UDC

P

中华人民共和国国家标准

GB 55029—2022

安全防范工程通用规范

General code of security engineering

2022－03－10 发布　　2022－10－01 实施

中华人民共和国住房和城乡建设部
国家市场监督管理总局　联合发布

中华人民共和国国家标准

安全防范工程通用规范

General code of security engineering

GB 55029—2022

主编部门：中华人民共和国公安部
批准部门：中华人民共和国住房和城乡建设部
施行日期：2022年10月1日

中国计划出版社

2022 北 京

中华人民共和国国家标准

安全防范工程通用规范

GB 55029—2022

☆

中国计划出版社出版发行

网址：www.jhpress.com

地址：北京市西城区木樨地北里甲 11 号国宏大厦 C 座 3 层

邮政编码：100038　电话：（010）63906433（发行部）

北京市科星印刷有限责任公司印刷

850mm×1168mm　1/32　2 印张　50 千字

2022 年 7 月第 1 版　2022 年 7 月第 1 次印刷

☆

统一书号：155182·0919

定价：30.00 元

中华人民共和国住房和城乡建设部
公　告

2022年　第48号

住房和城乡建设部关于发布国家标准《安全防范工程通用规范》的公告

现批准《安全防范工程通用规范》为国家标准，编号为GB 55029-2022，自2022年10月1日起实施。本规范为强制性工程建设规范，全部条文必须严格执行。现行工程建设标准中有关规定与本规范不一致的，以本规范的规定为准。同时废止下列工程建设标准相关强制性条文：

一、《安全防范工程技术标准》GB 50348-2018第1.0.6、6.1.3、6.1.5、6.3.6(1、2、4、5)、6.3.8(2、3)、6.3.11(1、3)、6.3.12(3、4)、6.3.13(2、3、4)、6.4.3(2、3、4、5、6、7、8、14)、6.4.5(1、2、3、4、5、7、10)、6.4.7(8、11、13)、6.4.9(5)、6.4.10(1、3、4、9)、6.4.12(5、9)、6.6.2(1、2、3)、6.6.4(3、5、6)、6.6.5(1、3)、6.12.4(3)、6.13.1(4)、6.13.3(2)、6.13.4(4、5、6)、6.14.2(1、2、3、4)、6.14.3(2)、7.2.4(3、5、12)、9.1.3、11.1.5、11.1.6、11.2.7条(款)。

二、《入侵报警系统工程设计规范》GB 50394-2007第3.0.3、5.2.2、5.2.3、5.2.4、9.0.1(3)条(款)。

三、《视频安防监控系统工程设计规范》GB 50395-2007第

3.0.3、5.0.4(3)、5.0.5、5.0.7(3)条(款)。

四、《出入口控制系统工程设计规范》GB 50396-2007 第3.0.3、5.1.7(3)、6.0.2(2)、7.0.4、9.0.1(2)条(款)。

本规范在住房和城乡建设部门户网站(www.mohurd.gov.cn)公开,并由住房和城乡建设部标准定额研究所组织中国计划出版社有限公司出版发行。

中华人民共和国住房和城乡建设部

2022年3月10日

前　言

为适应国际技术法规与技术标准通行规则，2016 年以来，住房和城乡建设部陆续印发《深化工程建设标准化工作改革的意见》等文件，提出政府制定强制性标准、社会团体制定自愿采用性标准的长远目标，明确了逐步用全文强制性工程建设规范取代现行标准中分散的强制性条文的改革任务，逐步形成由法律、行政法规、部门规章中的技术性规定与全文强制性工程建设规范构成的“技术法规”体系。

关于规范种类。强制性工程建设规范体系覆盖工程建设领域各类建设工程项目，分为工程项目类规范（简称项目规范）和通用技术类规范（简称通用规范）两种类型。项目规范以工程建设项目整体为对象，以项目的规模、布局、功能、性能和关键技术措施等五大要素为主要内容。通用规范以实现工程建设项目功能性能要求的各专业通用技术为对象，以勘察、设计、施工、维修、养护等通用技术要求为主要内容。在全文强制性工程建设规范体系中，项目规范为主干，通用规范是对各类项目共性的、通用的专业性关键技术措施的规定。

关于五大要素指标。强制性工程建设规范中各项要素是保障城乡基础设施建设体系化和效率提升的基本规定，是支撑城乡建设高质量发展的基本要求。项目的规模要求主要规定了建设工程项目应具备完整的生产或服务能力，应与经济社会发展水平相适应。项目的布局要求主要规定了产业布局、建设工程项目选址、总体设计、总平面布置以及与规模相协调的统筹性技术要求，应考虑供给能力合理分布，提高相关设施建设的整体水平。项目的功能要求主要规定项目构成和用途，明确项目的基本组成单元，是项目

发挥预期作用的保障。项目的性能要求主要规定建设工程项目建设水平或技术水平的高低程度，体现建设工程项目的适用性，明确项目质量、安全、节能、环保、宜居环境和可持续发展等方面应达到的基本水平。关键技术措施是实现建设项目功能、性能要求的基本技术规定，是落实城乡建设安全、绿色、韧性、智慧、宜居、公平、有效率等发展目标的基本保障。

关于规范实施。强制性工程建设规范具有强制约束力，是保障人民生命财产安全、人身健康、工程安全、生态环境安全、公众权益和公众利益，以及促进能源资源节约利用、满足经济社会管理等方面的控制性底线要求，在工程建设项目的勘察、设计、施工、验收、维修、养护、拆除等建设活动全过程中必须严格执行，其中，对于既有建筑改造项目（指不改变现有使用功能），当条件不具备、执行现行规范确有困难时，不应低于原建造时的标准。与强制性工程建设规范配套的推荐性工程建设标准是经过实践检验的、保障达到强制性规范要求的成熟技术措施，一般情况下也应当执行。在满足强制性工程建设规范规定的项目功能、性能要求和关键技术措施的前提下，可合理选用相关团体标准、企业标准，使项目功能、性能更加优化或达到更高水平。推荐性工程建设标准、团体标准、企业标准要与强制性工程建设规范协调配套，各项技术要求不得低于强制性工程建设规范的相关技术水平。

强制性工程建设规范实施后，现行相关工程建设国家标准、行业标准中的强制性条文同时废止。现行工程建设地方标准中的强制性条文应及时修订，且不得低于强制性工程建设规范的规定。现行工程建设标准（包括强制性标准和推荐性标准）中有关规定与强制性工程建设规范的规定不一致的，以强制性工程建设规范的规定为准。

目　　次

1 总　则

1.0.1 为规范安全防范工程建设、安全防范系统运行与维护，提高安全防范水平，保护人身安全和财产安全，维护社会安全稳定，制定本规范。

1.0.2 安全防范工程必须执行本规范。

1.0.3 安全防范工程建设、安全防范系统运行与维护应遵循下列原则：

1 防范与风险相适应；

2 人力防范、实体防范、电子防范相结合，探测、延迟、反应相协调；

3 满足纵深防护、均衡防护的要求；

4 满足安全防范系统安全、可靠、稳定运行的要求。

1.0.4 工程建设所采用的技术方法和措施是否符合本规范要求，由相关责任主体判定。其中，创新性的技术方法和措施应进行论证并符合本规范中有关性能的要求。

2 基本规定

2.0.1 安全防范工程建设、安全防范系统运行与维护应做到全生命周期协调管理。

2.0.2 安全防范系统应由实体防护系统和电子防护系统构成，并应符合下列规定：

1 应选择利用天然屏障、人工屏障、防护器具（设备）等构建实体防护系统；

2 应选择入侵和紧急报警系统、视频监控系统、出入口控制系统、停车库（场）安全管理系统、安全检查系统、楼寓对讲系统、电子巡查系统、安全防范管理平台等构建电子防护系统。

2.0.3 安全防范系统使用的设备、材料应检测合格。

2.0.4 安全防范系统和设备登录密码不应为弱口令，不应存在网络安全漏洞和隐患。当基于不同传输网络的系统和设备联网时，应采取相应的网络边界安全管理措施。

2.0.5 安全防范工程建设、安全防范系统运行与维护应落实安全保密责任，应具有保护国家秘密、商业秘密和个人隐私的措施。

3 工程设计

3.1 布防设计

3.1.1 安全防范工程设计应明确保护对象(包括保护单位、保护区域或部位、保护目标等)及其安全需求,确定需要防范的风险。

3.1.2 安全防范工程设计应根据风险防范要求,确定防护点位和系统、设备的功能、性能。高风险保护对象安全防范工程设计前应进行现场勘察。

3.1.3 周界防护应根据现场环境和安全防范管理要求,选择设置实体防护、入侵探测、视频监控等设施,有效覆盖需要防护的区域,并应符合下列规定:

1 实体防护设施应具有阻挡或延迟相应风险的能力;

2 入侵探测设备应具有对攀爬、翻越、挖凿、穿越等一种或多种入侵行为的探测能力;

3 视频监控装置采集的图像应能清晰显示关注目标的活动情况。

3.1.4 出入口防护应根据现场环境和安全防范管理要求,选择设置实体防护、出入口控制、入侵探测、视频监控等设施,并应符合下列规定:

1 在满足通行能力的前提下,应减少周界出入口数量。与周界相连且无人值守的出入口,其实体屏障的防护能力应与周界实体防护能力相当。

2 出入口控制装置应能满足目标识别、出入管理的要求,并应具有防拆卸、防技术开启等防护能力。

3 入侵探测设备应具有针对出入口部位入侵行为的探测能力。

4 视频监控装置采集的图像应能清晰显示行人出入口处进

出行人的体貌特征和车辆出入口处通行车辆的号牌。

3.1.5 走道、通道和公共活动场所防护应根据现场环境和安全防范管理要求，选择设置视频监控、入侵探测、实体防护等设施，并应符合下列规定：

1 视频监控装置采集的图像应能清晰显示监控区域内人员、物品、车辆的通行、活动情况；

2 入侵探测设备应具有针对通道、公共活动场所入侵行为的探测能力；

3 实体屏障应具有限制或阻挡人员、车辆通行的相应能力。

3.1.6 人员密集场所起隔离疏导作用的实体防护、出入口控制设施等，应满足紧急情况下人员疏散的要求。

3.1.7 重要保护部位的防护应根据现场环境和安全防范管理要求，选择设置实体防护、入侵探测、出入口控制、视频监控等设施，防护能力应满足相应的阻挡延迟、入侵行为探测、出入目标控制、场景监视等要求。

3.1.8 高风险保护对象的安全防范系统应设置监控中心，监控中心选址应远离产生粉尘、油烟、有害气体的场所，以及生产或贮存腐蚀性、易燃、易爆物品的场所，并应远离强震源和强噪声源。

3.1.9 高风险保护对象的监控中心防护应符合下列规定：

1 应设置视频监控装置，且其采集的图像应能清晰显示人员出入及室内活动的情况；

2 应配备内外联络的通信设备；

3 应设置紧急报警装置，并能够向外发送报警信息；

4 当监控中心值守区与设备区为两个独立物理区域且不相邻时，两个区域之间的传输线缆应采取保护措施；

5 独立的监控中心设备区除应符合本条第1款～第3款的规定外，还应设置入侵探测、出入口控制装置。

3.1.10 对保护目标的防护应根据现场环境和安全防范管理要求，选择设置实体防护、入侵探测、位移探测、视频监控等设施，并

应符合下列规定：

1 实体防护设施应满足不同保护目标抵御相应风险的要求；

2 入侵探测、位移探测等装置应能探测接近、移动保护目标的入侵行为；

3 视频监控区域应覆盖保护目标，采集的图像应能清晰显示监控区域内人员的活动情况；

4 当保护目标涉密或有隐私保护需求时，视频监控应满足保密或隐私保护的要求。

3.1.11 当需要对通行人员、物品、车辆安全检查时，应在保护区域的出入口或其附近设置安全检查区，并应配备相应的安全检查和处置设施。

3.1.12 易燃、易爆等特殊环境的安全防范系统设计前，应进行危险源辨识，并应根据危险场所类型，选择设备及部署位置，规划管线路由。

3.1.13 当保护对象被确定为恐怖袭击重点目标时，除应符合本规范第3.1.2条～第3.1.12条的规定外，尚应选择下列一种或多种防护措施：

1 加强周界防范措施；

2 对出入人员、物品、车辆等进行安全检查；

3 重要的出入口、走道和通道设置人行通道闸、车辆实体屏障、安全缓冲区、隔离区等；

4 人员密集区域加强视频监控和动态监测、预警；

5 监控中心及其他重要部位(区域)联合设置实体防护和电子防护设施；

6 对无人飞行器采取防御措施；

7 加强人力防范资源配置。

3.2 系统架构设计

3.2.1 应按照安全可控、开放共享的原则，确定安全防范系统的

子系统组成、集成/联网方式、传输网络、系统管理、存储模式、系统供电、接口协议等要素。

3.2.2 应根据现场勘察和风险防范要求以及布防设计情况，确定安全防范系统的各子系统。

3.2.3 应根据各类信息资源共享、交换的实际需要以及系统复杂程度，选择下列一种或多种系统集成/联网方式：

1 子系统设备之间信号驱动联动；

2 子系统之间协议通信联动；

3 安全防范管理平台对各子系统集成；

4 安全防范管理平台之间联网；

5 安全防范管理平台与其他系统联网。

3.2.4 高风险保护对象的安全防范系统应采用专用传输网络。

3.2.5 安全防范管理平台应具有集成管理、信息管理、用户管理、设备管理、联动控制、日志管理、数据统计等功能。

3.2.6 应根据安全防范系统信息存储与管理的需要，确定存储模式。

3.2.7 应根据安全防范系统及其设备的分布特点、供电条件和安全保障需求，确定供电模式和保障措施。

3.2.8 应根据安全防范系统集成/联网以及信息共享应用的需要，确定系统接口以及信息传输、交换、控制协议。

3.3 人力防范措施

3.3.1 应综合考虑实体防范、电子防范能力以及系统正常运行、应急处置的需要，进行人力防范资源配置。

3.3.2 应配备安全保卫、系统值机操作和维护等人员，并应对各岗位人员进行技术、技能培训。

3.3.3 应配备必要的个人防护、对抗性装备。

3.3.4 应针对可能发生的治安和恐怖风险事件制订应急预案，并应组织演练。

3.4 实体防护系统设计

3.4.1 实体防护系统设计应与建筑选址、建筑设计、景观设计统筹规划、同步设计。

3.4.2 实体防护系统设计应针对需要防范的风险，通过周界实体防护设计、建(构)筑物设计和实体装置设计，实现相应的威慑、阻挡、延迟等防护能力。

3.4.3 周界实体防护设计应符合下列规定：

1 应根据场地条件和防范的风险确定周界实体屏障的类型和位置；

2 当保护对象有防御爆炸攻击要求时，应选择具有相应防护能力的实体屏障，并应合理确定实体屏障与保护对象的安全距离；

3 穿越周界的河道以及涵洞、管廊等可容纳防范对象进入的孔洞，应设置实体屏障进行防护；

4 应根据防范车辆的种类、重量、速度等因素，确定周界出入口车辆实体屏障的类型、规格尺寸、结构强度、固定方式等。

3.4.4 建(构)筑物设计应符合下列规定：

1 应进行建(构)筑物场地的交通流线设计，并应利用场地和景观形成障碍、缓冲区、隔离带等。

2 易燃、易爆、有毒、放射性等保护目标的存放场所应设置在隐蔽和远离人群的位置。

3 当高风险保护对象建(构)筑物的洞口、管沟、管廊、吊顶、风管、槽盒、管道等空间尺寸可容纳防范对象进入时，应采用实体屏障或实体构件进行封闭或阻挡。

4 当建(构)筑物的墙体有防爆炸要求时，应进行防爆结构设计。当门窗有防盗、防爆炸、防弹、防砸等要求时，应采用相应的防护措施。

3.4.5 应根据保护目标的防盗窃、防窥视、防砸、防撬、防弹、防爆炸等安全需求，配置相应的实体装置。

3.4.6 当设置具有锐利边缘、触碰时易对人体造成伤害的防护设施时，应在其安装区域设置警示标识。

3.5 电子防护系统设计

3.5.1 入侵和紧急报警系统设计应根据需要防范的风险和现场环境条件等因素，选择相应的设备，设计安装位置和传输路由，具备对隐蔽进入、强行闯入以及撬、挖、凿等入侵行为的探测与报警功能，并应符合下列规定：

1 系统应准确、及时地探测入侵行为和紧急报警装置触发状态，发出报警信号；

2 入侵探测器和控制指示设备应具有防拆报警功能；

3 当报警信号传输线缆断路或短路、探测器电源线被切断时，控制指示设备应能发出报警信号；

4 系统应具有参数设置和用户权限设置功能；

5 系统应具有设防、撤防、旁路、胁迫报警等功能；

6 系统应能对入侵、紧急、防拆、故障等报警信号准确指示；

7 系统应能对操作、报警和警情处理等事件进行记录，且不可更改；

8 单控制器系统报警响应时间不应超过 2s；

9 备用电源应能保证系统正常工作时间不少于 8h。

3.5.2 视频监控系统设计应根据视频图像采集、目标识别的需要和现场环境条件等因素，选择相应的设备，具备对监控区域和目标进行视频采集、传输、处理、控制、显示、存储与回放等功能，并应符合下列规定：

1 系统的监控区域应有效覆盖保护区域、部位和目标，监视效果应满足场景监控或目标特征识别的需求；

2 系统应具备按照授权对前端视频采集设备进行实时控制，或进行工作状态调整的能力；

3 系统应具备按照授权实时调度指定视频信号到指定终端

的能力；

4 系统应能实时显示系统内的所有视频图像；

5 视频图像信息存储的时间不应少于30d；

6 系统应具备设备管理、用户管理及日志管理等功能。

3.5.3 出入口控制系统设计应根据通行对象进出各受控区的安全管理要求，选择适当类型的识读、控制与执行设备，具备凭证识别查验、进出授权、控制与管理等功能，并应符合下列规定：

1 安装于受控区以外的部件应采取防拆保护措施；

2 疏散通道的出入口控制点应满足紧急情况下人员不经凭证识读操作即可通行的要求；

3 断电开启的出入口控制点应配置备用电源，并应确保执行装置正常工作时间不少于48h；

4 当系统与其他非安防业务系统共用凭证或凭证为“一卡通”应用模式时，出入口控制系统应独立管理；

5 执行装置的连接线缆位于该出入口的受控区以外的部分应封闭保护。

3.5.4 停车库(场)安全管理系统设计应根据车辆进出停车库(场)的安全管理要求，选择适当类型的识读、控制与执行装置，具备对进出的车辆进行识别、通行控制和信息记录等功能，并应符合下列规定：

1 系统应能通过对车辆的识读做出能否通行的指示；

2 执行装置应具有防砸车功能；

3 执行装置应具有在紧急状态下人工开启的功能。

3.5.5 安全检查系统设计应根据保护对象对人员、车辆和禁限带物品的安全管理要求，选择相应的设备，具备对进入保护单位或区域的人员、物品、车辆进行安全检查，对禁限带的爆炸物、武器、管制器具或其他违禁品进行探测、显示、报警和记录的功能，并应符合下列规定：

1 当选择成像式人体安全检查设备时，应对人体隐私部位的

图像采取保护处理措施；

2 当微剂量X射线安全检查设备正常工作时，工作人员工作位置周围剂量当量率不应大于0.5μSv/h；

3 系统应配备防爆处置设施。

3.5.6 楼寓对讲系统设计应根据安全管理要求，选择对讲或可视对讲设备，具备被访人员通过音视频方式确认访客身份、控制开启出入口门锁的功能，并应符合下列规定：

1 访客呼叫机与用户接收机之间应具有双向对讲功能；

2 当受控门开启时间超过预设时长、访客呼叫机防拆装置被触发时，应能够发出现场警示信息。

3.5.7 电子巡查系统应能按照预先编制的巡查方案，实现对人员巡查的工作状态进行监督管理，具有巡查路线、巡查时间、巡查人员设置和统计报表等功能。在线式电子巡查系统应能对不符合巡查方案的异常情况及时报警。

4 工程施工

4.0.1 安全防范工程应按深化设计文件进行施工。

4.0.2 应在施工前查验进场设备和材料及其质量证明文件，并应在查验合格后安装。

4.0.3 隐蔽工程应进行工序验收，验收合格后方可进行下一道工序。

4.0.4 安全防范工程的线缆接续点、线缆两端、线缆检修孔、分支处等应统一编号，并设置永久标识。

4.0.5 文物保护单位的安全防范设备安装、管线敷设应采取对文物本体和文物风貌的保护措施。

4.0.6 在易燃、易爆等特殊环境中安装安全防范设备时，应根据危险场所类别采用相应的施工工艺。

4.0.7 安全防范工程初步验收通过或项目整改完成后，应进行系统试运行，时间不应少于30d。

5 工程检验与验收

5.0.1 高风险保护对象的安全防范工程应进行检验。

5.0.2 工程检验时，应对系统功能、性能等进行检验。

5.0.3 工程竣工后应组织竣工验收，包括施工验收、技术验收和资料审查。

5.0.4 工程竣工验收应对工程质量做出验收结论。

5.0.5 工程竣工验收合格后，施工单位应整理、编制、移交完整的工程竣工资料，并将安全防范系统正式交付使用。验收不合格的工程不应交付使用。

6 系统运行与维护

6.0.1 安全防范工程竣工移交后，应开展安全防范系统的运行与维护工作。

6.0.2 应制订安全防范系统运行与维护方案，建立人员、经费、制度和技术支撑在内的运行维护保障体系。

6.0.3 系统运行工作应确认作业内容，编制作业指导文件，制订日常管理、值机、现场处置、安全保密、培训和考核等制度。

6.0.4 同时接入监控中心和公安机关接警中心的紧急报警，监控中心值机人员应核实公安机关是否收到报警信息。

6.0.5 应按照系统维护工作方案，开展日常维护、故障处理、特殊时期保障等工作。特殊时期应采取加强工作协调、增加维护人员、补充备品备件等保障措施。

中华人民共和国国家标准

安全防范工程通用规范

GB 55029—2022

起 草 说 明

目　次

一、基本情况

按照《住房和城乡建设部关于印发2019年工程建设规范和标准编制及相关工作计划的通知》(建标函〔2019〕8号)要求，编制组在国家现行相关工程建设标准的基础上，认真总结实践经验，参考了国外技术法规、国际标准和国外先进标准，并与国家法规政策相协调，经广泛调查研究和征求意见，编制了本规范。

本规范的主要内容是：按照安全防范工程全生命周期质量管理的要求，对综合运用电子防范、实体防范、人力防范等多种措施开展的安全防范工程设计、工程施工、工程检验与验收以及安全防范系统运行与维护等各环节进行了规定。

本规范中，规定规模、布局的条款是：第2.0.2条，第3.1节、第3.2节、第3.3节全部条款。

本规范中，规定安全防范系统功能、性能的条款是：第2.0.4条，第3.4节、第3.5节全部条款。

本规范中，规定工程施工的条款是：第2.0.5条、第4.0.1条、第4.0.2条、第4.0.3条、第4.0.4条、第4.0.5条、第4.0.6条、第4.0.7条。

本规范中，规定工程检验与验收的条款是：第2.0.3条、第5.0.1条、第5.0.2条、第5.0.3条、第5.0.4条、第5.0.5条。

本规范中，规定系统运行与维护的条款是：第2.0.5条、第6.0.1条、第6.0.2条、第6.0.3条、第6.0.4条、第6.0.5条。

下列工程建设标准中的强制性条文按本规范执行：

《安全防范工程技术标准》GB 50348—2018

《入侵报警系统工程设计规范》GB 50394—2007

《视频安防监控系统工程设计规范》GB 50395—2007
《出入口控制系统工程设计规范》GB 50396—2007
本规范由住房和城乡建设部负责管理和解释。

二、本规范编制单位、起草人员及审查人员

（一）编制单位

公安部第一研究所

公安部科技信息化局

中国建筑标准设计研究院有限公司

公安部安全与警用电子产品质量检测中心

中国建筑设计研究院有限公司

北京中盾安全科技集团有限公司

北京艾克塞斯科技发展有限责任公司

北京声迅电子股份有限公司

富盛科技股份有限公司

上海天跃科技股份有限公司

中国兵器工业集团引信研究院有限公司

浩云科技股份有限公司

江苏固耐特围栏系统股份有限公司

（二）起草人员

施巨岭　杨国胜　周　群　王永升　张凡忠　朱　峰

聂　蓉　钟永强　赵　源　彭　华　李天銮　孙　兰

陈　琪　周慧敏　蒙　剑　季景林　解桂秋

（三）审查人员

刘希清　李秀林　牟晓生　杨　磊　王汝琳　洪卫军

张永刚　朱立彤　张　钊

三、术　语

1　安全防范　　security

综合运用人力防范、实体防范、电子防范等多种手段，预防、延迟、阻止治安和暴恐事件（包括入侵、盗窃、抢劫、破坏、爆炸、暴力袭击等）发生的活动。

2　人力防范　　personnel protection

具有相应素质的人员有组织地防范、处置等安全管理行为。

3　实体防范　　physical protection

利用天然屏障、建（构）筑物等人工屏障、器具、设备或其组合，延迟或阻止风险事件发生的防护手段。

4　电子防范　　electronic security

利用传感、通信、计算机、信息处理及其控制、生物特征识别等技术，提高探测、延迟、反应能力的电子防护手段。

5　安全防范系统　　security system

以安全为目的，综合运用实体防护、电子防护等技术构成的防范系统。

6　安全防范工程　　security engineering

为建立安全防范系统而实施的建设项目。

7　实体防护系统　　physical protection system

以安全防范为目的，综合利用天然屏障、人工屏障及防盗锁、柜等器具、设备构成的实体系统。

8　电子防护系统　　electronic protection system

以安全防范为目的，利用各种电子设备构成的系统。通常包括入侵和紧急报警、视频监控、出入口控制、停车库（场）安全管理、防爆安全检查、电子巡查、楼寓对讲等子系统。

9 入侵和紧急报警系统　intrusion and hold-up alarm system (I&HAS)

利用传感器技术和电子信息技术探测非法进入或试图非法进入设防区域的行为和由用户主动触发紧急报警装置发出报警信息、处理报警信息的电子系统。

10 视频监控系统　video surveillance system (VSS)

利用视频技术探测、监视监控区域并实时显示、记录现场视频图像的电子系统。

11 出入口控制系统　access control system (ACS)

利用自定义符识别或/和生物特征等模式识别技术对出入口目标进行识别并控制出入口执行机构启闭的电子系统。

12 停车库（场）安全管理系统　security management system in parking lots

对车辆进、出停车库（场）进行查验、监控以及人员和车辆在库（场）内的安全实现综合管理的电子系统。

13 安全检查系统　security inspection system

对人员、车辆携带、物品夹带的爆炸物、武器和（或）其他违禁品进行探测和（或）报警的电子系统。

14 电子巡查系统　guard tour system

对巡查人员的巡查路线、方式及过程进行管理和控制的电子系统。

15 楼寓对讲系统　building intercom system

采用（可视）对讲方式确认访客，对建筑物（群）出入口进行访客控制与管理的电子系统，又称访客对讲系统。

16 安全防范管理平台　security management platform (SMP)

对安全防范系统的各子系统及相关信息系统进行集成，实现实体防护系统、电子防护系统和人力防范资源的有机联动、信息的集中处理与共享应用、风险事件的综合研判、事件处置的指挥调度、系统和设备的统一管理与运行维护等功能的硬件和软件

组合。

17 保护对象　　protected object

由于面临风险而需对其进行保护的对象，包括单位、建（构）筑物及其内外的部位、区域以及具体目标。

18 高风险保护对象　　high risk protected object

依法确定的治安保卫重点单位和防范恐怖袭击重点目标。

19 防范对象　　defensing object

需要防范的、对保护对象构成威胁的对象。

20 风险　　risk

保护对象自身存在的安全隐患及其所面临的可能遭受人侵、盗窃、抢劫、破坏、爆炸、暴力袭击等行为的威胁。

21 风险评估　　risk assessment

通过风险识别、风险分析、风险评价，确认安全防范系统需要防范的风险的过程。

22 探测　　detection

对显性风险事件或/和隐性风险事件的感知。

23 延迟　　delay

延长或/和推迟风险事件发生的进程。

24 反应　　response

为应对风险事件的发生所采取的行动。

25 误报警　　false alarm

对未设计的事件做出响应而发出的报警。

26 漏报警　　leakage alarm

对设计的报警事件未做出报警响应。

27 周界　　perimeter

保护对象的区域边界。

28 防区　　zone

入侵和紧急报警系统能够探测到入侵或人为触发紧急报警装置行为的空间。

29 监控区域 surveillance area

视频监控系统的视频采集装置摄取的图像所对应的现场空间范围。

30 受控区 controlled area/protected area

出入口控制系统的一个或多个出入口控制点所对应的、由物理边界封闭的空间区域。

31 纵深防护 longitudinal-depth protection

根据保护对象所处的环境条件和安全防范管理要求，对整个防范区域实施由外到里或由里到外层层设防的防护措施。纵深防护分为整体纵深防护和局部纵深防护两种类型。

32 均衡防护 balanced protection

安全防范系统各部分的安全防护水平基本一致，无明显薄弱环节。

33 监控中心 surveillance center

接收处理安全防范系统信息、处置报警事件、管理控制系统设备的中央控制室，通常划分为值守区和设备区。

34 系统运行 system operation

利用安全防范系统开展报警事件处置、视频监控、出入控制等安全防范活动的过程。

35 系统维护 system maintenance

保障安全防范系统正常运行并持续发挥安全防范效能而开展的维修保养活动。

四、条文说明

本条文说明不具备与规范正文同等的法律效力，仅供使用者作为理解和把握规范规定的参考。

1 总　　则

1.0.1 本条规定了本规范制定的目的。

《中华人民共和国反恐怖主义法》第三十二条规定："重点目标的管理单位应当根据城乡规划、相关标准和实际需要，对重点目标同步设计、同步建设、同步运行符合本法第二十七条规定的技防、物防设备、设施。重点目标的管理单位应当建立公共安全视频图像信息系统值班监看、信息保存使用、运行维护等管理制度，保障相关系统正常运行。采集的视频图像信息保存期限不得少于九十日"。

《企业事业单位内部治安保卫条例》（国务院令第421号）第十三条规定："关系全国或者所在地区国计民生、国家安全和公共安全的单位是治安保卫重点单位"；第十四条规定："治安保卫重点单位应当确定本单位的治安保卫重要部位，按照有关国家标准对重要部位设置必要的技术防范设施，并实施重点保护"。

《保安服务管理条例》（国务院令第564号）第二条规定："本条例所称保安服务是指：（一）保安服务公司根据保安服务合同，派出保安员为客户单位提供的门卫、巡逻、守护、押运、随身护卫、安全检查以及安全技术防范、安全风险评估等服务；（二）机关、团体、企业、事业单位招用人员从事的本单位门卫、巡逻、守护等安全防范工作；（三）物业服务企业招用人员在物业管理区域内开展的门卫、巡逻、秩序维护等服务"。第二十五

条规定："保安服务中使用的技术防范产品，应当符合有关的产品质量要求。保安服务中安装监控设备应当遵守国家有关技术规范，使用监控设备不得侵犯他人合法权益或者个人隐私"。

为贯彻落实相关法律法规，通过规范安全防范工程建设、安全防范系统运行与维护，有效预防、延迟、阻止治安和恐怖事件（包括入侵、盗窃、抢劫、破坏、爆炸、暴力袭击等）的发生，制定本规范。

1.0.2 本条明确了安全防范工程的设计、施工、检验、验收、系统运行与维护必须遵循本规范。

1.0.3 本条提出了安全防范工程建设、安全防范系统运行与维护需要遵循的四项原则。

1 安全防范工程建设时，应针对不同的风险因素合理选择相应的防范措施，防止"防范不足"或"过度防范"。

安全防范工程是在充分识别风险的前提下，针对需要防范的治安和恐怖风险采取相应的防范措施，达到满足安全防范管理要求的防范效果。

安全防范管理要求是建设单位根据国家法律法规和现行标准等，结合保护对象的需求提出的要求。

2 人力防范、实体防范、电子防范是安全防范的三种基本手段，单一的防范手段难以达到安全防范目的，需多种手段协同配置。

探测、延迟、反应是安全防范的三个基本要素，只有在满足$T_{探测}+T_{反应}\leqslant T_{延迟}$的前提下，才能发挥应有的安全防范效能。

3 纵深防护是根据安全管理要求，对保护对象实施由外到里或由里到外层层设防的防护措施。均衡防护是指针对保护对象的防护能力基本一致，无明显薄弱环节。

4 安全防范系统的安全性应考虑电气安全、信息安全、防破坏能力以及系统对人员、环境的安全影响等各种安全因素。

安全防范系统可靠性的重要指标是平均无故障时间（MTBF）。通常采用降额设计、简化设计和冗余设计等措施提高系统

的可靠性。

系统的安全性、可靠性、环境适应性、电磁兼容性、可维护性等都是保障系统稳定运行的重要因素。

1.0.4 工程建设强制性规范是以工程建设活动结果为导向的技术规定，突出了建设工程的规模、布局、功能、性能和关键技术措施，但是，规范中关键技术措施不能涵盖工程规划建设管理采用的全部技术方法和措施，仅仅是保障工程性能的“关键点”，很多关键技术措施具有“指令性”特点，即要求工程技术人员去“做什么”，规范要求的结果是要保障建设工程的性能，因此，能否达到规范中性能的要求，以及工程技术人员所采用的技术方法和措施是否按照规范的要求去执行，需要进行全面的判定，其中，重点是能否保证工程性能符合规范的规定。

进行这种判定的主体应为工程建设的相关责任主体，这是我国现行法律法规的要求。《建筑法》《建设工程质量管理条例》《建筑节能条例》等以及相关的法律法规，突出强调了工程监管、建设、规划、勘察、设计、施工、监理、检测、造价、咨询等各方主体的法律责任，既规定了首要责任，也确定了主体责任。在工程建设过程中，执行强制性工程建设规范是各方主体落实责任的必要条件，是基本的、底线的条件，有义务对工程规划建设管理采用的技术方法和措施是否符合本规范规定进行判定。

同时，为了支持创新，鼓励创新成果在建设工程中应用，当拟采用的新技术在工程建设强制性规范或推荐性标准中没有相关规定时，应当对拟采用的工程技术或措施进行论证，确保建设工程达到工程建设强制性规范规定的工程性能要求，确保建设工程质量和安全，并应满足国家对建设工程环境保护、卫生健康、经济社会管理、能源资源节约与合理利用等相关基本要求。

2 基本规定

2.0.1 安全防范工程的全生命周期包括立项、设计、施工、检

验、验收以及系统的运行、维护等各阶段。安全防范工程建设应按全生命周期管理的理念进行整体规划，根据工程建设的程序要求，确定各阶段目标，有计划、有步骤地开展安全防范工程建设，同时为安全防范工程建设、系统运行与维护工作提供人员和经费保障。

2.0.2 本条规定了安全防范系统的构成。

1 本款给出了实体防护系统的构成要素。可根据实际情况，选择天然屏障、人工屏障、防护器具（设备）中的一种或多种防护措施。

天然屏障是指由天然而成的能够阻止进入、妨碍穿越、遮挡视线等功能的屏障，如山谷、丘陵、河流、丛林、沙漠等自然地貌和地形以及植被。

人工屏障包括建（构）筑物主体及其附属设施（如配套的道路、景观等）以及针对周界和具体保护目标所设置的围墙、栅栏、防盗门（窗）、车辆实体屏障等防护设施。

防护器具（设备）包括防盗保险柜（箱）、物品展示柜、防护罩、保护套管等防护设施。

2 本款给出了构成电子防护系统的主要子系统，每个子系统通常由前端、传输、信息处理/控制/管理、显示/记录等单元组成。可根据实际情况，选择其中的一个或多个子系统，也可设置安全防范管理平台对相关子系统进行集成管理。

2.0.3 安全防范工程中使用的设备、材料的质量直接关系到安全防范工程的质量和安全防范系统的效能。因此，工程中使用的设备、材料应该符合国家法规和现行相关标准的要求，并经检测合格。

2.0.4 本条提出了安全防范系统网络安全的基本要求。

弱口令一般指安全防范系统的设备、系统、应用等的账号密码的复杂度不足，容易被破解的编码，常见弱口令包括采用设备或系统出厂默认的密钥或编码，顺序升序或降序的数字，相邻、

相同数字使用两次以上，或与操作人员相关的生日、电话号码等具有一定规律、易被破解的编码。

网络安全漏洞和隐患一般指安全防范系统中的各类设备、系统、软件和协议等的具体实现或系统安全策略上存在的缺陷，可能被攻击者在未授权的情况下访问或破坏设备或系统。

在安全防范系统互联互通、信息共享的需求带动下，基于不同网络的安全防范系统互联应用越来越多，为保证安全防范系统的信息安全，需要在不同的传输网络之间采取相应的网络边界安全管理措施。

2.0.5 在安全防范工程设计、施工、检验、验收以及安全防范系统运行与维护等过程中涉及防护部位、防范手段、管理内容、处置预案（流程）、重要信息数据等，是安全防范管理工作中需要保密的基础数据和管理要求。这些信息的泄露可能会导致针对保护对象的防护措施失效，进而产生不可预知的后果。因此，保密责任落实和措施保障成为必须要考虑的要求。

任何单位和个人不得利用安全防范系统非法获取、扩散国家秘密、商业秘密或者侵犯个人隐私。

在涉及国家秘密的特殊领域开展安全防范工程建设时，应选择安全可靠的设计、施工和服务单位，选用的产品、设备应安全可控，防止涉密信息泄露。

3 工程设计

3.1 布防设计

3.1.1 安全防范工程设计时，首先应该明确保护对象（保护单位、建筑及其内外的保护区域或部位、具体保护目标）及其安全需求（防盗窃、防破坏、防范恐怖袭击等），通过现场勘察、风险评估等手段，确定需要具体防范的风险，从而进行有针对性的防护设计，确定安全防范工程的工作边界和工作目标，为人力防

范、实体防范和电子防范设计的均衡配置和统筹协调奠定基础。

保护区域或部位通常包括周界、出入口、走道、通道、公共区域、财务室、数据机房和水电气热设备间、监控中心等。

3.1.2 安全防范工程设计应根据需要防范的具体风险，确定防护点位、防范措施以及需要达到的防范效果，包括系统、设备的功能性能。

对于高风险保护对象安全防范工程，在设计前应进行现场勘察。现场勘察是指对保护对象所进行的、与安全防范工程设计有关的各方面情况的了解和调查，包括保护对象的基本情况，保护对象所在地及周边的地理、气候、雷电灾害、电磁等自然环境和人文环境等情况，防护区域、部位、目标的分布及其有关情况，防范对象及其攻击特点等。

本规范中所称的高风险保护对象是指依法确定的治安保卫重点单位和防范恐怖袭击重点目标。

（1）治安保卫重点单位。

《企业事业单位内部治安保卫条例》（国务院令第421号）第十三条规定，关系全国或者所在地区国计民生、国家安全和公共安全的单位是治安保卫重点单位。治安保卫重点单位由县级以上地方各级人民政府公安机关按照下列范围提出，报本级人民政府确定：广播电台、电视台、通讯社等重要新闻单位；机场、港口、大型车站等重要交通枢纽；国防科技工业重要产品的研制、生产单位；电信、邮政、金融单位；大型能源动力设施、水利设施和城市水、电、燃气、热力供应设施；大型物资储备单位和大型商贸中心；教育、科研、医疗单位和大型文化、体育场所；博物馆、档案馆和重点文物保护单位；研制、生产、销售、储存危险物品或者实验、保藏传染性菌种、毒种的单位；国家重点建设工程单位；其他需要列为治安保卫重点的单位。

（2）防范恐怖袭击重点目标。

《中华人民共和国反恐怖主义法》第三十一条规定，公安机

关应当会同有关部门，将遭受恐怖袭击的可能性较大以及遭受恐怖袭击可能造成重大的人身伤亡、财产损失或者社会影响的单位、场所、活动、设施等确定为防范恐怖袭击的重点目标，报本级反恐怖主义工作领导机构备案。

3.1.3 本条提出了用于周界防护的措施，包括实体防护、入侵探测、视频监控等防护措施，可根据现场环境条件和安全防范管理要求选择其中一种或多种防护措施。

1 实体防护可选择设置周界围墙、金属铁丝网、栅栏等。金属铁丝网或栅栏应具有防攀爬措施。

2 入侵探测应针对所要探测的攀爬、翻越、挖凿、穿越等不同行为，选择设置不同类型的产品，如主动红外入侵探测器、光纤振动入侵探测器、泄漏电缆等。根据需要，也可选择同时兼具实体防护和入侵探测功能的张力式电子围栏或脉冲式电子围栏等。

3 视频监视区域应避免树木等物体遮挡，监视效果应至少能看清周界范围内人员的活动情况。可选择采用具有视频图像智能分析功能的系统和设备，对人员入侵行为进行探测报警。

3.1.4 本条提出了用于出入口防护的措施，包括实体防护、出入口控制、入侵探测、视频监控等，可根据现场环境条件和安全防范管理要求选择其中一种或多种防护措施。

1 出入口是安全防范的重要部位，在满足通行能力的前提下，周界的出入口设置数量越少，越有利于对出入口的控制和管理，也有利于安保人员的反应处置。对于无人值守的周界出入口，实体屏障的防攀爬、防冲撞等能力应与周界实体屏障的防护能力相当，这是为了避免出现安全防范的薄弱环节，以达到均衡防护的效果。

2～4 这几款分别提出了在进行出入口防护设计时，出入口控制、入侵探测、视频监控等不同措施应该达到的防护能力。

3.1.5 本条提出了用于走道、通道和公共活动场所防护的措施，

包括视频监控、入侵探测、实体屏障等，可根据现场环境条件和安全防范管理要求选择其中一种或多种防护措施。

1 本款提出了在走道、通道和公共活动场所布防设计时，视频监控应该达到的防护能力。

2 高风险保护对象周边的走道、通道和公共活动场所可根据需要设置入侵探测装置，对人员入侵行为进行探测和报警。

3 重要的车辆通道和公共活动场所可选择防撞柱、防撞墩、升降式阻车路障、减速带等车辆实体屏障，重要人行通道和公共活动场所可选择人行通道闸、栅栏等实体屏障。

3.1.6 在人员密集场所进行防护设计时，既要考虑安全防范管理要求，还要考虑紧急情况下人员快速疏散的需要，防止人员拥挤、踩踏等事件的发生。

3.1.7 本条提出了重要保护部位（如财务室、数据机房、水电气热设备间等）的防护措施，包括实体防护、入侵探测、出入口控制、视频监控等，可根据现场环境条件和安全防范管理要求选择其中一种或多种防护措施。

3.1.8 监控中心是安全防范系统的信息存储、控制、交换、传输、显示等主要设备的存放场所，也是值守人员长期工作的场所。高风险保护对象的监控中心的位置不仅要考虑设备和系统可靠运行，还要考虑值守人员的身心健康。

3.1.9 本条规定了高风险保护对象的监控中心的防护要求。

1 监控中心内部设置视频监控装置是为了对值班人员及出入监控中心人员的活动情况进行监督管理。

2 监控中心值守人员需保持与外界的通信畅通。

3 当紧急情况发生时，通过紧急报警装置向上级监控中心或其他接警中心发送报警信息。

4 当监控中心的值守区与设备区为两个独立物理区域且不相邻时，为避免值守区与设备区的传输线路被轻易破坏或异常损坏，而导致安全防范系统无法正常工作，因此需要对传输线缆加

强防护措施。

5 监控中心设备区为独立物理区域且与值守区不相邻时，其防护措施应与监控中心的总体要求一致，特别强调了设备区的出入人员管理和防入侵要求。

3.1.10 本条提出了用于保护目标防护的措施，包括实体防护、入侵探测、位移探测、视频监控等，可根据现场环境条件和安全防范管理要求选择其中一种或多种防护措施。

1、2 这两款提出了实体防护、入侵探测、位移探测等不同措施应该达到的防护能力。

3 当保护目标为移动目标时，应确保保护目标持续处于视频监控区域内，以实现对目标的跟踪保护，如在文物交接的过程中，应对文物交接的全过程进行监控。

4 视频监控采集的图像可能会涉及个人信息或隐私，因此需对图像中相应的区域进行遮挡处理。

3.1.11 安全检查的目的是防止人员、物品、车辆携带或夹带违禁品（特别是易燃、易爆物品，管制刀具等）进入保护单位或区域。

在安全检查系统设计时需考虑安全检查区位置，评估流量，合理配置安全检查通道数量，针对违禁品类型选择相应的安全检查及处置设施。

3.1.12 在易燃、易爆环境中设计安全防范系统时，要根据现行国家标准《危险化学品重大危险源辨识》GB 18218 进行危险源辨识。根据危险源的类别，结合其相应行业的相关标准进行设计，现有的相关标准主要有国家现行标准《爆炸危险环境电力装置设计规范》GB 50058、《火炸药生产厂房设计规范》GB 51009、《地下及覆土火药炸药仓库设计安全规范 》GB 50154、《海洋石油平台电气设备防护、防爆等级要求》CB/T 4397、《爆炸危险场所防爆安全导则》GB/T 29304、《爆炸性环境　第 1 部分：设备　通用要求》GB 3836.1 等。

3.1.13 本条提出了针对防范恐怖袭击重点目标进行防护设计时，可采取的强化防范措施。

《中华人民共和国反恐怖主义法》第三十一条规定，公安机关应当会同有关部门，将遭受恐怖袭击的可能性较大以及遭受恐怖袭击可能造成重大的人身伤亡、财产损失或者社会影响的单位、场所、活动、设施等确定为防范恐怖袭击的重点目标，报本级反恐怖主义工作领导机构备案。

1 加强周界防范的措施可选择加高、加厚或多重设置周界实体屏障，联合设置周界实体防护和电子防护设施等。

2 针对爆炸和暴力袭击，强化安全检查要求。

3 强化对人员的管控、对机动车的阻挡以及缓冲和隔离措施。

4 加强对人员密集区的视频覆盖和预警预测能力。

5 强化对监控中心的防护措施。

6 针对无人飞行器提出了防范要求。

7 针对恐怖袭击除了要考虑安全防范系统的探测、延迟、反应能力外，还要增加人力配备，并配置个人防护和对抗性装备，如钢叉、盾牌、头盔、防刺背心等。

3.2 系统架构设计

3.2.1 本条提出了安全防范系统架构规划的基本要素。

3.2.2 安全防范系统通常由实体防护系统、电子防护系统构成。根据需要，安全防范系统还可配置对这些系统进行集成的安全防范管理平台。

应根据现场自然条件、物理空间等情况，合理利用天然屏障，综合设计和选择配置人工屏障、防护器具（设备）等实体防护系统。

电子防护系统可由一个或多个子系统构成。电子防护系统的子系统通常包括入侵和紧急报警系统、视频监控系统、出入口控

制系统、停车库（场）安全管理系统、安全检查系统、电子巡查系统和楼寓对讲系统等。

电子防护各子系统的基本配置包括前端、传输、信息处理/控制/管理、显示/记录等单元。不同的子系统，其各单元的具体设备构成有所不同。

3.2.3 本条提出了系统集成/联网的常见方式。

1 基于直接硬件级联动的方式，在设备之间、子系统之间进行直接的联动控制。

2 基于协议通信联动的方式，主要是指以 RS232/485、以太网等方式在子系统之间进行的联动方式。

3 基于安全防范管理平台对各子系统进行统一集成管理的方式。

4 基于安全防范管理要求进行的多平台、多层级的联网方式。

5 基于安全防范系统与其他系统的信息共享应用需求进行的联网方式。

3.2.4 安全防范系统专用传输网络可采用专线方式或公共传输网络基础上的虚拟专网（VPN）方式。

高风险保护对象安全防范工程的信息流的安全性将直接关系到系统的正常运行和效能发挥。采用专用传输网络可最大程度降低外部攻击和信息泄露的风险。

3.2.5 安全防范管理平台是安全防范系统集成与联网的核心。本条规定了安全防范管理平台需要满足的基本功能：

（1）集成管理：对安全防范各子系统进行统一管理与控制，实现各子系统的高效协同工作。

（2）信息管理：实现系统各类信息的存储、检索与回放等管理。

（3）用户管理：对系统用户进行创建、修改、删除和查询，对系统用户划分不同的操作和控制权限。

（4）设备管理：对系统内设备进行统一编址、寻址、注册和认证等管理，对设备的运行状态进行监测。

（5）联动控制：实现相关子系统间的联动，并以声和（或）光和（或）文字图形方式显示联动信息。

（6）日志管理：对系统用户的操作、系统运行状态等进行记录、查询、显示。

（7）数据统计：对系统数据进行统计，生成相关报表。

3.2.6 根据集成方式、信息安全的需要确定系统中的信息存储模式，存储模式可分为分布式存储、集中存储、云存储等多种模式。

3.2.7 安全防范系统的供电模式可以分为集中供电模式、本地供电模式和混合供电模式。

集中供电模式：对中心和前端负载统一提供电源。

本地供电模式：前端负载就近取电。

混合供电模式：综合运用集中供电和本地供电的模式。

安全防范系统供电的保障措施包括自备蓄电池、配备发电机等。

3.2.8 接口协议通常包括各子系统前端设备与安全防范管理平台之间的接入协议、安全防范管理平台与其他系统之间的数据交换服务接口协议等。这些接口协议的统一是安全防范系统、设备互联互通以及信息共享应用的基础。

3.3 人力防范措施

3.3.1 人力防范资源配置应充分体现人力防范、实体防范、电子防范相结合，探测、延迟、反应相协调的原则。根据 $T_{探测}+T_{反应}\leqslant T_{延迟}$ 和实体防范的延迟能力，合理配备和部署人力防范资源。人力防范资源的配备和部署应保障系统正常运行以及应急反应和现场处置的需要。

3.3.2 安全保卫人员、系统值机操作人员和维护人员需定期和

不定期地接受安全防范系统和设备操作的培训，不断提高相应人员能力和素质。

3.3.3 个人防护和对抗性装备包括头盔、棍棒、钢叉、盾牌、防刺服等，可根据实际需要选择配备。装备的数量及部署位置需满足安全防范系统运行、应急反应、现场处置和预期风险对抗能力的要求。

3.3.4 本条所说的应急预案是指保护对象的管理单位制订的突发事件应急预案中，针对可能发生的治安和恐怖风险事件而制订的专项预案，包括风险事件、人员及分工、处置流程与措施、目标保护和人员疏散等要求。

3.4 实体防护系统设计

3.4.1 建（构）筑物本身承担着实体防护的功能，建（构）筑物自身选址、功能布局、结构强度及场地道路、景观附属设施的规划都与实体防护能力密切相关，因此，新建、改建和扩建的建（构）筑物实体防护系统设计要与建（构）筑物设计同步进行。

3.4.2 本条规定了实体防护系统设计应实现的防护能力，按照其防护能力的不同分为威慑、延迟和阻挡。实体防护能够对防范对象形成心理上的威慑，能够延迟人侵时间和过程，采取适当的实体防护能够阻挡防范对象的人侵行为。

3.4.3 周界实体防护设计包括周界实体屏障、出入口实体屏障、车辆实体屏障、安防照明与警示标志等设计内容。

实体屏障一般分为天然屏障和人工屏障两大类。天然屏障是指能够阻止进入、妨碍穿越、遮挡视线等的自然屏障，如山谷、丘陵、河流、丛林、沙漠等自然地貌和地形以及植被。周界实体防护设计可利用天然屏障。人工屏障是指建筑景观、建（构）筑物等人工设计建设的可以阻止进入、防撞、防爬、防破坏等的屏障，如护城河、绿化带、围栏、栅栏、建（构）筑物本身以及相应的墙体、大门等。

车辆实体屏障是指用于限制或阻挡车辆擅自进入以及防止车辆撞击的各类人工建造或加工制造的实体屏障，如防撞柱、防撞墩、防撞翻板、防撞墙等。

1 根据保护对象所在的位置、场地条件和需要防范的攻击方式（如人员攀爬、翻越、车辆冲撞等）选择围墙、栅栏、壕沟等相应的实体屏障。

周界围墙、栅栏一般远离可供人借助攀爬的物体和设施，如立杆、树木、建（构）筑物、路灯杆、电线杆等。

当周界围墙、栅栏两侧存在便于攀爬、翻越的物体或设施且不可避免时，可通过设置多重实体周界，增加周界入侵探测装置、视频监控装置等措施，以满足周界防范的需要。

2 保护对象有防爆安全要求时，需根据防范爆炸物的种类、当量、爆炸破坏力等进行计算，确定实体屏障防冲击能力及其与保护对象间的安全距离。

3 穿越周界的河道、涵洞、管廊等可容纳防范对象进入的孔洞是周界的一部分，需设置实体屏障和（或）实体装置对孔洞进行防护。

4 车辆实体屏障需具有减速、吸能、阻停的防护功能，以车辆的设计载重和设计速度撞击后产生的冲量作为依据，设计车辆屏障的高度、结构强度、固定方式等。

国外的相关测试标准可供参考，如美国的 ASATM F2656 标准和英国的 PAS68 标准。

3.4.4 建（构）筑物设计应包括平面与空间布局、结构和门窗等设计内容，从安全防范的需求角度，综合考虑建（构）筑物的功能、平面布置、建筑立面、建筑构造、结构类型等方面的设计，使建（构）筑物中的场地道路、景观、停车场、建筑内通道、房间、附属设施（管廊、管沟等）、门窗等充分发挥实体防护功能。

建筑物门窗包括建筑物通道门、室内门、建筑外窗、建筑内

窗、天窗等。

1 建（构）筑物设计需避免出入口、场地道路直通保护对象或其所在建筑物的大堂（门厅），可采取设置S形车辆弯道或设计前广场、景观池（花坛）、台阶等缓冲区措施。

建（构）筑物场地道路与保护对象或其所在建筑物外侧墙体需设计一定的安全距离，如通过建筑景观灌木、绿篱或向建筑物外侧放坡等。

2 为避免或减小易燃、易爆、有毒、放射性等物质对人造成的危害，此类保护目标的平面与空间布局需隐蔽并尽可能地远离人群；当布置在厂区或库区时，最好选择单独偏僻区域；需尽量利用地形等自然屏障，并避开易发生山洪、滑坡和其他地质灾害的区域。

3 能够容纳防范对象进入的建（构）筑物的洞口、管沟、管廊、吊顶、风管、槽盒、管道等，在不影响建筑功能的前提下，可采用防护栅栏、防护钢丝网、可闭锁盖板等实体屏障或实体构件进行封闭或阻挡。

4 防爆墙体设计可参照现行国家标准《人民防空地下室规范》GB 50038的规定。门、窗有防盗、防爆炸、防弹、防砸要求时，可按照国家现行标准《防盗安全门通用技术条件》GB 17565、《金库门通用技术要求》GB 37481、《防爆安全门》GA/T 1707、《防爆炸透明材料》GA 667、《防弹透明材料》GA 165、《防砸透明材料》GA 844等选择相应的产品或材料。

3.4.5 实体装置包括防盗保险柜（箱）、物品展示柜、防护罩、保护套管等，需选择不同的产品以满足相应的安全防护要求。

3.4.6 要在滚刺网、脉冲式电子围栏等设施的安装区域设置警示标识，以防止人员误触碰时造成人身伤害。

3.5 电子防护系统设计

3.5.1 入侵和紧急报警系统的探测手段多种多样，其技术原理

也各不相同，可应用于不同的场合，如防越线（界）、撞击、撬、挖、凿、攀爬等，探测的手段不限于某种探测装置，可以是红外线、微波、振动、激光、超声波、音频、视频、磁开关、压力开关等探测装置中的一种或组合。在实际应用设计中，要根据需要防范的风险和现场情况选择相应的探测手段，各类技术原理不同的探测装置可联合应用，即采用多传感器探测技术，互为补充，构成点、线、面、空间或其组合的综合防护体系。

1 入侵和紧急报警系统是应用于安全防范系统的重要子系统之一，是安全防范的三个基本要素（探测、反应、延迟）中“探测”的关键环节，系统能否准确、及时地探测入侵行为的发生，能否发出报警信息，直接决定了所构建的系统是否有效。入侵和紧急报警系统的主要特点是探测手段的多样性、入侵探测的实时性、信息传输的快捷性、报警响应的及时性等，由于受气候、环境等外界因素的影响，如果采用单一的探测手段，很可能会出现误报警，甚至漏报警现象，因此要结合实际情况，采用合适的探测方式和手段构建系统，以达到准确、及时探测的目的。

紧急报警装置要采用 24h 设防。

2 入侵和紧急报警系统的探测装置、控制指示设备等进行防拆报警设计是保障系统安全性和有效性的重要措施。

在不少的入侵和紧急报警系统工程建设中，经常出现设备的防拆装置没有安装和连接，或连接方式不恰当，在撤防状态下，系统对探测器的拆改就不会响应，导致系统无法知道探测装置的状况。因此，为保证系统使用的有效性，对于入侵探测器和控制指示设备的防拆装置要设为独立防区，且为 24h 设防。

3 为了保证报警信号的正常传输，除了在物理上对传输线路采取防护措施（如采用保护管、暗埋等）外，当系统传输线缆、电源线缆被断路、短路等破坏时，系统应能及时发现。

4 为了适应用户的不同需求，需对系统进行参数设置，对不同区域、部位的探测装置，根据要求可设置为瞬时防区、24h

防区、延时防区等；在不同的时间段，各防区又可设置为设防、撤防、旁路状态。紧急报警装置、防拆装置通常设置为24h防区。为了便于管理和责任认定，需要对系统用户的权限进行分类设置。

瞬时防区是指防区处于设防状态时，一旦触发该防区将立即产生报警，不提供延时，这是系统最常用的防区类型，通常用于除出入口外的其他防区。24h防区是指防区不论处于设防状态还是撤防状态，一旦触发该防区将立即产生报警，不提供延时，大多用于紧急报警类、火灾报警和设备防拆防区应用。延时防区是指防区处于设防状态时，一旦触发该防区将产生延时报警，即从触发探测器到引发报警之前有延时时间，延时时间可以设定（一般为1s～300s可调），此时间足以让用户正常退出或进入而不发生报警状态，通常是用于出入口防区而设置的。

5 设防、撤防、旁路、胁迫报警等是入侵和紧急报警系统的基本功能。

设防是指使系统或其一部分处于能通告报警状态的操作，也称为布防。

撤防是指使系统或其一部分处于不能通告报警状态的操作。

旁路是指报警系统的部分报警状态不能被通告的状态，此状态会一直保持到手动复位，即操作人员执行了旁路指令后，所指定的防区就会被旁路掉（失效），而不能进入工作状态，在一个报警系统中，可以将其中一个防区单独旁路，也可以将多个防区同时旁路掉（又称群旁路）。

胁迫报警是为了最大可能地保护人身安全，适用于远程报警，当使用胁迫钥匙撤防时，控制指示设备能够正常撤防，同时发送远程胁迫报警信号和（或）信息，且不给出本地报警指示。

6 指示是由入侵和紧急报警系统产生的可听、可视或者其他可感知形式的信息，通过指示，用户可以了解系统的入侵、紧急、防拆等的报警状态和故障情况。

7 为了能够对发生的事件进行追溯，了解系统的操作和运行情况，需要对系统操作、报警和有关警情处理等事件的各种信息进行记录和存储。记录的信息一般包括系统操作信息、报警信息、警情处理信息等。

系统操作信息一般包括操作人员、开机、关机、参数设置、设防、撤防、旁路、更改等。

报警信息一般包括入侵报警、紧急报警、防拆报警、故障报警、被破坏报警、胁迫报警等。

警情处理信息一般包括事件（发生的时间、地点、性质）、操作人员、处理预案、处理人员、处理结果等。

8 报警响应时间是指从探测器探测到目标或人为触发紧急报警装置后产生报警状态信息，到控制指示设备接收该信息并发出报警信号所需的时间。报警响应时间越短，越可以缩短为应对风险事件的发生所采取行动的时间，从而可以降低风险事件的发生概率。

9 入侵和紧急报警系统的备用电源需保证在主电源断电后，系统仍能连续工作不少于 8h。

3.5.2 视频监控系统通常由视频采集、传输、处理、存储、显示和相应控制管理等部分构成。应针对进入保护区域的人员、物品、车辆等通行、活动或目标特征识别要求，结合现场环境条件，设计视频图像采集点位布置、传输路由，选择相应类型采集装置、显示和存储设备，设计安装位置、角度，最大可能及时、有效地获取监控区域和监控目标的实时成像信息。

1 本款对视频监控系统的监控范围和监视效果提出了要求。系统视频图像的显示和回放应能根据防护要求的不同，清晰显示人员、物品、车辆等的通行、活动情况，人员体貌特征、脸部特征，车辆号牌，物品形状等。

2 对前端视频采集设备的实时控制通常是指 PTZ 控制，即对云台的水平（Pan）和垂直（Tilt）转动控制、对镜头的变焦

（Zoom）控制。视频采集设备的工作状态调整包括编码方式、码流、帧率、加密等内容。

3 根据授权，用户可对系统内的现场实时视频图像或存储的历史图像进行实时调取，并切换到指定显示设备界面上显示。这里的终端是指在监控中心或分控中心的监视器或计算机显示器，也可以是移动显示终端。实时调度强调的是调取图像的操作响应时间不能太长。

4 系统应能通过调阅显示系统内的所有视频图像（可以不同时显示）。视频图像的调阅取决于用户的操作权限。

5 30d是系统中视频图像信息的最低存储时间要求，对于防范恐怖袭击重点目标，根据《中华人民共和国反恐怖主义法》的规定，视频图像信息保存期限不得少于90d。

6 设备管理是指对视频监控系统设备进行参数配置和在线状态监测，对系统内设备进行统一编址、寻址、注册和认证等管理。

用户管理是指对系统用户进行创建、修改、删除和查询，对系统用户划分不同的操作和控制权限。

日志管理是指对系统用户的操作、系统运行状态等进行记录、查询、显示。

3.5.3 本条提出了出入口控制系统功能的总体要求和建设目标。

1 本款主要针对入侵者在进入受控区前，在最易受攻击的设备安装部位提出了相关安全措施要求。

出入口控制系统的设计应考虑对手可能通过攻击系统，达到入侵的目的。在出入口控制系统中，应特别注意受控区域的权限，以及现场设备安装位置和连接线缆的防护措施等因素对安全的影响。

在出入口控制系统中，执行部分的输入线缆及其连接端是易于被攻击的薄弱点。

这里的“受控区”是指出入口对应的受控区、同权限受控区

和高权限受控区。

举例来说：一个管理了从A～G共7个受控区域的出入口控制系统（如某个公司的多个办公室）如图1所示。

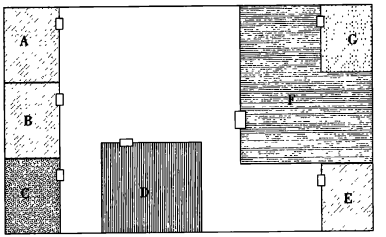

图1　出入口控制系统受控区示意图

图1中，A、B、E三个区域为同权限受控区，即它们对目标的授权是一致的，能进入A区的目标也可进入B、E区，能进入B、E区的目标也同样能进入A区。G区是相对于F区的高权限受控区，即能进入G区的目标一定能进入F区，而能进入F区的目标不一定能进入G区。C区和D区分别是相对于其他受控区的非同权限受控区，即能进入该区的目标不一定能进入其他区，而能进入其他区的目标也不一定能进入该区。若能进入G区的目标也能进入其他任何区，则G区就是该出入口控制系统的最高权限受控区。

该举例若是某公司的多门联网门禁系统，则有许多问题值得探讨：

问题一：采用多门门禁控制器应特别注意其安装位置（图2）。

目前采用直流或脉冲信号等非编码信号直接驱动电控锁具的门禁控制器占很大比例，在本例中采用双门控制器控制A区和B区两个门是合理的，若控制B区和C区两个门就存在问题，控制器安装在B区内，C区就不安全，控制器安装在C区内，B区就不安全。

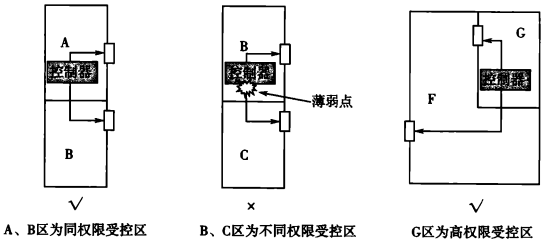

图 2　出入口控制系统受控区的设备安装示意图

安装在 G 区的双门控制器控制 F 区和 G 区两个门是合理的。

问题二：采用多门门禁控制器应特别注意对电控锁连接线的防护（图 3）。

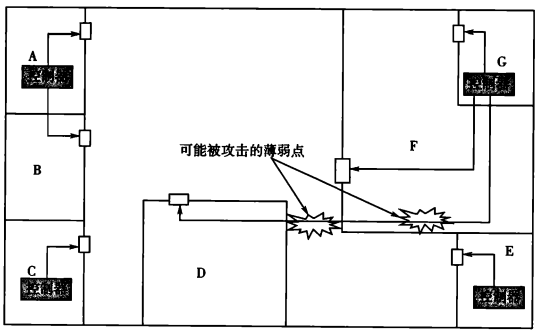

图 3　出入口控制系统受控区的设备安装及布线示意图

当电控锁的连接线必须离开本受控区、同权限受控区、高权限受控区敷设时，有可能成为被实施攻击的薄弱点，必须严格防护。

在多出入口系统中要想提高安全性和可靠性，减少工程施工带来的安全隐患，建议尽量采用联网控制的单出入口控制器。若必须采用多出入口控制器，则应安装在高权限受控区内并做好对执行部分输入线缆的防护。

2 本款主要解决出入口控制系统与消防等紧急疏散中的应用矛盾，贯彻了“safety”优先的原则。

出入口控制系统的设计，应充分考虑“安全”因素，英文“security”和“safety”翻译成中文都是“安全”，但它们的含义有所不同，“security”是“安全”的社会属性，“safety”是“安全”的自然属性。以防入侵、防盗窃、防抢劫、防破坏、防爆炸等为目的的安全技术防范系统主要针对的是“security”，而防火、防目标被非人为因素伤害等是“safety”涉及的问题。当同时出现这两种“安全”问题时，在大多数情况下应优先解决“safety”问题。这是设计系统与产品的基本原则。

在出入口控制系统中，识读部分与执行部分是出入目标最易接触的部分，也是最有可能对出入目标造成伤害的部分。但不同的产品类型对安全的影响也是不同的。

在生物特征识别中，指纹、掌形识别等需人体直接接触的识读装置就不如面部、眼虹膜识别这类不需人体直接接触的识读装置安全，因为直接接触的识读装置的接触面若不能及时清洁，就有可能成为某些传染性疾病传播的媒介。

另外，直接担负阻挡作用的执行机构，其启闭动作本身必须考虑出人目标的安全，如电动门的关闭动作必须等待出入目标安全离开后方可进行，挡车器必须等待车辆离开后方可落下挡车臂等。

在安全防范系统中与紧急疏散及消防系统联系最为紧密的就

是出入口控制系统。出入口控制系统强调的是对空间的隔离，以保证“security”；而紧急疏散及消防系统强调的是能快速逃离，以保证“safety”。

在“safety”优先的原则指导下，出入口控制系统的设计必须满足紧急疏散及消防的需要，这并不是说出入口控制系统所管理与控制的每个出入口必须与消防联动。但在本条相关约定的条件下必须联动，保证在火灾等紧急情况发生时，用于闭锁或起到阻挡作用的出入口控制执行部件能自动释放疏散出口，人员不经凭证识读过程也能迅速安全地疏散。

3 断电开启设备的供电需要特别重视，为避免断电产生的防护疏漏，执行装置（锁闭阻挡装置等）对供电的可靠性要求更高。

配置备用电源是提高出入口控制系统防护能力的措施之一。主电源断电后，备用电源应在规定的时间内保持出入口控制点的锁定状态。

4 所谓“一卡通”，是指能用1个介质凭证完成2个以上应用的一种系统集成功能，本款的“一卡通”特指与其他非安全防范系统业务共用介质凭证的集成系统。在出入口控制系统中，常用“卡”作为编码凭证供系统识读使用，这张“卡”也可能同时用于食堂消费等其他应用系统中，这给使用者带来了便利。

由于安全防范系统抗攻击的安全特性要求必须独立运行，其凭证等重要数据信息不应放置在其他非安防业务系统中。如不能将门禁数据库服务器开放给财务等其他非安保业务部门；同样地，消费充值等其他业务信息也不宜由安保部门管理，而应当将门禁系统数据与其他业务系统隔离。通常“一卡通”的正确做法可以是由制证部门统一将人员信息及卡的基本信息录入后，分别分发给门禁服务器及其他业务系统服务器，再由各系统分别管理。

因此，在“一卡通”的应用模式中，作为授权凭证的卡的载

体是可以共用的，但需要在不同的系统中去分别设置权限或规则。在一个单位里，管理出入口控制系统的系统管理员与管理其他业务系统的管理员不应是一个人，他们有各自的管理责任，在系统级就需要采用独立设置与管理。这也是确保系统自身安全的重要措施。

5 本款“受控区”是指该出入口的对应受控区、同权限受控区、高权限受控区，在对应受控区、同权限受控区、高权限受控区以外的执行装置连接线缆是出入口控制系统的薄弱点，为确保出入口控制系统执行装置的安全可靠操作，需对这部分连接线缆采取相应的自我保护措施，可采用抗拉伸、抗弯折强度不低于壁厚 2.0mm 的镀锌钢管。

3.5.4 停车库（场）封闭管理是发挥停车场安全管理的基本前提。停车库（场）安全管理系统设计内容应包括出入口车辆识别、挡车/阻车、行车疏导（车位引导）、对通行车辆的保护（防砸车）、库（场）内部安全管理、指示/通告、管理集成等。

1 系统对车辆的识读有车牌识别、IC 卡、ID 卡、二维码、电子标签等多种方式，通过对车辆的识读，给出是否允许通行的指示，常见的指示方式有栏杆机起落、指示灯、语音、文字等。

2 防砸车功能是停车库（场）安全管理系统对人员、车辆的一种保护措施。

3 在停电、系统故障或出现应急事件时，人工开启栏杆机等执行装置是为了保证车辆的正常通行。

3.5.5 安全检查的对象通常包括进入被保护单位或区域的人员、物品和车辆，禁限带物品主要包括武器类（枪支及仿制品、管制刀具等）、爆炸类（弹药、爆破器材、烟火制品等）、易燃易爆物品类（氢气、天然气等压缩气体和液化石油气、氧气、水煤气等液化气体）、毒害品类（氰化物、汞、剧毒农药等）、腐蚀性物品类（盐酸、氢氧化钠、氢氧化钾、硫酸、硝酸等）。针对不同行业的安全检查要求不同，所采用的技术设备设施、技术系统亦有

差异，如现阶段城市轨道交通的安全检查系统，通常采用金属探测门和手持式金属探测器对人员进行安全检查，采用微剂量X射线安全检查设备对物品进行检查。

1 随着安全检查技术的发展，成像式人体安全检查设备开始在有些安全检查场所使用，包括毫米波技术、太赫兹技术的人体安全检查设备，本款规定设备显示的被检人体图像要通过图像处理技术模糊敏感部位，不显示清晰人体图像，保护被检人员隐私，可以卡通人体图像或标准人体模板图像显示，突出显示违禁品图像。

2 本款提出了物品安全检查采用的微剂量X射线安全检查设备的电离辐射防护要求。

为保障微剂量X射线安全检查设备正常使用时不对周围人员产生辐射伤害，要求设备在单位时间内穿过辐射屏蔽防护泄漏到设备外部的电离辐射强度要小于一定的限值，周围剂量当量能体现辐射剂量的累积（周围剂量当量率乘以时间是累积的辐射剂量当量）。设备正常工作时，工作人员工作位置的周围剂量当量率不大于0.5μSv/h，能够保障微剂量X射线安全检查设备正常使用时不对周围人员产生辐射伤害。

3 安全检查现场配置的防爆处置设施包括防爆毯、防爆球或防爆罐等。配备数量可根据安全检查现场实际情况和需求来确定。

3.5.6 楼寓对讲系统也称为访客对讲系统，具有可视功能的系统通常称为可视对讲系统。系统通常由访客呼叫机、用户接收机、管理机、电源及辅助设备组成。

1 访客呼叫机和用户接收机是楼寓对讲系统的基本组成单元，双向对讲的目的是确认访客身份。较大规模的楼寓对讲系统除访客呼叫机和用户接收机外，还可能配备管理机，管理机与访客呼叫机、用户接收机之间也可实现双向对讲。

2 楼寓对讲系统的重要功能就是通过关闭的受控门将用户

和访客进行隔离，通过用户对访客的甄别，由用户选择是否开启受控门。因此，确保受控门的正常关闭非常重要。当受控门开启时间超过预设时长时，意味着系统处于不安全状态；当访客呼叫机防拆开关被触发时，意味着可能有人破坏访客呼叫机、尝试非法开启受控门。以上情况均应在现场发出告警提示。

3.5.7 电子巡查系统分为在线式和离线式两种形态。随着技术的发展，系统产品形态出现了较大的变化，如通过移动通信技术使用手机、平板电脑等作为巡查终端，也是在线式电子巡查系统的一种应用形式。

在线式电子巡查系统通过设定不同的巡查路线、巡查时间、巡查人员等可以形成不同的巡查方案，当巡查人员的实际巡查路线、巡查时间等与巡查方案不相符时，系统能发出报警信号进行提示。

4 工程施工

4.0.1 根据《建筑工程设计文件编制深度规定（2016年版）》“5 专项设计”规定，智能化专项设计根据需要分为方案设计、初步设计、施工图设计及深化设计四个阶段。

深化设计是在审查通过的施工图设计文件基础上，对施工图设计的内容进行审查、核算和修订，准确并量化表达设计内容及设备、材料、工艺要求等，对施工作业的特殊要求等进行详尽说明，满足设备材料采购、非标准设备制作、施工和调试的需要。

在施工过程中，局部调整和变更时应填写更改审核单，需经建设单位、设计单位、施工单位、监理单位相关责任人会签批准。更改审核单概括深化设计文件的调整或更改情况，包括更改内容、更改原因、更改前后状态描述、申请单位、审核单位、分发单位、更改实施日期等。

4.0.2 安全防范工程材料、设备的质量状况直接影响安全防范系统的功能、性能。安全防范工程中使用的设备材料应符合国家

法规和现行相关标准的要求。质量证明文件包括有效期内的产品检测报告、认证证书等。

4.0.3 在施工过程中，根据施工要求对隐蔽工程进行工序验收，做好随工记录，并形成隐蔽工程随工验收单。隐蔽工程随工验收单需经建设单位、设计单位、施工单位、监理单位相关责任人会签。

隐蔽工程随工验收单概括隐蔽工程情况，包括隐蔽工程的检查内容、检查结果，并综合安装质量的检查结果，形成验收意见。

4.0.4 线缆敷设作为安全防范工程的关键环节，在合理位置设置编号是为了保障建成后的安全防范系统能够便利运行维护。线缆编号标识规则参考现行行业标准《安防线缆应用技术要求》GA/T 1406 的相关规定。

4.0.5 本条是针对文物保护单位的特点提出的。安全防范工程的设备选型、施工工艺等均不能对文物本体造成破坏。施工过程中可采取非接触式或近距离安装、非实体性的钻入安装部件、实体安装部件最小化以及与文物风貌协调安装等保护措施。

4.0.6 在易燃、易爆等环境中安装和使用安全防范设备时，要根据现行国家标准《危险化学品重大危险源辨识》GB 18218 进行危险源辨识。根据危险源的类别，结合其相应行业的相关标准进行施工，现有的相关标准主要有国家现行标准《电气装置安装工程　爆炸和火灾危险环境电气装置施工及验收规范》GB 50257、《海洋石油平台电气设备防护、防爆等级要求》CB/T 4397、《爆炸危险场所防爆安全导则》GB/T 29304、《爆炸性环境　第 1 部分：设备　通用要求》GB 3836.1 等。

4.0.7 安全防范工程施工完成后，通常由建设单位、施工单位、监理单位等共同进行初步验收，形成初步验收报告。

初步验收通过或项目整改完成后的安全防范工程，经过不少于 30d 的系统试运行，能够较好地验证系统的功能、性能、稳定

性，充分发现问题，以便对系统进一步优化完善。

系统试运行期间，值机人员或系统管理员需完整、翔实地记录系统试运行情况。

5 工程检验与验收

5.0.1 对安全防范工程进行工程检验是验证安全防范工程质量和系统是否达到预期效能的有效手段，高风险保护对象对安全防范工程的质量要求更加严格。

工程检验是按照约定程序对安全防范工程的一种或多种特性进行测量、检查、试验、度量并将这些特性与规定进行对比以确定其符合性的活动，检验的基本要点包括检验对象、检验依据、检验手段、检验数据、检验结论等。

工程检验机构应具备从事安全防范工程检验所需的基本条件和技术能力，包括获取的资质证书和授权范围，资质证书一般可包括为：CMA（China Metrology Accredidation）、CAL（China Accredited Laboratory）、CNAS（China National Accreditation Service for Conformity Assessment），各资质的授权能力范围主要是指能力、方法、项目和涉及的标准，该机构能力范围必须包含本标准以及在本标准中相关的其他标准内容，如金融、博物馆等领域的国家标准或行业标准及电磁兼容等的方法标准。

5.0.2 系统功能、性能是反映安全防范工程质量的基本要素，工程检验是依据工程深化设计文件和国家现行相关标准中对系统架构及各子系统功能、性能的要求进行的技术验证。

5.0.3 安全防范工程的竣工验收是对工程建设质量和成果进行评定的重要环节。为确保工程质量，在工程竣工后组织验收是非常必要的。

施工验收应对设备安装、线缆敷设、线缆连接、隐蔽工程等施工质量进行查验，技术验收应对系统应达到的基本要求、主要功能和技术指标进行检查，资料审查是对安全防范工程建设过程

资料的准确性、完整性、规范性进行查验。

验收组可根据实际情况设置施工验收组、技术验收组和资料审查组，并根据项目的性质、特点和管理要求确定验收组成员，验收组中技术专家比例一般不低于50%，未经检验的工程验收时，可适当增加技术专家的比例。

不利于验收公正的人员不能参加验收组，包括与该工程相关的设计、施工、产品制造、设备供应等相关人员以及其他需要回避的人员。

5.0.4 验收结论是工程竣工验收的结果，验收组需客观、公正地给出验收结论。验收通过的工程，验收组可在验收结论中提出建议或整改意见；验收基本通过或不通过的工程，验收组应在验收结论中明确指出发现的问题和整改要求。

5.0.5 移交的工程竣工资料要真实、完整地反映安全防范工程的建设情况，竣工资料编制深度参见现行行业标准《安全防范工程技术文件编制深度要求》GA/T 1185的相关内容。

验收合格的工程，施工单位、设计单位、建设（使用）单位等应根据验收组提出的建议与要求落实整改措施。施工单位、设计单位的整改落实后应提交书面报告并经建设（使用）单位确认。

验收不合格的工程，施工单位、设计单位、建设（使用）单位等应根据验收组提出的意见与要求，落实整改措施后再次组织验收；工程复验时，对原不通过部分的抽样比例应加倍。

6 系统运行与维护

6.0.1 安全防范系统的运行与维护是安全防范工程全生命周期管理的重要环节，通过系统运行与维护落实安全防范管理要求，持续保持系统防范效能。

通过规范的系统运行活动，可以实现安全防范管理中事件/警情的有效处置。通过有效的系统维护活动，可以在一定程度上

规避由于系统和设备的使用寿命、使用环境等因素造成的系统防范效能下降，延长系统和设备的使用期限，提升系统和设备的可靠性，排除系统和设备的隐患和故障。

系统运行与维护工作中应该如实反映系统的运行和维护状态，积累运行与维护数据，为系统效能评估提供依据。

6.0.2 建立科学、规范的运行维护保障体系，可最大程度地发挥系统的防范效能。

系统运行与维护工作需要系统化的工作思路，其中一项重要内容就是运行与维护方案的制订，主要包括以下内容：

（1）确定系统运行工作目标、工作范围、工作要求、工作团队等，编制系统运行工作费用预算。

（2）确定维护工作范围、内容和要求、工作团队等，编制系统维护工作费用预算。费用预算可参考现行行业标准《安全防范工程建设与维护保养费用预算编制办法》GA/T 70 的相关规定。

系统运行维护工作可以由建设（使用）单位承担，也可以由建设（使用）单位委托的第三方运行维护服务机构承担。

6.0.3 系统运行作业内容包括安全防范系统值机任务和处置流程等。

作业指导文件包括值机员、现场处置员岗位职责，运行作业内容、要求与处置流程，突发事件应急预案，值机日志要求，值机交接班要求等。

培训包括岗前培训和在岗培训，培训内容包括法律法规常识、职业道德、纪律作风、安全保密知识、工作规范、管理制度、系统与设备的基本知识、前端设备的分布情况、基本操作技能、风险事件的发生规律和特点、信息分析研判、应急处置预案及演练等。

6.0.4 为确保紧急报警事件能准确及时处置，监控中心值机人员在接到紧急报警后，还需对接入公安机关的紧急报警信息进行人工复核。

6.0.5 日常维护工作可参照现行行业标准《安全防范系统维护保养规范》GA/T 1081 的相关规定。

故障处理是根据安全防范管理要求和（或）服务合同规定，及时对系统发生的故障进行处置，对故障维修情况进行记录，对故障设备后续运行情况进行跟踪。

特殊时期通常是指国家重要节假日、政府或相关职能部门组织的重大活动期间，以及涉及重大自然灾害、生产、食品卫生、社会治安等应急管理时期。在特殊时期，需强化相应的保障措施。

9 155182 091900

统一书号：155182·0919

定　　价：30.00 元