GD

中华人民共和国广播电视和网络视听行业技术文件

GD/J 119—2020

演播室互动系统的网络安全基本要求

Baseline of network security for studio interactive system

2020－09－28 发布　　2020－09－28 实施

国家广播电视总局科技司　　发布

目　　次

前言 II
引言 III
1　范围 1
2　规范性引用文件 1
3　术语、定义和缩略语 1
3.1　术语和定义 1
3.2　缩略语 1
4　演播室互动系统概述 2
5　系统安全技术要求 2
5.1　安全物理环境 2
5.2　安全通信网络 2
5.3　安全区域边界 3
5.4　安全计算环境 4
6　系统安全管理要求 7
6.1　安全管理制度 7
6.2　安全管理机构 7
6.3　安全管理人员 7
6.4　安全建设管理 8
6.5　安全运维管理 8
参考文献 10

前　言

本技术文件按照GB/T 1.1—2009给出的规则起草。

请注意本文件的某些内容可能涉及专利。本文件发布机构不承担识别这些专利的责任。

本技术文件由国家广播电视总局科技司归口。

本技术文件起草单位：国家广播电视总局广播电视规划院、中央广播电视总台、北京电视台、上海文化广播影视集团有限公司、腾讯科技（北京）有限公司、北京奇安信科技有限公司、北京华云安信息技术有限公司、北京时代远景信息技术研究院有限公司、北京汇智云科技有限公司。

本技术文件主要起草人：肖辉、琚宏伟、邓晖、朱剑、王立冬、李程、王燕青、邵勇、杨君蔚、蒋晓峰、胡恺、常树磊、董升来、赵占永、陈奇、王祥刚、王彦磊、沈传宝、石毅、万会来、张海峰、路琨、李安颖、吕大垒、侯晓雄。

引　言

演播室系统由传统的封闭隔离模式向融合、开放网络接口的方式转变。融合媒体环境下有互联网交互接口、需与观众进行实时互动并播出互动信息的演播室互动系统，将制作域和播出域与互联网连接，在强调互动的同时也带来了安全管理的挑战。为降低网络安全风险，保障核心生产系统的播出安全，需要对其网络安全相关要素进行规范。

演播室互动系统是广播电视媒体通过互动应用程序实现与观众之间信息互动的一种信息处理系统，主要适应节目同用户的信息交互和直播连线互动的业务需求。本技术文件基于2019年发布并实施的GB/T 22239—2019《信息安全技术　网络安全等级保护基本要求》中第三级安全要求对演播室互动系统提出了细化的安全要求，为演播室互动系统的安全运行和管理提供依据。

演播室互动系统网络安全基本要求

1 范围

本技术文件规定了演播室互动系统的网络安全基本要求，主要分为系统安全技术要求和系统安全管理要求两个方面。

本技术文件适用于演播室互动系统网络安全的管理、自评估和运行维护。

2 规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件，仅注日期的版本适用于本文件。凡是不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

GB/T 22239—2019 信息安全技术 网络安全等级保护基本要求

3 术语、定义和缩略语

3.1 术语和定义

下列术语和定义适用于本文件。

3.1.1

演播室互动系统 studio interactive system

在演播现场，通过互动应用程序实现广播电视媒体与场内外观众之间信息互动的一种信息处理系统。

3.1.2

互动信息 interactive date

演播室互动系统存储传输的用户数据、文字图片、声音视频、网页内容等数据信息。

3.1.3

互动准备 interactive preparation

在互动系统开始运行前的系统检查、用户审核、内容分析、视频检测等一系列工作。

3.1.4

互动在线包装 interactive online package

在互动过程中，将图像、图形、图表、文字、数据、视频、虚拟等信息，在直播、准直播或录播时实时生成输出信号的包装合成过程。

3.2 缩略语

下列缩略语适用于本文件。

APP　应用程序（Application）
CPU　中央处理器（Central Processing Unit）
HTTPS　超文本传输安全协议（Hyper Text Transfer Protocol over SecureSocket Layer）
IP　网际互连协议（Internet Protocol）
SDI　数字分量串行接口（Serial Digital Interface）

4　演播室互动系统概述

典型的演播室互动系统主要包括用户互动客户端软件、互动信息汇聚/交互模块、互动准备模块、互动在线包装模块、演播室展现设备及相关网络传输和安全设备等，基于网络系统之间逻辑关联性、物理位置、功能特性，划分为互联网域、安全交换域、演播域，互联网域包括互动客户端软件，安全交换域包括互动信息汇聚/交互模块，演播域包括互动准备模块、互动在线包装模块、演播室展现设备。本技术文件适用的演播室互动系统框架图见图1（图中实线箭头为IP信号，虚线箭头为SDI信号）。

典型的演播室互动业务模式主要包括以下两种：

a）　演播室互动系统的信息互动模式是用户通过微信、微博、互动APP、互动网站等渠道，将互动信息发送到互动信息汇聚/交互模块，经过安全检测后传送到互动准备模块，由互动在线包装模块处理后进入演播室播出流程；

b）　演播室互动直播连线模式是用户通过互动专用客户端，将实时采集的音视频信号经过安全交换域回传到互动准备模块，由互动在线包装模块处理后或直接进入演播室播出流程。

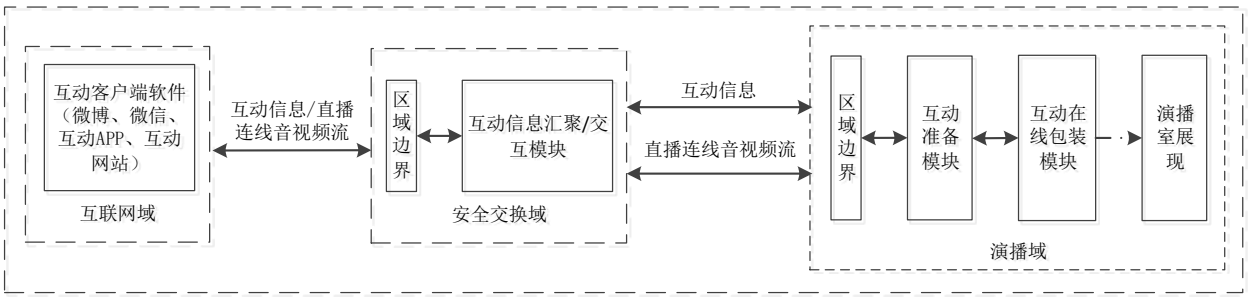

图1　演播室互动系统框架图

5　系统安全技术要求

5.1　安全物理环境

应遵循GB/T 22239—2019中8.1.1对安全物理环境进行管理的要求。

5.2　安全通信网络

5.2.1　网络架构

网络架构应至少满足如下要求：

a）　应保证网络设备的业务处理能力满足互动演播业务高峰期需要；

b）　应保证接入网络和核心网络的带宽满足互动演播业务高峰期需要；

c）　应将允许外部公开直接访问的互动信息汇聚/交互模块，划分在单独的安全交换域中或与演播室网络逻辑隔离的子网络上；

d） 在重要活动保障期应提供不同路由的互联网双链路接入保障。

5.2.2 通信传输

通信传输应至少满足如下要求：

a） 对互动客户端软件和系统之间传输的敏感信息（如账号口令等）应加密后再传输。

b） 演播室互动系统中除演播业务功能需求的情况下，所有设备和工作站宜禁止无线网络功能，当演播域中演播业务需要使用无线网络功能时，应在满足业务需求的前提下，使用指定设备开放最低程度的无线网络功能，并开启无线网络安全保护措施；安全措施包括但不限于控制无线信号的范围和频段、采用用户名口令或者白名单技术限制未授权设备接入该无线网络。

c） 应保证互动客户端安装、运行的互动应用软件由指定的开发者开发，并对开发者进行资格审查。

d） 应保证开发互动业务应用软件的签名证书合法性。

e） 系统中使用的密码产品与服务，应保证密码产品与服务通过国家密码管理部门核准。

5.3 安全区域边界

5.3.1 边界防护

边界防护应至少满足如下要求：

a） 在互动信息汇聚/交互模块和互动准备模块直接相连的关键边界上，应对网络通信进行监控；

b） 在与外部网络或信息系统连接的互动信息汇聚/交互模块的外连接口上，应部署边界安全保护设备；

c） 在安全交换域中应部署针对应用层防护的安全保护设备,防止诸如SQL注入、跨站攻击、溢出攻击等恶意行为，对非法输入进行明确的错误提示并告警。

5.3.2 安全审计

安全审计应至少满足如下要求：

a） 应在网络边界、重要网络节点进行安全审计，审计覆盖到每个系统用户，对重要的用户行为和重要安全事件进行审计；

b） 演播室互动系统可审计事件至少应包括：账号登录、账号管理、客体访问、策略变更、特权功能和系统事件等；

c） 审计记录项目应至少包括：事件类型、事件发生的时间和地点、事件来源、事件结果及与事件相关的用户或主体的身份；

d） 审计记录应至少保存六个月；

e） 对系统发生审计过程失败的情况，应制定相应告警机制；

f） 应定期完成审计分析报告，报告内容至少包括：演播室互动系统安全状态整体描述、审计中发现的异常及处置情况、系统远程访问的总体情况及统计分析等；

g） 系统审计信息和审计工具应受到保护，防止非授权访问、篡改和删除；

h） 应对审计记录进行保护，避免受到未预期的删除、修改或覆盖等。

5.3.3 访问控制

访问控制应至少满足如下要求：

a） 应在网络边界或区域之间根据访问控制策略设置访问控制规则，默认情况下应拒绝所有通信，除非明确允许，否则就禁止；

b) 应删除多余或无效的访问控制规则，优化访问控制列表，并保证访问控制规则数量最小化；
c) 应对源地址、目的地址、源端口、目的端口和协议等进行检查，以允许/拒绝数据包进出；
d) 应能根据会话状态信息对数据流进行明确的允许/拒绝访问控制，控制粒度为端口级；
e) 应确保互动信息汇聚/交互模块与互动准备模块在逻辑层面实现网络隔离与单向访问，只允许互动准备模块主动连接汇聚服务器获取数据，不允许汇聚服务器反向主动连接。

5.4 安全计算环境

5.4.1 身份鉴别

5.4.1.1 演播室互动系统身份鉴别

演播室互动系统身份鉴别应至少满足如下要求：
a) 对演播室互动系统用户账号应进行唯一标识和鉴别，身份鉴别信息具有复杂度要求并定期更换；
b) 演播室互动系统的客户端及管理终端接入系统前，应对该终端进行唯一性标识和鉴别，如利用设备IP地址、MAC地址、智能终端识别码等进行标识；
c) 对直播连线模式应确保参与互动的账号是通过本系统或符合要求的实名认证的账号,才允许向系统发送连线请求信息；
d) 对系统特权账号和视频直播连线账号的访问应采用密码技术结合口令、生物技术等两种以上组合的鉴别技术进行身份鉴别。

5.4.1.2 互动客户端身份鉴别

互动客户端身份鉴别应至少满足如下要求：
a) 互动客户端应对访问账号提供有效的身份认证机制，在访问互动业务前，客户端软件应对终端账号身份进行鉴别；
b) 互动客户端应防止鉴别信息在网络传输过程中被窃听；
c) 互动客户端用户账号登录应提供鉴别失败处理措施，应配置并启用结束会话、限制非法登录次数；
d) 互动客户端用户账号登录应具备登录超时后的锁定或注销功能；
e) 应强制用户账号首次登录互动客户端应用时修改初始口令；
f) 用户身份鉴别信息丢失或失效时，应采用鉴别信息重置或其他技术措施保证系统安全；
g) 互动客户端的用户账号口令在使用过程中不应以明文形式显示和存储,并具备口令复杂度检查机制和修改或找回口令的验证机制；
h) 用户账号登录入口应具备防暴力破解能力。

5.4.2 访问控制

5.4.2.1 演播室互动系统访问控制

演播室互动系统访问控制应至少满足如下要求：
a) 应分配个人账号，设置最小权限；
b) 应重命名系统默认账号或修改这些账号的默认口令，不允许匿名用户登录；
c) 应定期检查用户账户使用情况，及时删除或停用多余的、过期的账号，避免共享账号的存在；
d) 应授予管理用户所需的最小权限，实现管理用户的权限分离；

e） 对演播室互动信息汇聚/交互模块的管理端口或地址，应限制从互联网远程访问，对系统管理的连接实施监视，在发现非授权连接时，应立即进行应急处置；
f） 应对演播室互动直播准备模块远程执行特权命令进行限制（如互动信息上屏、直播连线上屏等），应由操作人员在服务器本地执行；
g） 应明确由授权人对演播室互动系统用户、角色或设备的标识符进行设定、分配或禁用操作，并防止标识符的重用。

5.4.2.2 互动客户端访问控制

互动客户端访问控制应至少满足如下要求：
a） 从互动信息汇聚/交互模块向互动准备模块传送互动信息过程中，应能对互动信息中的有害信息和垃圾信息进行自动识别和过滤，并能对指定来源信息设置黑、白名单；
b） 使用互动客户端发送互动信息时，除了文字、图片和音视频之外禁止传输其他类型文件；
c） 互动信息上传到演播室大屏前，应通过互动准备模块操作人员的人工审核后方可进行；
d） 对互动客户端软件的接入制定访问控制策略。

5.4.3 安全审计

5.4.3.1 演播室互动系统安全审计

演播室互动系统安全审计应至少满足如下要求：
a） 演播室互动系统应启用安全审计功能，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计；
b） 审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息；
c） 应对审计记录进行保护，避免受到未预期的删除、修改或覆盖等。

5.4.3.2 互动客户端安全审计

应确保每条回传到系统的互动信息与其用户的安全属性（如账号等）相关联，以保障信息的安全溯源和审计。

5.4.4 入侵防范

入侵防范应至少满足如下要求：
a） 应遵循最小安装的原则，仅安装需要的组件和应用程序；
b） 应关闭不需要的系统服务、默认共享和高危端口；
c） 应通过设定终端接入方式或网络地址范围对需要接入系统的终端进行限制；
d） 应能发现可能存在的漏洞，并在经过充分测试评估后，及时修补漏洞；
e） 应对互动信息汇聚/交互模块进行安全加固，提高互动信息汇聚/交互服务的安全性。

5.4.5 恶意代码防范

恶意代码防范应至少满足如下要求：
a） 应采用白名单、黑名单或其他方式，在互动信息汇聚/交互模块所在网络出入口上实施恶意代码防护机制；
b） 应安装防恶意代码软件或配置具有相应功能的软件，建立相应维护机制，确保恶意代码库及时更新；

c) 应配置恶意代码防护机制每日定期扫描消息汇聚模块，当检测到恶意代码后立即执行阻断或隔离恶意代码，并向管理员通告；
d) 在互动活动开始前，演播室互动或网络直播相关的管理终端和存储介质，应进行恶意代码扫描，确认无风险后再与互动系统或设备连接。

5.4.6 资源控制

5.4.6.1 演播室互动系统资源控制

演播室互动系统资源控制应至少满足如下要求：
a) 应限制单个用户或进程对演播室互动系统资源的最大使用限度；
b) 应对演播室互动系统重要服务器的运行状态、CPU使用率、内存使用率、应用联网及带宽等情况进行监控；
c) 应对演播室互动系统数据库的运行状态、进程占用CPU时间及内存大小、配置和告警数据等进行监控；
d) 应对演播室互动系统重要应用软件的运行状态、响应时间等进行监控。

5.4.6.2 互动客户端资源控制

互动客户端资源控制应至少满足如下要求：
a) 应能够对互动客户端的最大并发会话连接数进行限制；
b) 应能够对单个账号的多重并发会话进行限制。

5.4.7 虚拟化安全

虚拟化安全应至少满足如下要求：
a) 应提供实时的虚拟机监控机制，通过带内或带外的技术手段对虚拟机的运行状态、资源占用、迁移情况等信息进行监控；
b) 应确保虚拟机的镜像安全，提供虚拟机镜像文件的完整性校验功能；
c) 支持不同应用场景间的物理资源与虚拟资源、虚拟资源与虚拟资源之间的安全隔离；
d) 提供虚拟化平台操作管理员权限分离机制，设置网络管理、账号管理、系统管理等不同的管理员账号；
e) 应对虚拟机网络接口的带宽进行管理；
f) 逻辑或物理存储体应受到存储数据安全控制的监控和保护；
g) 将虚拟化平台的各类操作和事件作为可审计源，进行记录和追溯；
h) 应保证平台的管理流量与业务流量分离；
i) 应能识别和监控虚拟机之间、虚拟机与物理机之间、虚拟机与宿主机之间的流量；
j) 应保证本系统的计算资源池与其他无关计算资源池之间的隔离；
k) 应避免虚拟机通过网络非授权访问宿主机，并依据安全策略控制虚拟机间的访问；
l) 当进行远程管理时，管理终端和虚拟化平台边界设备之间应建立双向身份验证机制。

5.4.8 内容检测

内容检测应至少满足如下要求：
a) 对汇聚的互动信息内容，应能对有害信息和视频进行识别和过滤，并将有害内容自动隔离；
b) 对于跨功能域边界的互动数据，需要进行完整性校验，避免传输过程中的数据丢失或篡改。

5.4.9 软件容错

软件容错应至少满足如下要求：

a) 互动客户端应用软件应提供数据有效性检验功能，保证通过人机接口输入或通信接口输入的数据长度、格式、范围、数据类型等符合设定要求；
b) 互动直播连线期间发生信号中断时，应能检测并切换到演播室垫播信号或应急信号；
c) 演播室互动系统应采用缓存技术、完整性校验和恢复技术降低互动直播连线音视频传输的误码率；
d) 互动客户端应用软件应提供自动保护功能，当故障发生时保证数据不丢失。

5.4.10 数据备份恢复

数据备份恢复应至少提供演播室互动系统重要数据的本地数据备份与恢复功能。

5.4.11 剩余信息保护

当互动客户端软件卸载时，用户鉴别信息所在的存储空间应保证被释放或重新分配前得到完全清除。

6 系统安全管理要求

6.1 安全管理制度

系统安全管理制度应至少满足如下要求：

a) 应制定演播室互动系统网络安全规章制度，覆盖物理、网络、主机系统、数据、应用和管理等层面，并发布至内外部相关人员；
b) 在网络安全策略或计划发生变更时，应评审和更新网络安全规章制度，以确保其持续适用和有效；
c) 应对系统管理员建立操作规程和管理规定；
d) 应建立监督机制以检查和确保网络安全规章制度的落实情况。

6.2 安全管理机构

系统安全管理机构应至少满足如下要求：

a) 应设立安全岗位，如安全管理员，明确岗位职责，并由该岗位负责人负责与网络安全管理部门沟通协调，对其进行安全意识教育和岗位技能培训；
b) 应根据各个部门和岗位的职责明确授权审批部门及批准人，对系统投入运行、网络系统接入和重要资源的访问等关键活动进行审批，并保存关键活动的审批过程记录。

6.3 安全管理人员

安全管理人员应至少满足如下要求：

a) 应指定专人负责操作演播室互动信息发布和直播连线的信号切换，并对该人员进行安全操作和安全意识培训，确保发布的互动信息内容安全；
b) 安全管理员应对演播室互动系统网络安全资源需求进行详细分析，并确保这些资源的可用性；
c) 人员离职后应立即禁止该人员对系统的访问，终止或撤销该人员的身份鉴别凭证，收回该人员所有涉及安全的本机构相关资产；
d) 第三方供应商（如服务组织、合同商、系统开发商、集成商等）应具有人员安全管理要求，包括安全角色和责任，要求第三方供应商遵守本机构的人员安全策略与管理规程。

6.4 安全建设管理

应遵循 GB/T 22239—2019 中 8.1.9 对安全建设管理进行管理的要求。

6.5 安全运维管理

6.5.1 运维操作安全

运维操作安全应至少满足如下要求：

a) 应编制并保存演播室互动系统资产清单，包括资产责任部门、重要程度和使用人等内容，并根据资产的重要程度对移动终端进行标识管理，根据其价值选择相应的管理措施；
b) 应根据运行维护计划进行检查和记录，并对维护记录进行审查；
c) 应审批和监视所有维护行为，包括现场维护、远程维护；
d) 在对系统组件进行维护或维修后，应检查所有可能受影响的安全措施，以确认其仍正常发挥功能；
e) 在维护记录中，至少应包括：维护日期和时间、维护人员姓名、陪同人员姓名、维护活动描述、被转移或替换的设备列表等信息；
f) 应对维护工具的使用进行审批、控制和监视，确保维护工具未被非授权使用；
g) 应建立对维护人员的授权流程，并对已获得授权的人员建立列表；
h) 确保只有列表中的维护人员才可在陪同人员的监管下开展维护活动；
i) 应定期对系统的安全功能实施验证，验证失败时通知安全管理员；
j) 应建立完整性评估流程，确保系统的软件、固件和信息的完整性，并具备检测系统软件非授权更改的能力；
k) 演播室互动客户端软件应支持更新，至少采取一种安全机制，保证升级的时效性和准确性，并保证终端应用软件安全机制的有效性。

6.5.2 配置管理安全

配置管理安全应至少满足如下要求：

a) 应按照演播室互动系统配置要求制定、记录并维护系统的基线配置；
b) 当系统重新安装、更新系统组件、发生重大变更时，应重新审查和更新系统基线配置，以便必要时恢复配置；
c) 应明确需要定期变更的受控配置列表，并每周对病毒库、入侵检测规则库、防火墙规则库、漏洞库等网络安全相关重要配置项进行更新；
d) 应保留系统中受控配置的变更记录；
e) 对系统实施变更之前，应对受控配置变更项进行测试、验证和记录；
f) 应限制系统开发方和集成方对生产环境中信息系统依赖的硬件、软件和固件进行直接变更。

6.5.3 远程维护安全

远程维护安全应至少满足如下要求：

a) 应禁止系统远程运维管理策略，信息系统和各类终端设备禁止开通互联网远程控制权限，严禁私自安装远程控制类软件。
b) 针对系统运维，原则上只允许通过安全认证的运维终端通过堡垒主机对后台服务器进行操作，不允许运维终端直接访问后台服务器。
c) 如确因工作原因，需要互联网远程控制权限或安装远程控制软件的，开通前应报网络安全管理部门审批同意，在使用过程中加强对远端设备操作行为的管理和监控，在建立远程维护和诊断

会话时应采取强鉴别技术，保存相应活动记录并定期进行审计和审查。工作任务完成后及时关闭，并再次将相关情况通知网络安全管理部门。对于存在外部控制或认证中心的特殊互动系统，须由该设备提供商或服务提供商提供对设备使用期间的审计记录和日志，以备检查。

6.5.4 安全事件处置

安全事件处置应至少满足如下要求：

a) 应制定安全事件报告和处置管理制度，明确不同安全事件的报告、处置和响应流程，规定安全事件的现场处理、事件报告和后期恢复的管理职责等；

b) 应在安全事件报告和响应处理过程中，分析和鉴定事件产生的原因，收集证据，记录处理过程，总结经验教训。

6.5.5 应急预案管理

应急预案管理应至少满足如下要求：

a) 应制定演播室互动系统的应急预案和应对不同安全事件的专项预案，并每年至少进行一次演练；

b) 应制定安全事件处理计划，并对安全事件进行监控和报告；

c) 应对系统操作人员进行应急响应培训，并在演播室互动系统有重大变更时，重新开展培训。

参 考 文 献

[1] GD/J 037—2011 广播电视相关信息系统安全等级保护定级指南
[2] GD/J 038—2011 广播电视相关信息系统安全等级保护基本要求
[3] 新闻出版广播影视网络安全管理办法（试行）（新广办发[2017]4号）