# Research on Security Construction of County-Level Converged Media Information Systems (Postprint)

**Authors:** Xu Xu

**Date:** 2025-07-09T00:00:00+00:00

## Abstract

【Objective】Currently, information technology is developing rapidly and has been extensively applied in radio and television technology systems. However, due to various factors, the construction of county-level converged media information systems is characterized by widespread security issues that cannot be effectively countered by traditional control measures alone. 【Methods】 To address these security issues, Jianhu Converged Media has undertaken construction research encompassing information system architecture, operation and maintenance, networking, and management. 【Results / Conclusion】 Additionally, through the establishment of multi-faceted security safeguards and the construction of an integrated security system, the overall security of county-level converged media information systems is effectively enhanced.

## Full Text

### Research on Security Construction of County-Level Converged Media Information Systems

*(Jianhu County Converged Media Center, Jianhu, Jiangsu 224700)*

## Abstract

[**Objective**] With the rapid development of information technology and its extensive application in broadcast television technical systems, county-level converged media information systems face widespread security issues due to various factors, which cannot be effectively addressed through traditional control measures alone. [**Methods**] To tackle these security challenges, Jianhu Converged Media conducted research on security construction across system architecture, operations, network, and management dimensions. [**Results/Conclusion**] By

establishing multi-faceted security safeguards and building an integrated security system, the overall security of county-level converged media information systems has been effectively enhanced.

**Keywords:** Broadcast Television; Information System; Security Construction; County-Level Converged Media; System
**CLC Number:** G202
**Document Code:** A
**Article ID:** 1671-0134(2025)03-150-04
**DOI:** 10.19483/j.cnki.11-4653/n.2025.03.033
**Citation Format:** Xu Xu. Research on Security Construction of County-Level Converged Media Information Systems[J]. China Media Technology, 2025, 32(3): 150-153.

## 1. Construction Objectives of Broadcast Television Information Systems

Information system construction serves as the technical foundation and critical guarantee for the normal operation of broadcast television institutions at all levels. Overall, broadcast television information system construction is characterized by three key features: operability, transmission capability, and security, with security being the top priority and a key indicator of successful system construction. County-level converged media must attach great importance to information system security, integrating security design and implementing security strategies throughout the construction process to ensure that information systems meet security requirements.

## 2. Current Security Issues in County-Level Converged Media Information Systems

### 2.1 Inadequate Infrastructure

As the primary technical platform for converged production, broadcast television information systems require unified and standardized infrastructure without stability issues. Core equipment should be redundantly backed up to eliminate single points of failure while meeting program production business needs under the premise of system security. However, due to insufficient budgetary funds, county-level converged media information systems commonly suffer from inadequate infrastructure during the design and construction phases. This manifests primarily in the adoption of hybrid topological structures that degrade overall system stability, and the operation of core equipment such as servers, storage devices, and switches in single-node configurations without redundant backup. Infrastructure deficiencies pose significant security challenges, particularly in later stages of system operation.

### 2.2 Non-Standardized System Operations and Maintenance

Early broadcast television technical system maintenance focused primarily on physical-level issues such as aging proprietary equipment, power failures, and cable connections. With the widespread application of broadcast television information systems, county-level converged media face challenges due to insufficient technical staff capabilities in computer hardware, software, and networking. System operations and maintenance are generally non-standardized, manifesting as: unfamiliarity with technical standards, parameters, operating status, and failure characteristics of complex hardware equipment, preventing proactive detection and timely reporting of information system failures; lack of understanding of system software kernels, underlying technologies, security policies, and permission management, preventing active monitoring of system cluster status to ensure normal service access and timely closure of high-risk ports and unnecessary services to block network attack vectors; and inadequate database maintenance with non-standardized backup plans and procedures, including failure to perform regular database file backups and incomplete terminal image backups.

### 2.3 Unprofessional Network Protection

Computer and network technologies serve as important technical support for information systems and play an increasingly vital role in county-level converged media production platform construction, media convergence, and IP-based distribution. However, the application of advanced technologies is hampered by the lack of necessary network security equipment and weak network security technical capabilities, resulting in numerous system security vulnerabilities that are not promptly patched, exposing systems to serious network attacks and virus infection threats.

**2.3.1 System Vulnerabilities** As the fundamental platform for software operation, operating systems allocate system hardware and software resources, control input/output devices, manage file systems, and control permissions to ensure stable information system operation. However, operating systems inherently contain known or unknown security vulnerabilities that pose security risks to system operation and require regular scanning and patching. For broadcast television information systems that support safe program production and broadcasting, operating systems must be regularly patched according to security risk levels; otherwise, normal and stable production will be directly affected. Due to the lack of professional equipment and talent, vulnerability detection and remediation present significant challenges and represent a weak link in the security chain for county-level converged media information systems.

**2.3.2 Network Attacks** Network attacks have become a critical factor affecting the secure operation of various information systems. Depending on their severity, attacks can range from partial data theft and short-term system failures to illegal network occupation and severe data destruction. As the primary

technical system for news program production, broadcast television information systems must strictly guard against network attacks to ensure operational security. County-level converged media information systems lack professional network equipment such as network firewalls, centralized monitoring systems, log auditing systems, vulnerability scanning systems, terminal threat defense systems, and bastion hosts, resulting in relatively low network protection capabilities and significant network attack risks.

**2.3.3 Virus Infections** Computer virus infection is one of the most common security issues in information systems. By executing illegal instructions and malicious code, viruses can destroy information system component functions or delete data, posing serious security threats. With the rapid development of computer coding technology, virus transmission channels and infection methods have become increasingly complex and difficult to defend against. For county-level converged media information systems, although file type format access control and virus/malicious code scanning are implemented through network gates and antivirus hosts, there remain significant deficiencies in preventing and handling new types of computer viruses, representing a considerable security risk.

### 2.4 Inadequate Security Management

Effective security management plays a crucial role in the stable operation of any system, and this is equally true for broadcast television information systems. County-level converged media information systems face four primary security management issues: First, lack of security management planning prevents unified management of critical security components due to personnel and organizational constraints. Second, insufficient security management technical capabilities lack professional talent support. Third, inadequate security mechanism support means that although county-level converged media have established security management departments for safe broadcasting and technical operations with clearly defined responsibilities, system security supervision, detection, and response mechanisms remain incomplete due to objective constraints. Fourth, security awareness needs strengthening, as some personnel treat security work as a formality and fail to correct behaviors that impact system security.

## 3. Security Construction of Jianhu Converged Media Information System

The core information system of Jianhu County Converged Media Center is a converged production platform that relies on the cloud services, technical capabilities, and infrastructure resources of the provincial "Litchi Cloud" platform to support content acquisition, data analysis, converged production, and converged distribution operations. By reasonably applying current broadcast television technologies, computer technologies, and network technologies, Jianhu Converged Media has achieved a relative balance between security and efficiency

while meeting converged production business requirements. Through analysis of infrastructure, system operation, data interaction, and post-implementation management, security construction can be categorized into four aspects: structural security, operational security, network security, and management security. By actively implementing reinforced redundancy for service nodes, storage devices, and network equipment to address infrastructure risks, combined with system control to achieve structural security; implementing software and hardware security monitoring and prevention during system operation while actively establishing user operation norms to effectively manage user behavior for operational security; implementing network security through independent physical lines, access control, content detection, vulnerability scanning, and virus protection to address data interaction risks when connecting to provincial technical platforms via public networks; and achieving management security through strengthened institutional and behavioral management with regular security assessments, the overall security of Jianhu Converged Media information systems has been effectively enhanced.

### 3.1 Structural Security Construction

Structural security can be divided into four aspects for Jianhu Converged Media information systems: service security, storage security, link security, and control security, forming the foundation of the entire information system security construction.

**3.1.1 Service Security** For county-level converged media information systems, uninterrupted services are typically achieved through multi-server cluster operation. With the rapid development of computer network technology, distributed service architecture has gradually become mainstream and has been applied in county-level converged media information systems, albeit with relatively smaller node scales. Jianhu Converged Media information system employs a three-node distributed service architecture characterized by low budget investment, easy scalability, and convenient maintenance, while ensuring that single-point failures do not severely impact overall services. Services such as backend management, packaging and synthesis, cluster transcoding, and cluster migration are deployed in a modular fashion across different node servers, with unified scheduling management achieved through real-time task monitoring, resulting in relatively high overall security.

**3.1.2 Storage Security** Media data represents the core resource of all converged media unit information systems, making storage system security construction critically important. Storage infrastructure should be strengthened with redundant backup to avoid single points of failure and achieve high security and availability of storage devices. The broadcast television industry currently employs two primary storage architectures: traditional redundant hot backup storage and multi-node distributed storage. Based on practical application requirements, Jianhu Converged Media information system adopts redundant hot

backup storage. Although this offers lower security compared to multi-node distributed storage, years of deployment and use in the broadcast television industry have proven it capable of meeting data storage security requirements.

**3.1.3 Link Security** As two network topology structures commonly adopted in the broadcast television industry, FC-SAN offers higher transmission bandwidth and functionality compared to IP-NAS network architecture, with obvious advantages for core data connectivity. However, for county-level converged media, budget constraints, technical limitations, and insufficient experience more commonly lead to the adoption of IP-NAS architecture. With the maturation and popularization of 10 Gigabit Ethernet technology, its performance can also meet requirements. Jianhu Converged Media information system employs IP-NAS network architecture with a security design featuring primary-backup deployment of two core switches. Gigabit Ethernet interconnects switches to terminal stations, while 10 Gigabit Ethernet connects switches to servers, ensuring data link security through multiple 10 Gigabit and Gigabit Ethernet connections.

**3.1.4 Control Security** Jianhu Converged Media information system deploys system management software to monitor equipment status, network traffic, and computing resources in real time. It monitors program production workflows, connection configurations between business systems, process node operations, and execution progress, adjusting priorities for backend packaging synthesis and data migration through security control to handle emergency events first. Through system control, technical personnel can accurately understand information system operation status and obtain complete operational data, enabling better system maintenance.

### 3.2 Operational Security Construction

Operational security ensures the normal operation of system hardware and software, preventing data destruction due to failures and damage, and forms the fundamental guarantee for information system operation. For broadcast television information systems, software and hardware constitute the main body of the information system and are critical to its security. Daily work should include regular inspection of information system operation status, with timely resolution of identified software and hardware security issues. Failure to address these issues promptly can constitute a serious system security threat.

**3.2.1 Hardware System Security** Hardware devices form the physical foundation for system security operation. County-level converged media technical personnel should regularly inspect the hardware system operating environment to ensure electrical and temperature control indicators meet system operation requirements. Core equipment such as servers, storage arrays, and core switches should be redundantly backed up and regularly inspected through dedicated

monitoring software to ensure equipment redundancy is online, with timely reporting and repair of operational failures. Hardware systems should be reasonably and scientifically configured, with regular inspection and replacement of equipment and boards that have exceeded their service life or are severely aged, and physical closure of unnecessary bus interfaces to prevent unauthorized access.

**3.2.2 Software System Security** For county-level converged media information systems, the hardware system as the foundation has relatively fixed and predictable security factors. In contrast, software systems pose greater security risks due to their operational complexity and unpredictability, making management from system software to application layer crucial. For system software management, strict user permission access control should be implemented with standardized settings for permissions, passwords, and software policies. User behavior should be regulated through operational norms to prevent users from modifying operating system settings, technical means should be employed to close configuration interfaces affecting software system stability, and unnecessary service ports should be disabled. For application software management, to avoid security failures caused by applications, reliable software with secure development guarantees should be prioritized during installation. Scientific and reasonable upgrade plans should be developed based on actual usage to improve application stability, and unauthorized software installation should be strictly prohibited.

### 3.3 Network Security Construction

Due to insufficient professional equipment and talent, network security has become a critical security factor commonly faced by the broadcast television industry and represents a weak link and prominent difficulty in broadcast television information system security construction. Current county-level converged media information systems face primary threats from network attacks, virus infections, and unauthorized access. Jianhu Converged Media information system deploys security firewalls and intrusion detection systems for boundary security protection, vulnerability scanning systems to detect and repair network security vulnerabilities, security network gates and virus scanning hosts for virus and malicious code scanning, and employs access control, log auditing, internet behavior management, and bastion hosts to achieve permission control and security auditing of network access, effectively enhancing information system network security protection.

**3.3.1 Boundary Protection** Information systems achieve boundary protection for internal network zones through security firewalls, managing network access permissions for internal users and implementing access control for inbound and outbound traffic. Intrusion detection equipment filters network transmission data in real time to detect network intrusion behaviors and anomalies, meeting information system network security requirements. Jianhu Converged

Media information system deploys a NetGuard Power V6000 firewall for boundary protection. Considering equipment failure emergency recovery and network security level protection enhancement requirements, plans are in place to add one additional cold backup firewall with the same configuration and one intrusion detection system to further improve boundary protection capabilities.

**3.3.2 Vulnerability Remediation** Network security vulnerability management has long been a challenge in network security protection. For network security technical personnel, vulnerability scanning systems are key to effective vulnerability management. By scanning and analyzing network core equipment such as servers and switches, security vulnerabilities can be identified and repaired to improve network security performance. Jianhu Converged Media information system deploys NetGuard vulnerability scanning systems to detect security vulnerabilities and defects in systems, networks, and applications. Vulnerability scanning tools also perform automated testing on systems to identify potential security vulnerabilities and defects for timely remediation.

**3.3.3 Virus Protection** Broadcast television information systems experience frequent data interactions with diverse file formats. Viruses disguised and hidden in file transmissions can cause serious system failures, and even timely removal can cause severe damage to the system. Therefore, proactive protection measures against viruses should be prioritized. Jianhu Converged Media information system employs two methods for virus protection: network gate isolation and virus scanning. For network gate isolation, security network gates are deployed to perform data validation, allowing data to enter the information system only after security confirmation, thereby blocking direct interaction between the information system and external data and logically preventing external dangerous data from launching virus attacks. For virus scanning, system resources and permissions are reasonably configured, normal business processes are optimized, and real-time virus scanning is implemented. All external data entering the information system must undergo antivirus scanning and security confirmation before entry, ensuring the information system remains free from virus infection threats.

**3.3.4 Access Control** Access control through core network devices such as routers or switches enables permission control for network access. Broadcast television information systems must control system access permissions, allowing entry only under security premises. Jianhu Converged Media information system employs dual H3C core switches to transmit traffic, achieving high-speed data processing and forwarding while carrying access control settings. ACL access control policies are configured to isolate different zones, reducing the possibility of illegal intrusion.

**3.3.5 Log Auditing** Log auditing systems record and analyze information system security events and user operation behaviors in bypass mode, enabling

traceability of system security behaviors and timely identification of system security vulnerabilities. Jianhu Converged Media information system deploys Topsec log auditing systems to comprehensively collect operation logs from system information equipment for auditing, analysis, and reporting, effectively enhancing information system network security.

**3.3.6 Internet Behavior Management** For county-level converged media, internal internet behavior management and content auditing in information systems are crucial. Through internet behavior management, functions such as behavior management, traffic management, application control, and information control can be achieved, effectively preventing personnel from engaging in work-unrelated network behaviors within the information system and ensuring data security. With limited export bandwidth, Jianhu Converged Media information system implements internet behavior management to guarantee system application bandwidth, ensuring priority traffic transmission for critical information system services and effectively improving network stability and security.

**3.3.7 Bastion Host** Bastion hosts implement fine-grained security control strategies to effectively ensure the security and reliability of core equipment such as network devices, security devices, servers, and databases, reducing human operational security risks and effectively improving system security. Jianhu Converged Media information system deploys Topsec bastion hosts to provide full-process auditing for remote IT operation and maintenance, ensuring manageable and controllable remote IT operations and achieving unified operation and maintenance entry points and unified asset management.

### 3.4 Management Security Construction

Security is 30% technology and 70% management, with security issues largely stemming from insufficient understanding of threats and risks, lack of clear security policies, incomplete security management systems, and lax implementation. Jianhu Converged Media attaches great importance to information system management security construction. In terms of institutional development, it clearly defines the objectives and direction of information system security management, organizational responsibilities, management principles, and security frameworks. Standardized documents are issued for computer room management and personnel management systems, which are regularly updated. In terms of personnel management, system usage training is conducted to regulate end-user behavior, targeted education is provided for 违规 operations, and comprehensive emergency response plans are developed to comprehensively improve technical personnel emergency handling capabilities. In terms of inspection and assessment, regular information system security evaluation and testing are conducted through multiple methods including daily self-inspections, vendor patrol inspections, and professional institution assessments to identify potential hidden security issues early and repair them promptly.

## 4. Conclusion

The broadcast television information system security system comprises the management layer, operation layer, and technical layer. From these three perspectives, county-level converged media information systems face common security issues that represent key construction challenges and difficulties. The construction of Jianhu Converged Media information systems aligns with current media convergence development trends. However, from the perspective of high standards, high reliability, and high availability, numerous security issues remain. Through targeted construction in structural security, operational security, network security, and management security, the overall security of information systems has been effectively enhanced. Currently, information technology continues to evolve rapidly, bringing ever-increasing security risks. Broadcast television technical personnel should adopt a system security perspective, strengthen security knowledge learning, improve security skill levels, and make due contributions to maintaining information system security.

## References

[1] Wu Yongsheng. Construction and Implementation of TV Safe Broadcasting Guarantee System for Nanjing Broadcasting Group[C]. 2021 Annual Conference of China Federation of News Technology Workers, 2021: 386-392.
[2] Li Ping. Research on Security Construction of Broadcast Television Information Systems[J]. China Media Technology, 2021(12): 158-160.
[3] Chai Xiaoyu. Analysis of Current Situation and Strategies for Network Security in Broadcast Television Industry[J]. Broadcasting and Television Network, 2024(7): 52-54.
[4] Yang Zhen. Design and Construction of HD Integrated Non-Linear Editing Media Asset Network[J]. Modern TV Technology, 2016(8): 105-110.
[5] Zhong Chao, Jia Ruoyu. Program Production Security Solution for Xuzhou TV Station Non-Linear Editing Network[J]. Broadcasting Realm, 2017(6): 92-95.
[6] Zhang Xiaocun. Research on Construction of Jianhu County Converged Media Center in Jiangsu Province[J]. Broadcasting and Television Information, 2021(12): 26-29.
[7] Ren Xiaowei. Research on Network Security Hardening Methods for Broadcast Television Information Systems[J]. Broadcasting and TV Technology, 2019(2): 12-16.
[8] Yang Shuhai. Security Design of All-Media Content Production Network for Small and Medium TV Stations[J]. TV Technology, 2016(8): 80-83.
[9] Gao Xiaoqing. Network Security Risks and Strategies for Broadcast Television Information Systems[J]. Communication World, 2019(11): 51-52.
[10] Xu Jimeng. Reflections on Network Security Protection for Broadcast Television Information Systems[J]. Digital Media Research, 2024(1): 78-80.
[11] Yang Yang. Design and Implementation of Network Security for Broadcast Converged Media Production[J]. Broadcasting and TV Technology, 2022(11):

45-49.
[12] Jiang Yuncui. Application of Network Security Technology in Broadcast Television[J]. Electronics World, 2020(1): 181-182.
[13] Wu Chongfeng, Zhang Gaopeng. Application of Network Security Level Protection System in Broadcast Television Field[J]. TV Technology, 2024(7): 196-198.
[14] Hu Limin. Application of Network Security Technology in County-Level Converged Media Technical Systems[J]. Shanxi Youth, 2024(17): 196-198.
[15] Yu Tao. Practice in Information Security Strategy Design for Research Institutes[J]. Network Security and Informatization, 2019(1): 107-109.
[16] Yang Jing. Reflections and Practice on Broadcast Television Information Security Situation[J]. New Media Research, 2017(1): 120-121.

**Author Profile:** Xu Xu (1981–), male, from Jianhu, Jiangsu, bachelor' s degree, engineer. Research interests: broadcast television information system construction, operation and maintenance, signal transmission and broadcasting.
*(Responsible Editor: Li Yansong)*

*Note: Figure translations are in progress. See original paper for figures.*