浙江省应急广播体系安全运行管理规范
（征求意见稿）

前　　言

本文件按照GB/T 1.1—2020 《标准化工作导则 第1部分： 标准化文件的结构和起草规则》的规定起草。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别专利的责任。

本文件由　　归口。

本文件起草单位：

本文件主要起草人：

引　言

为进一步促进我省的应急广播体系建设，加强应急及广播安全播出、网络安全、设施安全等。浙江省广播电视局组织专家，结合我省的这些年来的在应急广播推进中的工作经验的积累和产业链现状，本着普适、提高、规范的原则，在参考其他国内外规范、标准的基础上结合我省已有研究和实践，通过从吸收、借鉴和创新等手段制定了本规范。

1　范围

本规范适用于浙江省各级应急广播调度控制平台、传输覆盖网络和应急广播终端的安全运行管理。

2　规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件，仅注日期的版本适用于本文件。

凡是不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

GY/T 220.4—2007 移动多媒体广播 第4部分：紧急广播

GD/J 051—2014 卫星直播应急广播技术要求和测量方法

GD/J 080—2018 应急广播系统资源分类及编码规范

GD/J 081—2018 应急广播安全保护技术规范 数字签名

GD/J 082—2018 应急广播消息格式规范

GD/J 083—2018 应急广播平台接口规范

GD/J 084—2018 中波调幅广播应急广播技术规范

GD/J 085—2018 模拟调频应急广播技术规范

GD/J 086—2018 有线数字电视应急广播技术规范

GD/J 087—2018 地面数字电视应急广播技术规范

GD/J 089—2018 应急广播大喇叭系统技术规范

应急广播系统建设技术白皮书（2020）

国家广播电视总局、应急管理部《应急广播管理暂行办法》的通知

3　术语和定义

下列术语和定义适用于本标准。

3.1　应急广播

一种利用广播电视系统向公众发布应急信息的方式。

3.2　应急信息

通过县级以上人民政府及其有关部门、专业机构发布，应急广播系统接收的源信息。内容包括自然灾害、事故灾难、公共卫生和社会安全等各类信息。

3.3 应急广播消息

各级应急广播调度控制平台之间，以及应急广播调度控制平台到广播电视频率频道播出系统、各类应急广播传输覆盖资源和终端之间传递的播发指令等相关数据。应急广播消息包括应急广播信息主体文件、应急广播信息主体签名文件、应急广播节目资源文件、应急广播消息指令文件、应急广播消息指令签名文件。

4 网络安全

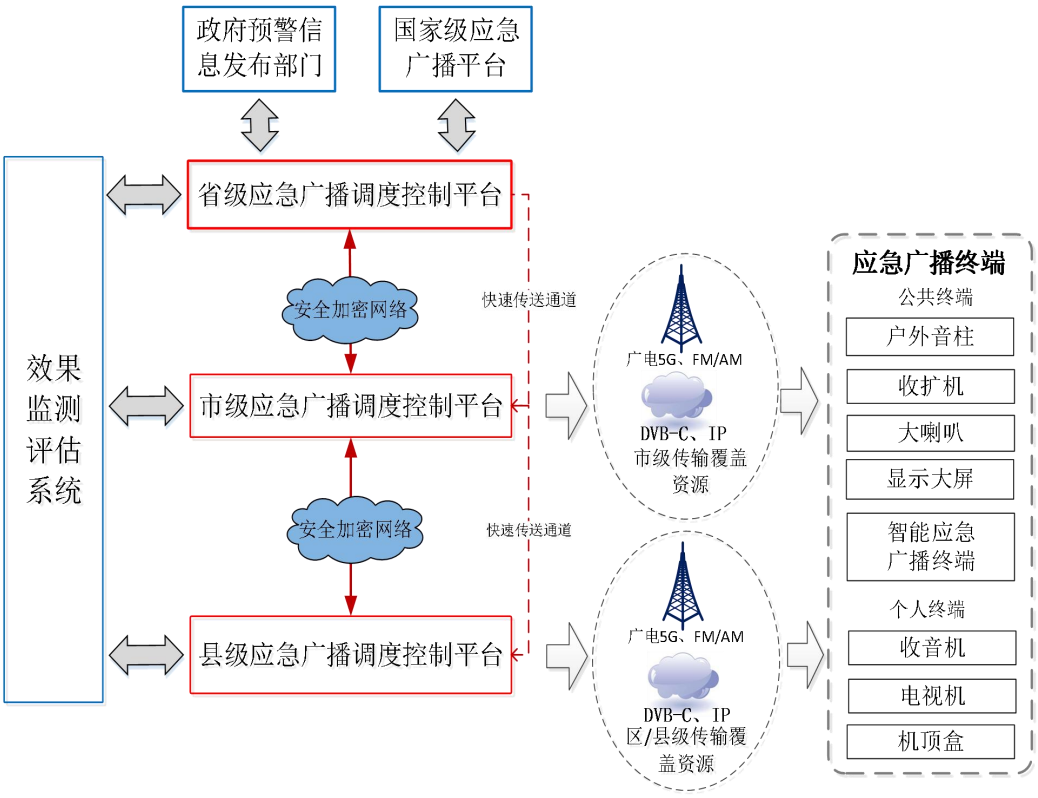

图1 浙江省应急广播体系总体架构图

4.1 职责主体

4.1.1. 县级以上人民政府广播电视行政部门负责本行政区域内的应急广播管理和督察工作，负责协调保障落实本级应急广播系统安全防护、升级改造、运行维护、网络传输等所需

运行维护经费。

4.1.2. 县级以上人民政府广播电视行政部门应明确本级应急广播网络的运行维护机构，应急广播系统运行维护机构应由具备有线广播电视传输资质的运营商来承担。

4.1.3. 应急广播系统运行维护机构应合理配备工作岗位和人员，建立健全技术维护、运行管理、例行检修等制度，承担应急广播正常运行和安全播出主体责任，维护和管理平台系统相关支撑软件和硬件设备，保障网络传输稳定可靠，数据加密安全高效，预警播发及时准确。

4.2 安全等级防护

4.2.1. 省级应急广播调度控制平台应满足三级安全等级保护要求，市级、县级应急广播调度控制平台应满足二级安全等级保护要求。各级应急广播调度控制平台应满足其相应等级保护所涉及的网络设备物理安全、设备安全漏洞、网络边界安全、入侵防护、访问控制、数据分级保护、敏感数据保密等方面的安全性要求。

4.2.2. 应急广播系统运行维护机构应定期组织开展应急广播系统和终端的安全检测，避免出现应急广播系统和终端被群控或感染蠕虫病毒的风险。

4.3 互联互通网络

4.3.1. 浙江省级应急广播调度控制平台主要基于广播电视网络建立基于有线/无线快速传送通道，调度控制平台间信令传输应采用安全加密传输，实现应急信息的快速传送任务。

4.3.2. 省级、市级、县级应急广播调度控制平台应当进行系统对接，通过安全加密传输专网络实现互联互通，确保应急广播信息完整、准确、快速传送到指定区域范围的应急广播终端。

4.3.3. 应急广播调度控制平台互联互通网络应遵循统一的 IP 地址分配规范，由省级应急广播运行维护机构负责 IP 地址的统一管理与分配，其他任何单位和个人禁止擅自修改。

4.3.4. 各级应急广播调度控制平台应明确网络边界，部署必要的网络安全防护设备，满足网络层至应用层安全防护控制策略，以保障平台南北向和东西向访问数据安全。各级应急广播调度控制平台应根据等级保护级别，按以下清单配置网络安全有关设备：

序号	名称	二级等保	三级等保
1	Web 应用防火墙服务	可选	√
2	边界防火墙	√	√
3	堡垒机（统一安管平台等）	可选	√

4	综合日志审计	√	√
5	数据库审计	可选	√
6	入侵防护系统	√	√
7	防毒杀毒	√	√
8	网站 HTTPS 证书	√	√
9	上网行为管理	可选	可选
10	终端准入	可选	可选
11	运维监控系统	可选	可选

4.3.5. 网络安全其他有关要求：

1、 防火墙端口开放及权限控制必须基于最小配置及最小权限原则，专线互联接口实行严格的安全访问策略，禁止配置不受限制的防火墙访问规则；

2、 具备入侵防御和恶意代码防范，检测能力，防止或限制从外部和内部发起的网络攻击行为并有效阻断，同时保持病毒库的更新频率；

3、 部署网络审计系统，对网络行为、流量等进行审计，实时监控网络攻击行为；

增强终端设备安全准入管理，及时发现潜在威胁，避免非法终端接入

4.3.6. 数据加密传输

省应急广播调度控制平台与各市、县级应急广播平台对接的加密机对接要求如下：

1、 市、县级平台必须配置应急广播专用加密机，加密机需符合《GD/J 081—2018 应急广播安全保护技术规范 数字签名》，需通过第三方专业测评机构测试。

2、 与省平台对接的市、县级应急广播平台都需要遵循《GDJ 081-2018 应急广播安全保护技术规范 数字签名》，市、县级应急广播平台能够调用本级的应急广播加密机完成上级平台消息、指令的验签，并且签名下发应急广播消息和指令给下级平台、适配器、终端。

4.4 运维管理

4.4.1. 根据本级应急广播系统等级保护的技术要求和安全性原则进行网络区域划分，实现网络运维的分级分类控制管理。

4.4.2. 运维管控平台应部署在专门的运维操作室或监控室，并按照等保要求，使用堡垒机进行运维操作。

4.4.3. 运维人员应密切监视应急广播平台系统设备运行情况，定期排查故障风险点，预防

和解决平台系统故障，使上下级平台全天 24 小时处于正常连通状态，确保平台系统数据的完整、准确。

4.4.4. 制定应急预案，加强应急演练，及时、正确处理网络故障和突发事件，确保应急广播正常运行。

4.5 设备管理和用户管理

4.5.1. 针对分布到乡镇甚至村一级的运营终端，应建立专用的设备管控平台，建立用户登录审查制度，明确用户在创建、使用过程中的安全控制要求，具备以下管控能力：

1) 采用网关模式实现网络隔离，非认证的终端无法直接访问应急广播平台。
2) 支持客户端双因素认证，短信或手机 APP 的 OTP。
3) 具有终端管控功能，可以管控这些终端非法外联、防病毒、防 U 盘私插等。
4) 支持检测终端非法外联、中病毒、扫描内网、运行黑客工具等行为，发现风险后实时断开内网应用访问。

4.5.2. 建设统一的用户管控平台，集中运维，满足各级运营客户端、人员和账号的安全管控。应急广播平台账号分配和运营终端管控的账号分配应当一致，均采用实名制管理，账号分配到人，通过安全策略设置限制不同的登录用户的访问范围及访问权限。