体育场馆直播系统布设指南

（试　行）

2022 年 9 月 13 日

目　　录

前　言

为贯彻落实《国务院办公厅关于加强全民健身场地设施建设发展群众体育的意见》（国办发〔2020〕36号）关于加强信息化建设、推进互联网＋健身，以及《体育强国建设纲要》（国办发〔2019〕40号）关于推进全民健身智慧化发展有关要求，指导各地利用AI、5G、大数据等技术，打造一批智慧化体育场馆，为群众提供更时尚、更有粘性的运动健身场景，提高全民健身公共服务智能化、信息化、数字化水平，体育总局群体司、体育信息中心组织相关单位研究编制了《体育场馆直播系统布设指南（试行）》，供各地在工作中参考。

一、范围

本文件适用于体育场馆体育赛事活动直播系统的布设。该系统可以实时直播各项各类体育赛事。系统需满足露天或室内，大型或小型体育场馆的直播功能需求，并同时充分考虑5G功能。

二、术语和定义

模拟运镜：基于场地周边安装的固定（特写或全景）拍摄设备获取的赛事活动视频影像，通过人工智能技术对视频进行处理，在无人工干预情况下，对视频进行矫正及适当画面处理，从而能够达到模拟推、拉、摇、移直播效果的技术形式。

自动导播：基于场地周边安装的固定拍摄设备获取的赛事活动视频影像，通过人工智能技术对视频进行处理，在无人工或少人工干预的情况下，从而实现直播信号切换，回放及各种直播包装的技术形式。

VR直播：通过在赛场周边部署的VR相机，采用自内向外的环绕拍摄方式，用户可借助手机和VR眼镜等设备观看全景视频，获得全方位沉浸式的体验和获得身临其境的视觉感受。

自由视角直播：自由视角是以赛场为中心，通过自外向内环绕式的拍摄方式，为观众提供任意时间、任意角度的自由角度观看赛事体验。观众可以通过遥控器控制电视，或者滑动手机屏幕来自由切换视角观看赛事。

多视角直播：在现场部署多台高清摄像机，分别拍摄远景、全景、近景特性等，覆盖不同的角度，最终输出时间同步的多路

视频信号并推送至分发平台。用户可以在终端选择不同的视角，灵活进行切换，观赛更加自由。

事件识别及分析：基于赛事直播及影像内容，针对不同的赛事，识别重要事件及动作。同时，准确解析识别事件相关人物或器材的速度、点位、高度、轨迹等基本数据。

三、技术指标

（一）拍摄设备

1. 对于广角/全景拍摄设备：分辨率需不低于2K，帧率不低于25帧/秒，色彩逼真。需具备网络推流能力。需具备一定的防雨、防风、防冲击能力。宜具备软件远程配置、调试、升级能力。

2. 对于非广角/全景拍摄：分辨率需不低于1080P、帧率不低于25帧/秒，色彩逼真、无畸变。需具备网络推流能力。需具备一定的防雨、防风、防冲击能力。针对户外场地的夜间拍摄，宜具备一定的补光效果。宜具备软件远程配置、调试、升级能力。

（二）场馆直播系统软件（系统功能示意图可参考附录A）

1. 提供多分辨率直播内容。直播观看用户可依据实际网络情况，进行分辨率调节。

2. 场馆直播系统需支持在无人值守情况下完成赛事直播，包括但不限于全景模拟运镜、自动导播等。

3. VR直播视频质量宜采用4K/8K信号，视频帧率应不低于60fps，以保障直播的清晰度和流畅性。场馆可通过本地的计算服务，实现视频编转码。

4. 事件识别及分析算法识别准确率在95%以上为宜，延迟应不高于1秒。事件视频片段产生的延迟应低于10秒。

5. 需向体育主管部门提供必要的活动统计数据，包括但不限于活动线上浏览量、活动时间、地域信息，及上述各项的汇总信息。

6. 需提供场馆直播相关的场馆、场地、设备管理能力，视频流生产及上传到视频云平台，通过云服务提供必要的活动直播订阅能力。

7. 场馆直播系统宜具备二级信息系统安全等级保护资质，视频云平台需具备三级信息系统安全等级保护资质。相关安全防护事项可参考附录E。

8. 自由视角直播：支持1080P/4K的视频信号，生成的内容具备时间＋空间双重自由度，观众可自行滑动、旋转和缩放，实现360°任意观看。旋转视角时，视角之间的切换时延不高于200ms。场馆可通过本地计算服务，实现几十到上百路4K视频的实时编转码。

9. 多视角直播：至少支持2路1080P视频流帧级同步观赛，多机位之间同步误差不超过1帧。能适应网络波动，自动对齐，保证多机位之间的同步。多机位之间视角切换时延不高于200ms。

四、安装部署

（一）标准直播布设

1. 乒乓球场地直播所需拍摄设备最低数量不应少于1个。

拍摄设备侧方距离应不近于2.5米，侧方距离应不远于3米，距地面高度1.5米为宜。

2. 羽毛球、篮球半场及网球场地直播所需拍摄设备最低数量不应少于2个。全景拍摄设备以距球场边线距离不超过1.5米，高度不高于5米为宜；特写拍摄设备以距球场底线距离不低于1.5米，高度不超过1.5米为宜。

3. 篮球全场及三人制足球场地直播所需拍摄设备最低数量不应少于2个。全景拍摄设备距球场边线距离不超过1.5米，高度不高于7米为宜。非全景拍摄设备位于球场周边，以距球场边线、底线距离不大于1.5米，高度不低于2.5米，不高于3.5米为宜。

4. 对于其他类型的场地，可参考上述场地布设方案进行调整。

（二）扩展VR直播布设

1. 乒乓球场地2个VR相机、VR拍摄设备距球台侧方距离2—3米，距地面高度1.3—1.5米。

2. 羽毛球、篮球半场及网球场地VR相机部署2个，距球场双打边线距离3—5米，且与球场中线对齐，高度不低于3—5米。

3. 篮球全场及三人制足球场地VR相机部署4个，VR摄像头距球场边线距离3—5米，高度不低于3—5米。

4. 标准11人制足球场地VR相机至少部署6个，VR摄像头距球场边线距离3—5米，高度不低于3—5米。

5. 其他类型的场地可参考上述场地布设方案进行调整。

（三）自由视角观赛场地布设

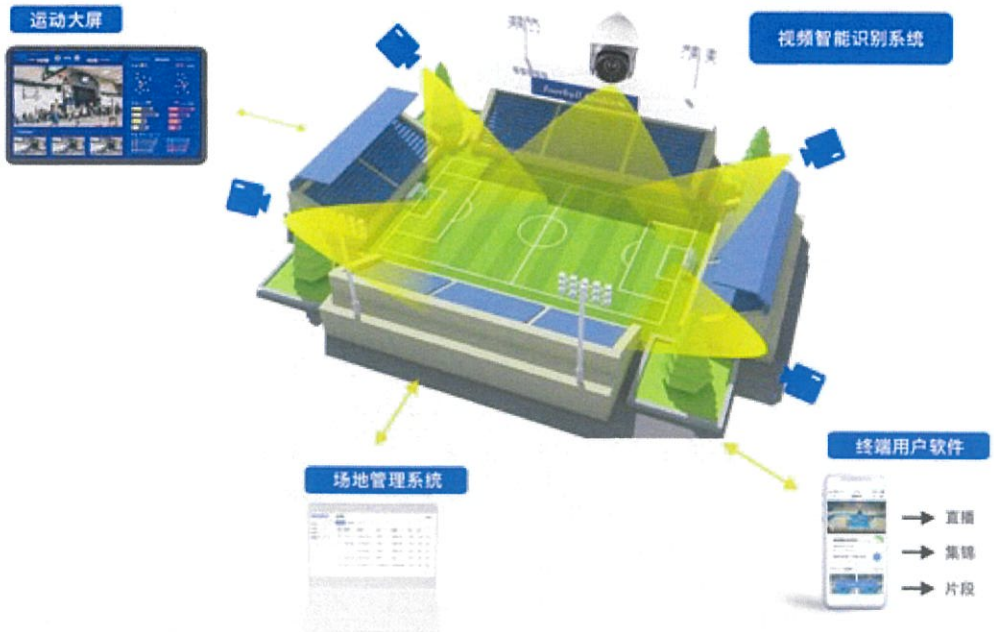
1. 乒乓球、羽毛球、篮球半场、网球场地建议自由视角环形180—360度部署，18—36个相机，相机高度3—5米，相机俯视角度小于15度。

2. 篮球全场、三人制足球场及标准11人制足球场地建议双自由视角部署，上半场和下半场各一个，每个半场36个相机，全场至少72个相机，自由视角自由度在180—240度之间。相机高度根据场地情况确认，相机俯视角度在10—15度之间。

（四）多视角观赛场地布设

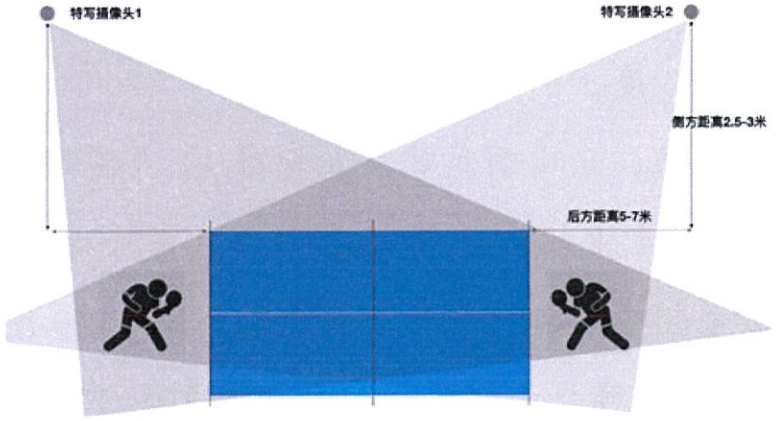
分别从近景、全景、特写等多个不同角度布设相机进行拍摄。以跳水为例，宜从正面、侧面、水底、运动员特写等多个角度部署相机进行拍摄。

附录A　直播系统架构示意图

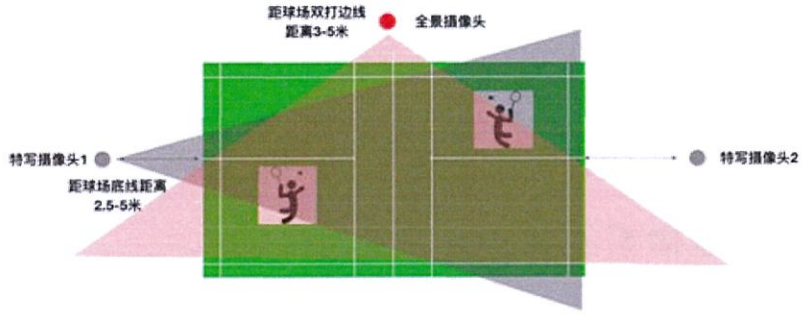


附录 B　标准直播拍摄设备布设建议

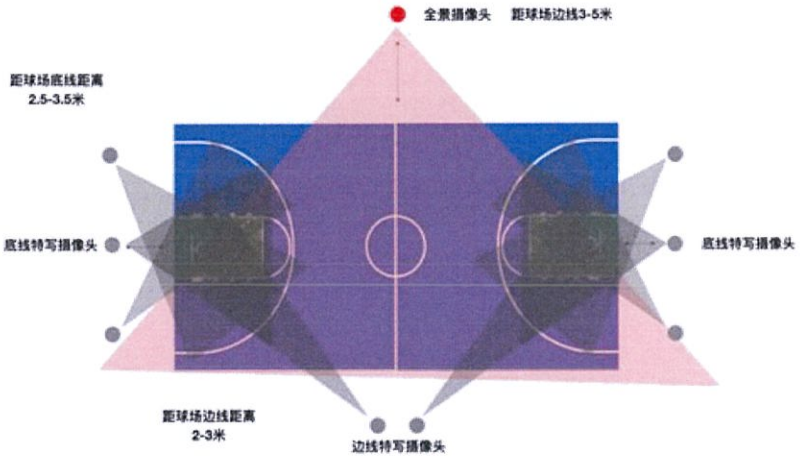
1. 乒乓球场地拍摄设备布设建议：



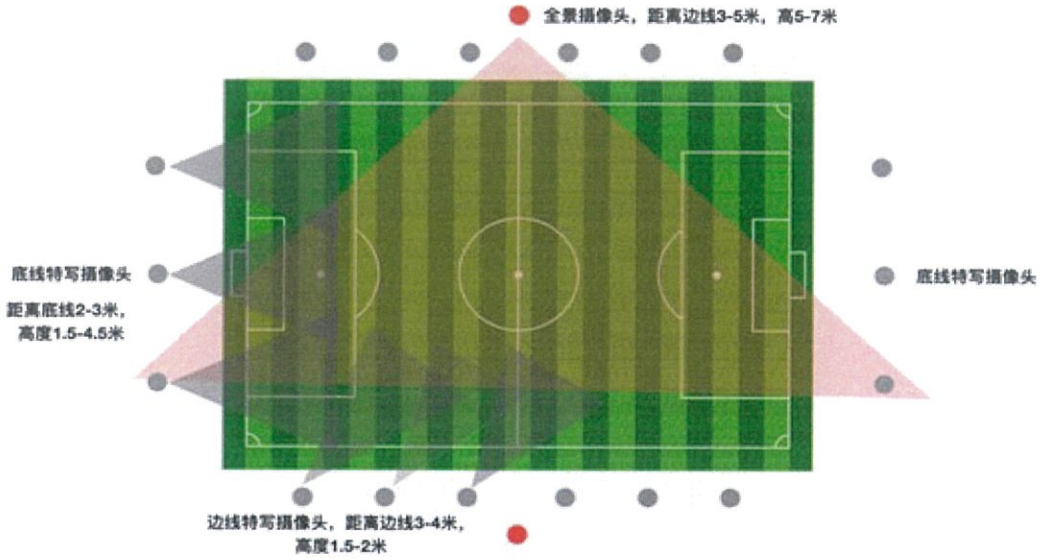
2. 羽毛球、网球球场地拍摄设备布设建议：



3. 篮球场地、三人制足球场地、五人制足球场地拍摄设备布设建议：

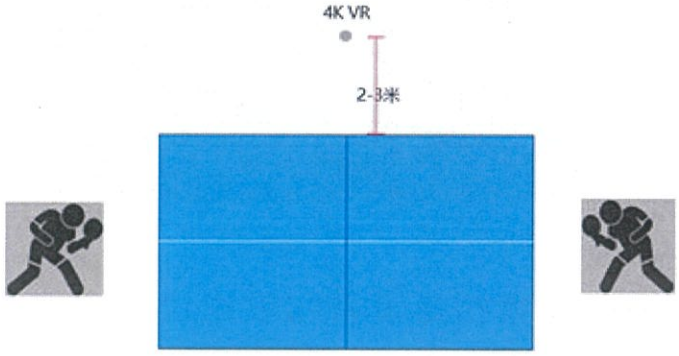


4. 标准 11 人制足球场地拍摄设备布设建议：

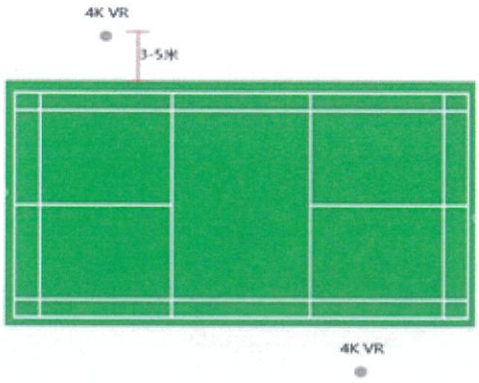


附录 C　VR 直播拍摄设备布设建议

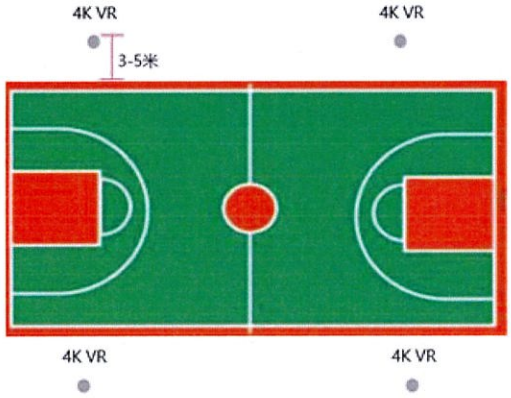
1. 乒乓球场地拍摄设备布设建议：



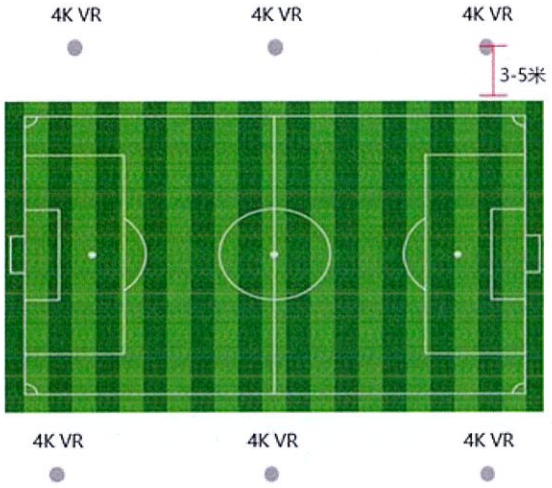
2. 羽毛球场地拍摄设备布设建议：



3. 篮球场地、三人制足球场地、五人制足球场地拍摄设备布设建议：

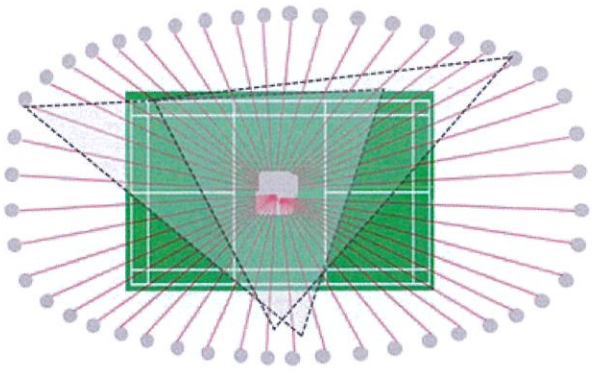


4. 标准 11 人制足球场地拍摄设备布设建议：

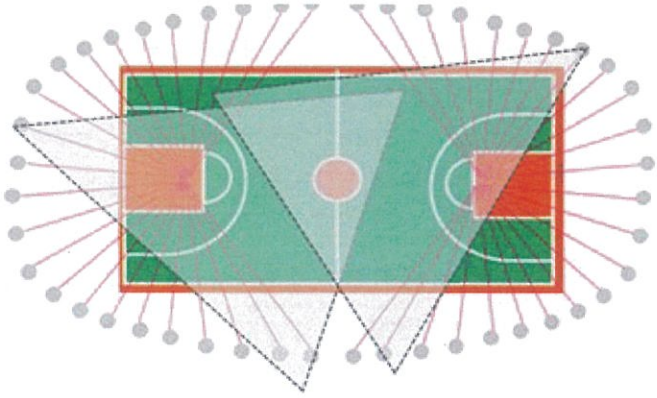


附录 D　自由视角拍摄设备布设建议

1. 羽毛球场地拍摄设备布设建议：



2. 篮球场地拍摄设备布设建议：



附录E　系统安全及用户隐私保护

安全事项		描述
应用层	身份认证	防止弱口令、默认口令导致业务系统管理员、操作员帐号口令被暴力破解，进而避免业务系统被控制。 业务系统口令要加密存储/传输，防止口令被窃取，进而避免业务系统被控制。 要对root用户远程登录做限制，防止root用户帐号密码扩散、泄露，进而避免业务系统被控制。 具备身份认证口令防暴力破解机制，防止业务系统管理员、操作员帐号口令被暴力破解，进而避免业务系统被控制。 具备健全的系统口令管理策略，防止口令泄露或被暴力破解，进而避免业务系统被控制。
	输入验证威胁	对输入数据的类型、长度、格式和范围等做约束和验证，避免缓冲区溢出和XSS攻击。 对用户和系统输入数据进行校验，避免SQL注入及HTTP响应拆分攻击。 来自用户或系统输入的数据在Web页面上输出时进行输出编码，防止跨站脚本攻击。 对文件上传功能所支持的文件类型做限制，防止非法用户向系统上传恶意软件。 对文件上传/下载的路径做限制，防止文件上传、下载目录跨越攻击。

安全事项		描述
应用层	授权威胁	合理的系统权限控制模型，防止不能对用户（管理员、操作员及终端用户）操作进行合理的权限控制，进而避免越权访问攻击。
	敏感数据威胁	系统敏感数据加密存储、传输，防止被非法窃取。
	会话管理威胁	对会话信息进行有效安全保护，防止会话被劫持、会话重放及会话被非法利用等攻击。
	加密技术威胁	选用合适的加密技术，防止加密数据被破解。
	异常处理威胁	异常处理不可向用户返回敏感信息，防止系统、敏感信息泄露。
	安全审计威胁	记录用户操作日志，防止用户否认执行过某项操作。 防止攻击者删除日志文件，避免日志记录丢失。
	内容安全	提供节目防盗观看机制，防止节目被免费盗链观看。 对节目进行加密保护，防止节目被非法复制。
系统安全威胁	主机威胁	防止操作系统、数据库、Web 服务器配置漏洞，避免业务系统被控制。 防止操作系统、数据库、Web 服务器自身漏洞对系统发起攻击，避免控制业务系统。
	足迹威胁	关闭不使用的服务，防止攻击者利用这些服务探查系统信息。配置适当的防火墙策略，防止系统服务、端口暴露给不必要的用户，防止攻击者可利用这些服务的弱点对系统发起攻击。 合理配置操作系统、DB、Web 服务器标示信息，防止系统信息泄露，避免攻击者利用这些信息对系统发起攻击。
	密码破解威胁	避免操作系统、数据库、Web 服务器控制台默认帐号口令或弱口令控制业务系统。 避免操作系统、应用程序用户帐号缺乏帐号锁定机制，防止攻击者可通过暴力破解弱口令获取系统控制权。

安全事项		描述
网络安全威胁	网络设备威胁	避免网络设备自身配置漏洞，防止业务网络被控制。
	足迹威胁	避免网络设备开启了不必要的服务和端口，防止攻击者利用这些服务探查系统信息或对系统发起攻击。
	网络隔离威胁	合理进行网络平面隔离，防止管理平面、信令平面、业务平面任何一个网络平面遭受攻击或出现故障会影响其他两个平面。 合理进行 VLAN 和安全域划分，防止攻击者一旦控制某台主机就可能控制整个业务网络。 进行合理的 ACL 策略配置，防止导致域（安全域）间隔离不彻底，进而导致非法网络访问。
	拒绝服务威胁	对网络设备进行合理安全配置，避免存在如下拒绝服务攻击威胁。 SYN Flood 攻击 UDP 洪水攻击 泪滴（teardrop） 攻击 Land 攻击
管理安全威胁	管理安全威胁	规范的系统账号管理。 版本需经病毒扫描软件扫描，防止携带病毒发布，避免所发布版本作为病毒源在网络上传播病毒。 完整的安全资料，便于支撑安全特性实施。

信息公开选项：主动公开