

Discussion on Network Information and Data Security in Television Broadcasting Systems: Post-print

Authors: excessive yang

Date: 2023-10-08T00:00:00+00:00

Abstract

Advances in science and technology have propelled countries worldwide into the information age, where vast amounts of electronic information play a critically important role. Within television stations, broadcast playout systems serve a vital function, acting not only as the central nervous system for both internal and external signals but also maintaining an intimate connection with television program transmission. Consequently, ensuring the security and stability of television broadcast playout systems is imperative. These systems necessitate the utilization of substantial information and data; guaranteeing the security and reliability of such data can effectively enhance broadcast quality. This study, based on the author's practical professional experience and employing a specific television station as a case study, investigates network information and data security in television broadcast playout systems, with the objective of improving emergency response capabilities.

Full Text

Discussion on Network Information and Data Security of TV Broadcast Systems

Abstract

Advancements in science and technology have ushered the world into an information age where electronic information plays a crucial role. In television stations, the broadcast system serves as the central nervous system for both internal and external signals and is intimately connected with program transmission. Therefore, ensuring the security and stability of TV broadcast systems is essential. These systems process vast amounts of information and data; guaranteeing the

security and reliability of this data can significantly improve broadcast quality. Drawing from practical experience and using a specific television station as a case study, this paper investigates network information and data security issues in TV broadcast systems to enhance emergency response capabilities.

Keywords: TV broadcast system; network information; data security

1.1 Network Internal Security

Network internal security comprises several components, including physical access control, terminal system security, and privilege policy management. To establish an effective network management module, strict control over personnel identification and authorization is required, ensuring that users authenticate properly when logging into applications. All user operations are logged for audit purposes, enabling detailed operator tracking and centralized management. During application and component installation, workstations can disable unnecessary services. Furthermore, deploying terminal management systems can block external media access across all operation terminals.

1.2 Network Communication Security

From a communication perspective, all network designs are configured adaptively. During normal operation, this enhances system efficiency. When failures occur, secure switching mechanisms ensure continued safe operation. Logs are transmitted to a log auditing system for unified management. Additionally, security zones must be scientifically divided with careful attention to zone design. VLANs can be implemented to logically isolate business subnet systems within networks, thereby improving both network efficiency and security. IP-MAC binding enables terminal switch connections, while monitoring systems provide real-time surveillance of switch operations, issuing technical ID alerts when service levels fall below requirements. Simultaneously, security hardening configurations for all switches should be strengthened, and out-of-band management systems should be deployed to enable remote operation and maintenance of core switches.

1.3 Network Boundary Security

From a boundary security perspective, TV broadcast systems at different security levels can implement strict data management through firewall deployment, with control extending to destination IP addresses, protocols, and other parameters. By leveraging firewall capabilities, intrusion detection systems can be integrated to monitor all network traffic, immediately alerting upon detecting intrusion attempts. Deploying security gateways also enhances protection against malicious code. Currently, most broadcast systems in China operate

as well-isolated closed networks, separated from office automation (OA) systems and the internet. At broadcast boundaries, media links and information links are distinguished. High-performance firewalls enable fine-grained access control; network gate products deployed on information links facilitate data ferrying; detection products provide real-time monitoring of illegal intrusions; and core reinforcement systems deployed on FTP and interface servers enforce mandatory access control.

2. TV Broadcast System Data Security

2.1 Data Storage Security

Modern broadcast systems primarily employ nearline and online storage for data management. Nearline storage, also known as secondary storage, consists of high-capacity disk arrays located outside video servers, using migrated data for material sharing and storage. Secondary storage also serves as an intermediary for modifying and uploading materials from broadcast servers and upload terminals, thereby reducing the burden on video servers while ensuring comprehensive file protection. When storage system failures occur, secondary storage can identify fault locations and reconstruct files. Combining file-level and node-level fault tolerance enables online data replacement, safeguarding data integrity.

2.2 Database Security

The database serves as both the source data storage management center and the data core of TV broadcast systems, requiring 24/7 availability. To protect database security, EMC AutoStar can be employed for dual hot backup, enhancing system flexibility and achieving real-time database backup. Additionally, to ensure data integrity, time-lag backup databases should be configured to automatically save system data from eight hours prior. In the event of severe database errors, this time-lag backup can be manually imported to improve recovery efficiency.

3.1 Program Schedule Processing Flow

From an operational perspective, both backup broadcast and high-definition broadcast systems can utilize a shared database. When the chief editorial office issues a schedule, a single transmission suffices for both backup and broadcast software to access and prepare the program list. Receiving schedules from the chief editorial office requires cut-off time control: before the cut-off, the editorial office can modify and resend schedules multiple times; after the cut-off, emergency modifications must be performed by the broadcast department, with the program department or editorial committee responsible for unified changes. Upon receiving a schedule from the chief editorial office, the system must determine based on channel and broadcast date whether the cut-off time has passed. If not, the schedule is accepted and stored in the broadcast database; if the

cut-off has passed, acceptance is rejected with feedback provided. After the cut-off time, if the broadcast control machine has already loaded the schedule, emergency modifications must be made at the broadcast control workstation, with emergency videos delivered to the broadcast system via tape for uploading; if the broadcast control machine has not loaded the schedule, emergency programs can be uniformly modified at the high-definition system's scheduling workstation.

3.2 Program Broadcast Preparation Process

Program preparation software manages program readiness and requires configuration of opening and cut-off times. The specific implementation is as follows: The software can adjust program schedule dates within an 8-day range. After configuration, it loads all schedules within this window and prepares all programs. The software provides cut-off time settings, typically configured as eight times the program duration (minimum 2 hours 40 minutes). When programs in the schedule are not ready but reach the cut-off time, preparation halts and the software interface generates alerts for those programs. The interface service that receives production requests for program ingestion requires opening time parameters. When the interface receives a request from the production island, it queries schedules within the 8-day window. If the program does not exist in the schedule, the ingestion request is rejected. If it exists, the system checks whether the broadcast time is before the cut-off; if so, the request is rejected; if after, the program is permitted to enter the library. Upon successful push notification, the program preparation software is informed via messaging, allowing it to set preparation status on the client interface and prevent direct delivery.

4. Conclusion

In summary, although network technology in China has made considerable progress, cybersecurity issues remain inadequately addressed, posing threats to TV broadcast systems. Consequently, television station leadership must prioritize network security concerns in broadcast systems and implement targeted, effective management measures to systematize operations, thereby advancing network information security development and delivering higher-quality services.

References

- [1] Xiang Zujun. Analysis of Software Architecture's Role in TV Broadcast System Software Design[J]. Modern TV Technology, 2015(07).
- [2] Yang Kun. Maintenance and Management of Modern TV Broadcast Systems[J]. Information System Engineering, 2015(02).
- [3] Chen Chen. Reflections on Maintenance and Management of Modern TV Broadcast Systems[J]. Radio & TV Journal, 2015(05).

[4] Zhang Haitao. Research on Digital TV Broadcast System Architecture[J]. Electronic Technology & Software Engineering, 2015(10).

[5] Cui Rui. Maintenance and Management of TV Broadcast Systems[J]. Science and Technology Innovation and Application, 2015(18).

(Author's affiliation: Guangdong Radio and Television Station)

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

Source: ChinaXiv — Machine translation. Verify with original.