

DB32

江苏省地方标准

DB32/T XXXX-202X

体育场馆反恐怖防范要求

Requirements for counter-terrorism of gymnasium and stadium

(征求意见稿)

XXXX-XX-XX 发布

XXXX-XX-XX 实施

目 次

前言 III

1 范围 1

2 规范性引用文件 1

3 术语和定义 2

4 重点目标和重点部位 3

5 重点目标等级与防范级别 3

6 总体要求 4

7 常态防范要求 4

8 非常态防范要求 7

9 安全防范系统技术要求 8

10 制度防范 10

11 应急预案 11

12 检查 11

附录 A（规范性）体育场馆常态防范设施配置 11

附录 B（资料性）反恐怖防范管理制度 16

参考文献 18

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。

本文件由苏州市安全技术防范行业协会提出，由江苏省公安厅、江苏省体育局归口。

本文件起草单位：苏州市安全技术防范行业协会、江苏省公安厅反恐总队、江苏固耐特围栏系统股份有限公司、中国电信股份有限公司苏州分公司、苏州市东亚电脑监控工程有限公司、苏州中瀚通信科技有限公司、苏州国泰实业公司、江苏亚太伟业智能科技有限公司、苏州苏高新智能科技发展有限公司、浙江大华技术股份有限公司、苏州信颐系统集成有限公司、苏州市力发电子有限公司、上海国沃电子科技有限公司、苏州江南嘉捷电梯有限公司、嘉兴市蓝剑工程检测有限公司、杭州海康威视科技有限公司苏州分公司、徐州诚诺检测科技有限公司、中亿丰数字科技集团股份有限公司、江苏和诚保安服务有限公司、中国移动通信集团江苏有限公司昆山分公司、江苏大学、镇江市安全技术防范行业协会、连云港市安全技术防范行业协会。

本文件主要起草人：周慧敏、朱雨真、尚智、肖圣兵、吴雪芳、傅军、徐律、王建锋、韩剑、刘雨、王苏、田秋分、恽陈豪、张安、朱利民、杨国梁、张彬、高岩、丁阳、李海玲、沈恒山、张刚、黄世军、李慰祖、朱方、司勇。

体育场馆反恐怖防范要求

1 范围

本文件规定了体育场馆反恐怖防范重点目标和重点部位、重点目标等级与防范级别、总体要求、常态防范要求、非常态防范要求、安全防范系统技术要求、制度防范、应急预案和检查。

本文件适用于体育场馆的反恐怖防范工作与管理，举办大型活动时的反恐怖防范要求另行规定。

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 2894 安全标志及其使用导则
- GB/T 7946 脉冲电子围栏及其安装和安全运行
- GB 10408-2025 入侵和紧急报警系统 入侵探测器
- GB/T 15408 安全防范系统供电技术要求
- GB 17565-2022 防盗安全门通用技术条件
- GB/T 22239 信息安全技术 网络安全等级保护基本要求
- GB/T 22240 信息安全技术 网络安全等级保护定级指南
- GB/T 28181 公共安全视频监控联网系统信息传输、交换、控制技术要求
- GB/T 30147 安防监控视频实时智能分析设备技术要求
- GB/T 32581-2016 入侵和紧急报警系统技术要求
- GB/T 33170.2-2016 大型活动安全要求 第2部分：人员管控
- GB/T 33170.5-2016 大型活动安全要求 第5部分：安保资源配置
- GB 35114 公共安全视频监控联网信息安全技术要求
- GB/T 37078-2018 出入口控制系统技术要求
- GB 37300 公共安全重点区域视频图像信息采集规范
- GB 50348 安全防范工程技术标准
- GB 50394 入侵报警系统工程设计规范
- GB 50395 视频安防监控系统工程设计规范
- GB 50396-2007 出入口控制系统工程设计规范
- GB/T 50526 公共广播系统工程技术标准
- GB 55029 安全防范工程通用规范
- GA 69 防爆毯
- GA/T 394 出入口控制系统技术要求
- GA/T 644 电子巡查系统技术要求
- GA/T 761 停车库(场)安全管理系统技术要求

DB32/T XXXX-202X

GA/T 1032 张力式电子围栏通用技术要求

GA/T 1081-2020 安全防范系统维护保养要求

GA/T 1127-2025 安全防范视频监控摄像机

GA/T 1343 防暴升降式阻车路障

GA/T 1797 钢丝焊接网安全围栏

GA/T 2306 实体防护产品防护性能分类分级要求和试验方法

T/SSPIA 007 数字化张力钢丝焊接网安全围栏技术要求

3 术语和定义

GB 50348-2018 界定的以及下列术语和定义适用于本文件。

3.1

体育场馆 *gymnasium and stadium*

为满足体育竞赛、运动训练、体育教学、全民健身等活动需要而专门修建的公共运动场（馆）的总称。

[来源：GB 34311-2017，3.1，有修改]

3.2

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。

[来源：GB 50348-2018，2.0.1]

3.3

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。

[来源：GB 50348-2018，2.0.2，有修改]

3.4

实体防范 *physical protection*

利用建（构）筑物、屏障、器具、设备或其组合，延迟或阻止风险事件发生的实体防护手段。

[来源：GB 50348-2018，2.0.3，有修改]

3.5

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、反应能力的防护手段。

[来源：GB 50348-2018，2.0.4，有修改]

3.6

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。

[来源：GB 50348-2018，2.0.5]

3.7

反恐怖防范 *counter-terrorism precaution*

以维护公共安全为目的，为避免恐怖袭击（如破坏、爆炸、暴力袭击、劫持、撞击、纵火、投毒、施放放射性物品、生物化学攻击和网络攻击等）或伤害，运用科技手段、防护设施、管理制度应对恐怖威胁的行为。

3.8

常态防范 regular protection

运用人力防范、实体防范、电子防范等多种手段和措施，常规性预防、延迟、阻止发生恐怖事件的管理行为。

3.9

非常态防范 unusual protection

在重要会议、重大活动等重要时段以及获得涉恐怖袭击等预警信息或发生上述事件时，临时性加强防范手段和措施，提升反恐怖防范能力的管理行为。

4 重点目标和重点部位

4.1 重点目标

下列目标为体育场馆防范恐怖袭击的重点目标：

- a) 体育场；
- b) 体育馆。

4.2 重点部位

下列部位为体育场馆防范恐怖袭击的重点部位：

- a) 周界；
- b) 周界出入口及门卫室；
- c) 比赛区、训练区、演出区、展区；
- d) 看台、运动员区、裁判区、贵宾区、媒体区、竞赛管理区等重要区域；
- e) 体育场（馆）建筑的进出通道、馆内环廊、各类人员进出及疏散通道、楼梯、电梯等；
- f) 枪弹库、危险用品保管场所、安防监控中心（室）、网络与信息中心、消防中心、强弱电机房、空调机房、水泵房等功能用房；
- g) 其他经风险评估需要防范的部位。

5 重点目标等级与防范级别

5.1 体育场馆反恐怖防范的等级按场馆座席数由低到高分三级重点目标、二级重点目标、一级重点目标，具体见表 1。

表 1 重点目标等级

等级	三级	二级	一级
体育场座席数 (座)	10 000 ~ 19 999	20 000 ~ 39 999	40 000 (含) 以上
体育馆座席数 (座)	6 000 ~ 9 999	10 000 (含) 以上	/

5.2 防范级别

5.2.1 反恐怖防范分为常态反恐怖防范和非常态反恐怖防范。

5.2.2 重点目标的常态防范级别分为三级，按防范能力由低到高分别是常态三级防范、常态二级防范、常态一级防范，常态防范级别应与重点目标等级相适应。三级重点目标对应常态三级防范，二级重点目标对应常态二级防范，一级重点目标对应常态一级防范。

5.2.3 常态三级防范要求为重点目标应达到的最低标准，常态二级防范要求应在常态三级防范要求基础上执行，常态一级防范要求应在常态二级防范要求基础上执行。

5.2.4 非常态防范要求应在对应常态防范等级要求基础上执行。

6 总体要求

6.1 一般规定

6.1.1 新建、改建、扩建体育场馆的安全防范系统应与主体工程同步规划、同步设计、同步建设、同步验收、同步运行。已建、在建的体育场馆应按本文件要求补充完善安全防范系统。

6.1.2 应定期开展风险评估工作，综合运用人力防范、实体防范、电子防范和制度防范手段，遵循 $T_{\text{探测}} + T_{\text{反应}} \leq T_{\text{延迟}}$ 的原则，按照常态防范与非常态防范不同要求，落实各项反恐怖防范措施。

6.1.3 应针对利用无人驾驶航空器实施的恐怖袭击，加强安全防范系统建设。

6.1.4 应根据公安机关和有关部门的要求及时报告防范措施落实情况，提供重点目标的相关信息和重要动态。

6.1.5 网络与信息系统应按 GB/T 22240 明确安全保护等级，采取 GB/T 22239 中相应安全保护等级的防护措施，应能在发生或可能发生信息泄露、篡改、丢失等情况时立即采取补救措施。

6.1.6 应结合体育场馆地理环境、面积、建筑结构、建筑分布、重要部位分布等反恐怖防范工作实际需要，配备足够的安保力量，明确常态安保力量人数，并对重要岗位人员进行安全背景审查。

6.1.7 安全防范系统中涉及公民个人信息的，应依法依规进行处理，包括收集、存储、使用、加工、传输、提供、公开、删除等。

6.1.8 重点目标的安全防范系统应工程检验合格。

6.1.9 安全防范系统使用的设备、材料应该符合国家法规和现行相关标准的规定，并经检测合格。

6.1.10 常态防范设施配置应符合附录 A 的要求。

6.2 责任体系

6.2.1 应全方位落实人员、设施、制度等多层面的反恐怖防范安全责任。

6.2.2 应建立反恐怖管理小组，落实责任人员，明确岗位职责。

6.2.3 应明确对内的安全管理及对外的协助工作职责。

6.2.4 应设立反恐怖防范专项资金，将反恐怖防范涉及费用纳入单位预算，并建立反恐怖工作专项经费保障和使用制度。

6.3 管理制度

6.3.1 应建立健全反恐怖防范制度。

6.3.2 应建立反恐怖防范系统建设、运行与维护的保障体系和长效机制。

6.3.3 应与属地公安机关等有关部门和单位建立信息共享和联防、联动、联治工作机制。

6.3.4 应根据自身风险等级制定相应的应急预案、培训和演练方案。

7 常态防范要求

7.1 常态三级防范要求

7.1.1 人力防范要求

7.1.1.1 应设立与安全保卫任务相适应的反恐怖防范保卫机构，配置专/兼职保卫管理人员，建立健全

包括值守、巡逻、培训、检查、考核、安全防范系统运行与维护等制度。

7.1.1.2 重要部位及重要岗位保安人员配备原则如下：

- a) 安防监控中心（室）应 24 h 值守，每班应不少于 2 人；
- b) 巡查岗位每班应不少于 1 人；
- c) 备勤、周界等机动岗位应不少于 1 人。

7.1.1.3 在重点目标开放、人员相对集中时段，保安人员应持续对重点部位实施巡逻。在其他时段，巡逻间隔应不大于 6 h。

7.1.1.4 安防监控中心（室）应建立视频图像信息监看机制，重点关注重点部位动态。

7.1.1.5 应每年至少组织一次反恐怖教育培训。

7.1.1.6 应每年至少组织一次恐怖事件应急预案综合演练。

7.1.1.7 保安人员应配备棍棒、钢叉、盾牌、头盔、防刺背心等防卫防护装备器材，并配备通信工具。

7.1.2 实体防范要求

7.1.2.1 体育场馆或所在场所（园区）周界应设置金属围（栅）栏等实体屏障，实体屏障防护面高度应不低于 2 m，防机械暴力开口穿越性能应不低于 GA/T 2306 中规定的 FCA-JA2-2M 防护级别。实体屏障的防护面一侧的区域内不应有可供攀越和穿越的物体或设施。

7.1.2.2 周界车辆、人员出入口应分开设置。出入口应设置钢制平移门、平开门等实体屏障，实体屏障应能实现远程控制，并有限制或阻挡车辆、人员强行闯入的相应能力。机动车出入口设置的实体屏障抗撞击穿越性能应不低于 GA/T 2306 中规定的 FCB-JD3-14.8kJ 级别。无人值守的出入口实体屏障防攀爬、抗破坏等防护能力应不低于周界实体屏障的防护能力。应急出入口的实体屏障应满足消防的要求。

7.1.2.3 周界机动车出入口应设置减速装置。

7.1.2.4 与机动车道相连的广场、健身步道应设置被动式防冲撞车辆实体屏障。

7.1.2.5 重点区域应配置符合 GA 69 要求的防爆毯等处置设备。

7.1.2.6 安防监控中心（室）、网络与信息中心、消防中心、枪弹库、危险用品保管场所等出入口安装的防盗安全门，其防盗安全等级应不低于 GB 17565-2022 规定的 3 级要求。应急通道出入口门应满足消防的要求。

7.1.2.7 体育场馆应按照 GB 2894 的规定设置禁止行为、导向标志、紧急疏散标志等安全标志，地面标志应清晰耐磨。

7.1.3 电子防范要求

7.1.3.1 周界实体屏障应设置入侵探测装置。入侵探测系统应具有对攀爬、翻越、破坏实体屏障等入侵行为的探测能力，探测范围应能对周界实现有效覆盖，探测应无盲区。对应防区设置视频图像采集装置，并进行报警、视频联动。

7.1.3.2 强弱电机房、空调机房、水泵房等重要设备用房及库房应设置入侵探测器。

7.1.3.3 体育场馆周界出入口应设置视频图像采集装置，视频监视和回放图像应能清晰显示出入人员的体貌特征及进出车辆的号牌。

7.1.3.4 体育场馆重点部位应设置视频图像采集装置，视频监视和回放图像应能清晰显示出入人员的体貌特征和活动情况。

7.1.3.5 安防监控中心（室）、消防中心应设置出入口控制系统。

7.1.3.6 设有内部停车场（库）的体育场馆，应配置停车场管理系统并满足 GB 50348 的相关要求。

7.1.3.7 应设置电子巡查系统，在周界上设电子巡查点。

7.1.3.8 应设置公共广播系统，保证区域内人员能够听到广播发布的指令、通知。

7.1.3.9 电子显示屏应具备安全宣传、提示、警示等内容显示功能，并具有内容防篡改安全功能。

7.1.3.10 安防监控中心（室）应配置有线/无线（内部）通讯设备。

7.1.3.11 安防监控中心（室）应配置紧急报警装置，并与属地公安机关 110 报警服务台联网。

7.1.3.12 体育场馆应设置安全防范管理平台，实现安防系统集成、联动功能，实现对资源的统一调配和应急事件的快速处置。

7.2 常态二级防范要求

7.2.1 人力防范要求

7.2.1.1 周界主要出入口应设置门卫室或岗亭，实行 24 h 值班制度。

7.2.1.2 在重点目标开放、人员相对集中时段，保安人员应持续对重点部位实施巡逻。在其他时段，巡逻间隔应不大于 4 h。

7.2.1.3 应每半年至少组织一次反恐怖教育培训。

7.2.1.4 应每半年至少组织一次反恐怖应急预案演练。

7.2.2 实体防范要求

7.2.2.1 体育场馆或所在场所（园区）周界实体屏障防护面高度应不低于 2.5 m，抗破坏防护性能应不低于 GA/T 1797 中规定的 A1 级别。

7.2.2.2 周界机动车出入口实体屏障抗撞击穿越性能应不低于 GA/T 2306 中规定的 FCB-JD3-59.27kJ-1 级别。

7.2.2.3 周界机动车出入口应设置车辆阻挡装置，阻挡能力等级应不低于 GA/T 1343 中规定的 B1 或 A2 级别。采用电动操作的车辆阻挡装置，应具有手动应急操作功能。

7.2.3 电子防范要求

7.2.3.1 门卫室、值班室宜设置紧急报警装置，并与属地公安机关 110 报警服务台联网。

7.2.3.2 周界出入口应设置出入口控制装置，对进出人员及车辆进行权限识别和出入控制。

7.2.3.3 重点部位的图像采集装置宜具备视频图像智能分析功能。

7.2.3.4 强弱电机房、空调机房、水泵房等重要设备用房及库房应设置出入口控制系统和入侵探测器。

7.2.3.5 重要的出入口、走道和通道应设置人行通道闸、车辆实体屏障、安全缓冲区、隔离区等。

7.2.3.6 应设置在线式电子巡查系统，在重要部位设电子巡查点。

7.2.3.7 体育场馆门卫室、值班室应配置有线/无线（内部）通讯设备。

7.2.3.8 体育场馆应设置无线信号全覆盖系统。

7.3 常态一级防范要求

7.3.1 人力防范要求

7.3.1.1 重要部位及重要岗位保安人员配备原则如下：

a) 安防监控中心（室）应 24 h 值守，每班应不少于 3 人；

b) 巡查岗位每班应不少于 2 人；

c) 备勤、周界等机动岗位在岗应不少于 2 人。

7.3.1.2 应建立视频远程巡视的操作规程以及与现场保安人员的联动机制，安防监控中心（室）的值班人员应对所有视频图像进行远程巡视作业。

7.3.1.3 在重点目标开放、人员相对集中时段，保安人员应持续对重点部位实施巡逻。在其他时段，巡逻间隔应不大于 2 h。

7.3.1.4 应每季度至少组织一次反恐怖教育培训。

7.3.1.5 应每季度至少组织一次反恐怖应急预案演练。

7.3.2 实体防范要求

周界机动车出入口实体屏障抗撞击穿越性能应不低于 GA/T 2306 中规定的 FCB-JD6-887kJ-1 级别。

7.3.3 电子防范要求

7.3.3.1 体育场馆人员密集区应配备可视报警装置，并能与安防监控中心（室）进行实时通话。

7.3.3.2 视频监控系统应能与对应区域的报警、门禁系统实现联动。

7.3.3.3 体育场馆应配备无线通信指挥调度系统。

7.3.3.4 重点部位的图像采集装置应具备视频图像智能分析功能。

7.3.3.5 宜设置电磁环境监测与抑制系统，实现对场馆及重点区域电磁信号的全域监测、异常识别、快速预警与分级抑制。

7.3.3.6 应配备、使用符合国家法律、法规和有关要求的反无人机主动防御系统。

7.3.3.7 应设置安检与违禁品探测，可在主要入口及安检区域配置 X 光安检机、金属探测门、液体检测仪、爆炸物探测设备，对人员、物品实行强化安检，提升对管制器具、易燃易爆等危险物品的发现能力。

8 非常态防范要求

8.1 人力防范要求

8.1.1 重点目标管理单位应启动应急响应机制，组织开展反恐怖动员，管理单位负责人或其授权人员应带班组织防范工作，在常态防范基础上加强保卫力量；获得涉恐怖袭击等预警信息或发生上述案事件时，管理单位负责人或其授权人员应 24 h 带班组织防范工作。

8.1.2 重点目标周界出入口未设置门卫室的增设岗亭，实行 24 h 值班制度。

8.1.3 重要部位巡视频率较常态提高 100%，巡查人员可利用手持式探测仪对可疑人员、包、物及运输车辆进行检查。

8.1.4 应加大视频图像监看的频次。

8.1.5 重点目标周界出入口应设置警戒区域，限制人员、车辆进出。

8.1.6 应加强对出入重点目标的人员、车辆及所携带物品的安全检查。

8.1.7 其他安全措施应符合 GB/T 33170.2 和 GB/T 33170.5 的规定。

8.2 实体防范要求

8.2.1 应加强对防护器具、救援器材、应急物资、周界及出入口实体屏障、门、窗、锁、车辆阻挡装置等设施的有效性检查。

8.2.2 应减少重点目标周界出入口的开放数量。

8.2.3 周界出入口的车辆阻挡装置应设置为阻截状态。

8.3 电子防范要求

8.3.1 应加强对电子防范设施、设备的检查和维护，确保安全防范系统正常运行及通信设备的正常使用。

8.3.2 应提高出入口控制系统对各受控区的出入识别权限与核验规则配置，强化出入口控制系统对各区域的人员管理。

8.3.3 重点部位（出入口、通道、要害部位）宜增设移动监控设施。

8.3.4 加强出入口身份核验与车辆管控，所有人员出入口实行人脸比对、人证合一、白名单/黑名单布控联动。

8.3.5 加强出入口车辆管控，实现车牌识别、车身特征抓拍、危化品/违禁品联动预警，对重点管控车辆自动拦截并上报监控指挥中心。

- 8.3.6 启动全域应急广播，支持实时喊话、驱散指令、紧急通知。
- 8.3.7 应设置反恐指挥中心，满足非常态实战处置需求，系统互联互通、集中管控、统一调度。
- 8.3.8 安防平台切换至反恐实战态势界面，实现视频集中上墙、安保力量可视化、保安人员统一调度。

9 安全防范系统技术要求

9.1 一般要求

- 9.1.1 应对安全防范设施内具有计时功能的设备进行校时，设备的时钟与北京时间误差应不大于 5 s。
- 9.1.2 安全防范设施应符合 GB 50348、GB 55029 的相关规定。
- 9.1.3 安全防范设施和设备的登录密码不应是弱口令，应采取措施防范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防范措施。
- 9.1.4 安全防范系统维护保养要求应符合 GA/T 1081-2020 的相关规定。

9.2 入侵和紧急报警系统

- 9.2.1 系统的防区划分、入侵探测装置安装位置的选择，应有利于及时报警和准确定位。各防区的距离、区域应按产品技术要求设置。
- 9.2.2 周界入侵探测系统应具有对攀爬、翻越、破坏实体屏障等入侵行为的感知能力，感知范围应能对实体屏障实现有效覆盖，不应有盲区。
- 9.2.3 周界入侵探测装置应和实体屏障联合设置，入侵探测系统并与视频监控系统联动，监视及回放图像应能清晰显示周界区域人员活动情况。
- 9.2.4 采用脉冲电子围栏时，应符合 GB/T 7946 的规定；采用张力电子围栏时，应符合 GA/T 1032 的规定；采用张力探测技术与实体屏障一体化产品时，应符合 T/SSPIA 007 的规定。
- 9.2.5 系统探测到报警区域的入侵事件后，应实时将报警信息传送到安防监控中心（室），安防监控中心（室）应能有声、光指示，并能准确指示发出报警的位置。
- 9.2.6 系统应具备防拆、开路、短路报警功能。
- 9.2.7 应具备自检功能和故障报警、断电报警功能。
- 9.2.8 系统应配备备用电源，保证市电断电后正常工作时间不应小于 8 h。
- 9.2.9 系统布防、撤防、故障和报警信息存储时间不应少于 180 d。
- 9.2.10 入侵探测器应满足 GB 10408-2025 中相应的规定要求。
- 9.2.11 系统的安全等级不应低于 GB/T 32581-2016 中规定的 2 级要求。

9.3 视频监控系统

- 9.3.1 系统应符合 GA/T 1127-2025 的相关规定。
- 9.3.2 重要部位设置的视频图像采集装置，监视及回放图像的水平像素数不应小于 1 920，垂直像素数不应小于 1 080，视频图像帧率不应小于 25 fps，且能清晰显示区域内人员活动情况、车辆通行情况。具有视频图像智能分析功能的摄像机分辨率不低于 2 560×1 440。
- 9.3.3 视频录像保存时间不应少于 90 d。
- 9.3.4 系统的备用电源不应少于维持系统 2 h 正常工作的需要。
- 9.3.5 系统应配置统一时钟源对所有系统设备进行自动校时和时钟同步。
- 9.3.6 系统应留有与公共安全视频图像信息共享交换平台联网的接口，联网信息传输、交换、控制协议应符合 GB/T 28181 的相关规定，联网信息安全应符合 GB 35114 的相关规定。
- 9.3.7 系统采用智能化视频分析处理技术时，应能实现运动目标检测、遗留物检测、物体移除检测、绊线检测、入侵检测、逆行检测、徘徊检测、流量统计、密度检测、目标分类以及声音检测、报警联动等

一种或多种实时智能分析功能及应用，其技术要求应符合 GB/T 30147 的有关规定。

9.3.8 涉及公共区域的视频图像信息的采集要求应符合 GB 37300 的相关规定。

9.4 出入口控制系统

9.4.1 系统应能对强行破坏、非法进入的行为发出报警信号，报警信号应与相关出入口的视频图像联动。

9.4.2 系统应满足紧急逃生时人员疏散的相关要求。

9.4.3 系统信息存储时间不应少于 180 d。

9.4.4 系统的安全等级不应低于 GB/T 37078-2018 中规定的 2 级要求。

9.4.5 系统的其他要求应符合 GB 50396-2007、GA/T 394 的相关规定，停车库（场）安全管理系统的其他要求应符合 GA/T 761 的相关规定。

9.5 电子巡查系统

9.5.1 系统应根据安全管理的需求制定巡查方案，并覆盖重要部位，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。

9.5.2 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。

9.5.3 系统巡查记录保存时间不应少于 180 d。

9.5.4 系统的其他要求还应符合 GA/T 644 的相关规定。

9.6 公共广播系统

9.6.1 公共广播应具有最高级别的控制优先权。公共广播系统应能在手动或警报信号触发的 10 s 内，向相关广播区播放警示信号、警报语声文件或实时指挥语声。

9.6.2 以现场环境噪声为基准，紧急广播的信噪比应大于或等于 12 dB。

9.6.3 系统设备应处于热备用状态，或具有定时自检和故障自动告警功能。

9.6.4 系统应符合 GB/T 50526 的要求。

9.7 电子显示屏系统

9.7.1 系统应建立多媒体信息审核机制，规范多媒体信息发布流程。

9.7.2 采取技术措施对播放的多媒体信息进行检测，及时识别并有效阻断被篡改的多媒体信息。

9.8 有线/无线（内部）通讯系统

9.8.1 重点目标区域内对讲机接通率应保持大于 98%。

9.8.2 系统应支持单呼、组呼、全呼、脱网呼叫功能。

9.8.3 系统应能具有实时定位与指挥调度功能。

9.8.4 系统应采用加密认证技术，保障通信安全。

9.8.5 系统宜具有融合 AI 智能分析策略，实现动态信道分配与资源优化。

9.9 安防监控中心

9.9.1 安防监控中心（室）应单独设置。

9.9.2 视频监控、入侵和紧急报警、电子巡查的终端设备，以及出入口控制系统的报警信号输出终端均应设置在安防监控中心（室），应具有对各子系统的操作、记录、显示等功能。

9.9.3 安防监控中心（室）应配备有线、无线专用通讯工具；应配备保安专用防护器械和消防专用设备、器材、装备。

9.9.4 安防监控中心（室）其他要求应符合 GB/T 15408、GB 50348、GB 50394、GB 50395 和 GB 50396-2007 的相关规定。

9.10 安全防范管理平台

9.10.1 平台应包括集成管理、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、预案管理、人机交互、联网共享、指挥调度、智能应用、系统运维、安全管控等功能。

9.10.2 其他应满足 GB 50348-2018 中相应功能要求。

9.11 电磁环境检测与抑制系统

9.11.1 系统应能对重点目标区域进行电磁环境监测、采样，建立频谱模板。

9.11.2 系统应能快速查找和验证未授权的电磁信号源，调查、记录、存储、分析有关信号源电磁情况。

9.11.3 系统应能对异常电磁信号进行干扰抑制，阻断异常信号传输。

9.12 反无人机主动防御系统

9.12.1 系统发射功率和使用频段应符合国家有关规定。

9.12.2 系统应能自动 24h 持续工作，无需人员值守。

9.12.3 系统的应用不应应对周边合法通信产生干扰。

9.13 防爆安检系统

9.13.1 防爆安检系统部署应根据需求进行设置，定期进行校准。

9.13.2 防爆电气设备应通过专业机构的防爆认证，确保其能够在潜在爆炸性环境中安全使用。

10 制度防范

10.1 管理制度

10.1.1 应制定反恐怖防范管理组织制度,明确责任领导的管理职责和责任部门的工作职责。配置专人负责反恐怖防范制度管理工作,所有制度文件应受控,确保制度的宣贯、实施与持续改进。

10.1.2 应建立健全包括值守、巡逻、培训、检查、考核、反恐怖防范系统运行与维护等制度。

10.1.3 应建立反恐怖防范系统建设、运行与维护的保障体系和长效机制。

10.1.4 应建立反恐怖工作专项经费保障制度,将反恐怖防范涉及费用纳入企业预算成本,保障反恐怖防范工作机制运转正常。

10.1.5 应与属地公安机关等有关部门和单位建立联防、联动、联治工作机制。

10.1.6 应建立反恐怖与安全生产等有关信息的共享和联动机制。

10.1.7 应定期开展反恐怖风险评估工作,根据评估结果,针对常态防范与非常态防范的不同要求,落实各项反恐怖防范措施。

10.1.8 应建立健全反恐怖防范管理档案和台账,包括重点目标的名称、地址或位置、目标等级、防范级别、重点目标管理单位负责人、保卫部门负责人,现有人力防范、实体防范、电子防范、制度防范相关材料,平面布置图、结构图、重要部位分布图、3D 全景效果图、VR 视频全景图等。

10.1.9 重点目标的反恐怖防范管理制度可视工作需要按附录 B 选择。

10.2 岗位标准

10.2.1 制定重点目标管理单位责任领导、责任部门的正(副)职、联络员等岗位标准,应包括反恐怖防范工作职责和权限。

10.2.2 制定技防、值守、巡查、网管、机动等岗位标准,每个岗位按作业流程列出工作细节,明确与其他工作接口相互协调要求。

10.2.3 有定额的岗位应明确定额,有数量和时间方面要求的,应量化。

10.2.4 制定考核条件和奖惩办法,明确检查、考核部门、时间要求,明确考核程序和考核办法,应有考核记录。

10.3 操作规程

10.3.1 配备反恐怖防范有关设备设施涉及到国家、行业、地方的标准及文件。

10.3.2 配备反恐怖防范关键设备的操作规程或系统作业指导书。

10.4 制度落实与监督

10.4.1 管理运营单位应将制度文本公开并组织宣贯培训,确保所有从业人员知悉并遵守。

10.4.2 管理运营单位应建立制度执行台账,做到可追溯、可核查。

10.4.3 管理运营单位应主动接受公安机关及行业主管部门的监督检查,对存在的问题及时整改。

11 应急预案

11.1 应针对恐怖事件的规律、特点和可能造成的社会危害,分级分类制定、实施应急预案,应对可能遭受的恐怖袭击或危害等紧急情况,并对本单位的应急准备和应急能力进行评估。

11.2 应急预案应规定恐怖事件应对处置的组织指挥体系、恐怖事件安全防范、应对处置程序以及事后社会秩序恢复等内容:

- a) 应包括目标概况、应急基本原则、组织机构、应急联动、信息报告、应急指挥、应急措施、保障、应急解除等内容;
- b) 根据情况应提供基本情况说明、工作人员信息详表、应急联络通讯表、实景照片、地理位置标示图、周边环境图、单位平面图、重要部位分布图、应急疏散通道(路线)图、应急装备(设备)分布图、消防设施分布图、防范设施标示图;
- c) 宜提供电路设施网分布图、自来水管网分布图、地下管网分布图、信息系统网络分布图及相应的视频资料或三维建模(配合 3D 地图采集建模)等。

11.3 宜建立相应的数据库和应急指挥系统。

11.4 应组建具有组织人员疏散、保护重要部位、控制损失和准确反馈现场情况等能力的先期应急队伍,加强反恐最小应急单元建设。

11.5 应定期按照应急预案开展演练,按规定修订和完善应急预案。

12 检查

12.1 重点目标管理单位每年应开展至少一次的自我检查,对反恐怖防范工作中存在的问题实施持续改进,不断完善人防、物防、技防和制度防范,提高其反恐怖防范能力。

12.2 编制检查报告归档备查。

附 录 A
(规范性)
体育场馆常态防范设施配置

体育场馆常态防范设施配置应符合表 A.1 的规定。

表 A.1 体育场馆常态防范设施配置

序号	重点部位	防范设施		配置要求		
				三级 重点目标	二级 重点目标	一级 重点目标
1	周界	实体防护设施	金属围（栅）栏	●	●	●
2		视频监控系统	视频图像采集装置	●	●	●
3		公共广播系统	公共广播装置	●	●	●
4		入侵和紧急报警系统	入侵报警装置	●	●	●
5		巡查系统	电子巡查装置	●	●	●
6			在线电子巡查系统	—	●	●
1	周界出入口	实体防护设施	钢制平移门、平开门等	●	●	●
2			车辆减速装置	●	●	●
3			车辆阻挡装置	—	●	●
4		视频监控系统	视频图像采集装置	●	●	●
5		公共广播系统	公共广播装置	●	●	●
6		出入口控制系统	出入口控制装置	—	●	●
1	门卫室	防卫防护装备	棍棒、钢叉、盾牌、头盔、防刺背心	●	●	●
2		安全处理装置	防爆毯	●	●	●
3		视频监控系统	视频图像采集装置	●	●	●
4		公共广播系统	公共广播装置	●	●	●
5		紧急报警系统	紧急报警装置	—	○	●
6		通信设备	有线/无线通信	—	●	●

表 A.1 体育场馆常态防范设施配置（续）

序号	重点部位	防范设施		配置要求		
				三级 重点目标	二级 重点目标	一级 重点目标
7	门卫室	巡查系统	在线电子巡查系统	-	●	●
1	比赛区、训练区、演出区、展区	视频监控系统	视频图像采集装置	●	●	●
2		公共广播系统	公共广播装置	●	●	●
3		巡查系统	在线电子巡查系统	-	●	●
4		实体防护设施	安全标志/地面标志	●	●	●
1	看台、运动员区、裁判区、贵宾区、媒体区、竞赛管理区	视频监控系统	视频图像采集装置	●	●	●
2		公共广播系统	公共广播装置	●	●	●
3		巡查系统	在线电子巡查系统	-	●	●
4		出入口控制系统	人行通道闸	-	●	●
5		紧急报警系统	可视报警装置	-	-	●
6		实体防护设施	安全标志/地面标志	●	●	●
1	体育场（馆）建筑的进出通道、馆内环廊、各类人员进出及疏散通道、楼梯、电梯	视频监控系统	视频图像采集装置	●	●	●
2		公共广播系统	公共广播装置	●	●	●
3		巡查系统	在线电子巡查系统	-	●	●
4		紧急报警系统	可视报警装置	-	-	●
5		实体防护设施	安全标志/地面标志	●	●	●
1	广场	实体防护设施	被动式防撞实体屏障	●	●	●
2		公共广播系统	公共广播装置	●	●	●
1	安防监控中心（室）	实体防护设施	防盗安全门	●	●	●
2		安全处理装置	防爆毯	●	●	●
3		视频监控系统	视频图像采集装置	●	●	●
4		出入口控制系统	出入口控制装置	●	●	●
5		巡查系统	在线电子巡查系统	-	●	●

表 A.1 体育场馆常态防范设施配置（续）

序号	重点部位	防范设施		配置要求		
				三级 重点目标	二级 重点目标	一级 重点目标
6	安防监控中心 （室）	通信设备	有线/无线通信	●	●	●
7		紧急报警系统	紧急报警装置	●	●	●
8		安防平台	安全防范系统管理平台	●	●	●
1	网络与信息中 心	实体防护设施	防盗安全门	●	●	●
2		视频监控系统	视频图像采集装置	●	●	●
3		入侵和紧急报警系统	入侵报警装置	●	●	●
4		出入口控制系统	出入口控制装置	—	●	●
5		巡查系统	在线电子巡查系统	—	●	●
1	消防中心	实体防护设施	防盗安全门	●	●	●
2		视频监控系统	视频图像采集装置	●	●	●
3		出入口控制系统	出入口控制装置	●	●	●
4		巡查系统	在线电子巡查系统	—	●	●
1	强弱电机房	入侵和紧急报警系统	入侵报警装置	—	●	●
2		视频监控系统	视频图像采集装置	●	●	●
3		出入口控制系统	出入口控制装置	—	●	●
4		巡查系统	在线电子巡查系统	—	●	●
1	空调机房	入侵和紧急报警系统	入侵报警装置	—	●	●
2		视频监控系统	视频图像采集装置	●	●	●
3		出入口控制系统	出入口控制装置	—	●	●
4		巡查系统	在线电子巡查系统	—	●	●
1	水泵房	入侵和紧急报警系统	入侵报警装置	—	●	●
2		视频监控系统	视频图像采集装置	●	●	●
3		出入口控制系统	出入口控制装置	—	●	●

表 A.1 体育场馆常态防范设施配置（续）

序号	重点部位	防范设施		配置要求		
				三级 重点目标	二级 重点目标	一级 重点目标
4	水泵房	巡查系统	在线电子巡查系统	-	●	●
1	枪弹库、危险 用品保管场所	实体防护设施	防盗安全门	●	●	●
2		视频监控系统	视频图像采集装置	●	●	●
3		入侵和紧急报警系统	入侵报警装置	-	●	●
4		巡查系统	在线电子巡查系统	-	●	●
1	停车场	停车场管理	停车场管理系统	●	●	●
2		视频监控系统	视频图像采集装置	●	●	●
3		公共广播系统	公共广播装置	●	●	●
4		实体防护设施	安全标志/地面标志	●	●	●
5		巡查系统	在线电子巡查系统	-	●	●
注：表中“●”表示应配置，“-”表示不要求，“○”表示宜配置。						

附 录 B
(资料性)
反恐怖防范管理制度

B.1 管理制度

重点目标的反恐怖防范管理制度见表B.1。

表 B.1 管理制度

序号	项目	
1	人防	教育培训及考核制度
2		人员背景审查制度
3		人员档案及备案制度
4		门卫与寄递物品管理制度
5		巡查制度
6		安全检查制度
7		值班监看和运维制度
8		训练演练制度
9		检查督导制度
10		人防增援配置制度
11	物防、技防	采购管理制度
12		设备设施档案制度
13		技防系统管理制度
14	综合	工作报告制度
15		网络安全管理制度
16		专项经费保障制度
17		情报信息管理制度
18		恐怖威胁风险评估制度
19		联动配置机制
20		应急管理制度
21		应急预案管理制度
22		保密制度

B.2 部分制度内容

B.2.1 反恐怖工作责任制度

应建立层级责任体系，明确主要负责人总责、分管负责人专责、部门分责、岗位全责。管理运营单位应与内部各部门及相关责任人签订反恐怖防范责任书，建立责任追究机制。

B.2.2 重点部位管理制度

应建立重点部位的专人值守、出入登记、警示标志和防护设施全覆盖管理制度。

B.2.3 人员安全管理制度

应对重要岗位人员实施安全背景审查，建立人员档案；安保人员应持证上岗；对从业人员开展常态化反恐怖防范意识和技能教育。

B.2.4 出入安检管理制度

应制定人员、车辆、物品进出安全检查规范，明确安检流程、禁限带物品清单，对进入场馆的人员、车辆、物品实行全覆盖安全检查及身份核验。

B.2.5 安全隐患排查整治制度

应建立日常巡查、定期排查与重点时段专项排查相结合制度。建立隐患排查整改台账，实行“排查、登记、整改、复核、销号”的闭环管理。

B.2.6 安防设施运维管理制度

应建立安防设施运维机制，明确维护频次和标准，确保设施全天候正常运行，严禁擅自停用或拆除。

B.2.7 培训演练制度

应制定年度反恐怖培训计划，对从业人员定期开展法律法规、防范知识和应急处置技能培训。应每半年至少组织一次反恐怖应急综合演练，重要岗位人员应熟练掌握应急技能。

B.2.8 信息报告与值班值守制度

应实行24小时值班值守和领导带班制度。建立涉恐可疑信息快速上报机制，发现可疑人员、物品或线索，应立即向公安机关报告，不得迟报、漏报、瞒报。

B.2.9 应急管理制度

应制定针对性的反恐怖应急预案，明确恐怖袭击、可疑物品、爆炸威胁等突发事件的处置流程。组建应急队伍，配备应急物资和装备，并定期维护。

B.2.10 监督检查与考核评价制度

应建立内部自查和问题隐患整改督办制度，将反恐怖防范工作纳入年度绩效考核，建立奖惩机制。

参考文献

- [1] GB 22185 体育场馆公共安全通用要求
- [2] GA/T 1459 大型群众性活动安全检查规范
- [3] JGJ 31 体育建筑设计规范
- [4] TY/T 1009.1-2024 体育赛事信息化 网络安全规范 第1部分：通用网络安全架构
- [5] TY/T 1105-2024 群众体育赛事活动安全评估技术导则
- [6] DB32/T 4580-2023 公共体育场馆大型群众性活动安全保障规范
- [7] 建标（2024）50号 城市公共体育场建设标准
- [8] 建标（2024）51号 城市公共体育馆建设标准
- [9] 建标（2024）52号 城市公共游泳馆建设标准
- [10] 中华人民共和国反恐怖主义法（中华人民共和国主席令第36号）
- [11] 中华人民共和国突发事件应对法（中华人民共和国主席令第69号）
- [12] 企业事业单位内部治安保卫条例（国务院令第421号）
- [13] 大型群众性活动安全管理条例（国务院505号令）
- [14] 国家突发公共事件总体应急预案
- [15] 省政府关于印发江苏省大型群众性活动安全管理规定的通知（苏政发〔2021〕78号）
