

新技术时代广播电视播控技术及安全维护

童晓渊

杭州华数传媒电视网络有限公司紫荆分公司 浙江 杭州 310008

摘要: 本文聚焦新技术时代,深入剖析广播电视播控技术及安全维护。先阐述播控技术架构,涵盖信号源、制作、播出、传输与接收系统,点明信号处理、网络传输等核心技术。接着强调播控系统安全维护的重要性,如保障信息传播、维护媒体公信力等。随后分析面临的网络安全、数据安全等挑战。最后从网络安全防护、数据安全、系统稳定性维护以及人员培训等方面提出全面的安全维护策略,旨在为广播电视行业在新技术背景下的安全稳定发展提供理论与实践指导。

关键词: 新技术时代; 广播电视; 播控技术; 安全维护

引言: 在科技飞速发展的当下,广播电视行业迎来了新技术时代。5G、云计算、大数据等技术的融入,让广播电视播控技术发生了深刻变革。播控系统架构不断优化,核心技术持续升级,为节目制作、播出与传输带来了更高的效率和更好的体验。然而,技术的进步也带来了诸多安全隐患。网络攻击、数据泄露等问题频发,严重威胁着广播电视播控系统的安全稳定运行。

1 广播电视播控技术的架构与核心技术

1.1 播控技术架构

广播电视播控技术架构主要包括信号源系统、节目制作系统、节目播出系统、传输系统和接收系统等几个部分。(1) 信号源系统: 负责采集和提供各种节目信号源,包括卫星信号、地面微波信号、网络信号、本地素材库信号等。信号源系统需要具备多种信号接入接口和信号转换设备,以确保不同类型信号的稳定接入和格式转换。(2) 节目制作系统: 用于对采集到的节目素材进行编辑、剪辑、特效处理、配音等后期制作工作,生成符合播出要求的节目成品。节目制作系统通常包括非线性编辑设备、音频工作站、视频特效合成设备等。(3) 节目播出系统: 是播控技术的核心部分,负责按照预定的节目播出计划,将节目成品准确、及时地播出。节目播出系统包括视频服务器、播出控制软件、切换台等设备,能够实现节目播出的自动化控制和管理。(4) 传输系统: 负责将播出的节目信号传输到各个发射站点或网络平台,以便信号能够覆盖到广大用户。传输系统包括光纤传输网络、卫星传输系统、地面无线传输系统等多种传输方式,不同的传输方式具有不同的特点和适用范围。(5) 接收系统: 由各种接收设备组成,如电视机、机顶盒、手机、电脑等终端设备,用于接收广播电视信号并将其还原为图像和声音,供用户观看和收听。

1.2 核心技术

(1) 信号处理技术: 包括信号的采集、转换、编码、解码、调制、解调等技术,是保障信号质量和传输效率的关键。例如,高效的视频编码技术(如H.265等)能够在保证图像质量的前提下,降低信号传输带宽需求,提高传输效率;先进的音频处理技术可以实现音频信号的降噪、增强、环绕声处理等功能,提升音频质量。(2) 网络传输技术: 随着网络化的发展,网络传输技术在广播电视播控中变得越来越重要^[1]。包括高速光纤网络技术、卫星通信网络技术、无线通信网络技术等。同时,为了保障信号在网络传输过程中的稳定性和安全性,还需要采用一系列网络传输协议和安全机制,如TCP/IP协议、HTTP协议、SSL/TLS加密协议等。(3) 自动化控制技术: 通过自动化控制软件和设备,实现对播控系统各个环节的自动化操作和管理。例如,自动节目编排系统可以根据预设的规则自动生成节目播出单;自动播出控制系统能够按照播出单的要求,自动控制视频服务器、切换台等设备进行节目播出,减少人工干预,提高播出的准确性和稳定性。(4) 存储技术: 广播电视节目素材和成品的数据量巨大,需要高效的存储技术来进行管理和保存。目前,常用的存储技术包括磁盘阵列、磁带库、网络存储设备(如NAS、SAN等)。为了保障数据的安全性和可靠性,还需要采用数据备份和恢复技术,定期对重要数据进行备份,以防止数据丢失。

2 新技术时代广播电视播控系统安全维护的重要性

2.1 保障信息传播的准确性和稳定性

广播电视作为重要的信息传播媒介,承担着向广大观众传递新闻资讯、文化娱乐、政策法规等各种信息的重要任务。如果播控系统出现安全问题,如信号中断、信号干扰、节目内容错误等,将导致信息传播的不准确

或不稳定,影响观众对信息的获取和理解,甚至可能造成不良的社会影响。

2.2 维护广播电视媒体的公信力和形象

安全稳定的播控系统是广播电视媒体公信力和形象的重要保障。一旦播控系统出现安全事故,如节目被非法插播、篡改等,将严重损害广播电视媒体的声誉和公信力,导致观众对媒体的信任度下降,进而影响媒体的市场竞争力和发展前景。

2.3 保障国家安全和社会稳定

广播电视在国家安全和社会稳定方面发挥着重要的舆论引导作用。播控系统的安全直接关系到国家信息安全和意识形态安全。如果播控系统被恶意攻击或利用,传播有害信息、虚假信息等,将对国家安全和社会稳定造成严重威胁。

2.4 保护用户权益

观众作为广播电视节目的接收者,有权享受到高质量、安全可靠的节目服务。安全维护工作能够确保广播电视信号的正常传输和节目内容的合法合规,保护用户免受信号中断、不良信息干扰等问题的影响,维护用户的合法权益。

3 广播电视播控技术安全面临的挑战

3.1 网络安全威胁

随着广播电视播控系统的网络化和IP化,网络安全成为首要面临的挑战。黑客攻击、恶意软件入侵、网络钓鱼等网络安全事件频发,可能导致播控系统瘫痪、节目信号中断、用户数据泄露等严重后果^[2]。比如,黑客可能通过攻击播控系统的服务器,篡改节目播出内容,造成恶劣的社会影响;恶意软件可能感染播控设备,窃取系统敏感信息,破坏系统正常运行。

3.2 数据安全风险

广播电视播控系统中存储着大量的节目数据、用户数据等重要信息。数据在采集、传输、存储和使用过程中,面临着数据泄露、篡改、丢失等风险。如果用户个人信息被泄露,可能引发用户隐私安全问题;节目数据被篡改或丢失,将影响节目正常播出和内容质量。此外,随着大数据技术的应用,数据的集中存储和处理也增加了数据安全管理的难度。

3.3 系统兼容性与稳定性问题

新技术的应用使得广播电视播控系统的设备和软件种类繁多,不同厂家的设备和系统之间可能存在兼容性问题。在系统升级和更新过程中,如果兼容性处理不当,可能导致系统运行不稳定,出现信号中断、画面卡顿等故障。播控系统长时间运行,设备老化、硬件故障

等也会影响系统的稳定性,需要及时维护 and 更换。

3.4 人员安全意识与技术能力不足

广播电视播控技术的安全维护不仅依赖于先进的技术手段,还需要具备专业知识和安全意识的人员。部分工作人员可能对网络安全风险认识不足,缺乏必要的安全操作技能,如设置弱密码、随意点击不明链接等,容易引发安全事故。此外,新技术的快速发展要求工作人员不断更新知识和技能,但目前一些从业人员对新技术的掌握程度不够,难以满足安全维护工作的需求。

4 广播电视播控技术安全维护策略

4.1 网络安全防护措施

(1) 防火墙与入侵检测系统部署:在广播电视播控系统的网络边界部署防火墙,对进出网络的流量进行过滤和控制,阻止非法访问和恶意攻击。同时安装入侵检测系统(IDS)和入侵防御系统(IPS),实时监测网络流量,及时发现并阻止入侵行为^[3]。比如,通过设置防火墙规则,禁止外部未经授权的IP地址访问播控系统的核心服务器;利用IDS实时监测网络流量中的异常行为,如端口扫描、大量的恶意数据包等,一旦发现异常,及时发出警报并采取相应的防御措施。(2) 加密技术应用:对广播电视信号传输和数据存储过程进行加密处理,确保数据的保密性和完整性。采用SSL/TLS等加密协议对网络传输的数据进行加密,防止数据在传输过程中被窃取或篡改。在数据存储方面,使用加密算法对敏感数据进行加密存储,即使数据被非法获取,也难以破解其内容。(3) 网络安全漏洞管理:定期对播控系统的网络设备、服务器、软件等进行安全漏洞扫描,及时发现并修复存在的安全漏洞。建立安全漏洞管理机制,跟踪漏洞修复情况,确保系统的安全性。关注软件供应商发布的安全补丁,及时进行更新,防止黑客利用已知漏洞进行攻击。

4.2 数据安全策略

(1) 数据备份与恢复:制定完善的数据备份策略,定期对播控系统中的重要数据进行备份,并将备份数据存储在异地安全的存储设备中。建立数据恢复机制,确保在数据丢失或损坏时能够及时恢复数据,保障节目正常播出。比如,每天对节目素材、用户数据等进行全量备份,每周进行一次异地备份存储。当出现数据丢失情况时,能够迅速从备份数据中恢复,将损失降到最低。

(2) 数据访问控制:建立严格的数据访问权限管理机制,根据工作人员的职责和工作需要,为其分配相应的数据访问权限。采用身份认证、授权管理等技术手段,确保只有经过授权的人员才能访问和操作相关数据。比

如,对不同岗位的工作人员设置不同的用户账号和密码,并根据其工作内容为其分配相应的数据查看、修改、删除等权限,防止数据被非法访问和滥用。(3)数据加密存储:对存储在播控系统敏感数据,如用户个人信息、节目版权信息等,采用加密算法进行加密存储。选择高强度的加密算法,确保数据在存储过程中的安全性。同时妥善管理加密密钥,防止密钥泄露。

4.3 系统稳定性维护

(1)设备定期维护与更新:制定设备维护计划,定期对播控系统硬件设备进行检查、清洁、保养和维修,及时更换老化、损坏的设备部件,确保设备正常运行。关注设备制造商发布的设备更新信息,及时对设备进行升级更新,提高设备性能和稳定性。比如,定期对服务器进行硬件检查,清理灰尘,检查硬盘健康状态;根据设备制造商的建议,及时更新服务器的BIOS、驱动程序等,提高设备的兼容性和稳定性。(2)系统兼容性测试:在引入新的设备或软件到播控系统之前,进行充分的兼容性测试,确保其与现有系统能够正常协同工作。在系统升级和更新过程中,也要进行全面的兼容性测试,避免因兼容性问题导致系统故障。比如,在采购新的视频编码器时,先在实验室环境中与现有播控系统兼容性测试,测试通过后再进行正式部署;在对播控软件进行升级时,提前进行模拟测试,确保升级后系统各项功能正常。(3)建立应急响应机制:制定完善的应急响应预案,针对可能出现的系统故障、信号中断等突发事件,明确应急处理流程和责任分工^[4]。建立应急演练制度,定期组织工作人员进行应急演练,提高应对突发事件的能力。在突发事件发生时,能够迅速启动应急预案,采取有效的措施进行处理,尽快恢复系统正常运行。

4.4 人员培训与安全意识提升

(1)专业技术培训:定期组织工作人员参加广播电视播控技术相关的专业培训,学习新技术、新设备的使用和维护方法,提高工作人员的技术水平。邀请行业专

家进行技术讲座和培训,分享最新的技术发展动态和实践经验。比如,每季度组织一次内部技术培训,邀请设备供应商的技术人员对新采购的设备进行操作和维护培训;定期邀请行业专家举办技术讲座,介绍5G、云计算等新技术在广播电视播控领域的应用。(2)安全意识教育:加强对工作人员的网络安全意识教育,通过培训、宣传等方式,提高工作人员对网络安全风险的认识和防范意识。教育工作者遵守安全操作规程,如不随意连接未知网络、不使用弱密码、不随意点击不明链接等。

(3)安全考核机制:建立安全考核机制,将工作人员的安全意识和安全操作行为纳入绩效考核体系。对违反安全规定的行为进行严肃处理,对在安全工作中表现突出的人员进行表彰和奖励,激励工作人员积极参与安全维护工作。

结束语

综上所述,新技术时代广播电视播控技术在架构和核心技术上取得显著进展,极大地推动了行业发展。但安全维护方面的挑战也不容忽视,网络安全威胁、数据安全风险等严重影响着播控系统的稳定运行。通过实施网络安全防护、数据安全、系统稳定性维护以及人员培训与安全意识提升等策略,能有效应对这些挑战。随着未来技术不断的更新,广播电视播控技术及安全维护需持续探索创新,以适应新的发展需求,保障广播电视行业的健康可持续发展。

参考文献

- [1]陈妮娅.广播电视播控技术及其维护管理分析[J].中国传媒科技,2024(6):146-149.
- [2]王慧.广播电视安全播出技术维护与管理措施[J].卫星电视与宽带多媒体,2024(12):28-30.
- [3]王博岩.新时期广播电视播控技术管理及安全维护[J].卫星电视与宽带多媒体,2023(14):52-54.
- [4]李玮.广播电视技术的发展及播控管理分析[J].传播力研究,2024,8(8):151-153.