增强级：采用口令、数字证书或生物特征识别等两种或两种以上组合的鉴别技术对用户进行身份验证	基本级	基本级	增强级	增强级
C 数据传输	5	基本级：本地识别系统联网应用时，应采用校验技术保证通信过程中数据的完整性 增强级：本地识别系统联网应用时，应采用数据加密技术满足人脸数据和人脸关联数据在传输过程中的保密性	基本级	增强级	增强级	增强级
	6	基本级：远程识别系统联网应用时，应采用密码技术保证通信过程中数据的完整性 增强级：远程识别系统联网应用时，1.应采用端到端加密或传输通道加密的传输安全策略2.具备在构建传输通道前对两端主体身份进行鉴别的能力、3.支持数据真实性检测，采用国密算法	基本级	增强级	增强级	增强级
D 访问控制	7	基本级：应能对非授权设备连接系统的行为进行检查 增强级：1.满足基本级要求2.应能设置访问控制规则，默认情况下除允许通信外受控接口拒绝所有通信	基本级	基本级	增强级	增强级
	8	基本级：应能对系统内部设备连接到外部网络的行为进行检查 增强级：1.满足基本级要求2.应能设置访问控制规则，默认情况下除允许通信外受控接口拒绝所有通信	基本级	基本级	增强级	增强级

表3（续）

项目	序号	要求	安全等级			
			1	2	3	4
E 数据存储	9	基本级：在采集和存储数据主体的原始证件图像、现场图像、人脸图像时，应遵循最小够用原则，根据实际应用需求，选择需要保存的最小数量、最少类型的图像	基本级	基本级	基本级	基本级
	10	基本级：人脸数据和人脸关联数据不应使用图片、明文或Base64等直接图像文件或简单编码方式直接存储。 增强级：1.满足基本级要求2.数据库存储的人脸数据和人脸关联数据应采用加密技术并分表，宜分区存储	基本级	基本级	增强级	增强级
	11	基本级：人脸数据和人脸关联数据的使用应能配置使用期限，到期应自动删除相关数据或匿名化处理或去标识化处理	基本级	基本级	基本级	基本级
F 数据脱敏	12	基本级：针对人脸数据和人脸关联数据的展示时，应采取匿名化等措施防止信息过量展示	基本级	基本级	基本级	基本级
F 用户权限	13	基本级：应具有用户权限管理，用户在授权范围内完成对人脸识别应用的登录、注册、编辑、存储、使用、查询、删除、备份等操作	基本级	基本级	基本级	基本级
G 操作日志	14	基本级：1.进行与人脸数据和人脸关联数据的相关操作（如编辑信息、导出数据、告警处理等）时，均应生成操作日志。2.操作日志应包含操作人员、操作时间、操作地址、操作行为等信息。3.操作日志应不能更改或删除 增强级：1.满足基本级要求2.操作日志应至少保存6个月	基本级	基本级	增强级	增强级

9 重点单位安全等级要求

在DB31/T 329系列标准覆盖的重点单位的安全技术防范系统部署了主动配合式人脸识别系统，其一般部位和重点部位的系统安全等级应符合表4的要求，其他系统可参照执行。

表4 重点单位安全技术防范系统中部署的主动配合式人脸识别系统安全等级要求

序号	重点单位	一般部位	重点部位
1	展览馆、博物馆	等级2及以上	等级3及以上 包括但不限于：数据机房、监控室、一、二级风险展品/藏品的库区、库房、技术保护用房、需双人双锁管理的出入口及设计中规定的其他重点部位
2	危险化学品、放射性同位素集中存放场所	等级2及以上	等级3及以上 包括但不限于数据机房、监控室、剧毒化学品仓库、需双人双锁管理的出入口及设计中规定的其他重点部位
3	金融单位	等级3及以上	等级4 包括但不限于数据机房、监控室、银行自助设备加钞间出入口、大额现金类银行自助设备放置区、需双人或多人组合进入出入口、金库门、守库室及设计中规定的其他重点部位
4	公共供水	等级2及以上	等级3及以上 包括但不限于数据机房、监控室、危化品加药间出入口、重要物资仓库出入口及设计中规定的其他重点部位
5	电力设施	等级2及以上	等级3及以上 包括但不限于数据机房、监控室、重要物资仓库出入口及设计中规定的其他重点部位
6	中小学、幼儿园、托育机构	等级2及以上	等级3及以上 包括但不限于数据机房、监控室、危化品存储实验室出入口及设计中规定的其他重点部位
7	城市轨道交通	等级2及以上	等级3及以上 包括但不限于数据机房、监控室、重要物资仓库出入口、需双人双锁管理的出入口及设计中规定的其他重点部位
8	旅馆、商务办公楼	等级2及以上	等级3及以上 包括但不限于数据机房、监控室、贵重物品寄存处及设计中规定的其他重点部位
9	零售商业	等级2及以上	等级3及以上 包括但不限于数据机房、监控室及设计中规定的其他重点部位
10	党政机关	等级2及以上	等级3及以上 包括但不限于数据机房、监控室、档案资料室、机要室、需双人双锁管理的出入口及设计中规定的其他重点部位

表4（续）

序号	重点单位	一般部位	重点部位
11	医疗机构	等级2及以上	等级3及以上 包括但不限于数据机房、监控室、危化品存储仓库出入口、医疗废物集中存放场所出入口、需双人双锁管理的出入口及设计中规定的其他重点部位
12	通信单位	等级2及以上	等级3及以上 包括但不限于数据机房、监控室、需双人双锁管理或多人组合进入的出入口及设计中规定的其他重点部位
13	枪支弹药生产、经销、存放、射击场所	等级2及以上	等级3及以上 包括但不限于数据机房、监控室、枪支弹药库室出入口、档案（资料）室、需双人双锁管理或多人组合进入的出入口及设计中规定的其他重点部位
14	燃气系统	等级2及以上	等级3及以上 包括但不限于数据机房、监控室、需双人双锁管理的仓库出入口及设计中规定的其他重点部位
15	公交车站和公交专用停车场库	等级2及以上	
16	港口、码头	等级2及以上	
17	监管场所	等级2及以上	等级3及以上 包括但不限于数据机房、监控室、警用装备室、档案资料室、需双人双锁管理的仓库出入口及设计中规定的其他重点部位
18	渡轮、游览船	等级2及以上	
19	寄递单位	等级2及以上	
20	游乐场所	等级2及以上	等级3及以上 包括但不限于数据机房、监控室、重要动力机房出入口、需双人双锁管理的仓库出入口及设计中规定的其他重点部位
21	养老机构	等级2及以上	等级3及以上 包括但不限于数据机房、监控室、档案资料室、需双人双锁管理的仓库出入口及设计中规定的其他重点部位

22	军工单位	等级3及以上	
23	大型活动场所	等级2及以上	等级3及以上 包括但不限于数据机房、监控室、需双人双锁管理的仓库出入口及设计中规定的其他重点部位
24	高校	等级2及以上	等级3及以上 包括但不限于数据机房、监控室、承担涉及国家机密项目（课题）的研究机构场所，机要室、档案室、国家实验室、国家重点实验室、高价值教学与科研设备存放场所，核、生、化、爆等实验室及危险品生产、使用、储藏场所，管制物品、贵重物品集中存放或生产、制作及销毁场所、需双人双锁管理的仓库出入口及设计中规定的其他重点部位
25	民用机场航站楼	等级3及以上	
26	化工企业	等级3及以上	