广播电视播出安全与技术维护探析

闵　亮
重庆广播电视集团（总台）　重庆　401147

摘　要： 随着广播电视行业的不断发展，播出安全与技术维护成为确保其稳定运行的关键。本文深入分析了广播电视播出的特点，包括其作为主流媒体的舆论导向作用、制作与播出的复杂性，以及传播速度快、覆盖范围广等优势。同时，探讨了技术维护在保障播出安全中的基础作用及面临的挑战。在此基础上，提出了加强技术研发、完善管理制度、提升技术人员素质、加强行业合作等策略，旨在为广播电视行业的播出安全与技术维护提供有效保障。

关键词： 广播电视；播出安全；技术维护

引言：广播电视作为信息传播的重要渠道，其播出安全不仅关乎媒体公信力，更直接影响社会稳定与公共安全。随着技术的飞速发展，广播电视系统日益复杂，播出过程中的安全威胁与技术挑战也随之增多。本文旨在深入探析广播电视播出安全与技术维护的现状与需求，通过综合分析播出特点、技术挑战及维护策略，为构建安全、高效、可靠的广播电视播出体系提供理论依据与实践指导，促进广播电视事业的健康可持续发展。

1 广播电视播出安全概述

1.1 广播电视播出的特点

（1）舆论导向作用：广播电视作为主流媒体，承担着引导社会舆论、传播核心价值观的重要职责。其节目内容直接影响公众认知和社会思潮，在重大事件、政策解读等方面具有不可替代的导向功能，是维护社会稳定、凝聚社会共识的关键载体。（2）制作与播出的复杂性：广播电视节目制作涉及策划、采访、拍摄、编辑、审核等多个环节，每个环节都需专业团队协作完成。而播出过程更是依赖复杂的技术系统，包括信号传输、设备运行、应急调度等，任何环节的疏漏都可能影响播出质量，甚至导致播出中断。（3）传播速度快、覆盖范围广：借助无线、有线、卫星等传输手段，广播电视信号能在瞬间覆盖广泛区域，从城市到乡村、从国内到海外，实现信息的快速扩散。这种特性使其在突发新闻发布、公共信息传递等方面具有显著优势，能在短时间内让海量受众获取信息[1]。

1.2 播出安全的含义与内容

（1）节目播放过程中不受恶意篡改与破坏：播出安全首先要求节目信号在传输和播放环节保持完整性，防止被黑客攻击、信号劫持等恶意行为篡改内容或插入非法信息。这需要建立严密的技术防护体系，保障播出系统的物理安全和网络安全。（2）确保信息传输的安全与顺畅：信息传输的稳定性是播出安全的基础，需通过冗余备份、故障预警、应急抢修等措施，避免因设备故障、自然灾害等因素导致信号中断或衰减。同时，要保障传输过程中的信息保密性，防止信号被非法截取或泄露。（3）节目内容符合审核标准，具有社会正能量：播出安全不仅涉及技术层面，还包括内容层面的安全。所有节目必须经过严格审核，确保符合国家法律法规和社会公序良俗，杜绝暴力、低俗、虚假等不良内容，传播积极向上的社会正能量，维护健康的文化传播环境。

2 广播电视技术维护的重要性与挑战

2.1 技术维护在保障播出安全中的基础作用

（1）设备安全与维护：广播电视播出依赖发射机、服务器、切换台等大量专业设备，技术维护通过定期巡检、性能测试、故障排查，确保设备处于稳定运行状态。例如，对发射设备进行功率校准，可避免信号失真；及时更换老化部件，能预防突发停机，从硬件层面筑牢播出安全防线。（2）传输系统安全与稳定性：传输系统是连接节目源与受众的关键链路，技术维护通过优化信号路由、部署冗余传输线路、建立实时监控系统，保障信号传输的连续性。当主传输链路出现中断时，维护系统能快速切换至备用链路，将信号中断时间压缩至秒级，最大限度减少对播出的影响。（3）节目内容的审核与播出安全：技术维护为内容审核提供技术支撑，如搭建智能审核平台，通过AI算法自动识别违规画面或音频，辅助人工审核提高效率。同时，维护播出系统的权限管理机制，防止未审核内容被误播出，确保最终呈现给受众的节目符合安全标准[2]。

2.2 新型广播电视技术带来的挑战

（1）数字化、信息化技术的发展：传统模拟信号向数字信号转型后，技术系统对网络的依赖性增强，面临黑客攻击、病毒入侵等网络安全风险。同时，数字化设

备的更新迭代速度加快，要求技术维护人员不断学习新知识，适应新技术环境。（2）传输系统及播控系统的复杂性增加：融合媒体时代，播控系统需兼容传统广播电视、IPTV、移动端等多平台播出需求，系统架构从单一封闭走向开放互联，技术接口增多，故障排查难度显著提升，对维护人员的综合技术能力提出更高要求。（3）传输容量的快速增加与传输手段的多样化：4K/8K超高清、VR等技术推动节目数据量呈指数级增长，传输容量需求激增。而卫星、光纤、5G等多样化传输手段，虽提升了覆盖能力，但也导致技术维护需应对不同传输协议、不同设备标准的适配问题，维护成本和复杂度大幅上升。

3 广播电视播出安全的技术维护措施

3.1 制定完善的安全播出管理制度

（1）涵盖设备、人员、网络、节目内容等多方面的管理制度。需构建全流程管理制度体系：设备管理明确采购标准、使用规范及报废流程；人员管理规范岗位职责与操作权限；网络管理设定接入控制与数据加密规则；内容管理制定审核标准与责任追溯机制。通过制度细化各环节要求，形成“人人有职责、事事有规范”的管理闭环。（2）建立应急响应机制，确保快速处理突发事件。制定分级应急预案，明确信号中断、黑客攻击等不同级别事件的处置流程。组建专业应急团队，配备应急设备与通讯工具，定期开展实战演练。建立跨部门联动机制，与技术厂商、监管部门保持实时沟通，确保突发事件发生时能快速响应、协同处置，将播出中断时间控制在最短范围内。

3.2 加强设备的安全管理与维护

（1）日常保养与定期检查。每日对播出设备进行外观检查与参数监测，及时清理灰尘、调整散热装置；每周开展线路连接与接口稳定性检测；每月对电源系统、存储设备等关键部件进行性能评估。建立设备维护台账，详细记录检查结果与维修情况，为设备更换提供数据支撑。（2）关键设备的冗余备份与故障切换。对发射机、主备服务器等核心设备采用“一主一备”或“多机热备”模式，通过同步技术确保主备设备数据实时一致。配置智能切换系统，当主设备出现异常时，自动触发切换机制，保障信号无缝衔接。每月进行人工切换测试，验证备份系统的可靠性。（3）加强对播出机房、制作机房等重点部门的安全检查。实施物理隔离管理，机房入口设置门禁系统与24小时监控，仅限授权人员进入。定期检查机房温湿度、消防设施及供电稳定性，配备UPS不间断电源应对突发断电。每周排查线路布局与设备摆放，避免线路杂乱引发短路或信号干扰[3]。

3.3 提升传输系统的安全性

（1）防御恶意攻击与非法信号干扰。部署防火墙与入侵检测系统，对网络流量进行实时过滤；采用信号加密技术，防止传输内容被篡改或窃取。安装干扰监测设备，一旦发现异常信号，立即启动屏蔽装置并定位干扰源，联合相关部门快速处置。（2）建立传输系统监控与报警机制。搭建集中监控平台，实时采集传输链路的信号强度、带宽占用等数据，设置多级预警阈值。当指标超出正常范围时，通过声光报警、短信通知等方式同步推送信息，确保维护人员15分钟内响应。对高频预警点进行专项排查，从源头解决隐患。（3）优化传输网络，提升传输效率与稳定性。采用光纤为主、卫星为辅的混合传输模式，减少单点故障影响。定期清理网络冗余节点，升级老旧传输设备，将信号延迟控制在毫秒级。通过负载均衡技术合理分配网络资源，避免高峰期拥堵，保障超高清节目等大流量内容的稳定传输。

3.4 加强节目内容的审核与监管

（1）建立节目内容审核流程与标准。实行“三审三校”制度，初审聚焦政治导向与法律法规，复审核查文化内涵与社会影响，终审确认技术指标与播出规范。针对新闻、综艺等不同类型节目制定差异化标准，明确禁播内容清单与边界条款。（2）利用技术手段加强节目内容的监控。引入AI审核系统，通过关键词识别、画面分析等技术自动筛查违规内容，将人工审核效率提升50%以上。对直播节目实施“延迟播出”机制，预留3-5分钟缓冲时间，便于发现问题后及时切断信号。（3）对违规节目内容进行及时处理与通报。发现违规内容立即停播并启动回溯机制，排查问题环节与责任人员。建立违规案例库，定期通报典型案例，组织全员学习。对重大违规事件实行“一票否决”，追究相关部门与个人责任，形成刚性约束。

4 完善广播电视播出安全与技术维护的建议

4.1 加强技术研发与创新

（1）引进与自主研发相结合，提升技术水平。在技术发展中需平衡引进与自主创新的关系，有针对性地引进国际领先的智能播控系统、抗干扰传输设备等，快速填补技术空白。同时，设立专项研发基金，联合高校实验室、科技企业攻关核心技术，如研发具有自主知识产权的信号加密算法、超高清节目容错传输技术等。通过“引进吸收+自主突破”的模式，构建覆盖信号采集、传输、播出全链条的技术体系，实现从“跟跑”到“领跑”的跨越。（2）针对新型攻击手段进行防范技术研究。成立专项研

究小组，密切跟踪网络攻击技术的迭代趋势，重点分析AI深度伪造、分布式拒绝服务攻击（DDoS）等新型威胁的原理与特征。研发适配性防御技术，如基于区块链的内容溯源系统、智能异常流量识别算法等，构建动态防御体系。定期开展攻防演练，检验新技术的实战效能，确保防御能力与攻击手段同步升级[4]。

4.2 完善管理制度与应急预案

（1）建立健全的播出安全管理制度体系。构建“横向到边、纵向到底”的制度网络，横向覆盖设备采购、人员管理、内容审核等全环节，纵向细化从高层管理到一线操作的权责划分。引入风险管理理念，对各环节进行安全评估，针对高风险点制定专项管控措施。建立制度执行督查机制，每月开展合规检查，对违规行为严肃追责，确保制度落地见效。（2）制定详细、可行的应急预案与处置流程。按“一般、较大、重大”三级事件划分预案等级，明确不同等级事件的响应时限、处置权限与资源调配方案。预案内容需具体到操作步骤，如信号中断时的设备切换指令、黑客入侵时的系统隔离路径等。每季度组织跨部门联合演练，模拟极端场景，根据演练结果优化流程，确保预案具备“拿来即用”的实操性。

4.3 提升技术人员素质与能力

（1）加强技术培训与考核。构建“基础+进阶+专家”的三级培训体系，基础培训针对新入职人员，涵盖设备操作规范与安全基础知识；进阶培训面向在岗人员，重点讲解5G融合传输、IP化播出等新技术；专家培训选拔骨干人员，邀请行业顶尖专家开展攻防实战教学。实行“月度考核+年度认证”制度，考核内容包含理论知识与实操能力，考核不合格者暂停上岗资格，直至补考通过。（2）鼓励技术人员进行自主学习与交流。搭建内部技术分享平台，每周组织“故障案例复盘会”，由技术人员轮流主讲处置经验。设立学习奖励基金，对考取CCIE（思科认证互联网专家）、注册信息安全专业人员等资质的员工给予补贴。每年选派20%的技术骨干参加国际广播电视技术峰会，与国外同行交流前沿技术，建立行业人脉网络，促进技术视野拓展。

4.4 加强行业合作与信息共享

（1）建立行业联盟，加强技术交流与合作。由国家广电总局牵头，组建包含中央级、省级、地市级广电机构及华为、中兴等技术企业的播出安全联盟，设立年度技术合作专项资金。联盟内开展“技术难题众筹攻关”，如联合开发适配不同地区信号标准的统一监测平台；定期举办“攻防演练大赛”，模拟新型攻击场景检验防护能力；共享技术专利池，降低中小机构的研发成本。（2）共享安全事件信息与处理经验，提升整体防范能力。建立全国广播电视安全事件共享平台，要求各机构在事件发生后2小时内上报基本情况，24小时内提交详细处置报告。平台定期汇总分析数据，发布月度安全态势报告，标注高发攻击区域与时段。每半年召开行业安全论坛，选取典型案例进行深度剖析，如某地信号被干扰的72小时处置过程，形成可复制的解决方案，推动全行业安全防护能力协同提升。

结束语

综上所述，广播电视播出安全与技术维护是确保信息传播准确性和时效性的基石。面对日益复杂的技术环境和安全挑战，我们必须不断创新技术手段，完善管理制度，提升人员能力，加强行业内外合作。只有这样，才能构建起坚不可摧的播出安全防线，保障广播电视节目的顺利播出，满足人民群众的多元化信息需求。未来，广播电视行业应继续致力于技术革新与安全维护，为社会的和谐稳定与文化的繁荣发展贡献力量。

参考文献

[1]谢丽华.浅谈广播电视安全播出技术维护管理策略[J].中小企业管理与科技(上旬刊),2020,(04):48-49.

[2]冯青松.大数据时代的广播电视安全播出技术分析[J].西部广播电视,2020,(07):72-73.

[3]黄若轩.广播电视安全播出技术维护管理对策分析[J].新闻研究导刊,2020,(08):87-88.

[4]高岩.简述新时期广播电视安全播出技术的运用[J].电视技术,2020,(10):103-104.