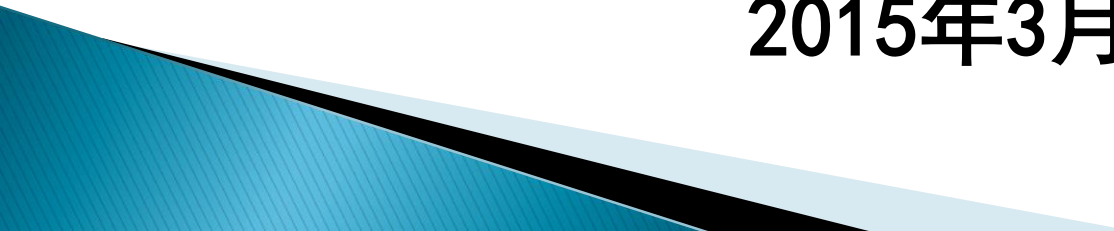


网络电视台和IPTV集成播控平台

安全播出管理要点和案例分析

杜国柱

2015年3月



主要内容



安播管理概述



新媒体安播管理框架



安播管理规范要点和案例分析



工作建议

一、安播管理概述

广播电视新媒体技术系统现状

互联网视听节目网站：613家

网络广播电视台：27家



手机视听节目网站：138家

手机电视集成播控平台：6家

互联网电视集成播控平台：7家



IPTV集成播控平台：
1个总平台，12个分平台

为什么新媒体也要高度重视安全播出

- ▶ 广播电视是宣传舆论的主阵地
 - 技术事故、其它事故演可能变成政治事故（中央台11.18事故；央视2.9大火）
 - ▶ 安全播出是确保内容安全、文化安全的重要屏障
 - 技术是内容传播的载体，安播是节目安全的最后一道防线，安播管理是内容安全管理的前置环节
 - ▶ 安全播出是提升媒体服务质量的重要保障
 - 安全播出是提升技术质量、服务效率的基础
- 网络电视台、IPTV集成播控平台等新媒体的政治属性、媒体属性、产业属性共同决定了：
安全播出也是新媒体的生命线

技术保障视角下新媒体与传统媒体特点比较

▶ 传统广播电视的特点

- 业务模式：音视频直播单一业务；
- 信号流程：集中发布、单向、广播式；
- 系统架构：模块化、链路式、封闭网络；
- 技术保障：环节少、自动播出；
- 终端展现：实时信号解析展现

▶ 视听新媒体的特点

- 业务模式：直播、点播、互动、社交等全业务集成；
- 信号流程：分散式发布、双向、IP化、网络化；
- 系统架构：IT化架构、多平台聚合、跨网络互联、终端开放；
- 技术保障：环节多、人工干预下的自动播出；
- 终端展现：智能终端，实时及非实时音视频、图片、文字、数据等多媒体信息展现

新媒体安全播出特点——范围扩展、难度提高、重心变化

新媒体安全播出与传统媒体的联系与差异

▶ 传统广播电视安全播出

- 管理范围：内部人员、信号、系统（边界在传输层）；
- 保障重点：信号安全；
- 职责分工：上下游界面清晰；
- 考核指标：停播率、事故；
- 规范体系：相对成熟；

▶ 视听新媒体安全播出

- 管理范围：内外部人员、信号、系统（边界在业务层）；
- 保障重点：信息安全；
- 职责分工：业务分层、网络化链接，外部接口多；
- 考核指标：停播率、事故、服务质量和效率；
- 规范体系：相对之后；

安全播出的范围扩展、重心变化、要求更高、难度提高

当前新媒体安全播出管理面临的主要问题

一、以互联网技术为基础的新媒体平台运营，突破了传统媒体的边界，且与互联网联系日趋紧密，信息与内容安全的风险明显增加。

二、新媒体平台建设时间不长，缺乏统一的技术标准、管理手段和运维规范，给业务监管带来了挑战。

三、技术形态发生了较大的变化，且相关事故、事件发生后处置手段不力，给原有的应急体系敲响了警钟。

新媒体运营单位如何确保安全播出

- ▶ 高度重视，坚持不懈
- ▶ 建立科学、高效的制度流程体系
- ▶ 抓好系统配置、人员培训、应急演练
- ▶ 抓好理念创新、手段创新，提高效率。
- ▶ 努力实现运行工作规范化、科学化、常态化，安全播出管理工作精细化、体系化、标准化

基础是：严格遵守总局62号令和相关专业实时细则

二、新媒体安播管理框架

新媒体安全播出工作的指导思想

对于新媒体，我们必须从促进业务发展，提供端到端的业务支撑角度来调整安全播出工作思路、总方针和评价指标体系，创新安全播出体系。指导思想：

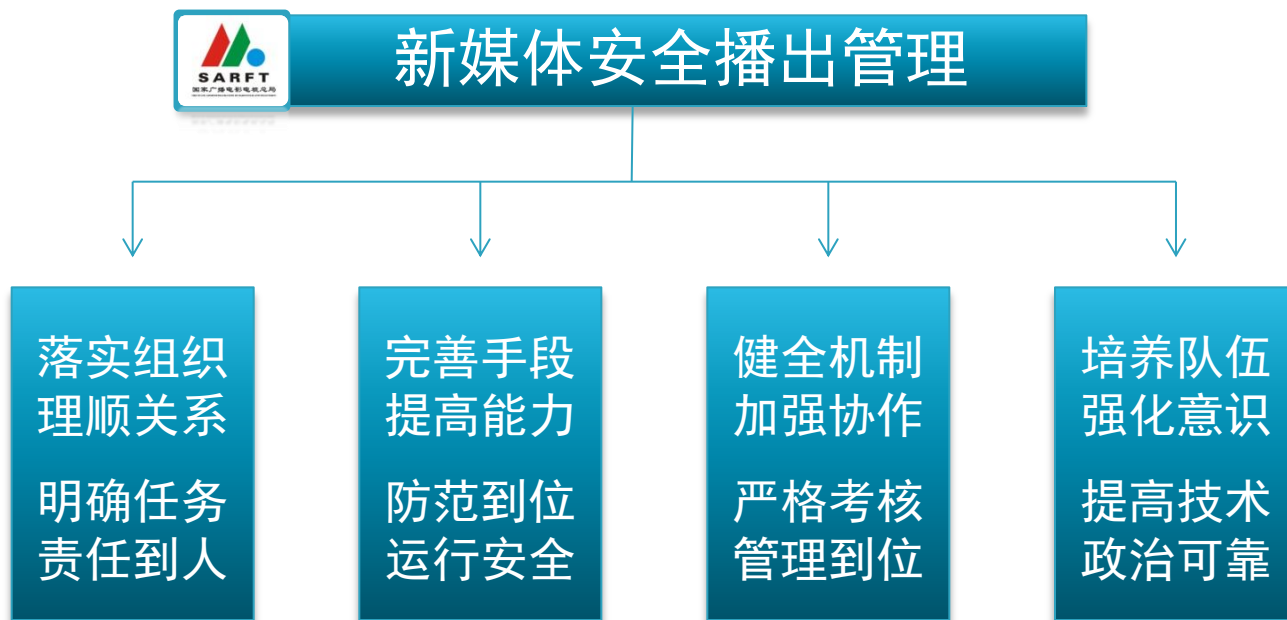
从“确保不中断、不停播”到“为发展提供安全、优质、高效的服务”

(1) 从“不出事故就是安全播出”到“安全优质高效服务支撑才是安全播出”

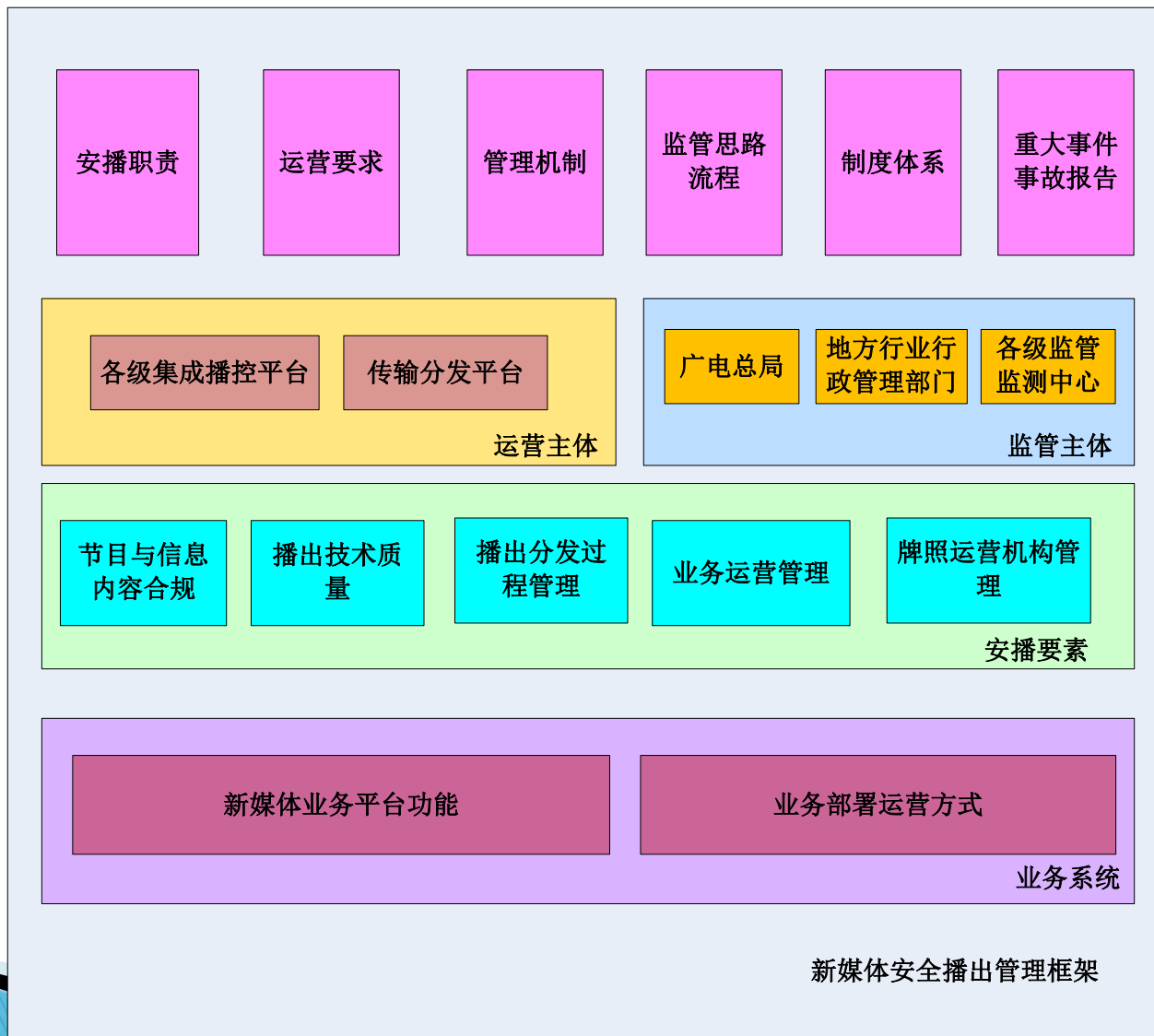
(2) 从QoS到QoE。

在保障节目播出、传输质量，杜绝重大停播和信息安全事故的基础上，更加关注对用户体验服务的支撑。

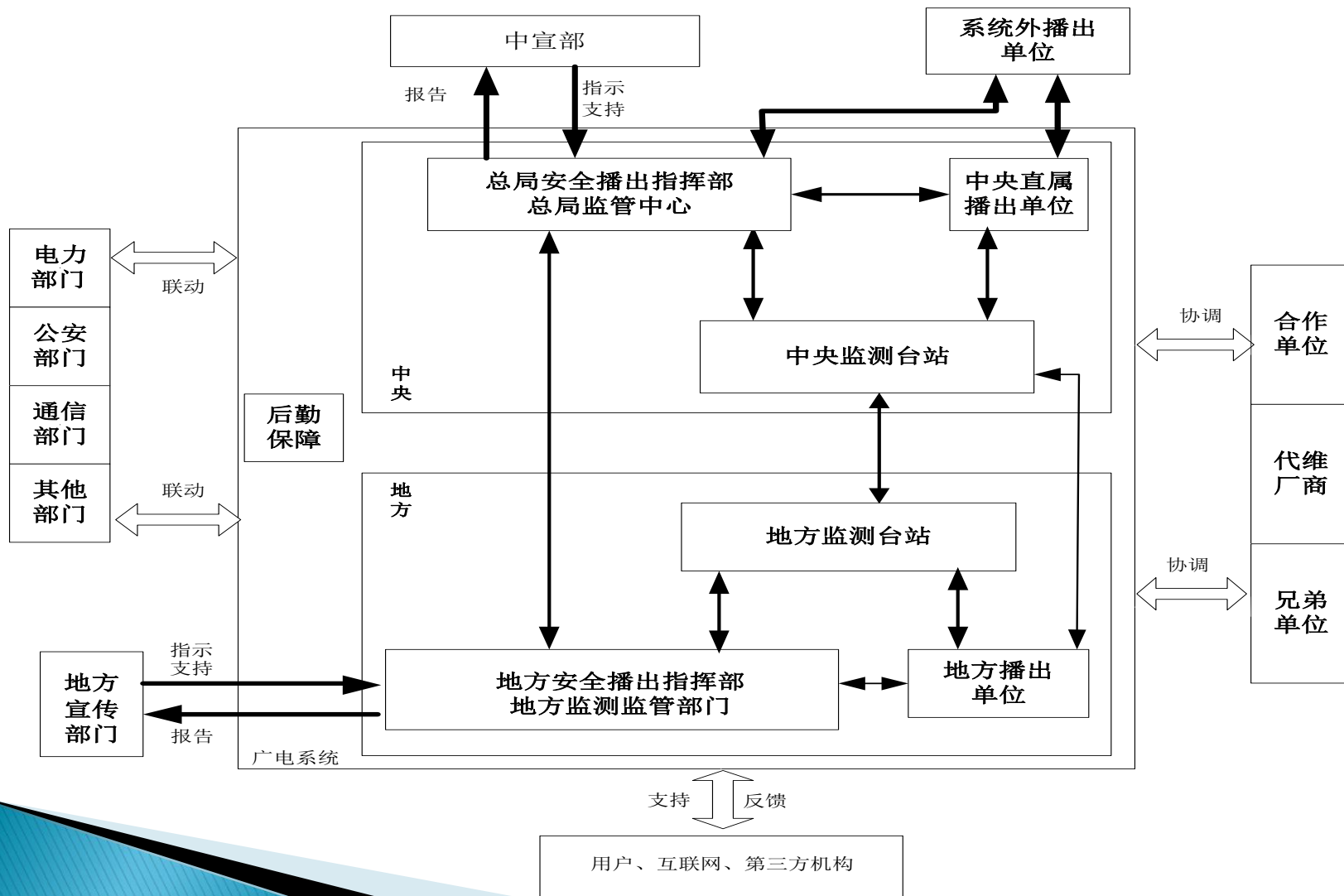
新媒体安全播出思路



新媒体安全播出管理框架



新媒体安全播出监测监管体系



三、安播管理规范要点 和案例分析

《规定》和实施细则的定位

- ▶ 总局关于广播电视安全播出的唯一政策法规
- ▶ 《规定》和实施细则是广播电视行政部门、监测监管部门对安全播出责任单位进行**安全播出监管**的主要依据：**管什么**和**管到什么程度**
- ▶ 《规定》和实施细则是安全播出责任单位在安全播出相关工作中必须遵守的行政法规：**做什么**和**做到什么程度**
- ▶ 《规定》和实施细则也是在出现重大事件、事故时，**保护未违规的**广播电视行政部门、监测监管部门、安全播出责任单位及安全播出相关工作人员的重要依据
- ▶ 《规定》和实施细则应当做到**全员掌握**，各单位、各部门、各岗位、各工作环节、各技术系统均遵照实施，要融入到各项工作中度、流程和应急预案中，要做到**哪里涉及安全播出，哪里就要对照《规定》和实施细则执行**

新媒体实施细则的要点

一是把握新媒体领域技术发展的规律，梳理和分析IPTV集成播控平台和网络广播电视台各关键环节可能出现的安全问题，有针对性地提出科学的配置办法或规避措施，通过技术手段提升安全的保障系数。

二是完善机制，将管理制度和流程覆盖全流程、各环节，将责任分解至与安全相关的岗位，避免出现脱节，推动新媒体安全管理工作体系化、标准化。

三是在运维过程中严谨工作程序，强化培训和值守管理，使新媒体平台的日常运维体现新流程、新方法，推动安全运维工作科学、规范。

四是进一步增强底线思维，从保证业务连续性和系统安全性角度，突出了对突发事故、事件的应急处理，在发生信息安全事件后及时消除不良影响，确保新媒体系统运行过程中万无一失。

五是充分尊重新媒体业务的发展规律，提出了IPTV集成播控平台以及网络广播电视台安全的总体概念以及相关技术工作衡量的标准。

实施细则的内容框架

▶ 第一章 总则

目的和依据、规范范围、系统构成

▶ 第二章 系统配置要求

总体网络架构、供配电系统、业务系统、信源技术系统、内容生产技术系统、内容发布技术系统、传输分发网络、业务运营管理系统、其它技术系统、安全监控管理中心、基础软硬件设备技术要求、机房环境、维护器材、灾备与应急播出

▶ 第三章 运维和技术管理

运维管理、技术管理、信息安全管理、人员管理

▶ 第四章 应急管理

应急机构、应急预案、应急演练、应急通报机制、事件事故应急处置、灾备与应急响应

▶ 第五章 附则

实施细则重点内容解读---总体网络架构

- ▶ 网络结构设计

层次清晰、子网边界清晰，有隔离、访问控制

- ▶ 网络设备冗余

带宽、关键设备冗余，关键环节无单点故障

- ▶ 划分网络安全域

构建纵深防御体系、后台系统隔离

- ▶ 重要业务系统间专网（线）连接

冗余、组合采用信息安全措施防止外部网络攻击

- ▶ 管理链路与数据交换链路隔离

访问控制、传输安全措施、用户终端不得直接接入核心网络设备

实施细则重点内容解读---信源系统

- ▶ 直播信号

 - 重要节目双路由和切换

 - 有应急垫播设施

 - 重要设备有冗余备份

 - 现场直播信号有延时和切断装置

- ▶ 各类信源接入

 - 信源安全检测、防入侵攻击、内容审核接口

实施细则重点内容解读---内容生产、发布和分发

- ▶ 节目入库

 - 入库前设置内容和技术审核

 - 节目库有恢复机制、定期进行节目文件完整性校验

- ▶ 节目上下线、内容发布

 - 有日志记录和审计功能

- ▶ EPG模板发布、页面模板发布

 - 预发布和审核、归档备份并加密保护、备份模板使用前进行完整性检查

- ▶ 节目发布库

 - 节目发布库与对应节目数据库分开存储

- ▶ 节目分发

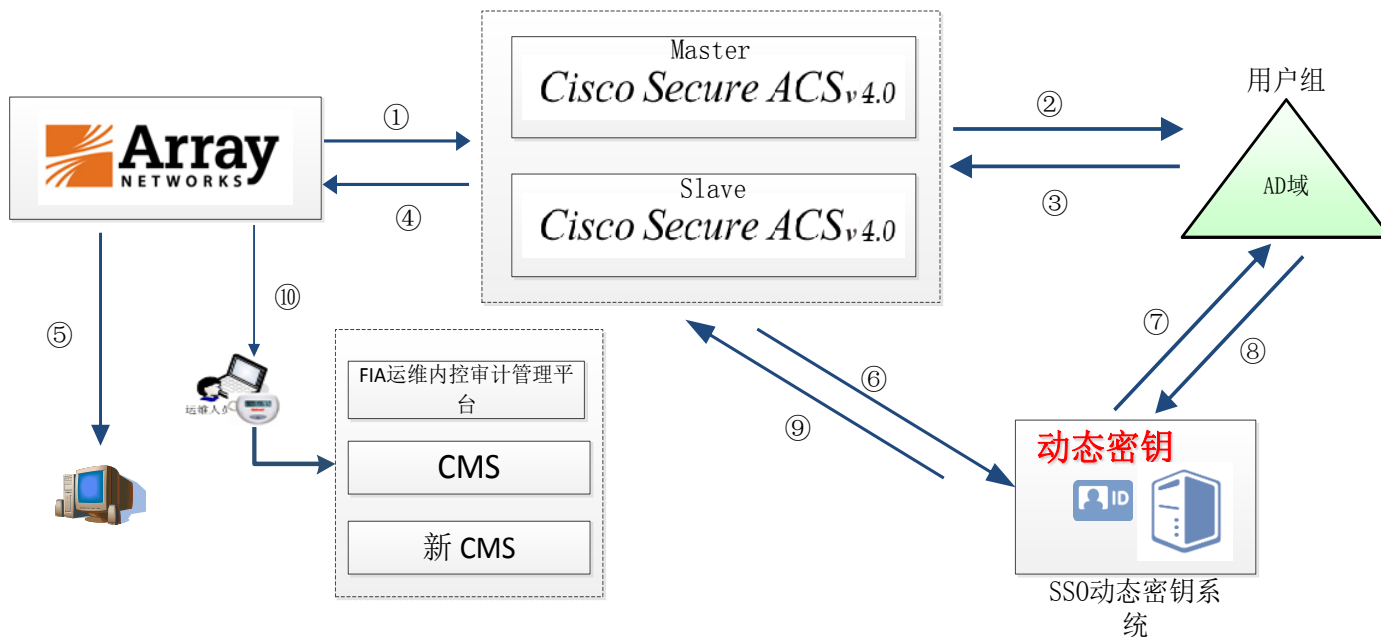
 - 分发链路畅通、冗余，要求第三方网络及时解决故障

2012年11月6日18时16分，由于江苏电信iTV承载网核心设备引擎故障，导致江苏电信网络传输的IPTV节目平台中CCTV-10、江苏城市、央视精品、女性时尚、东方卫视、辽宁卫视、天津卫视、靓装、旅游卫视、风云足球、湖北卫视等11套电视节目播出为彩条，经抢修，19时10分，其中8套节目恢复正常，20时30分剩余3套节目恢复正常，最长停播时长为2小时14分。

实施细则重点内容解读---业务管理系统及其它

- ▶ 用户认证鉴权
有认证鉴权、计费管理等功能
- ▶ 用户、计费等核心数据
进行安全防护，防泄露、窃取及篡改，不少于2个备份
- ▶ 其它技术系统
增值服务系统、数据库有可靠的安全措施、配置有效的产品测试环境

某网络电视台用户准入机制框架



静态密钥登陆

- ① 用户帐号, 静态密钥登陆
- ② radius用户关联
- ③ 登陆用户认证通过
- ④ 分配用户IP
- ⑤ 用户授权, 允许访问内网

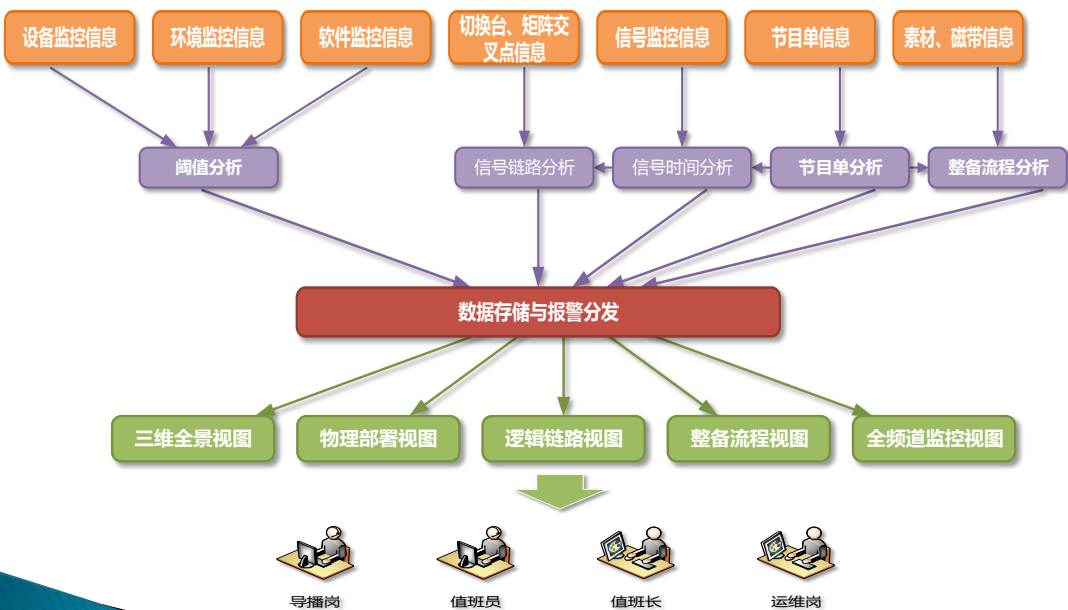
动态密钥登陆

- ① 用户帐号, 静态密钥+动态密钥登陆
- ⑥ radius用户关联
- ⑦ 寻找匹配用户组用户ID
- ⑧ 登陆用户认证
- ⑨ 登陆用户静态密钥+动态密钥 认证通过
- ④ 分配用户IP
- ⑩ 用户授权, 分配SSO隧道, 允许访问 FIA, 新, 老CMS系统

实施细则重点内容解读——安全监控管理中心

传统广播、电视实施细则中均要求设置自台监测系统，主要目的是对视音频信号以及电力系统的运行状况进行监测，并具备实时报警、异态信息记录等功能。《IPTV集成播控平台实施细则》、《网络广播电视台实施细则》更加高度重视监控系统的重要作用，要求配置安全监控管理中心。

通过配置安全监控管理中心，可对生产环境、设备、信号、流程、业务、管理等多种层面的关键信息



进行统一监控管理，让IPTV集成播控平台及网络广播电视台的业务运营流程更加直观，业务信息完全可视，管理要求能够得到更有效的传达，从而对于远程访问、异态事件、病毒入侵等实施细则重点关注的安全风险能够第一时间获知并处理。

实施细则重点内容解读——运维与技术管理

- 运维与技术管理一章主要内容涵盖了运维管理、技术管理、人员管理和信息安全管理。
- 运维管理包括备品备件、维护器材、应急灾备，应急处置等；
- 技术管理包括规章制度、重要播出保障、安播考核检查等；
- 人员管理保罗定岗定编，岗位职责，检查考核，人员培训等；
- 信息安全管理包括信息安全的依据标准、安全架构、安全防护、数据安全、安全监测与管理等。
- 重点强化了四项管理措施的落实：安全管理组织架构的建设；与新媒体业务运行和运营相关的制度、流程的建设、信息系统安全管理和重要保障期安全管理。

实施细则重点内容解读——制度和流程

制度、流程的制定是安全管理的重要内容，制度建立要体现科学、可操作；流程建立要体现时效性。在对国内IPTV集成播控平台及网络广播电视台的工作经验进行了认真地总结和分析后，在常态制度、流程基础上，根据新媒体业务运行和运营的特点，对与新媒体日常运营相关的制度及流程内容进行了建议。

如网络广播电视台建议的业务制度包括风险管理制度、安全服务制度、网络维护制度等，建议的流程包括直播系统传输分发流程、节目上下线流程、EPG管理流程等。

实施细则重点内容解读---信息安全管理

《广播电视相关
信息系统安全等
级保护定级指南》

《广播电视相关
信息系统安全等
级保护基本要求》

划分出
相关信
息系统
的安全
等级

按等级要求进行规划、设计、建设、
评估、整改

制定网络安全管理策略

制定管理制度和操作规程

从访问控制、运行维护、应急处
置、人员管理和培训、文件档案
管理、审核检查等方面规范信息
安全管理工作

信息安全事件案例

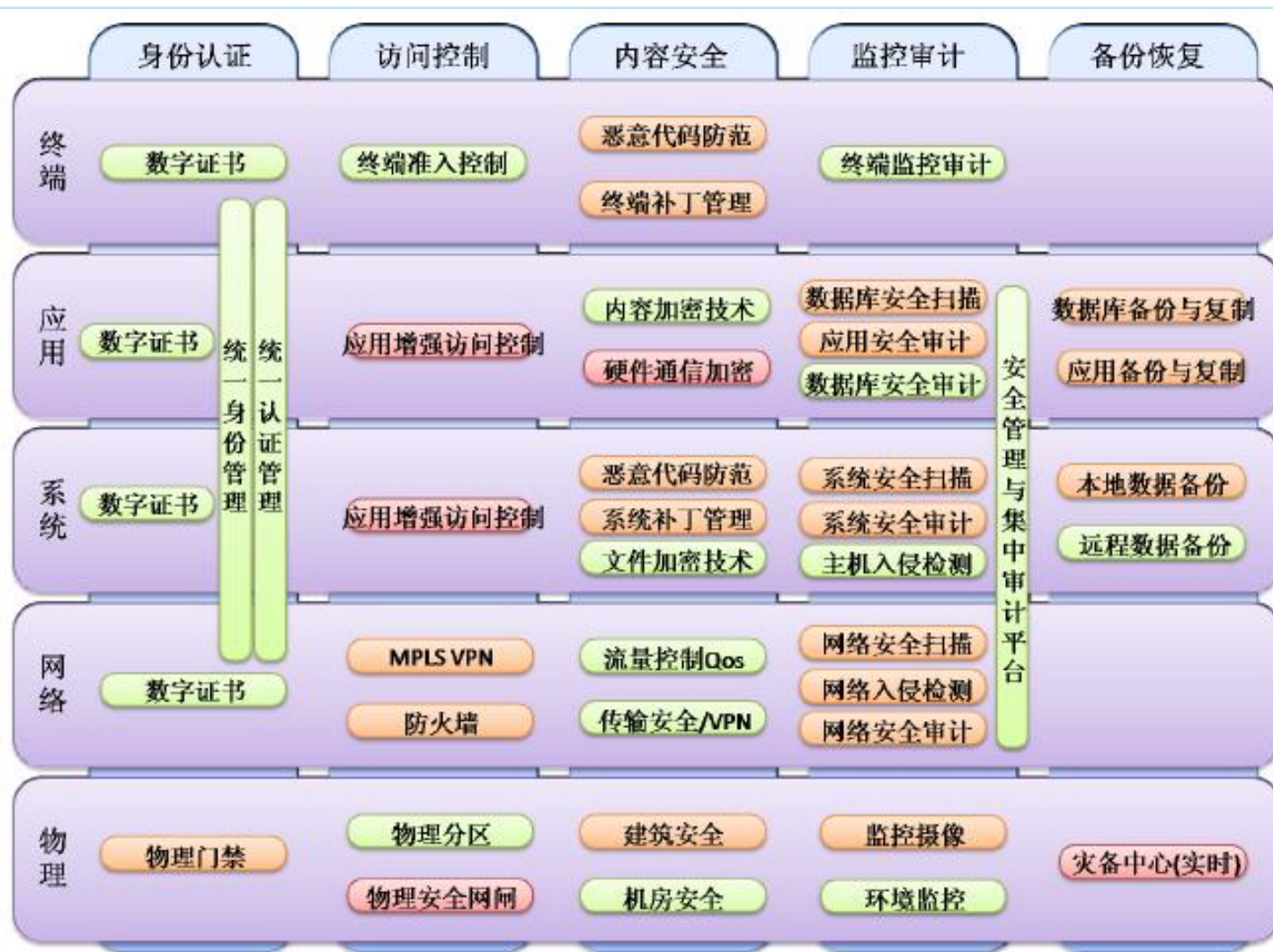
2012年3月11日18点55分，中国网络电视台监控系统报警，网站位于北京联通的源站无法访问。值班工程师立即按照应急预案进行处理，将基于联通的业务按照业务重要程度逐步向没有遭到攻击的电信节点进行迁移，整体迁移时间为25分钟，其中首页访问在10分钟左右即恢复。迁移期间网站联通用户受影响，电信用户无影响。根据监测，该攻击于21时25分消失。

中国网络电视台经对联通源站进行故障分析，通过网站部署的IDS（入侵检测系统）发现联通源站（北京西单电报局机房）遭受DDOS攻击（分布式拒绝服务攻击，利用信息系统缺陷或暴力攻击手段，以大量消耗信息系统的CPU、内存、磁盘空间或网络带宽等资源，从而影响信息系统正常运行为目的的攻击事件），攻击次数超过400万次/秒。经过深入分析后，确认攻击类型为SYN Flood攻击。

信息安全事件案例

- ▶ 2014年8月1日19:25，**中广有线温州分公司**在浙江温州市龙湾区、瓯海区、鹿城区和洞头县三区一县的有线数字电视节目播出画面叠加了反动字幕和图片，影响用户约30万户。温州有线前端立即将机房断电紧急中断播出信号。经采取技术处理等措施，8月2日1:10，有线网络全面恢复了电视信号，绝大部分机顶盒恢复正常，停播时间约5小时
- ▶ 经公安部门侦查，初步判定是一起**人为破坏事故**，一个技术设备公司的工程师通过互联网远程登录，将事先编制好的两个破坏程序和非法内容分布植入温州有线前端的EPG广告播发系统和信息通知OSD系统，并设定定时程序，分别于8月1日19:00和20:00自动启动，将事先准备的反动图文信息自动传送至用户机顶盒
- ▶ 从现场调查看，温州有线前端机房**管理不规范**，系统设备和安全管理制度不严密，播出系统有多个通道直接连接互联网，系统维护操作流程不规范，有多人掌握播出业务系统的密码口令，致使破坏分子有机可乘；备播系统和应急预案不健全，致使事故处理时间较长

等保设计方案案例



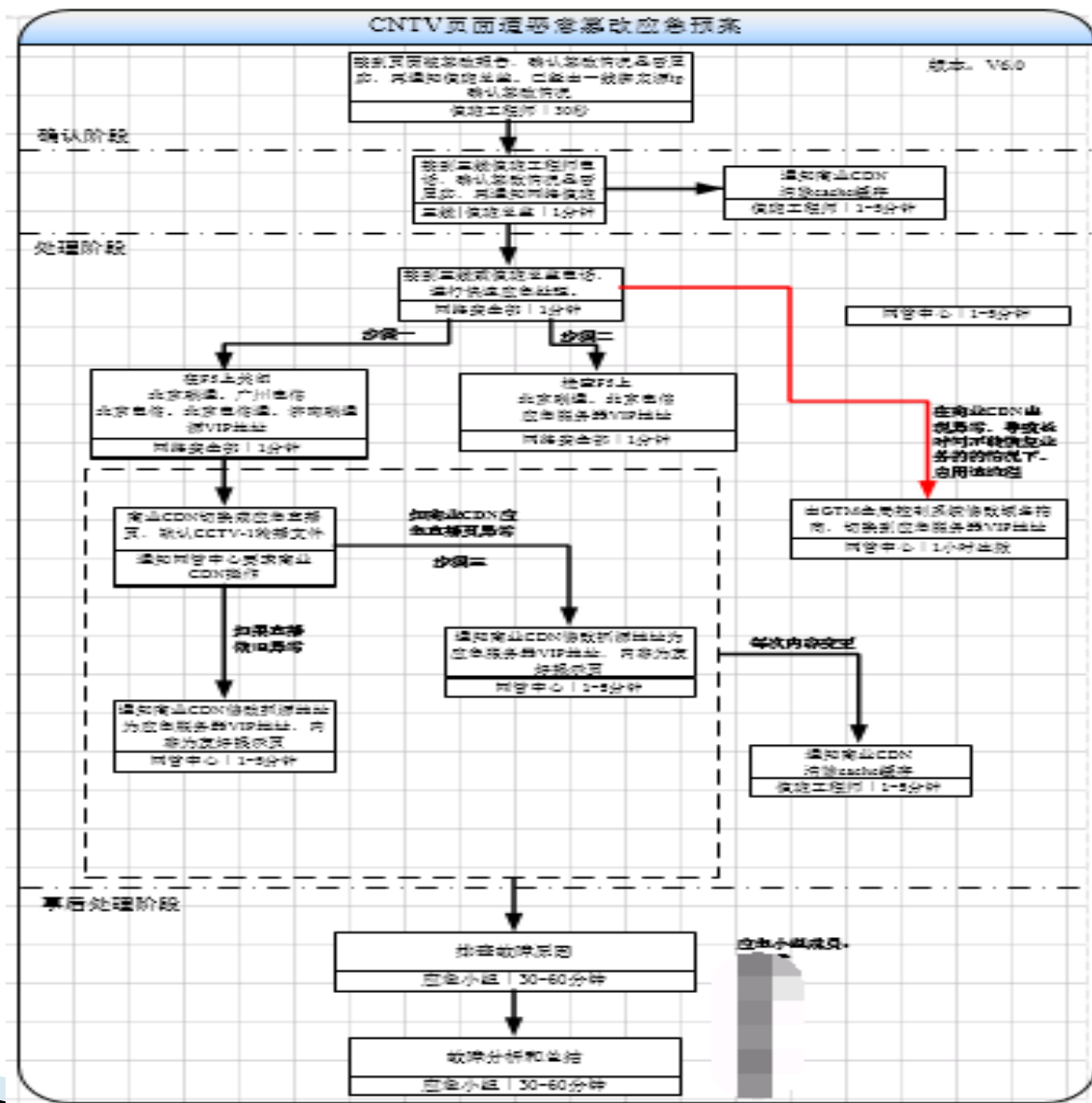
实施细则重点内容解读——应急管理

- 与《广播、电视中心实施细则》不同的是，增加了应急管理要求一章。这是在近期相关安全事件的背景下，提出不因为IPTV集成播控平台和网络广播电视台增加了应用和服务而降低系统安全性，在发生信息安全事件后应该能够及时消除不良影响，从保证业务连续性和系统安全性角度，从确保数据完整性和系统信息不被篡改角度出发增加的相关内容。从而使整个篇幅中组织体系（安全中心）、制度体系、运行体系、技术体系和应急体系框架更为完善。
- 应急管理一章涵盖了应急机构、应急预案、应急演练、应急通报机制以及事故事件应急处理五个部分内容。

实施细则重点内容解读——应急管理

- 首先要求健全机制，建议设立应急管理领导小组，以便统一指挥，协调有序地开展应急管理工作；
- 二是建立完善的应急预案。在此过程中，由于IPTV集成播控平台以及网络广播电视台的运行牵涉到众多相关单位，因此实施细则特别指出，应急预案的编制过程中应当征求其他合作单位、专家的意见，与相关的预案作好衔接。
- 第三，应通过应急演练，熟悉应急的指挥机制、决策、协调和处置的程序，并检验应急预案的可行性，并不断改进应急预案。
- 四是强调在事故事件发生后，应及时将相关情况汇报给应急管理领导小组，并通报受到负面影响的外部机构、互连单位以及相关设备及服务提供商，并上报主管部门及公安机关。并提醒要严格按照组织相关规定和要求对外发布信息。
- 五是处置高效。要实施细则分别针对内容篡改、非法入侵、病毒传播、技术故障及相关灾害提出了应急措施。确保突发事件发生时反应快速、措施得力、资源充足、操作准确，以尽可能降低突发事件、事故可能造成的损失。

应急预案案例



值班员应急处置不当事故案例

- ▶ 2014年8月24日上午8时35分08秒，湛江分公司总前端机房数字电视系统主用复用加扰系统故障，经多次重启无效。在该情况下，应急处置人员未切换备用复用加扰系统，而是对该主用设备进行了更换和参数重新配置，造成62套标清数字电视节目播出中断1小时58分钟。
- ▶ 2012年7月16日1时，辽宁省网络公司发生一起在上级变电站对外电进行例行中断检修过程中，因UPS故障造成部分设备失电，导致6套付费频道分别停播40分15秒的重大停播事故。

安全播出重大事故界定标准及上报单位

台站类型	停播类型	停播时长			上报单位
		重保期的重点时段	日常重点时段/重保期	日常	
IPTV、手机电视集成平台	全台性停播	≥10分钟	≥20分钟	≥30分钟	逐级报总局
	直播频道中断	≥30分钟	≥1小时	≥3小时	逐级报总局
网络广播电视台	全台性停播	≥10分钟	≥20分钟	≥30分钟	逐级报总局
	直播频道中断	≥30分钟	≥1小时	≥3小时	逐级报总局

报告流程

发生安全播出事件、事故的安全播出责任单位

立即报告

当地广播影视行政管理
部门或监测监管部门

特别重大事件、
重大事件

应上报总局的事件、
事故

立即电
话报告 是

是

省级监测监管
部门

应上报总局的
事件、事故

是

2小时填报
事故库，12
小时简要报
告，24小时
详细报告

2小时内传真快
速报告单或填
报事故库

省级广播影视
行政部门

总局监测监管部门

立即
开展
事件
事故
初步
调查

特别重大、重大
事件、特大事故

4小时内报简
要书面报告，
12小时内报送
详细书面报告

核实情况，及时上
报，提交书面报告

总局科技司

是

四、工作建议

完善体系，认真做好实施细则的贯彻落实

- ❑ 细则内容的掌握理解关键在于所引用文件和标准，加强相关内容学习
- ❑ 加强培训和对照检查，贯彻落实细则各项要求，及时整改
- ❑ 积极对细则修订提出宝贵意见
- ❑ 积极开展信息安全风险评估
- ❑ 积极探索提出安播创新手段
- ❑ 积极开展突发事件应急演练

关注细节，预防事件事故发生

- ❑ 外部环境的变化（天气、节目调整、直播延长等）
- ❑ 系统的变化
- ❑ 人员的变化
- ❑ 流程的变化
- ❑ 场景的变化（施工、检修等）

谢谢！