建筑安全防范通用规范

（征求意见稿）

目　次

1　总则 1
2　基本规定 2
3　布防设计 3
4　系统设计 5
4.1　一般规定 5
4.2　实体防护系统设计 5
4.3　入侵和紧急报警系统设计 6
4.4　视频监控系统设计 7
4.5　出入口控制系统设计 7
4.6　停车库(场)安全管理系统设计 8
4.7　防爆安全检查系统设计 8
4.8　楼寓对讲系统设计 8
4.9　电子巡查系统设计 8
5　工程施工 10
6　工程检验与验收 11
7　系统运行与维护 12
编制说明

1　总则

1.0.1　为了规范建筑安全防范工程建设和系统运行维护，提高安全防范工程建设质量和系统运行、维护水平，保护人身安全和财产安全，制定本规范。

1.0.2　建筑安全防范工程建设和系统运行维护应遵守本规范。

1.0.3　本规范是建筑安全防范工程建设过程和系统运行维护等的技术和管理的基本要求。当建筑安全防范工程中采用的技术措施与本规范不一致时，但经合规性评估后符合本规范第2章，应允许使用。

1.0.4　建筑安全防范工程建设和系统运行维护，除应遵守本规范外，尚应遵守国家现行有关规范的规定。

2　基本规定

2.0.1　安全防范工程的建设应科学合理，并通过有效运行与维护，构建满足安全防范管理要求、具有相应风险防范能力的综合防控体系。

2.0.2　安全防范工程应进行全生命周期管理。

2.0.3　安全防范工程的建设应遵循下列原则：

1　满足人防、物防、技防相结合，探测、延迟、反应相协调要求。

2　满足保护对象的防护级别与风险等级相适应要求。

3　满足系统和设备的安全等级与防范对象及其攻击手段相适应要求。

4　满足防护的纵深性、均衡性、抗易损性要求。

5　满足系统的安全性、可靠性要求。

6　满足系统的电磁兼容性、环境适应性要求。

7　满足系统中信息的实时性和原始完整性要求。

8　满足系统的兼容性、可扩展性、可维护性要求。

2.0.4　安全防范工程建设和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、商业秘密和公民个人隐私的措施。

2.0.5　安全防范系统监控中心应符合下列规定：

1　应远离产生粉尘、油烟、有害气体、强震源和强噪声源以及生产或贮存具有腐蚀性、易燃、易爆物品的场所，应避开发生火灾危险程度高的区域和电磁场干扰区域。

2　面积和环境应满足系统正常运行与维护的需要。

3　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封闭保护，其保护结构的抗拉伸、抗弯折强度不应低于壁厚 2.0mm 的镀锌钢管。

2.0.6　安全防范工程除应满足安全防范效能外，还应满足紧急情况下人员疏散的要求。

2.0.7　应采取措施，防止安全防范系统使用的设备产生的 X 射线、激光辐射、电磁辐射等对人体健康造成伤害。

2.0.8　安全防范系统应采取但不限于如下一种或多种措施保证系统的信息安全，并符合国家有关密码管理规定：

1　防病毒和防网络入侵措施。

2　密钥或编码不应是弱口令，用户名和操作密码组合应不同。

3　当基于不同传输网络的系统和设备联网时，采取边界安全管理措施。

2.0.9　安全防范系统供电暂时中断，恢复供电后，系统应能自动恢复原有工作状态。

2.0.10　高风险保护对象的安全防范工程还应符合下列规定：

1　采用专用传输网络。

2　进行工程检验和验收。

3　布防设计

3.0.1　安全防范工程建设应明确保护对象及其安全需求，确定需要防范的风险。按照纵深防护和均衡防护的原则，统筹人力防范能力，协调配置实体防护和电子防护设备、设施，对保护对象进行综合布防设计。

3.0.2　当对周界进行防护时，应符合下列规定：

1　应根据现场环境和安全防范管理要求，合理选择实体防护、入侵探测、视频监控等一种或多种防护措施；

2　所选择实体防护措施的防护能力应满足对抗相应风险的要求；

3　所选择入侵探测设备的探测能力应满足针对攀爬、翻越、挖凿等一种或多种入侵行为的探测要求；

4　所选择视频监控装置的监视效果至少应看清周界环境中人员的活动情况。

3.0.3　当对出入口进行防护时，应符合下列规定：

1　应根据现场环境和安全防范管理要求，合理选择实体防护、出入口控制、入侵探测、视频监控等一种或多种防护措施；

2　与周界相连的、无人值守的出入口，所选择实体屏障的防护能力应与周界实体屏障的防护能力相当；

3　所选择出入口控制装置应满足目标识别的要求，并应具有防拆卸、防尾随、防技术开启等一种或多种防护能力；

4　所选择入侵探测设备的探测能力应满足非法入侵出入口行为的探测要求，

5　所选择视频监控装置的监视效果，应能清晰辨别人行出入口进入人员的面部特征和车辆出入口通行车辆的号牌。

3.0.4　当对通道和公共区域进行防护时，应符合下列规定：

1　应根据现场环境和安全防范管理要求，合理选择视频监控、车辆实体屏障等一种或多种防护措施；

2　重要通道应安装视频监控装置，其监视效果应能看清监控区域内人员、物品、车辆的通行状况；

3　重点公共区域应安装视频监控装置，其监视效果应能至少看清区域内人员的活动状况；

4　所选择车辆实体屏障应具有限制或阻挡车辆通行的相应能力。

3.0.5　人员密集、大流量的出入口、通道等场所，应采取人员疏导和快速通行等措施。

3.0.6　当对财务室、数据机房、水电气热设备间等进行防护时，应符合下列规定：

1　应采取实体防护、入侵探测、出入口控制、视频监控等一种或多种防护措施；

2　所选择的防盗安全门、防盗保险柜等设施应满足相应安全等级的要求；

3　所选择的其他防护措施应满足防御非法入侵、出入目标控制、视频监视效果的具体要求。

3.0.7　监控中心的防护应符合下列规定：

1　应采取实体防护、出入口控制和视频监控等防护措施，保证自身安全。应有进行内外联络的通讯手段，并应设置紧急报警装置和留有向上一级接处警中心报警的通信接口。

2　门窗采取实体防护措施防盗安全门的防盗安全级别不应低于乙级。

3　出入口应设置视频监控和出入口控制装置。监视效果应能清晰显示监控中心出入口

外部区域的人员特征及活动情况。

4　监控中心内设置视频监控装置，监视效果应能清晰显示监控中心内人员活动的情况。

5　对设置在监控中心的出入口控制系统管理主机、网络接口设备、网络线缆等应采取强化保护措施。

3.0.8　当对保护目标进行防护时，应符合下列规定：

1　应根据现场环境和安全防范管理要求，合理选择实体防护、区域入侵探测、位移探测、视频监控等的一种或多种防护措施；

2　实体防护装置应满足不同保护目标对抗相应风险的要求；

3　采用区域入侵探测、位移探测等手段时，对目标被接近或被移动的情况应能实时探测报警；

4　采用视频监控进行防护时，应确保保护目标持续处于监控范围内，监视效果至少应能看清保护目标及其所在区域中人员的活动情况。

3.0.9　当需要对通行的人员、车辆进行安全检查时，应在保护区域的出入口或其附近设置安全检查区，安全检查区内设置的安全检查通道数量、配备的安全检查设施和人员应与被检人员、物品和车辆流量相适应。配置的专业安全检查人员和安全检查设备应满足检查目标的要求。

3.0.10　保护对象被确定为防范恐怖袭击重点目标时，应根据防范恐怖袭击的具体需求，强化以下一种或多种防护措施：

1　加强周界实体屏障；

2　联合设置周界实体防护装置和电子防护装置；

3　增加设置安全检查区，选择对出入人员、物品、车辆等进行安全检查，并配备排爆处置设施和防暴防护器具；

4　重要出入口和通道选择配置人行通道闸、车辆阻挡装置、设置安全缓冲或隔离区等一种或多种措施；

5　加强人员密集区域的视频监控和动态监测、预警；

6　监控中心及其他重要部位（区域）联合设置实体防护装置和电子防护装置；

7　对无人飞行器采取防御和反制措施。

4　系统设计

4.1 一般规定

4.1.1　安全防范系统应由实体防护系统和（或）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）等一种或多种措施构建实体防护系统。

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、防爆安全检查系统、电子巡查系统、楼寓对讲系统等一种或多种子系统构建电子防护系统。

3　当配置安全防范管理平台时，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、统计分析、系统校时等基本功能。

4.1.2　安全防范系统架构应包括子系统组成、集成/联网方式、传输网络、存储管理、系统供电、接口协议等基本要素。

4.1.3　安全防范系统及其组成设备（部件）的安全等级应根据不同的风险防范能力确定。系统中共用设备（部件)的安全等级应与相关联的设备(部件)的最高安全等级一致。

4.1.4　安全防范系统某一子系统的故障不应影响其它子系统的正常运行。安全防范管理平台的故障不应影响各子系统的正常运行。上级安全防范管理平台的故障不应影响下级安全防范管理平台的正常运行。

4.1.5　当安全防范系统与其他电子信息系统集成联网时，其他电子信息系统的故障不应影响安全防范系统的正常运行。

4.1.6　当安全防范系统采用人工智能等新技术时，应评估新技术对安全防范管理带来的次生风险。当存在次生风险时，应采取相应防范措施。

4.1.7　安全防范工程应结合人防能力，配备相应的防护、防御和对抗性设备、设施和装备。

4.2 实体防护系统设计

4.2.1　实体防护系统设计应针对需要防范的风险，实现相应的威慑、延迟、阻挡等防护能力。

4.2.2　实体防护设计应包括周界实体防护设计、建（构）筑物设计和实体装置设计等一种或多种。周界实体防护设计应包括周界实体屏障、出入口实体屏障、车辆实体屏障、安防照明与警示标志等一项或多项。建（构）筑物设计应包括平面与空间布局、结构和门窗等与风险防范相关的内容。

4.2.3　当采用周界实体屏障时，应符合下列规定：

1　应根据场地条件合理规划周界实体屏障的位置。周界实体屏障的防护面一侧的区域内不应有可供攀爬的物体或设施。

2　当保护对象有防爆安全要求时，应根据爆炸冲击波对防护区域的破坏力和／或杀伤力，选择具有相应防护能力的周界实体屏障，并设置有效的安全距离。

3　有防攀越、防穿越、防拆卸、防破坏、防窥视、防投射物等防护功能要求的周界实体屏障，其材质、强度、高度、宽度、深度（地面以下）、厚度等应满足防护性能的要求。

4　穿越周界的河道、涵洞、管廊等孔洞，应采取相应的实体屏障进行防护。

4.2.4　当采用车辆实体屏障时，应符合下列规定：

1　车辆实体屏障应具有减速、吸能、阻停等防护功能。应根据防范车辆的载重、速度及其撞击产生的动能，合理设计车辆实体屏障的材质材料、规格尺寸、结构强度、固定方式等，满足相应的防冲撞能力要求。

2　当保护对象有防爆安全要求时，车辆实体屏障应设置有效的安全距离。

4.2.5　建（构）筑物平面与空间布局设计应符合下列规定：

1　根据安全防范管理要求，应合理设计建（构）筑物场地道路的安全距离、线形和行进路线。应利用场地和景观形成缓冲区、隔离带、障碍等，发挥场地与景观的实体防护功能。

2　具有易燃、易爆、有毒、放射性等特性的保护目标，其存放场所或独立建（构）筑物应设置在隐蔽和远离人群的位置。

4.2.6　建（构）筑物结构设计应符合下列规定：

1　当有防爆炸要求时，建筑物墙体应进行防爆结构设计。当有保密要求的场所，应进行信息屏蔽、防窃听窃视设计。

2　当建（构）筑物的洞口、管沟、管廊、吊顶、风管、桥架、管道等空间尺寸能够容纳防范对象隐蔽进入时，应采用实体屏障或实体构件进行封闭和阻挡。

4.2.7　建筑门窗设计与选型应符合下列规定：

1　有防盗要求时，保护目标所在的部位或区域应采用相应安全等级的防盗安全门和相应防护能力的安全防盗窗；

2　有防爆炸和/或防弹和/或防砸要求时，保护目标的门、窗均应采用相应安全等级的防爆炸玻璃和/或防弹和/或防砸玻璃；

3　金库、文物库等特殊保护目标库房的总库门应采用具有防盗、防火、防水等功能的安全门。

4.2.8　当采用实体装置时，应满足对重要物品、重要设施、重要线缆等保护目标的防盗窃、防窥视、防砸、防撬、防弹、防爆炸等一种或多种防护要求。

4.2.9　当其锐利边缘或其触碰对人体有一定伤害的特殊防御功能的实体防护设施，应在其安装区域显著位置设置警示标识。

4.3 入侵和紧急报警系统设计

4.3.1　入侵和紧急报警系统应对保护区域的非法隐蔽进入、强行闯入以及撬、挖、凿等破坏行为进行实时有效的探测与报警。应结合风险防范要求和现场环境条件等因素，选择适当类型的设备和安装位置，构成点、线、面、空间或其组合的综合防护系统。

4.3.2　入侵和紧急报警系统应能准确、及时地探测入侵行为或触发紧急报警装置，并发出入侵报警信号或紧急报警信号。

4.3.3　当下列设备被替换或外壳被打开时，入侵和紧急报警系统应能发出防拆信号：

1　控制指示设备、告警装置；

2　安全等级 2、3、4 级的入侵探测器；

3　安全等级 3、4 级的接线盒。

4.3.4　当报警信号传输线被断路或短路、探测器电源线被切断、系统设备出现故障时，控制指示设备应发出声、光报警信号。

4.3.5　应能按时间、区域、部位，对全部或部分探测防区（回路）的瞬时防区、24 小时防区、延时防区、旁路、传输、告警、设防、撤防、胁迫报警等功能进行参数设置。应能对系

统用户权限进行设置。

4.3.6　系统操作人员应能根据权限级别不同，按时间、区域、部位对全部或部分探测防区进行自动或手动设防、撤防、旁路等操作，并应能实现胁迫报警操作。

4.3.7　系统应能对入侵、紧急、防拆、故障等报警信号来源、控制指示设备以及远程信息传输工作状态有明显清晰的指示。

4.3.8　当系统出现入侵、紧急、防拆、故障、胁迫等报警状态和非法操作时，系统应能根据不同需要在现场和（或）监控中心发出声、光报警通告。

4.3.9　应能对系统操作、报警和有关警情处理等事件进行记录和存储，且记录不可更改。

4.3.10　入侵和紧急报警系统不得有漏报警，报警响应时间应满足安全防范管理要求。

4.4 视频监控系统设计

4.4.1　视频监控系统应对监控区域和目标进行实时、有效的视频采集和监视，对视频采集设备及其信息进行控制，对视频信息进行记录与回放，监视效果应满足实际应用需求。

4.4.2　视频采集设备的监控范围应有效覆盖被保护部位、区域或目标，监视效果应满足场景和目标特征识别的不同需求。视频采集设备的灵敏度和动态范围应满足现场图像采集的要求。

4.4.3　系统的传输装置应保证视频图像信息和其他相关信息在前端采集设备到显示设备、存储设备等各设备之间的安全有效及时传递。视频传输应支持对同一视频资源的信号分配或数据分发的能力。

4.4.4　系统应具备按照授权实时切换调度指定视频信号到指定终端的能力。

4.4.5　系统应具备按照授权对选定的前端视频采集设备进行 PTZ 实时控制，或对前端视频采集设备进行工作状态调整的能力。

4.4.6　系统应能实时显示系统内的所有视频图像，系统图像质量应满足安全管理要求。声音的展示应满足对声音特征或语义辨识的需要。显示的图像和展示的声音应具有原始完整性。

4.4.7　除防范恐怖袭击重点目标外，其他目标的视频图像信息保存期限不应少于 30d。

4.4.8　系统应具有用户权限管理、操作与运行日志管理、设备管理和自我诊断等功能。

4.5 出入口控制系统设计

4.5.1　出入口控制系统应根据不同的通行对象进出各受控区的安全管理要求，在出入口处，对其所持有凭证进行识别查验，对其进/出实施授权、实时控制与管理，满足实际应用需求。

4.5.2　出入口控制系统应根据安全等级的要求，采用相应自我保护措施和配置。位于对应受控区、同权限受控区或高权限受控区域以外的部件应具有适当的防篡改/防撬/防拆保护措施。

4.5.3　当通向疏散通道方向为防护面时，系统接收到消防联动控制或紧急疏散信号时，人员应能不用进行凭证识读操作即可安全通过。

4.5.4　断电开启的出入口控制点执行装置在其满负荷状态下，当其按照安全等级 1 级、2 级、3 级配置时，其备用电源则不应小于 48h；当其按照安全等级 4 级配置时，其备用电源应能确保该执行装置正常运行不应小于 72h。

4.5.5　当系统与其它非安防业务系统共用凭证或其介质构成“一卡通”应用模式时，出入

口控制系统应独立设置与管理。

4.5.6 出入口执行部分的连接线缆在该出入口的对应受控区、同权限受控区、高权限受控区以外的部分应封闭保护，其保护结构的抗拉伸、抗弯折强度不应低于壁厚 2.0mm 镀锌钢管。

4.6 停车库(场)安全管理系统设计

4.6.1 停车库（场）安全管理系统应对停车场（库）的车辆进行出入控制、监视与图像抓拍、行车信号指示、人车复核及车辆防盗报警，并能对停车库（场）内的人员及车辆的安全实现综合管理。

4.6.2 停车库（场）安全管理系统应采取措施满足车辆通行的要求。高风险目标区域的停车库（场）安全管理系统还应满足阻车能力要求。

4.6.3 停车库（场）安全管理系统应具有正常通行车辆的安全保护措施。

4.6.4 停车库（场）安全管理系统应能对车辆的识读过程提供现场指示。当出现车辆出入口被非授权开启、故障等状态时，系统应能根据不同需要向现场、监控中心发出可视和/或可听的通告或警示。

4.7 防爆安全检查系统设计

4.7.1 防爆安全检查系统应能对进入保护单位或区域的人员和（或）物品和（或）车辆进行安全检查，对规定的爆炸物、武器、管制器具或其他违禁品进行实时、有效的探测、显示、记录和报警。

4.7.2 当选择成像式人体安全检查设备时，应对人体图像的隐私部分采取保护措施。

4.7.3 防爆安全检查系统探测时产生的辐射剂量不应对被检人员和物品产生伤害，不应引起爆炸物起爆。系统探测时泄漏的辐射剂量不应对非被检人员和环境造成伤害。

4.7.4 应配备防爆处置、防护设施。防护设施应安全受控，便于取用。

4.8 楼寓对讲系统设计

4.8.1 楼寓对讲系统应能使被访人员通过（可视）对讲方式确认访客身份，控制开启出入口门锁，实现建筑物（群）出入口的访客控制与管理。

4.8.2 当楼寓对讲系统管理的受控门开启时间超过预设时长、访客呼叫机防拆开关被触发时，应有现场告警提示信息。具有高安全需求的系统还应向管理中心发送告警信息。

4.8.3 除已采取了可靠的安全管控措施外，不应利用无线扩展终端控制开启入户门锁以及进行报警控制管理。

4.9 电子巡查系统设计

4.9.1 电子巡查系统应按照预先编制的人员巡查程序，通过信息识读器或其他方式对人员巡查的工作状态进行监督管理。

4.9.2 电子巡查系统应能对巡查线路轨迹、时间、巡查人员进行设置，应能设置多条并发线路。

4.9.3 在线式电子巡查系统应能在预先设定的巡查路线中，对人员的巡查活动状态进行监督和记录，并在发生意外情况时及时报警。

4.9.4　电子巡查系统应能对设置内容、巡查活动情况进行统计，形成报表。

5　工程施工

5.0.1　在安全防范工程施工阶段时，对设计文件进行更改，应得到原设计方批准。

5.0.2　安全防范工程施工前，应查验所采用设备和材料的质量证明文件。

5.0.3　安全防范工程的线缆接续点和两端应进行统一编号、设置永久标识，线缆检修孔、分支处等位置应设置标签。同轴电缆应一线到位，中间无接头。

5.0.4　在古建筑、石窟寺及石刻、古文化遗址、古墓葬等文物保护单位进行安全防范工程的管线敷设应采取对文物本体和环境的保护措施。

5.0.5　在研制、生产、使用、储存、经营和运输过程中存在易燃易爆的特殊环境中安装和使用安全防范设备时，应按现行国家标准的有关规定，进行危险源辨识，根据其规定的危险场所分类，采用相对应的材料，保持安全距离，做好协调工作，严格遵守所规定的施工工艺方法。

5.0.6　安全防范工程初步验收通过、项目整改及复验完成后，系统试运行不应少于 30d。

6　工程检验与验收

6.0.1　安全防范工程检验时，应对实体防护和电子防护系统的功能性能、安全性、电磁兼容性、防雷与接地、供电、信号传输、设备安装及监控中心等进行检验。

6.0.2　安全防范工程验收时，应组成验收组，对工程进行施工验收、技术验收和资料审查。不利于验收公正性的人员不得参加验收组。

6.0.3　对安全防范工程进行施工验收，应对下列内容进行现场检查和资料核查：

1　设备安装的位置与工艺、防雷接地措施、线缆标识及通电状态等设备安装质量；

2　线缆布放、 穿管（槽）、架空、地埋、电缆沟、管道等线缆敷设质量；

3　线缆连接、中间接续、光缆熔接等线缆连接质量；

4　隐蔽工程。

6.0.4　对安全防范工程进行技术验收，应对下列内容进行现场查验：

1　系统应达到的基本要求、主要功能与技术指标；

2　工程实施结果、设备数量、型号及安装部位；

3　实体防护和电子防护系统的的功能要求和技术指标；

4　监控中心。

6.0.5　对安全防范工程进行资料审查，应对下列资料的规范性、完整性、准确性进行审验：

1　项目合同书；

2　设计文件；

3　工程变更文件；

4　隐蔽工程资料；

5　系统试运行报告；

6　竣工图纸。

6.0.6　验收组应对工程质量做出客观、公正的验收结论。

6.0.7　安全防范工程验收通过后，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。验收不通过的工程不得正式交付使用。

7　系统运行与维护

7.0.1　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。

7.0.2　安全防范工程建设（使用）单位应制定安全防范系统运行与维护规划，建立包括人员、经费、制度和技术支撑系统在内的运行维护保障体系，确定运行与维护工作任务及考核指标。

7.0.3　系统运行单位应组建系统运行工作团队，制定日常管理、值机、现场处置、例会、安全保密、培训和考核等制度，统筹协调与系统运行有关的机构、人员等各项资源，开展运行作业。

7.0.4　系统运行单位应确认系统运行环境、作业内容，编制作业指导文件以及对系统运行环境、运行作业内容进行符合性检查。

7.0.5　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。

7.0.6　系统维护单位应组建系统维护工作团队，做好安全防范系统的日常维护、故障处理、特殊时期保障以及维护评价等。日常维护中遇故障报修时，应优先按故障处理程序对故障进行处理。特殊时期保障应根据需要加强维护资源配置。

附：起草说明

一、起草单位

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、公安部安全与警用电子产品质量检测中心、公安部安全防范报警系统产品质量监督检验测试中心、中国建筑设计院有限公司、北京中盾安全技术开发公司、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、西安北方信息产业有限公司、上海天跃科技股份有限公司、浩云科技股份有限公司、富盛科技股份有限公司、江苏固耐特围栏系统股份有限公司、北京蓝盾世安信息咨询有限公司、上海德梁安全技术咨询服务有限公司、上海现代建筑集团有限公司、上海广拓信息技术有限公司、福州米立科技有限公司、厦门立林电子科技有限公司、广州宏亮信息技术有限公司、云南省电子信息产品检验院。

二、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、阻止入侵、盗窃、抢劫、破坏、爆炸、暴力袭击等事件的发生。

2.人力防范 personnel protection

具有相应素质的人员有组织的防范、处置等安全管理行为，简称人防。

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，又称物防。

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，又称技防。

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.防爆安全检查系统 anti-explosion 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入侵、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.风险等级 level of risk

存在于保护对象本身及其周围的、对其安全构成威胁的单一风险或组合风险的大小，以后果和可能性的组合来表达。

23.防护级别 level of protection

为保障保护对象的安全所采取的防范措施的水平。

24.安全等级 security grade

安全防范系统、设备自身所具有的对抗不同攻击的能力水平。

25.探测 detection

对显性风险事件或/和隐性风险事件的感知。

26.延迟 delay

延长或/和推迟风险事件发生的进程。

27.反应　response

为应对风险事件的发生所采取的行动。

28.误报警　false alarm

对未设计的事件做出响应而发出的报警。

29.漏报警　leakage alarm

对设计的报警事件未做出报警响应。

30.周界　perimeter

保护对象的区域边界。

31.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。

32.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。

33.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。

34.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。

35.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。

36.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。

37.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。

38.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。

39.系统效能评估 system effectiveness evaluation

对安全防范系统满足预期效能程度的分析评价过程。

三、条文说明

为便于政府有关管理部门和建设、设计、施工、科研等单位有关人员在使用本规范时能正确理解和执行条文规定，规范起草组按照条、款顺序编制了本规范的条文说明。但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 本条规定源自《安全防范工程技术标准》GB50348-2018 第 1.0.1 条（非强制性条文）。

本条规定了本规范制定的目的。本规范按照中共中央办公厅、国务院办公厅印发《关于加强社会治安防控体系建设的意见》（中办发[2014]69 号）中“以确保公共安全、提升人民群众安全感和满意度为目标，以突出治安问题为导向，以体制机制创新为动力，以信息化为引领，以基础建设为支撑，坚持系统治理、依法治理、综合治理、源头治理，健全点线面结合、网上网下结合、人防物防技防结合、打防管控结合的立体化社会治安防控体系，确保人民安居乐业、社会安定有序、国家长治久安”的指导思想，以维护社会安全稳定、保护人身

安全和财产安全为目标，通过规范建筑安全防范工程设计、施工、监理、检验、验收及系统运行与维护，有效预防、延迟、阻止入侵、盗窃、抢劫、破坏、爆炸、暴力袭击等事件的发生。

1.0.2　本条规定源自《安全防范工程技术标准》GB50348-2018 第 1.0.2 条（非强制性条文）。

本条规定了本规范的适用范围。

本规范不适用于战争、自然灾害等不可抗力条件下对建筑安全防范工程的要求。

1.0.3　本规范是国家工程建设控制性底线要求，具有法规强制效力，必须严格遵守。

本规范提出的安全防范措施不是唯一的，如果采用其他措施替代本规范提出的方法，通过合规性评估同样能满足安全防范管理要求的情况下，也应该允许使用。

1.0.4　本条规定源自《安全防范工程技术标准》GB50348-2018 第 1.0.8 条（非强制性条文）。

其他现行法律法规对建筑安全防范工程建设和系统运行维护有其他规定的，也应遵循。

2　基本规定

2.0.1 本条规定源自《安全防范工程技术标准》GB50348-2018 第 1.0.4 条（非强制性条文）。

安全防范工程建设是构建社会安全综合治理体系的重要组成部分，它要服务于社会安全，更要服务于社会管理、服务于国家治理体系和治理能力的现代化建设。

实际上，任何一个安全防范系统在有限的资源和时空条件下，只能针对特定风险达到有限防范的效果，无法做到万无一失。

因此，努力追求在有限资源和时空条件下的最佳和最优的管理效能，努力降低或避免发生风险的概率是安全防范工程建设的重要目标。

2.0.2　本条规定源自《安全防范工程技术标准》GB50348-2018 第 3.0.1 条（非强制性条文）。

本规范的“全生命周期”包括安全防范工程的立项、设计、施工、监理、检验、验收以及安全防范系统的运行、维护等各阶段。安全防范工程建设之初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与系统运行维护工作提供人员和经费保障。

对于分期建设的安全防范工程，应进行统筹规划，在人力防范配置、实体防护设计和电子防护设计等方面综合考虑，确保分期建设的安全防范系统能够有机融合。

2.0.3　本条规定源自《安全防范工程技术标准》GB50348-2018 第 3.0.2 条（非强制性条文）。

第 1 款：人防、物防、技防是安全防范的三种基本手段，必须相结合，任何单一的防范手段都不可能实现真正的安全。探测、延迟、反应是安全防范的三个基本要素，必须相协调，在满足 $T_{探测}+T_{反应}\leqslant T_{延迟}$ 的条件下，安全防范系统才是一个有效的系统。

第 2 款：风险等级是指存在于保护对象本身及其周围的、对其安全构成威胁的单一风险或组合风险的大小，以后果和可能性的组合来表达。防护级别是指为保障保护对象的安全所采取的防范措施的水平。对于不同的风险等级，所采取的防范措施的水平也不同，且防护级别应该与风险等级相协调，防止“防护不足”或“过度防护”。

本规范定义的安全防范是指社会治安防范和反恐防范。特别是针对恐怖袭击的安全防范工程设计时，除了要考虑安全防范系统传统的探测、延迟、反应能力外，还要结合人力防范能力，配备必要的个人防护装备、有效的防御设施以及与恐怖分子对抗的装备等。反恐防范的安全防范工程设计需体现威慑、探测、防御、致胜四个要素。

第 3 款：安全防范系统是用于保护需要保护对象，对抗防范对象攻击的。因此其自身的安全特性，即自身的抗攻击能力是有效发挥防范效能的必要条件。安全防范工程建设时，应根据防范对象的能力和攻击手段，合理选择安全防范系统和设备的安全等级。如：在具体选择防盗保险柜产品时，应考虑攻击者使用的破坏工具以及保险柜应提供的防破坏时间，合理选择不同安全等级的产品。风险等级高的保护对象，通常情况下选择配置安全等级高的系统和设备。

根据有关国家标准，入侵和紧急报警系统、出入口控制系统按其性能分为四个安全等级，1 级为最低等级，4 级为最高等级。

例如，在《入侵和紧急报警系统技术要求》GB/T 32581-2016 中对安全等级进行了划分：

1　等级 1：低安全等级

入侵者或抢劫者基本不具备入侵和紧急报警系统知识，且仅使用常见、有限的工具。

2　等级 2：中低安全等级

入侵者或抢劫者仅具备少量入侵和紧急报警系统知识，懂得使用常规工具和便携式工具

（如万用表）。

3 等级 3：中高安全等级

入侵者或抢劫者熟悉入侵和紧急报警系统，可以使用复杂工具和便携式电子设备。

4 等级 4：高安全等级

入侵者或抢劫者具备实施入侵或抢劫的详细计划和所需的能力或资源，具有所有可获得的设备，且懂得替换入侵和紧急报警系统部件的方法。

第 4 款：纵深防护是根据保护对象所处的环境条件和安全管理的要求，对整个防护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。均衡防护是指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。抗易损防护是保证安全防范系统安全、可靠、持久运行并便于维修和维护的技术措施。纵深防护、均衡防护、抗易损防护是提高安全防范系统的防范效能的有效措施。

第 5 款：安全防范系统作为预防、延迟、阻止入侵、盗窃、抢劫、破坏、爆炸、暴力袭击等事件发生的重要手段，其本身必须安全、可靠，才能保证设备、系统的运行安全和使用者的人身安全。安全防范工程建设时，设计、施工、使用人员必须牢固树立“安全第一”的理念。只有安全的设备、完善的设计、精心的施工和严谨规范的管理相结合，才能真正发挥系统的防范效能。

第 6 款：安全防范系统建设时，应选用能够满足系统和设备安装、使用现场的自然环境、电磁环境等条件的设备和材料。

在《安全防范报警设备环境适应性要求和试验方法》GB/T 15211 中划分四种环境类别，具体如下：

1）环境类别Ⅰ。能够良好保持温度的室内环境（如在住宅或商业楼内）。

2）环境类别Ⅱ。无法良好保持温度的室内环境（如走廊、大厅、楼梯、可能产生冷凝的窗户和无供热的存放区或间歇性供暖的仓库等）。

3）环境类别Ⅲ。系统部件未完全暴露于室外（有遮蔽）或室内极端环境状态下经历的环境变化。

4）环境类别Ⅳ。系统部件完全暴露于露天环境下，环境因素受室外环境变化影响。

针对在自然环境,特别是海滨地区盐雾环境下工作的安全防范系统设备、部件、材料，其耐盐雾腐蚀的性能要能满足设计、使用寿命的要求。

针对在研制、生产、试验、储存、销售、使用等环节中含有腐蚀性气体和易燃易爆环境下工作的安全范范设备、部件、材料的抗腐蚀和防爆防护等级要符合其相应行业有关法律法规和标准的规定。

地埋的安全防范设备要根据环境和采取埋设方式的不同选用不同外壳防护等级，一般情况下，在电缆井、地下管网的外壳防护等级可以要求低一些，对于直埋的外壳防护等级要根据当地地质条件、埋设深度等可以高一些。

第 7 款：本款强调安全防范系统是一个对抗实战系统，兼具指挥调度的功能。系统中信息的实时性和原始完整性是实战系统的必然要求。安全防范系统中的电子防护系统就是要以极小的时延和极高的可靠度，将现场的信息及时准确完整地呈现给系统的后续环节或值机人员等，以便进一步进行各资源的协同配合和及时处置。这其中也包含了传输和存储的数据的不可篡改的要求。

第 8 款：安全防范系统建设应充分考虑系统的兼容性和可扩展性、可维护性，为在短期内的业务发展、需求变化后系统的扩容、升级奠定基础。

另外，安全防范工程建设在满足安全防范需求的前提下，尽可能选用经济、适用的设备材料，避免一味追求高端、先进，造成建设资金浪费。

作为涉及国家安全、社会安全和人民生命财产安全的建筑安全防范，根据国家《强制性产品认证管理规定》，列入强制性产品认证（3C 认证）目录的设备和材料，均应经认证合格后方可在工程中使用。未列入强制性产品认证（3C 认证）目录的，但制定了强制性国家标准或强制性行业标准的设备和材料，均应按相应标准检验合格后方可在工程中使用。

2.0.4　本条规定源自《安全防范工程技术标准》GB50348-2018 第 1.0.6 条（强制性条文）。

在涉及国家安全、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。

根据《中华人民共和国保守国家秘密法》“第二十九条　机关、单位公开发布信息以及

对涉及国家秘密的工程、货物、服务进行采购时，应当遵守保密规定。”、“第三十二条　机关、单位应当将涉及绝密级或者较多机密级、秘密级国家秘密的机构确定为保密要害部门，将集中制作、存放、保管国家秘密载体的专门场所确定为保密要害部位，按照国家保密规定和标准配备、使用必要的技术防护设施、设备。”的规定，保密要害部门部位安全防范工程建设必须采取严格的保密管理措施，包括：不得公开招标；对工程建设的勘察、设计、施工和监理单位进行保密审查；建设单位应制定具体的保密管理措施和方案，并与工程的勘察、设计、施工和监理单位签订保密协议；建设单位应进行全过程的保密监督管理；工程竣工后，建设单位应收回涉密图纸、资料等涉密载体，并办理移交手续；系统启用前必须通过安全保密检查检测等。

系统运行与维护所涉及的管理内容、处置预案（流程）、数据等信息，事关建设单位/使用单位的防护部位和防范手段等，是安全防范管理工作最需要保密的基础数据和管理要求。管理内容、处置预案（流程）、数据等信息的泄露，可能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、商业秘密或者侵犯公民个人隐私等合法权益。安防系统应采取相应措施支持防止被非法使用。

2.0.5　本条规定源自国家标准《安全防范工程技术标准》GB50348-2018 第 6.14.1 条第 1、3 款（非强制性条文）和第 6.13.4 条的第 4 款（强制性条文）。

第 1 款，监控中心是安全防范系统的存储、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，因此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。无法避开要求的场合时，应采取经过评估的隔离屏蔽、加固等防护措施，确保监控中心内部环境的稳定安全可控，满足设备运行和人员值守的需要。

第 2 款，安全防范系统的规模取决于需要管理的子系统数量、视频图像接入中心的数量和同时需要监视显示的画面屏幕数量以及值守终端数量等因素，辅助设施包括休息室、卫生间等。

合理的空间面积和布局、适当的环境条件是保证设备正常运行和人员值守的必要条件。

第 3 款：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。

监控中心作为安防系统自身最重要的部位（禁区），由于安防系统设备的 IT 化发展，愈来愈多的监控中心将其值守区与其设备区分离设置，两个区域间的信号传输链路往往会经由未防护或防护等级低的区域。对传输线缆采取抗拉伸、抗弯折强度不低于壁厚 2.0mm 的镀锌钢管的封闭保护措施，可有效降低传输线缆的信号干扰、物理损坏或人为破坏，提升系统运行稳定性和安全性。

2.0.6　本条规定源自《安全防范工程技术标准》GB50348-2018 第 6.1.3 条（强制性条文）。

安全防范工程的建设是为了保护人身安全和财产安全，维护社会安全稳定，其中保护人的生命安全是第一重要的。当需要人员疏散的紧急情况发生时，系统应满足人员疏散和逃生的要求。

2.0.7　本条规定源自《安全防范工程技术标准》GB50348-2018 第 6.6.2 条的第 2 款（强制性条文）。

应采取隔离、屏蔽和增大防护空间等方法，确保能够产生上述辐射或物质的设备正常工作时不会对人体健康造成伤害。

X 射线属于电离辐射，长时间照射对人体有损伤，射线越多，致癌的危险性越大。现阶段主要的标准有《电离辐射防护与辐射源安全基本标准》GB18871-2002。

激光辐射对人体的伤害主要是由激光热效应、光压效应和光化学效应所致，防护重点是眼和皮肤，有激光的工作场所应张贴醒目的警告牌。现阶段主要有《作业场所激光辐射卫生标准》GB 10435-1989、《工作场所物理因素测量 第 4 部分:激光辐射》GBZ/T 189.4-2007、《激光产品的安全 第 1 部分:设备分类、要求》GB 7247.1-2012、《激光产品的安全 生产者关于激光辐射安全的检查清单》GB/Z 18461-2001 等相关标准。

过量的电磁辐射同样会人体造成伤害，现阶段的标准主要有《电磁辐射防护规定》GB8702-88。

安全防范工程中选用的产品也应满足相关标准的要求，主要标准包括：《便携式 X 射

线安全检查设备通用规范》GB 12664-2003、《微剂量 X 射线安全检查设备 第 1 部分：通用技术要求》GB 15208.1-2005、《激光对射入侵探测器技术要求》GA/T1158-2014、《遮挡式微波入侵探测器技术要求》GB 15407-2010、《入侵探测器 第 3 部分：室内用微波多普勒探测器》GB 10408.3-2000、《微波和被动红外复合入侵探测器》GB 10408.6-2009 等。

2.0.8 本条规定源自《安全防范工程技术标准》GB50348-2018 第 6.6.4 条第 3、5、6、7 款（均为强制性条文）。

安全防范系统具有信息系统的很多特征，在系统正常工作中，应从信息安全的角度做好防病毒和防网络入侵的防护措施。常见的方法有：采用部署防火墙、入侵检测、安装防病毒软件、日志审计等，以进行预防入侵、检测、清除、追查；在系统内外网边界上配置防火墙，用于防止外网未经授权访问内网以及对内网的攻击，同时也能防止内网用户未经授权访问外网；配置入侵检测系统用于实时地应对来自内网已知的攻击；配置和运行防病毒软件主要用于检测、识别、清除系统中的病毒；配置日志审计系统用于在事件发生时或事后发现安全问题，有利于追查责任、定位故障、系统恢复等；为了更加有效地防止网络攻击，一般要将入侵检测系统和防火墙等安全系统进行联动设置。信息安全应遵循国家密码管理机构等给出的相关规定。密码技术是解决信息安全问题的核心技术，采用密码产品时应遵守国家密码局在产品生产、销售、使用等多个环节都做出的相应管理规定。

第 1 款强调了安全防范系统的信息安全的基本要求：防病毒和防网络入侵。

第 2 款强调了系统用户登录操作口令的有效性和健壮性。弱口令一般指设备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。

第 3 款强调了不同安全特性的网络互联时的必要安全隔离保护措施。目前用于安全防范系统传输的网络类型大致可分有线网络和无线网络，有线网络又分为专用网络和公共网络，随着各个行业互联互通、共享应用等的应用需求，安防系统内部各子系统的集成、安防系统与其他系统的集成、上下互联等应用已成为发展的趋势。众所周知，安防系统是为安全防范而建设的，系统本身的安全性是安防系统效能正常发挥作用的重要保障，因此，需要在安防系统与其他系统之间采取网络边界安全管理措施，管理措施包括建立网络通信防护机制，实现网络数据传输的完整性保护；进行网络安全规划，包括划分网络安全域、规划网络 IP 地址、设计网络安全策略等；选用合适的网络安全产品，包括防火墙、入侵检测系统、VPN、安全隔离网闸、安全审计等。

常见的其他安全性措施有：采用专用传输网络、信息加密传输、重要数据加密存储、用户和设备身份认证等。

2.0.9 本条规定源自《安全防范工程技术标准》GB50348-2018 第 6.6.5 条第 3 款（强制性条文）。要求系统控制设备具备各种信息的记忆功能，如停电前的状态为设防状态，当重新上电时，系统按照预先设定的配置，自动恢复设防状态。

2.0.10 本条规定源自《安全防范工程技术标准》GB50348-2018 第 4.2.5 条和第 3.0.6 条（非强制性条文）。

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.《企业事业单位内部治安保卫条例》（国务院第 421 号令）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：

(一)广播电台、电视台、通讯社等重要新闻单位；

(二)机场、港口、大型车站等重要交通枢纽；

(三)国防科技工业重要产品的研制、生产单位；

(四)电信、邮政、金融单位；

(五)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；

(六)大型物资储备单位和大型商贸中心；

(七)教育、科研、医疗单位和大型文化、体育场所；

(八)博物馆、档案馆和重点文物保护单位；

(九)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；

(十)国家重点建设工程单位；

(十一)其他需要列为治安保卫重点的单位。

2.《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。

第 1 款规定源自国家标准《安全防范工程技术标准》GB50348-2018 第 6.13.1 条 4 款（强制性条文）。

采用专用传输网络可最大程度降低通过信息网络的隐蔽式外部攻击，防止无形的窃听、窥视、改写等破坏，防止有形的盗窃、非法拷贝等犯罪。专用网络可以采用专线或虚拟专用网。

传输方式分为有线传输和无线传输两种方式。有线传输包括专线、虚拟专用网、公共电话网等传输模式。无线传输包括无线专网、无线局域网、数字微波、卫星、公共移动数据网等传输模式。根据系统规模、系统功能、现场环境和管理要求选择合适的传输方式，优先选用有线传输方式。

第 2 款规定源自国家标准《安全防范工程技术标准》GB50348-2018 第 3.0.6、3.0.7（非强制性条文）。

工程检验是按照约定程序对工程的一种和多种特性进行测量、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。

工程检验机构应具有安防工程检验资质且检验能力在资质能力授权范围内。安防工程检验资质是指检验机构所具有的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、CAL、CNAS，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它标准内容，如金融、小区、博物馆等领域的国家或行业标准及电磁兼容等的方法标准。

为保障安全防范工程质量和系统预期效能，除高风险保护对象的安全防范工程应进行工程检验外，建议对普通风险保护对象的安全防范工程进行工程检验。

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。

3　布防设计

3.0.1　本条规定源自《安全防范工程技术标准》GB50348-2018 第 4.1.3 条（非强制性条文）。

本条提出了安全防范工程布防设计需要遵循的原则。安全防范工程布防设计时，首先应该明确保护对象（单位、建筑及其内外的部位、区域以及具体目标）及其安全需求（防盗窃、防破坏、防范恐怖袭击等），通常需要进行风险评估，确定需要具体防范的风险，从而进行有针对性的布防设计，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的均衡配置和统筹协调奠定基础。

3.0.2　本条规定源自《安全防范工程技术标准》GB50348-2018 第 4.1.3 条第 1 款（非强制性条文），提出了周界防护的有关要求。

第 1 款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。进行周界防护布防设计时，需要根据现场环境条件和安全防范管理要求合理选择与组合。

第 2、3、4 款分别提出了在进行周界防护设计时，实体防护、入侵探测、视频监控等不同措施应该达到的防护能力和效果。

以对抗非法隐蔽进入的设计为例：

实体防护可选择设置周界围墙、金属铁丝网、栅栏等。防止单人徒手翻越的围墙高度至少应为 2.5m；防止双人叠加翻越的围墙高度至少应为 4m。金属铁丝网或栅栏应具有防攀爬措施。

入侵探测应针对所要探测的攀爬、翻越、挖凿等不同行为，选择设置不同类型的产品，如：主动红外入侵探测器、振动入侵探测器、光纤振动入侵探测器、甚低频感应入侵探测器、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。

视频监控应对周界进行全覆盖，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。

周界防护的人防响应能力应满足安全管理需要。

3.0.3　本条规定源自《安全防范工程技术标准》GB50348-2018 第 4.1.3 条第 2 款（非强制性条文），提出了出入口防护的有关要求。

第 1 款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、视频监控等防护措施。进行出入口防护设计时，需要根据现场环境条件和安全防范管理要求合理选择与组合。

第 2 款在 GB50348-2018 第 6.3.7 条第 1 款（非强制性条文）的基础上做了修改。本条提出了实体防护设计时应考虑安全与便捷的协调关系。

出入口的安全防范管理是关键控制点，在满足通行能力的前提下，周界的出入口设置数量越少、出入口宽度越窄，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，实体屏障布防设计时，需综合考虑实体屏障的防护能力，并与周界实体屏障的防护能力相当，避免出现安全防范的薄弱环节，以达到均衡防护的效果。

第 3 款、第 4 款、第 5 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和效果。

3.0.4 本条规定源自《安全防范工程技术标准》GB50348-2018 第 4.1.3 条第 3 款（非强制性条文），提出了通道和公共区域防护的有关要求，以及不同防护手段应达到的防护效果。

第 1 款提出了用于通道和公共区域防护的措施，包括视频监控、车辆实体屏障等防护措施。进行通道和公共区域防护设计时，需要根据现场环境条件和安全防范管理要求合理选择与组合。

第 2 款、第 3 款、第 4 款分别提出了在进行通道和公共区域防护设计时，视频监控、车辆实体屏障等不同措施应该达到的防护能力和效果。

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。常用的车辆实体屏障有：防撞墙、防撞柱、防撞礅、升降式阻车路障、穿刺放气式路障减速带等。

3.0.5 本条规定源自《安全防范工程技术标准》GB50348-2018 第 4.1.3 条第 6 款（非强制性条文）。人员密集、大流量的出入口、通道等处是容易发生拥挤、踩踏事故的区域，因此，在这些部位和区域进行出入口控制、加固围挡物防设施的同时，还要考虑采取人员疏导和快速通行措施，以防止人员拥挤、踩踏等事件的发生。

3.0.6 本条规定了当把财务室、数据机房、水电气热设备间等作为重要场所（除监控中心以外的场所）时采取的实体防护、入侵探测、出入口控制、视频监控等多种防护措施或手段。具体防护措施的选择与组合需要根据现场环境和安全防范管理要求而定。

第 2 款所提到的防盗安全门、防盗保险柜等设施的安全等级在现行国家标准中做出了明确规定。

3.0.7　本款规定源自 GB50348 的 6.14.2 条（强制性条文）第 1、2、3、4 款。

第 1 款，　监控中心是安全防范系统的中央控制室，必须保护其自身安全，并能实现紧急报警和内外通讯联络。值守区和设备区分开设置的，应按照相同级别进行防护。根据安全防范管理需要，必要时要向上一级接处警中心报警，监控中心必须要预留出相应的联网接口。

第 2 款，规定了监控中心门窗实体防护措施要求。

第 3 款，监控中心的出入口管控是自身防护的重点，出入口安装出入口控制装置用于对进出人员实施授权管理；出入口处设置视频监控装置是为了对出入或接近出入口人员的情况进行监视、记录。人员情况包括人员的一般体貌特征如高矮胖瘦，衣服穿戴/发型、肢体活动特征、人群组合等。

第 4 款，监控中心内部设置视频监控装置是为了对值班人员及进入监控中心人员的活动情况进行监督管理。

第 5 款，本款要求监控中心要按照最高权限受控区进行管理。

受控区是出入口控制系统的重要概念，监控中心是出入口控制系统网络与数据服务的汇集点，一般将监控中心设置为出入口控制系统的最高权限受控区。若系统中存在高于监控中心权限的其它受控区时，必须对放置在监控中心的出入口控制系统管理主机、网络接口设备、网络线缆等采取物理隔离和（或）视频监控等强化保护措施，否则，监控中心的出入口控制系统受到破坏会影响到最高权限受控区的安全。

3.0.8 本条规定源自《安全防范工程技术标准》GB50348-2018 第 4.1.3 条第 5 款（非强制性条文），提出了具体保护目标防护的有关要求。

第 1 款提出了用于保护目标防护的措施，包括实体防护、区域入侵探测、位移探测、视频监控等防护措施。进行保护目标防护设计时，需要根据保护目标的具体情况、现场环境和安全防范管理要求合理选择与组合。

第 2 款、第 3 款、第 4 款分别提出了实体防护、区域入侵探测、位移探测、视频监控等不同措施应该达到的防护能力和效果。

3.0.9 本条规定源自 GB50348 的 6.4.10 条第 6 款（非强制性条文），安全检查区位置设置在出入口，目的是防止进入被保护场所的人员、物品、车辆携带或夹带违禁品（特别是易燃易爆物、管制刀具等）进入被保护场所。

在安全检查系统设计时应考虑安全检查区位置设置，评估流量，合理配置安全检查通道数量，并根据流量高峰、平峰、低峰情况动态调整安全检查人员。

3.0.10 本条规定源自《安全防范工程技术标准》GB50348-2018 第 4.1.4 条（非强制性条文）。本条提出了对于防范恐怖袭击重点目标应采取的强化防范措施。

第 1 款中的加强方法可采取加高、加厚或多重设置等措施。

4　系统设计

4.1 一般规定

4.1.1 本条规定在《安全防范工程技术标准》GB50348-2018 第 4.2.2 条（非强制性条文）的基础上做了补充修改。

第 1 款给出了实体防护系统的设计方法。

实体防护系统通常由天然屏障和（或）人工屏障和（或）防护器具（设备）等构成。

1　本条文包含三个层面的要素：

1）首先要充分利用天然屏障；

2）建（构）筑物主体要与附属工程进行综合设计统一考虑；

3）要对周界、具体防护目标进行针对性设计。

2 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，例如：山谷、丘陵、河流、丛林、沙漠等自然地貌和地形以及植被。

3 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、栅栏等防护设施。

4　对于建筑物而言，建筑主体一般指供人们进行生产、生活或其他活动的房屋或场所。建筑物的主体工程包括：地基与基础分部工程、主体结构分部工程、屋面分部工程、楼地面分部工程、门窗分部工程、装饰装修分部工程六大部分。

5 建筑工程的附属工程包括：

1)与建筑物配套的围墙；

2)室外排水设施（排水沟、排水管、检查井）；

3)园林景观工程：道路工程、绿化工程、景观工程（含景观灯饰、室外照明灯）；

4)挡土墙、室外土石方等；

5)室外通道、楼梯；

6)停车场、车棚、垃圾站等。

第 2 款给出了电子防护系统的构成内容。电子防护系统一般包括前端、传输、信息处理/控制/管理、显示/记录等单元。

第 3 款根据需要，安全防范系统还可配置对实体防护系统和（或）电子防护系统进行集成联网的安全防范管理平台。安全防范管理平台是安全防范系统集成与联网的核心，其功能除本条规定的基本功能外，还可包括预案管理、联网共享、指挥调度、智能应用、系统运维、安全管控等功能。

4.1.2　本条规定源自《安全防范工程技术标准》GB50348-2018 第 4.2.1 条（非强制性条文）。

本条提出了安全防范系统架构设计的基本要素。

1、 组成的子系统可参见 4.1.1 的条文内容。

2、 安全防范系统的集成/联网方式通常包括下列几种：

1）通过不同子系统设备之间的信号驱动实现的简单联动方式。

2）通过不同子系统管理软件之间的通信实现的子系统联动方式。

3）通过安全防范管理平台实现对安全防范各子系统以及其他子系统集中控制与管理的集成方式。

4）通过对多级安全防范管理平台的互联，实现大范围、跨区域安全防范系统的级联方式。

5）根据安全防范管理的需要，安全防范系统还可与其他业务系统进行集成、联网的综合应用方式。

3、 传输网络通常采用以监控中心为汇接/核心点（根节点）的星型/树形传输网络拓扑结构。系统传输的通信链路应满足系统的信息传输、交换和共享应用的需要。当有线传输不具备条件时，可考虑采用具有相应安全措施的无线传输方式。

传输网络依据传输技术的不同，可分为有线网络、无线网络及其混合网络。有线网络按照传输介质的不同，可分为光纤网络和电缆网络。

这里推荐安全防范系统的主干传输网络优先采用独立设置的光纤网络。在目前的安防工程中，常见的主干传输网络是专用的 IP 光纤网络。

系统传输的通信链路指标包括传输衰耗、网络带宽、延时、延时抖动和丢包率等。

4、 存储管理模式可分为分布存储分布管理、分布存储集中管理、传统集中存储集中管理、云存储管理等多种模式。

分布存储分布管理模式是指各子系统独立存储自身数据，独立管理界面，各自授权。

分布存储集中管理模式是指各子系统独立存储数据，独立管理，但可以提供统一的集成界面，集中管理所有数据。

传统集中存储集中管理模式是指对各子系统的数据集中一个地点存储、由统一的管理平台进行管理授权，各子系统可以直接控制到各自所属的数据，但系统不可分割。

云存储是指通过集群应用、网格技术或分布式文件系统等方法，将网络中大量各种不同类型的存储设备通过应用软件集合起来协同工作，共同对外提供数据存储和业务访问功能的一个系统，保证数据的安全性，并合理调配存储空间。

云存储管理模式是指通过云存储架构对各子系统的数据进行统一存储管理。物理上，这些数据的存储地点可以集中在一起，也可以分布在多地，但数据的完整性一致性高，由统一的管理平台管理，具有更高的数据 I/O 能力，便于后续的大数据共享应用。各子系统可通过云存储专用接口对相关数据进行访问。

5、 根据安全防范系统及其设备的空间分布特点、供电条件和安全保障需求，合理选择主电源、备用电源及其供电模式和保障措施

6、 根据安全防范系统、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。

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；安全防范各级管理平台或分平台之间的信息传输、交换、控制协议；安全防范管理平台与其他业务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。

其他要素还有信息共享应用模式、安全防范管理平台、智能化应用、运行维护和系统安全等要素。

4.1.3 本条规定源自《安全防范工程技术标准》GB50348-2018 第 6.4.16 条（非强制性条文）。本条体现了安全防范系统中的各子系统和设备间的安全等级配置的均衡原则。

4.1.4 本条规定源自《安全防范工程技术标准》GB50348-2018 第 6.5.14 条（非强制性条文）。这是确保安全防范系统内部自身健壮性抗破坏能力的基本条件。联网系统由多级管理平台和多个子系统构成，当某一平台或子系统出现故障时不允许对联网系统中的其他系统/设施产生不良影响。

4.1.5 本条规定源自《安全防范工程技术标准》GB50348-2018 第 6.5.16 条（非强制性条文）。这是确保安全防范系统自身运行健壮性的必要条件。

4.1.6 本条规定源自《安全防范工程技术标准》GB50348-2018 第 1.0.5 条（非强制性条文）。

安全防范系统需具有安全性、可靠性、可维护性和可扩展性，做到技术先进、经济适用。当安全防范工程中选用先进技术和智能化设备时，应通过风险评估和系统效能评估等方法，认真评估设备自身存在安全隐患及其可能给安全防范系统带来的次生安全隐患。若发现存在风险，应采取措施加以避免。

4.1.7　本条规定源自《安全防范工程技术标准》GB50348-2018 第 4.3.2 条（非强制性条文）。

本标准定义的安全防范是指社会治安防范和反恐防范。特别是针对恐怖袭击的安全防范工程设计时，除了要考虑安全防范系统传统的探测、延迟、反应能力外，还要结合人力防范能力，配备必要的个人防护装备、有效的防御设施以及与恐怖分子对抗的装备等。因此，反恐防范的安全防范工程设计应体现威慑、探测、防御、致胜四个要素。高风险保护对象更是如此。

4.2 实体防护系统设计

4.2.1　本条规定源自 GB50348-2018 第 6.3.2 条（非强制性条文）。

本条规定了实体防护系统设计应具有的防护能力，按照其防护能力的程度由弱向强分为威慑、延迟和阻挡。实体防护能够对入侵对象形成心理上的威慑，能够延迟入侵时间和过程，采取适当的实体防护能够阻挡防范对象的入侵行为。

4.2.2　本条规定源自 GB50348-2018 第 6.3.4、6.3.5、6.3.10、条（非强制性条文），规定了实体防护设计应包括周界实体防护设计、建（构）筑物设计和实体装置设计等内容。

周界实体防护设计应包括周界实体屏障、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。周界实体防护设计是指针对保护对象外围周界所进行的实体防护设计，是安全防范纵深设计的第一道防线。设计时应在建筑选址、建筑总平面规划设计时利用天然屏障对保护对象的防护。

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。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，例如：防撞墙、防撞柱、防撞礅、液压防冲撞翻板、液压防冲撞柱等。

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、结构强度等方面的设计，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。

已建的建（构）筑物应根据实际情况进行合理的功能区域划分和实体防护方案设计。建（构）筑物本身为文物时，实体防护设计不应破坏建（构）筑物其本身，应采用施工简易、安装快速、新材料等结构形式的实体防护设计，宜与电子防护（入侵探测、视频监控）联合设置。

实体装置设计主要包括安防设备的自身实体保护和对保护目标的近身式保护箱柜体的设计选型与配置。实体防护装置的设计与选用具有防窥视、防砸、防撬、防弹、防爆炸等功能的实体防护装置，用于保护对象在保护区域内的存储和展示，防范保护对象的失窃和破损。

4.2.3 本条规定源自《安全防范工程技术标准》GB50348-2018 第 6.3.6 条的第 1、2、4、5 款（强制性条文）。

第 1 款规定了周界实体屏障应根据被保护对象所在的位置或其所在建（构）筑物及其场地条件设置。条件允许时，周界实体屏障应独立设置，不采用建筑物作为周界实体屏障。

周界实体屏障应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。

屏障设置的位置以及与保护对象的距离，应综合考虑入侵行为和实施处置的路径与时间的关联关系的合理安全距离。

第 2 款规定了保护对象有防爆安全要求时，应根据防范爆炸物的种类、当量、爆炸破坏力等进行计算，设计实体屏障与保护对象间适宜的安全距离。

第 3 款规定了周界实体屏障作为保护对象最外层防护手段，其设计功能主要应包含防攀越（徒手、借助工具）、防穿越（敲击、剪切、撬、撞击、钻孔、挖掘、爆破等破坏实体屏障后）防窥视（信息、情报等泄露）等，具体设计原则如下：

实体屏障应选用无着力点、支撑点、抓握点的结构形式有效提高防攀越能力。

实体屏障的防护有效高度一般不低于 1.8m，防攀越的能力与屏障的高度成正比关系。

封闭式周界屏障是砌筑墙时，高必须不低于 2.2m，顶部应设有防护装置，例如刺铁丝、刺刀圈等。仅使用刺铁丝时至少三股及以上，顶部防护装置应向外呈 45 度角，增加屏障垂直高度不小于 1m。

周界实体屏障采用通透式钢筋焊接网屏障的，网格尺寸面积宜不大于 1250 mm^2 且不能容纳成人 3 根手指伸入的抓握点以及脚伸入攀爬的着力点。有防挖掘要求的基础通常采用条形基础并深埋入地下 0.9m 以上，采用独立基础时，两基础间埋设防挖掘钢网。

防车辆撞击要求的实体屏障基础高出地面高度不应小于 0.81m，墙体宜为钢筋混凝土结构，结构厚度不低于 500mm,墙体基础埋入地下不低于 2000mm。

当有防投射物、防破坏要求时，实体屏障应具备相应的阻挡、缓冲、改变投射物轨迹等防护能力。如：通透式的实体屏障间隙应不大于 12.5mm（横向）＊75mm（纵向），同时，实体屏障的材质材料和结构的强度还能满足防投射物杀伤或破坏的要求。

通透式实体屏障选用的材料材质、设计结构、空隙尺寸、链接方式是防穿越、防攀爬性能的关键。通透式（可视）屏障可通过增加其他实体设施进行防窥视性能设计。清除区内层应采用通透性能较强的屏障。

通透式实体屏障应有防止人员穿越功能，竖向实体结构间隙应小于 110mm 并应能保证实体屏障的整体结构强度。其他有特殊要求，比如防止小动物穿越的实体屏障，通透式实体屏障孔面积不应大于防范对象的头围直径。

有防窥视要求时，通常不选用通透式实体屏障，或采取通透式实体屏障和其他实体屏障联合设置以遮挡视线。

为了确保清除区范围视线清晰，通常采用通透性较强的屏障。

第 4 款规定了穿越周界的河道、涵洞、管廊等孔洞，在不影响建（构）筑物功能的前提下，设置实体屏障和（或）实体装置对孔洞进行防护是很有必要的。此举弥补了容易被忽略的安全防范的薄弱点，解决了因视频监控和人力防范受环境和条件的限制很难发挥出最佳的防范效能的问题。例如：采用防护栅栏、防护钢丝网等封闭涵洞和管廊、在河道的水下设置防护栅栏阻止人员潜水进入、在水下建造桩或柱等阻止船通行等。

4.2.4　本条规定源自 GB50348 -2018 第 6.3.8 条的第 2、3 款（强制性条文）。

第 1 款规定了车辆实体屏障应具有减速、吸能、阻停的防护功能，以防范车辆的设计载重和设计速度撞击后产生的冲量作为设计依据，设计车辆屏障的高度、结构强度、固定方式等，国外建立一些相关的测试标准可供参考。

例如：目前，美国和英国的防撞测试以及级别划分，建立比较完善的测试标准。美国执行 ASATM F2656 标准，英国执行 PAS68 标准。

防冲撞能力的设计如:遭遇设计载重车辆以设计速度撞击后，车辆被阻挡停止且穿越屏障行进距离不超过 1m 以及撞击碎物飞溅距离小于 5m。车辆实体屏障本身可能发生损坏不能正常运行。

第 2 款规定了车辆实体屏障应设置在距保护对象有效的安全距离外，且防护效果与距离设置具有正相关性，距离越远，防护效果越佳。

4.2.5　本条规定源自 GB50348 -2018 第 6.3.11 条的第 1、3 款（强制性条文）。

第 1 款规定了建（构）筑物设计应避免出入口、场地道路直通保护对象或其所在建筑物的大堂（门厅）。车辆宜环形行驶靠近建（构）筑物，宜设计前广场、景观池（花坛）、台阶为缓冲区，可摆放大型盆栽或石刻饰物以及其他车辆实体屏障进行实体防护。

建（构）筑物场地道路与保护对象或其所在建筑物外侧墙体应保持安全距离。可设置建筑景观灌木、绿篱或向建筑物外侧放坡用于安全防护。

第 2 款规定了为避免或减小易燃、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应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;应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;不应让无关人员和物流通过库房区。同时，尚应遵循现行国家标准及管理规定。

4.2.6　本条规定源自 GB50348 -2018 第 6.3.12 条的第 3、4 款（强制性条文）。

第 1 款规定了建筑墙体防爆炸设计要求，具有保密性要求的屏蔽和防窃听与窃视设计。可根据防爆炸的要求，选择结构并参照相应设计规范与标准进行设计。

例如：防爆墙体设计可参照 GB50038-2005《人民防空地下室规范》。防爆墙体防爆墙体采用非燃烧材料,且不宜作为承重墙,其耐火极限不应低于 4H。防爆墙可采用配筋砖墙。当

相邻房间生产人员较多或设备较贵重时,宜采用现浇钢筋混凝土墙。配筋砖墙厚度应由结构计算确定,但不应小于 240mm,砖强度不应低于 MU7.5,砂浆强度不应低于 M 5。

建筑外墙为玻璃幕墙时，玻璃外墙和门窗的材质、厚度应符合 GB/T 29908-2013 《玻璃幕墙和门窗抗爆炸冲击波性能分级及检测方法》中的相关要求。

第 2 款规定了能够容纳防范对象隐蔽进入的建（构）筑物的洞口、管沟、管廊、吊顶、风管、桥架、管道等，在不影响建筑功能前提下，应采用适当的实体屏障或实体构件进行封闭和阻挡，例如：防护栅栏、防护钢丝网、可闭锁盖板等。加强上述薄弱环节的安全防范，避免其被防范对象选择作为入侵点。

4.2.7 本条规定源自 GB50348 -2018 第 6.3.13 条的第 2、3、4 款（强制性条文）。

第 1 款规定了选择防盗安全门时，应根据保护目标的风险等级和安全防范管理要求，按照国家现行标准选用相应安全等级的产品。在国家标准《防盗安全门通用技术条件》GB 17565-2007 中规定了甲、乙、丙、丁四个安全级别；

防盗窗目前没有国家标准和行业标准，选用时也应考虑其防护能力与风险等级相适应，窗户加工采用的玻璃、金属框架材料应具备相应的防砸、防破坏能力。同时，防盗门和防盗窗的安装与固定的构造和附件也要考虑防砸、防撬、防凿、防切割等防护能力。

第 2 款规定了有防爆炸和/或防弹和/或防砸安全防范要求时，保护目标的门、窗应具有相应安全等级材料加工制作而成，且整体结构与安装固定方式具有同等安全防护能力，材料应符合相关的行业标准。例如：现行公共安全行业标准《防爆炸复合玻璃》GA 667-2006、《防弹透明材料》GA 165-2016、《防砸复合玻璃通用技术要求》GA 844-2009 中分别对玻璃等防护材料的防爆炸、防弹、防砸性能进行了规定并划分了等级。

第 3 款规定了金库、文物库应有防盗、防火、防水等功能，其参照现行公共安全行业标准《金库门通用技术条件》GA/T 143-1996 以及正在制定的金库门国家标准的规定，其对金库门的防破坏、防火、防水等功能性能进行了规定和并划分了等级。

4.2.8 实体装置应具有的防护能力可以是防窥视、防砸、防撬、防弹、防爆炸等的一种或多种。

实体装置既保护已经确认的保护目标，同时也要保护安防系统自身。

4.2.9 本条规定源自《安全防范工程技术标准》GB50348-2018 第 6.6.3 条（非强制性条文）。具有特殊防御功能装置主要包括脉冲式电子围栏、炫目灯光、滚刺网等。

4. 3 入侵和紧急报警系统设计

4.3.1 本条规定源自《安全防范工程技术标准》GB50348-2018 第 6.4.2 条。本条规定了入侵和紧急报警系统功能的总体要求。

入侵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，比如：防越线（界）、撞击、撬、挖、凿、攀爬等，在这里，需要强调的是，探测的手段不限于某种探测装置，可以是红外、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其中一种或组合。在实际应用设计中，要根据现场情况和安全等级的要求不同，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，以达到相对合理的防范效果。

4.3.2 本条规定源自《安全防范工程技术标准》GB50348-2018 第 6.4.3 条第 2 款（强制性条文）。

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 24 小时设防。

4.3.3 本条规定源自《安全防范工程技术标准》GB50348-2018 第 6.4.3 条第 3 款（强制性条文）。这是入侵和紧急报警系统沿用至今、行之有效的对设备拆改进行防护的方法之一。

防拆功能的作用，不仅仅是系统功能的一部分，更重要的是从系统的安全性要求考虑，对于用于安全防范的电子防护系统，如果系统设备本身安全都保证不了，建设这样的系统还

有意义吗？对探测装置、接线盒（包括传输设备箱、分线箱）、报警控制设备或控制箱、告警装置等提出防拆报警功能要求，就是要求一旦设备被拆卸、植入其他物品等时，系统将发出防拆信息。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，对于探测装置、传输设备箱（包括分线箱）、报警控制设备或控制箱、告警装置等的防拆装置要设为独立防区，且为 24 小时设防。

4.3.4 本条规定源自《安全防范工程技术标准》GB50348-2018 第 6.4.3 条第 4 款（强制性条文）。这是入侵和紧急报警系统沿用至今、行之有效的对传输线路进行防护的方法之一。

在这里，主要强调的是系统传输链路的防破坏保护，因为，入侵和紧急报警系统的有线传输线路并不一定都处在探测器的探测范围之内，为了保证系统的正常传输，除了要求在物理上采取防护措施外（如采用保护管、暗埋等），还需在技术上解决线路被破坏时系统要能发现的问题，即当报警信号传输线被断路、短路时，报警控制指示设备能识别那条线路被破坏，同时还要能识别不能发出报警信息设备的故障。现阶段，大部分报警控制指示设备还不能识别探测设备内不影响报警输出的某部件老化、故障，如传感器性能降低等。

4.3.5 本条规定源自《安全防范工程技术标准》GB50348-2018 第 6.4.3 条第 5 款（强制性条文）。

防区属性（瞬时防区、24h 防区、延时防区）配置、设防、撤防、旁路、传输、告警、胁迫报警等是入侵和紧急报警系统最基本的功能。为了适应用户不同的应用需求，使系统既能保证安全等级不降低，又能方便使用，需对系统进行认真的设置，对不同区域、部位的探测装置/报警紧急装置/防拆装置等根据要求进行分别设置，即可设置为瞬时防区、24 小时防区、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；在进行系统设计时，要注意不同安全等级，其传输、告警方式的要求也有所不同；为尽最大可能保护人身安全，系统要有胁迫报警功能，即当权限类别为 1、2 或 3 的用户使用胁迫钥匙撤防时，控制指示设备要能正常撤防，同时要能发送远程胁迫报警信号和/或信息，且不给出本地报警声响。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，用户权限分为 4 类。

报警控制指示设备的防区可设置为瞬时防区、24 小时防区、延时防区。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。24 小时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，也可用于需要密切注意的安全等级较高的出入口防区。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，延时的时间可以设定（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。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，也可以将多个同时旁路掉（又称群旁路）。

4.3.6 本条规定源自《安全防范工程技术标准》GB50348-2018 第 6.4.3 条第 6 款（强制性条文）。

在《入侵和紧急报警系统技术要求》GB/T 32581-2016 中，入侵和紧急报警系统的用户（操作人员）访问系统部件和控制功能有下列四种权限类别：

a）类别 1：操作访问无任何权限限制。

注：该类别指任何人均可访问，但只能进行简单的设防操作，一般通过按钮（开关）对部分或局部入侵和紧急报警系统进行设防。

b）类别 2：在不改变入侵和紧急报警系统配置情况下，操作访问能影响系统运行状态的功能。操作访问应受密钥、编码开关、锁或者其他等同方法限制，其密钥或编码不能访问权限类别 3 或 4。

注 1：该类别通常适用于具有通行相应防护区域的使用、操作人和系统管理员。

c）类别 3：在不更改系统设备设计的情况下，操作访问能影响入侵和紧急报警系统配置的所有功能。操作访问应受密钥、编码开关、锁或者其他等同方法限制，其密钥或编码不能访问权限类别 4。如需访问权限类别 2，需获得权限类别 2 用户的许可，并在本地访问。

注：该类别通常适用于专业安装、维修人员。

d）类别 4：操作访问部件会改变设备的设计。操作访问应受密钥、编码开关、锁或者其他等效方法限制，其密钥或编码不能访问权限类别 2 和 3。除非权限类别 2 和权限类别 3 的用户授权，否则不允许使用权限类别 4。

注 1：该类别通常适用于设备制造商或代理商。

注 2：权限类别 4 只适用于在不触发控制指示设备或辅助控制设备上的防拆装置时更改操作程序软件。

4.3.7 本条规定源自《安全防范工程技术标准》GB50348-2018 第 6.4.3 条第 7 款（强制性条文）。

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，是用户了解入侵和紧急报警系统状态的必备媒介之一。通过指示，用户可以了解系统是否设防、撤防、旁路等工作状态，了解系统各防区工作、传输是否正常。

4.3.8 本条规定源自《安全防范工程技术标准》GB50348-2018 第 6.4.3 条第 8 款（强制性条文）。

通告是指将报警、防拆或故障状态传递给告警装置和/或报警传输系统的过程，是用户了解入侵和紧急报警系统出现报警、防拆或故障等状况的另一个媒介。通过声、光报警通告，能够起到警告、威慑入侵或抢劫者，提醒用户，向外求援，向相关人员和或机构报告等作用。在实际应用时，要根据各个单位的特点，设置不同形式的告警方式，可以采用现场声告警，也可以采用光告警，也可以采用声光同时告警。非法操作是指不具有权限类别的用户试图在其非权限范围、时间内访问和控制系统部件，此时，系统要能发出报警通告。

4.3.9 本条规定源自《安全防范工程技术标准》GB50348-2018 第 6.4.3 条第 10 款（非强制性条文）前一句。

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。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，有关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。

4.3.10 本条规定源自《安全防范工程技术标准》GB50348-2018 第 6.4.3 条第 14 款的前半句（强制性条文）和第 11 款（非强制性条文）。

如果发生入侵行为时出现漏报警，监控中心、报警接收中心就无法“反应”，无法向外求援，将导致人员的伤害和财产的损失，也就达不到防范的目的，因此，本条文提出系统不得有漏报警。

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，到控制指示设备或远程报警接收中心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，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。

随着信息技术的发展，入侵和紧急报警系统的远程传输逐步与公共或其他信息网络融合，由于公共或其他信息网络主要是为其他应用服务，并不是专为入侵和紧急报警系统应用的，且其网络内数据流量变化较大，由于入侵和紧急报警系统需要的报警响应时间要短，因此，为了保证监控中心能够及时知道各防范区域的情况，一般要求公共或其他信息传输网络要为入侵和紧急报警系统信号的传输有一个相对独立的信道，以保证报警响应的时间。

目前，对入侵和紧急报警系统报警响应时间有要求的标准是《入侵和紧急报警系统技术要求》GB/T 32581-2016，该标准中规定入侵、紧急、防拆以及故障信号和（或）信息的报警响应时间满足以下要求：

a) 单控制器模式：不大于 2s；

b) 本地联网模式：

1）安全等级 1：不大于 10s；

2）安全等级 2、3：不大于 5s；

3）安全等级 4：不大于 2s。

c) 远程联网模式：

1)安全等级 1、2 :不大于 20s;

2)安全等级 3、4:不大于 10s。

4. 4 视频监控系统设计

4.4.1 本条规定源自《安全防范工程技术标准》GB50348-2018 第 6.4.5 条（非强制性条文）。

本条规定了视频监控系统功能的一般要求。

视频是以人的视觉感知为基础设计生成的具有时间连续感和空间、颜色分布感（仅在可见光和伪彩色条件下）的信号，具有可感知现场场景的一维时间和二维空间（三维投影）特征的能力。

按照视频信息流的应用观点，视频监控系统由视频采集、视频传输、视频处理、视频存储、视频显示和相应控制管理等部分构成。

4.4.2 本条规定源自《安全防范工程技术标准》GB50348-2018 第 6.4.5 条第 1 款（强制性条文）。本条明确了视频采集设备的性能指标的依据。视频采集设备通常称作摄像机。摄像机的信噪比、空间分辨力、时间分辨力、色彩分辨力和几何特征保持能力等满足采集识别目标的要求。

应结合现场具体情况选择适当的位置角度，选用适当性能的摄像机和镜头，最大可能及时获取监控区域和监控目标的实时信息。非可见光成像设备的使用为恶劣光照条件下的目标发现提供了条件。视频采集设备具体安装位置的选择可参照第 3 章的相关内容。

一般地，针对相对固定的范围进行宏观观察时，宜选用固定安装的较为广角的镜头的摄像机，针对固定区域的特定目标的观察通常采用固定安装的焦距较大的定焦镜头的摄像机。对于具有较大活动范围的目标的观察可考虑选用多个固定安装的定焦摄像机接力观察范围的配置使用方式。对于既要对同一监控区域的宏观状况进行观察，又要对其中的特定范围进行特征观察（如人的步态、人脸、车牌和车型等）的情形，可考虑选择具有 PTZ 功能的摄像机。电梯轿厢内的摄像机一般用于观察乘员的面部特征和在轿厢内的活动情况，安装在轿厢顶部的轿门的左侧或右侧，也有的认为应包括乘员进入轿厢时的活动情况，进入人员面部特征和人员操作轿厢控制面板的情况，建议安装在轿厢顶部远离轿门的左侧或右侧，随着摄像机逆光观察性能的提升，上述方式的选择不再具有关键意义，而是取决于观察乘员的哪些活动情况。

摄像机采用可见光或近红外光成像的摄像机，宜考虑背对光源的方向或者顺着光线的方向观察目标。当需要逆光观察目标时，应考虑摄像机具有光照度宽动态响应的能力。

视频采集设备可同时具有音频直接采集功能，或具有音频采集的接口。

4.4.3 本条规定源自《安全防范工程技术标准》GB50348-2018 第 6.4.5 条第 2 款（强制性条文）。本条提出了视频监控系统信号传输的基本要求。

传输信道的衰耗、带宽、信噪比，误码率、时延、时延抖动等指标是通信网络的基本内容。其中，模拟信道更多体现为衰耗、带宽、信噪比、群时延等指标，数字信道则除了前述的指标外，更多体现为误码率、时延和时延抖动等指标。

传输信道编码和加密/加扰策略是为加强信号传输抗干扰和防窃听的常用方法。

模拟视频信号通常采用信号分配的方式，数字视频信号特别是 IP 视频信号一般采用视频数据分发的方式。视频传输支持对同一视频资源的信号分配或数据分发的能力，是确保多个设备或用户对同一视频源的访问的功能实现的前提。音频信号与此相似。

视频的传输和信号分配/分发构成了视频系统的传输网络的主要部分。在确保信息数据完整可靠的前提下，对系统内的各种信息源进行管理整合使用是视频系统建设追求的目标。

4.4.4 本条规定源自《安全防范工程技术标准》GB50348-2018 第 6.4.5 条第 3 款（强制性条文）。本条强调了根据预先的授权实时控制视频设备的基本能力之一——视频信号切换调度。

根据授权，用户或终端可对系统内的任意视频源进行调取、切换等操作。切换调度功能在广播电视领域用户端又会被称作视频节目的点播功能。这些功能对于实战指挥研判系统来说是至关重要的。

一般地，本地视频监控系统，其实时视频源切换显示响应时间不大于 1s，历史视频源的检索调取显示响应时间会有所延长。

4.4.5 本条规定源自《安全防范工程技术标准》GB50348-2018 第 6.4.5 条第 4 款（强制性条文）。本条强调了根据预先的授权实时控制视频设备的基本能力之一——视频设备状态控制。

PTZ（Pan/Tilt/Zoom，云台水平/云台垂直/镜头变焦）实时控制，是指用户或终端设备对前端的遥控摄像机的云台和镜头进行左右上下转动和光学成像放大或缩小等实时操作。远程控制功能是实战指挥系统所不可或缺的内容。这一功能特别适用于对于现场目标的实时搜索和跟踪。视频采集设备的工作状态调整包括编码方式（如全电视信号、视频音频的数字压缩编码方案、HD-SDI、HDMI 等）、码流、帧率调整、是否加密传输等内容。

PTZ 控制的延迟时间和视频的编码、解码延时引发的延迟时间的总和应满足摄像机的实时跟踪目标的要求。

4.4.6 本条规定源自《安全防范工程技术标准》GB50348-2018 第 6.4.5 条第 5 款（强制性条文）。本条明确了图像质量和声音质量的基本要求。

系统显示设备可以实时显示系统内的前端实时采集的视频图像，也可以实时播放已存储的视频图像。系统的显示设备具体显示内容取决于当前用户的操作权限。显示的效果取决于为指定用户设定的显示模式。显示的方式可以是单屏幕单路画面、单屏幕多画面或组合屏幕综合显示。

系统图像是指一个完整的视频系统中从采集、传输、存储到显示环节中所能最终展示的最低图像质量的图像（借自《高清视频监控系统技术要求》的描述）。从下面的表述看，系统图像的质量关乎满足安全管理要求的内容，特别是对特定场景和目标识别的需要。

图像质量包括图像的信噪比、图像的空间（静态和动态）和时间分辨力、灰度级别、几何特征和颜色特征、原始完整性等内容。对于非可见光的成像图像质量内容则可不包括颜色特征的内容。

视频音频的原始完整性是指视频、音频设备或系统获得的数据表述的场景和目标特征与原始现场的投影特征保持（物理意义和逻辑意义）一致性的程度。原始现场的投影特征主要是指现场和目标的时空特征：在特定光谱条件下投影（投射）空间中的比邻关系、几何及纹理特征、投影颜色（仅一定照度的可见光条件下）、灰度层次、观察区域内的事件变化的连续性和后继顺序、音频频谱特征和声音事件顺序等。评价方法目前主要采用客观化的主观评价方法。这是视频音频数据作为司法证据和查找案件线索的关键前提。

4.4.7 本条规定源自《安全防范工程技术标准》GB50348-2018 第 6.4.5 条第 7 款（强制性条文）。本条明确存储的视频图像信息的保存期限，又叫存储时间或者连续存储周期。

根据《中华人民共和国反恐怖主义法》第三十二条的规定：防范恐怖袭击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。

根据国家有关治安管理规定，其他目标的视频图像信息保存期限不应少于三十日。

本条所说的“保存期限”是指视频图像信息在系统中的连续存储时间，而不是指档案生成后的保存期限。有些重要的视频图像信息作为档案保存时，保存期限可能要求为几年、几十年甚至永久保存。

4.4.8 本条规定源自《安全防范工程技术标准》GB50348-2018 第 6.4.5 条第 9 款（强制性条文）。本条明确了系统基本功能——系统管理。

除了这里介绍的系统应具有对用户（操作与管理本系统人员）的操作权限管理、操作与运行日志记录与管理、自我诊断和检查外，系统基本功能还包括事件的触发联动配置与管理、相关数据的导入和导出、值守人员的人机交互界面配置等功能，并在特定环节上满足安全等级的要求。

目前视频系统管理通常以视频集成管理平台的形式出现。

4.5 出入口控制系统设计

4.5.1 本条规定源自国家标准《安全防范工程技术标准》GB50348-2018 第 6.4.7 条（非强制性条文）。本条提出了出入口控制系统功能的总体要求。

4.5.2 本条规定源自国家标准《安全防范工程技术标准》GB50348-2018 第 6.4.7 条第 8 款（强制性条文）。主要针对入侵者在未进入受控区前，最易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及其级别，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。

出入口控制等技防系统在某种意义上来说，好比设置了一个技术迷宫，它增加了非法入侵者的作案难度，延迟作案时间，并能提早报警以便及时处警。但在实际应用中，非法入侵者在初步了解技防系统后，并不去直接去解开迷宫通路而是寻找系统的薄弱点进行攻击从而到达犯罪目的。在出入口控制系统中，执行部分的输入线缆及其连接端，就是一个易于被攻击的薄弱点。

为此在本标准中对出入口控制系统特别提出了“受控区”等概念和对执行部分输入电缆

的端接与防护要求，以便指导我们的系统设计、施工安装、检测验收工作。

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（比如某个公司的多个办公室），如图 1：

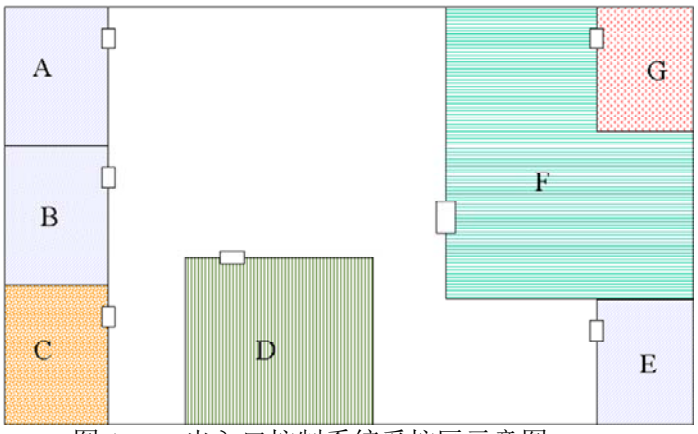

图 1　　出入口控制系统受控区示意图

其中：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 区分别是相对于其它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它区，而能进入其它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它任何区的话，那么 G 区就是该出入口控制系统的最高权限受控区。

该例子若是某公司的多门联网门禁系统的话，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 和 B 两个门是合理的，若控制 B 和 C 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。

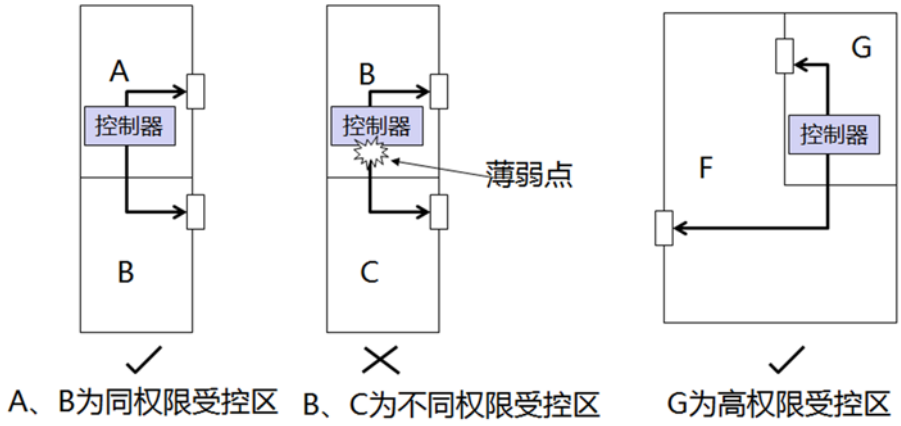

图 2　　出入口控制系统受控区的设备安装示意图

安装在 G 区的双门控制器控制 G 和 F 两个门是否合理呢？答案是肯定的。

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。

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。

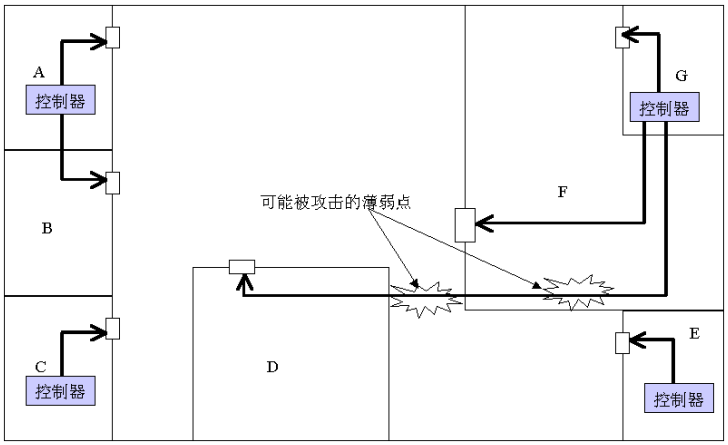

图 3　　出入口控制系统受控区的设备安装及布线示意图

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，图 3。若必须采用多出入口控制器，则应安装在高级别防区内并做好对执行部分输入线缆的防护。

4.5.3 本条规定源自国家标准《安全防范工程技术标准》GB50348-2018 第 6.4.7 条第 11 款（强制性条文）。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的造成伤害的部分。但不同的产品类型，其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入目标的安全，如电动门的关闭动作必须等待出入目标安全离开时方可进行，挡车器必须等待车辆离开方可落下档车臂等。

在安防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，人员不经使用识读过程也能迅速安全地疏散。

4.5.4 本条规定源自国家标准《安全防范工程技术标准》GB50348-2018 第 6.12.4 条第 3 款（强制性条文）。断电开启设备的供电需要特别的重视，为避免断电产生的防护疏漏，执行装置（锁闭阻挡装置等）对应急供电的可靠性要求更高。

备用电源是提高电子防护系统安全等级的前提之一。安全防范系统的主电源断电后，备用电源应在规定的应急供电时间内，保持系统状态，记录系统状态信息，并向安全防范系统特定设备发出报警信息。

4.5.5 本条规定源自国家标准《安全防范工程技术标准》GB50348-2018 第 6.4.7 条第 13 款（强制性条文）。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。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它应用系统中，这给使用者带来十分的便利。

由于安防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，不应放置在其它非安防业务系统中。比如：不能将门禁数据库服务器开放给财务等其它非安保业务部门；同样地，消费充值等其它业务信息，也不宜由安保部门管理，而应当将门禁系统数据与其它业务系统隔离。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它业务系统服务器，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。

4.5.6 本条规定源自国家标准《安全防范工程技术标准》GB50348-2018 第 6.13.4 条的第 6 款（强制性条文）。

为确保出入口控制系统执行装置的可靠安全工作，因此提出应根据不同受控区安全等级差异，采取相应的自我保护措施要求和配置，出入口执行部分的输入线缆，应采用抗拉伸、抗弯折强度不低于壁厚 2.0mm 镀锌钢管的封闭保护措施。

4.6 停车库（场）安全管理系统设计

4.6.1 本条规定源自国家标准《安全防范工程技术标准》GB50348-2018 第 6.4.9 条（非强制性条文）。该条提出了停车库（场）安全管理系统功能的总体要求。

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。

综合安全管理还可以包括车辆的驻车入位有序与否检查、人员车辆场区内的有序引导、车辆被破坏与否等。

综合管理通常还可以包括驻车收费等功能。

4.6.2 本条规定源自《安全防范工程技术标准》GB50348-2018 第 6.4.9 条第 2 款（非强制性条文）。

在车辆出入口设置的电动栏杆机等挡车指示设备应满足通行流量、通行车型（大小）的要求。电控阻车设备应满足高风险目标区域的阻车能力要求。

4.6.3 本条规定源自《安全防范工程技术标准》GB50348-2018 第 6.4.9 条第 4 款（非强制性条文）。

当车辆正常通行时，停车库（场）安全管理系统配置的挡车/阻车设备应具有防砸车等保护措施。

4.6.4 本条规定源自国家标准《安全防范工程技术标准》GB50348-2018 第 6.4.9 条第 5 款（强制性条文）。该条对停车库（场）的重要部位：出入口的现场识读指示功能做出了明确规定，并对报警功能提出了要求。

报警是安防系统的重要手段，停车库（场）安全管理系统作为安防系统的子系统，与其它安防子系统一样，将报警作为最重要的功能之一。

4.7 防爆安全检查系统设计

4.7.1 本条规定源自 GB50348 的 6.4.10 条第 1 款（强制性条文），安全检查主要针对的是被保护单位或区域。保护单位或区域是根据反恐怖工作和安全防范管理工作的需要而确定的，一般包括：防范恐怖袭击的重点目标场所（如大型活动场所、机场、火车站、码头、城市轨道交通车站、公路长途客运站、口岸等）、特殊场所（如核电站、重要物资存储地、监狱等）

以及人员密集公共场所（如科技馆、图书馆、影剧院等）。

安全检查的对象包括进入场所的人员、物品和车辆。

安全检查检测的违禁品主要包括武器类（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（水银）、剧毒农药等剧毒化学品等）、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。

4.7.2 本条规定源自 GB50348 的 6.4.10 条第 4 款（强制性条文），要求成像式人体安全检查设备要保护人体隐私。

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，本条规定要求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。

4.7.3 安全检查设备应采用安全的技术，对人体的影响要可控，不产生伤害，如射线的辐射剂量控制。

安全检查设备不应影响被检物品的功能和性能，如通道式 X 射线安全检查设备是微剂量 X 射线检查设备，其单次检查剂量要小于 5μGy。

安全检查设备的探测不能使被检爆炸物达到起爆条件。

微剂量 X 射线安全检查设备的泄漏射线剂量率要求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，以保障设备正常使用时不对周围人员产生辐射伤害。

安全检查设备正常运行时不应干扰周边其它设备设施的正常运转。

4.7.4 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，防护设施包括盾牌、钢叉等。配备数量可根据安全检查现场实际情况和需求来确定，安全检查区内或相邻安全检查区可共用。

防爆处置、防护设施要有权限管理，不是岗位人员不能取得，而且设施所放位置既要便于取用，又不影响快速处置。

4.8 楼寓对讲系统设计

4.8.1 本条规定源自 GB50348 的 6.4.11 条（非强制性条文）。本条提出了楼寓对讲系统功能的总体要求。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。用于居民住宅小区的楼寓对讲系统应用构成示意图如图 4 所示。

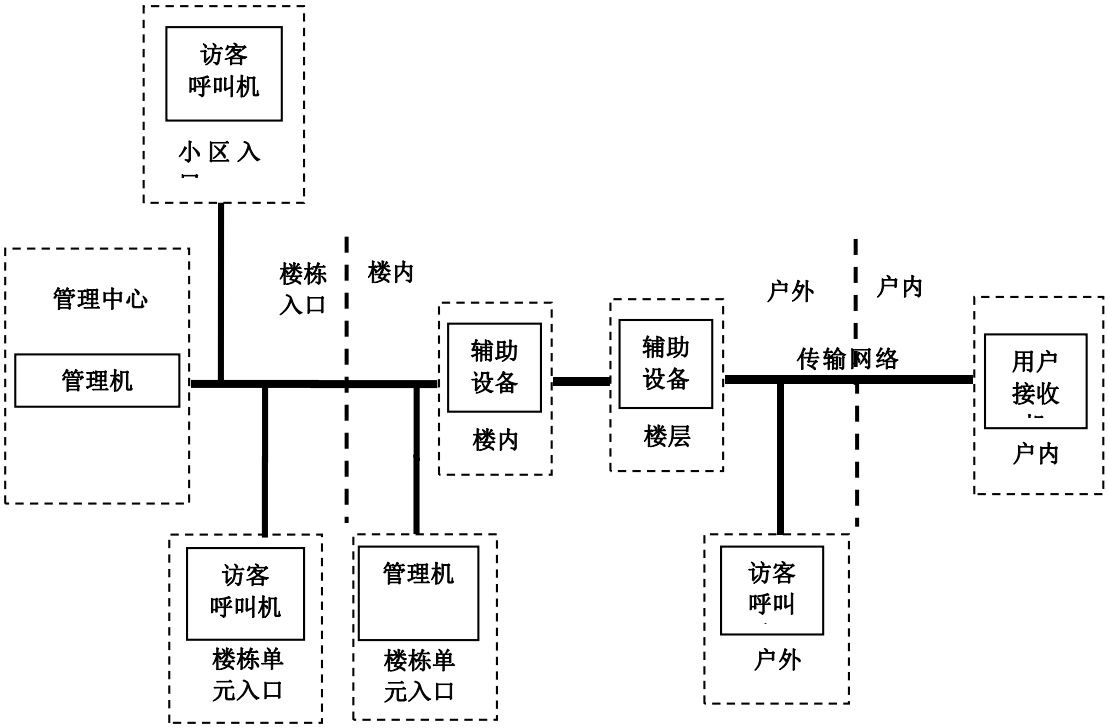

图 4　　楼寓对讲系统应用构成示意图

在图 4 中，系统组成设备可以根据系统规模和实际需求进行增减；系统至少应包含一台访客呼叫机和一台用户接收机；管理机和辅助设备为可选设备，根据系统需求加以选配。

4.8.2 本条规定源自《安全防范工程技术标准》GB50348-2018 第 6.4.12 条第 5 款（强制性条文）。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。

除已采取了可靠的安全管控措施外，不应利用无线扩展终端控制开启入户门锁以及进行报警控制管理。

用户寓所的入户门是指分隔住户私有空间与公共空间的门。由于当前无线网络的安全性得不到保障，因此，使用无线扩展终端控制开启入户门风险较大。产品供应商或系统集成商应采取安全管控措施，包括访问控制、控制指令保护、数据存储保护等安全措施，并提供相关产品检测报告，以确保不因这些措施失效而导致入户门被非法开启。

4.8.3 本条规定源自《安全防范工程技术标准》GB50348-2018 第 6.4.12 条第 9 款（强制性条文）。用户寓所的入户门是指分隔住户私有空间与公共空间的门。产品供应商或系统集成商应采取安全管控措施，包括访问控制、控制指令保护、数据存储保护等安全措施，并提供相关产品检测报告，以确保不因这些措施失效而导致入户门被非法开启。

4.9 电子巡查系统设计

4.9.1 本条规定源自国家标准《安全防范工程技术标准》GB50348-2018 第 6.4.13 条（非强制性条文）。该条提出了电子巡查系统功能的一般要求。

电子巡查系统分为在线式和离线式两种形态。在线式可以采用有线或无线方式。在线式具有较强的实时性。系统可独立设置，也可与出入口控制系统等联合设置，即利用出入口控制设备实现电子巡查功能。

4.9.2 本条规定源自国家标准《安全防范工程技术标准》GB50348-2018 第 6.4.14 条第 1 款（非强制性条文）。

该条明确了电子巡查系统必须具备的功能。

4.9.3 本条规定源自国家标准《安全防范工程技术标准》GB50348-2018 第 6.4.14 条第 3 款（非强制性条文）。

4.9.4 本条规定源自国家标准《安全防范工程技术标准》GB50348-2018 第 6.4.14 条第 4 款

（非强制性条文）。

巡查活动情况包括是否准时到达指定地点、是否遵守巡查顺序等。

5　工程施工

5.0.1 本条规定源自《安全防范工程技术标准》GB50348-2018 的第 7.1 节和第 7.2.1 条（非强制性条文）。

在施工过程中，需局部调整和变更时填写的更改审核单由建设单位或监理单位提供，经设计单位、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。

5.0.2 本条规定源自《安全防范工程技术标准》GB50348-2018 第 3.0.4 条（非强制性条文）。安全防范工程中使用的设备材料必须符合国家法规和现行相关强制性标准的要求。

本条是对安全防范工程选用的材料、设备提出的基本要求。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，直接关系到系统对于入侵、盗窃、抢劫、破坏、爆炸、暴力袭击等事件的防范能力，需求予以重点关注。

5.0.3 本条规定源自国家标准《安全防范工程技术标准》GB50348-2018 第 7.2.4 条第 3、4 款，其中第 3 款为强制性条文，第 4 款为非强制性条文。线缆敷设作为安全防范工程的关键环节，线缆敷设的质量将直接影响到建成后的安全防范系统能是否便利运行维护，寿命可靠，运行稳定，为此就安全防范工程的线缆敷设提出基本要求。

为了加强系统运行维护效率，在线缆敷设时应在合理位置设置编号，规范有效、稳定可靠设置标签。《安防线缆应用技术要求》GA/T 1406-2017 对线缆编号标识规则作了详细规定。

基于同轴电缆的结构及传输特性，接续后的同轴电缆往往带来信号衰减、连接故障等问题，降低系统可靠运行，加大日后运行维护工作，因此提出同轴电缆线缆敷设应一线到位，中间无接头的规定。

5.0.4 本条规定源自国家标准《安全防范工程技术标准》GB50348-2018 第 7.2.4 条第 11 款（非强制性条文）。本条是针对特殊保护对象化解施工矛盾的基本方法。即保护对象在需要配合保护措施时，应优先保护本身，而不是对保护对象造成伤害。采取的保护措施，可以是非接触式或近距离安装，非实体性的钻入安装部件，以及实体安装部件最小化，与保护目标的协调一体化等措施方法。

5.0.5 本条规定源自国家标准《安全防范工程技术标准》GB50348-2018 第 7.2.4 条第 12 款（非强制性条文）。

当存在易燃易爆环境时，要根据现行国家标准《危险化学品重大危险源辨识》GB18218 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、施工，现有的相关标准主要有现行国家标准《爆炸危险环境电力装置设计规范》GB50058、《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》GB50257、《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 》GB50154、《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 系列标准等。

5.0.6 本条规定源自国家标准《安全防范工程技术标准》GB50348-2018 第 5.5.3 条（非强制性条文）。

初步验收通过、项目整改及复验完成后的安全防范工程，没有经过一定周期的系统运行检验，往往存在或多或少、功能、性能、稳定性问题。如果直接竣工验收，由于系统的不可靠运行等潜在问题的显性化，将带来影响用户使用并难以定责等问题。为此，提出安全防范工程初步验收通过、项目整改及复验完成后至少应试运行 30 天的要求。

通过值机人员或系统管理员完整、翔实记录系统运行情况。建立系统运行、操作和维护等管理制度。以便及时发现系统存在的问题，优化完善系统的功能性能，达成系统与建设目标的符合性。

表 1　系统试运行记录表

工　程　名　称	
建设(使用)单位	

设计单位					
施工单位					
监理单位					
序号	日期/时间	试运行内容	试运行情况	备 注	值班人

注：

1.系统试运行情况栏中，正常打“ ”，并每天不少于填写一次；系统运行有异常情况时，在试运行情况栏中简要记录异常现象，并在备注栏中详细记录处置措施、实施人员、处置时间等。

2.系统有报警部分的，报警试验每天进行一次。出现误报警、漏报警的，在试运行情况和备注栏内如实填写。

工程验收一般由建设单位会同相关部门组织安排。做这样的规定是为了全面贯彻执行《行政许可法》，同时也考虑到安防行业的特殊性和我国安全防范工程管理的现状。

这里所指的相关部门是泛指在行政许可框架下的行业主管部门以及在行业主管部门监督指导下的社会中介组织。

6 工程检验与验收

6.0.1 本条规定源自国家标准《安全防范工程技术标准》GB50348-2018 第 9.1.1 条（非强制性条文）。

工程检验应根据工程所属行业、规模和设计要求，项目应覆盖工程所属行业的管理和标准要求以及工程设计的主要内容，以便对系统的主体特性作出全面评价。

6.0.2 本条规定源自国家标准《安全防范工程技术标准》GB50348-2018 第 10.1.2 条（非强制性条文）和第 10.1.4 条（非强制性条文）。

工程验收组可根据实际情况设施工验收组、技术验收组和资料审查组，并应根据项目的性质、特点和管理要求确定验收组成员，并由验收组推荐组长。

基于验收性质、任务本身的要求，同时考虑到安全防范工程的特点，以有利于更全面、更科学地把握好工程的技术质量目的，验收组中技术专家比例应不低于 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主要包括：施工单位人员、工程主要设备生产人员、供货单位人员以及其他需要回避的人员等。

6.0.3 本条规定源自国家标准《安全防范工程技术标准》GB50348-2018 第 10.2.1 条（非强制性条文）。

对于设备安装质量应重点检查安装位置是否合理、有效，符合设计文件要求，安装质量是否牢固、整洁、美观、规范，机柜（架）、操作台、电视墙的安装是否平稳、牢固，便于操作维护，控制设备是否操作方便、安全，开关、按钮是否灵活、方便、安全，机架、操作台、设备接地是否规范、安全，雷电防护措施和接地电阻是否符合标准要求，机架电缆线扎及标识是否整齐、有明显编号、标识并牢靠，电源引入线缆标识是否清晰、牢靠，通电工作是否正常。

对于线缆敷设质量应重点检查线缆的布防是否自然平直、标识清晰、编号统一并有适当保护，同轴电缆是否一线到位、中间无接头，光缆是否无断点、接头有预留，穿管(槽)线缆是否无接头或扭结，架空电缆的悬挂方式、挂钩间距、线缆最低点等是否符合设计要求，直埋线缆的线缆埋深、线缆保护等是否符合设计要求，电缆沟线缆是否与建筑物间隔离密封，管道线缆的线缆共管、线缆保护等是否符合设计要求。

对于线缆连接质量应重点检查线缆的连接器件是否连接可靠、绝缘良好、不易脱落，中间接续是否线序正确、连接可靠、密封良好，网络数据电缆是否连接器件的性能与电缆相匹配、线序正确、连接可靠，光缆接续时采用熔接方式和光缆熔接处是否有保护和固定。

6.0.4 本条规定源自国家标准《安全防范工程技术标准》GB50348-2018 第 10.3.1 条（非强制性条文）。

技术验收主要包括以下内容：

基本要求：系统主要技术性能、设备配置、主要安防产品的质量证明、供电模式；

实体防护：纵深防护设置实体防护设备、建筑施工出入口、车辆实体屏障功能、安防照明、警示标志；

入侵和紧急报警系统的探测、防拆、设置、操作功能，声音和/或图像复核功能，报警联动功能，报警响应时间；

视频监控系统的采集、监视、远程控制、记录与回放功能，视频/音频分析功能，系统管理功能，图像质量、信息存储时间；

出入口控制系统的目标识别、出入控制功能，自我保护措施和配置应急疏散功能；

停车库（场）安全管理系统的出入控制、车辆识别功能，内部安全管理措施；

防爆安全检查系统的防爆安全检查功能、监视和回放图像质量；

楼寓对讲(访客对讲)系统的 双向对讲、可视、开锁功能，系统管理功能，系统安全管控措施；

电子巡查系统线路设置、报警设置、统计报表功能；

系统集成：系统构架及集成方式、服务器冗余备份、管理平台功能；

监控中心：建设情况、通信手段、自身防护、应急对讲系统、应急广播系统和应急照明系统。

对于经检验机构检验合格的工程，验收组可根据工程性质、规模大小等情况确定抽样检查项目，没有经过工程检验的项目，技术验收应对检查项目逐项进行现场检查。

6.0.5 本条规定源自国家标准《安全防范工程技术标准》GB50348-2018 第 10.4.1 条（非强制性条文）。

资料准确性主要是指标记确切、文字清楚、数据准确、图文表一致，特别是要同工程实际施工结果一致；资料完整性主要是指所提供的资料内容要完整；资料规范性主要是指图样的绘制应符合《安全防范系统通用图形符号》GA/T74 等相关标准要求。图纸资料应按照工程建设的程序编制成套。

6.0.6 本条规定源自国家标准《安全防范工程技术标准》GB50348-2018 第 10.1.5 条（非强制性条文）。

验收结论是工程验收的结果，验收组应以高度认真、负责的态度，坚持标准、严格把关，以客观、公正为原则明确验收结论。验收结论分为通过、基本通过、不通过，为体现验收不是目的而是手段，确保工程质量才是根本，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。

6.0.7 本条规定源自国家标准《安全防范工程技术标准》GB50348-2018 第 5.6.5 条和第 10.5.5 条（非强制性条文）。竣工资料编制深度参见《安全防范工程技术文件编制深度要求》GA/T1185 的相关内容。

验收通过或基本通过的工程，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。

验收不通过的工程不得正式交付使用。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，落实整改措施后方可再次组织验收；工程复验时，对原不通过部分的抽样比例应加倍。

7　系统运行与维护

7.0.1 本条规定源自《安全防范工程技术标准》GB50348-2018 第 11.1.1 条（强制性条文）。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，也是确保系统满足安全防范管理要求，保持系统防范效能的基本要求。

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，落实安全防范工程设计的防护目标。系统运行一般还还包括针对保护对象的环境变化（如：增加某个风险部位的监视点位，以及相应警情等级调整等）所进行的人员资源配置和处置预案（流程）的优化等。

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护效能下降，延长系统和设备的使用期限，以及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，注意积累运行与维护数据，为系统效能评估提供坚实基础。

7.0.2 本条规定源自《安全防范工程技术标准》GB50348-2018 第 5.7.2 条（非强制性条文）。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。

建设（使用）单位应根据安全防范管理要求、系统规模和竣工文件，编制系统运行与维护的工作规划。

系统运行与维护工作需要系统化工作的思路，其中一项重要内容就是运行与维护的工作规划。主要可以包括以下内容：

1 系统运行规划一般包括：

（1）系统运行工作目标、工作范围、工作要求、工作团队建设要求等。

（2）系统运行工作费用预算。包括值机人员工资、办公等费用，系统和设备折旧和使用所产生日常性支出费用等（如：设备用电等费用。）。

2 系统维护规划一般包括：

（1）维护对象的系统组成、维护工作范围、主要工作内容和维护要求，以及工作团队建设要求等。

（2）维护需要的费用预算。费用预算编制办法可参考现行行业标准《安全防范系统维护保养规范》GA 1081-2014 和《安全防范工程建设与维护保养费用预算编制办法》GA/T70-2014 的规定。

保障机制是有效实施系统运行与维护的重要基础，保障机制一般包括：相应的工作团队，日常管理、值机、现场处置、例会、安全保密、培训和考核等制度以及作业指导技术文件。

安全防范系统运行与维护应根据保护对象的保护要求，确定考核指标。考核指标应具有易操作、能够反映系统运行的客观状况等特点。考核指标通常包括系统设备的在线率、完好率、故障修复时限等。

7.0.3 本条规定源自《安全防范工程技术标准》GB50348-2018 第 11.2.1 条（非强制性条文）。

1 根据工作目标、工作范围、工作要求，运行工作团队人员可分为管理人员、值机人员、现场处置人员等，负责日常具体的系统运行工作。

《公安部关于保安技防服务管理有关问题的批复》（公复字〔2012〕2 号）中，提出：“……在开展报警运营服务的企业中从事人工值守和现场处置工作的人员，应当依据《保安服务管理条例》和《公安机关实施保安服务管理条例办法》的有关规定纳入保安员管理。”，这是以国家行业规范方式明确报警运营服务的人员要求和管理要求。相关行业安全防范系统运行管理可以参考。

现行行业标准《报警运营服务规范》GA1383-2017 的第 3.1.9 条和第 3.1.11 条规定了“值机员”和“现场处置员”要求：

值机员：在报警运营服务中心负责接收、处理报警信息、视音频信息、故障信息及受理咨询、投诉的人员。

现场处置员：负责巡逻、值守以及报警现场处置的人员。

2 日常管理制度一般包括：值班制度、值机制度、现场处置制度、例会制度、安全保密制度、内部监督制度、环境检查制度和内务卫生制度等。

值机和现场处置制度建议参考现行行业标准《报警运营服务规范》GA1383-2017 相关要求编制。

例会制度应包括值机人员例会、相关负责人例会、管理部门例会等。

安全保密制度应该按照国家有关保密工作的法律法规和建设（使用）单位具体情况制定知密人员、知密范围、涉密文件、资料、信息等的管理与控制制度。

培训应该包括岗前培训和在岗培训，培训的内容一般包括法律法规常识、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、常见案（事）件的发案规律和特点、案（事）件处置预案以及经验交流、系统操作技巧、处置方法的运用和演练、案（事）件处置预案的模拟训练、信息的分析研判等。

在现行行业标准《基层公安机关社会治安视频监控中心（室）工作规范》GA/T 1072-2013 中专门对值机人员和监控中心提出了培训和考核要求，可结合实际情况参考实施。

3 在系统运行中，会涉及诸多需要协调管理的工作，如：

（1）与系统和设备维护团队相关的保障、报修等的协调、对接工作规则等；

（2）事件/警情处置中可能涉及的主管部门（保卫、后勤部门等）、相关其他职能部门，主管上级部门，公安机关等相关责任人、联系方法，相关的协调、对接工作规则等。

7.0.4 本条源自 GB50348-2018 的第 11.2 条。

系统运行环境是系统运行的基本保障，涉及各子系统配置和参数。

如：入侵和紧急报警系统中的布防时间和撤防时间。布撤防时间的确定，就意味着在这个时间段内对设防区域启动入侵探测报警，这个时间段的确认是与安全防范管理要求相一致的。如：银行营业场所的营业柜台紧急报警是 24h 布防，不允许撤防的，其他场所则可能是在下班后实施布防，上班后撤防。

7.0.5 本条规定源自《安全防范工程技术标准》GB 50348-2018 第 11.2.7 条（强制性条文）。紧急报警发生一般预示着重大警情。为确保重大警情能准确及时处置，在现行行业标准《报警运营服务规范》GA1383—2017 的第 5.2.3 条中专门对接入公安机关的紧急报警信息，提出了由监控中心人工向公安机关接警中心进行确认的要求。

7.0.6 系统维护工作团队应根据系统的规模、工作内容和维护要求组建。系统维护工作团队组建的目的是确保维护质量。

在《安全防范工程技术标准》GB 50348-2018 第 11.3.1 条（非强制性条文），将安全防范系统的维护细分为日常维护、故障处理、特殊时期保障几种模式的有机结合，是为了全面、高效地覆盖系统维护的需求，保障安全防范系统的防护效能。

特殊时期一般是国家重要节假日、政府或相关职能部门组织的重大活动期间，以及国家应急管理部门预报发布的涉及重大自然灾害、生产、食品卫生、社会治安等应急管理时期。

维护资源包括维护活动所需的值守人员、处置人员、协同措施（通信调度等）、安全防范系统的备品备件等等。