ICS 35.240
L 72

DB

北 京 市 标 准 化 指 导 性 技 术 文 件

DB11/Z 361—2006

应急指挥系统信息化技术要求

2006-06-14 发布

北京市质量技术监督局 发布

目　　次

前　言

制定北京市标准化指导性技术文件《应急指挥系统信息化技术支撑体系》（以下简称本文件）的目的是实现北京市各种应急相关技术资源的整合与共享，避免重复建设与数据交叉，使用统一通讯体系、统一基础资源库、统一基础应用支撑平台、统一安全子系统和统一备份子系统，使北京市应急指挥系统与各区县和各专项系统之间体系结构兼容、信息共享、系统联动，并支持综合决策分析，为北京市各专项应急指挥部及各区县应急指挥中心在研究和建设应急指挥系统的工作中提供指导。

本文件为第一次制订。

本文件由北京市信息化工作办公室提出并归口。

本文件起草单位：北京市信息资源管理中心、北京市政务网络管理中心、北京市信息安全测评中心、北京东方正通有限公司、北京天之华软件系统有限公司和华为技术有限公司。

本文件主要起草人：单青生、彭凯、黄晓斌、林绍福、毛东军、刘玉荣、冷飚、高顺尉、赵玉梅、王树全、刘旭日、赵琰昉、穆勇、王新、钱秀槟、谢艳丽、方理平、董渊、成金爱、张骥、赵金福、王山、王剑伟、苏革威、韦利刚。

应急指挥系统技术支撑体系

1 范围

本文件规定了北京市应急指挥系统技术总体框架，对总体框架、应用基础支撑平台、专项应急指挥系统、区县应急指挥系统、基础应急信息资源建设及管理、网络基础设施、安全体系等给出技术要求。

本文件适用于北京市各类应急指挥系统的规划和建设。

2 规范性引用文件

下列文件中的条款通过本文件的引用而成为本文件的条款。凡是注明日期的引用文件，其随后所有的修改单（不包括勘误的内容）或修订版均不适用于本文件。然而，鼓励根据本文件达成协议的各方研究是否可使用这些文件的最新版本。凡是不注日期的引用文件，其最新版本适用于本文件。

GB 7027-2002 信息分类和编码的基本原则与方法

GB/T 20001.3-2001 标准编写导则

SJ/T 11228－2000 数字集群移动通信系统体制

DB11/T 145-2002 政务公开网站通用安全技术要求

DB11/T 171-2002 党政机关信息系统安全测评规范

H.323 国际电信联合会（ITU-T）提出的基于分组交换的多媒体通信标准协议族。

H.263 国际电信联合会（ITU-T）提出的G.260系列视频压缩编码标准

京信息办[2001]26号 区域性公用信息平台网络建设技术规范

京信息办[2002]57号 关于北京市电子政务专网IP地址和域名的通知

京信发[2004]1号 关于全面推进电子政务建设的意见

京信息办函[2004]72号 关于本市各级党政机关网络与信息系统开展安全等级保护工作的通知

京信息办函[2004]129号 北京市电子政务总体技术框架（试行）

京政发[2005]17号 北京市突发公共事件总体应急预案（2005年修订）

京办字〔2005〕1号 关于印发《北京市800兆数字集群无线政务网编组、呼号方案》的通知

京办字[2005]7号 中共北京市委办公厅北京市人民政府办公厅关于成立北京市突发公共事件应急委员会的通知

3 术语和定义、缩略语

下列术语和定义、缩略语适用本标准化指导性技术文件

3.1 术语和定义

3.1.1

突发公共事件 public emergency

突然发生的，造成或者可能造成人员的重大伤亡、财产的重大损失，并对社会造成重大影响，危及公共安全的事件。

3.1.2

总体应急预案 emergency response ensure plan of Beijing

组织管理、指挥协调相关应急资源和应急行动的整体计划和程序规范。

3.2 缩略语

ＣＤＭＡ	Code Division Multiple Access（码分多址)
ＣＴＩ	Computer Telephony Integration（计算机电话集成）
ＤＩＡＡ	Dispatcher Interface Audio Adapter (调度台音频接口适配器)

ＤＩＡＣ	Dispatcher Interface Audio Controller (调度台音频接口控制器)
ＤＳＣ	Dispatcher Station Controller (调度台控制器)
ＤＷＳ	Dispatcher Workstation (调度台工作站)
ＤＸＴ	Digital Exchange for TETRA (TETRA数字集群交换机)
ＧＫ	Gatekeeper (网关)
ＧＳＭ	Global System for Mobile Communications（全球移动通信系统）
ＩＤＳ	Intrusion Detection System（入侵检测系统）
ＭＣＵ	Multipoint Control Unit (多点控制单元)
ＮＡＴ	Network Address Translation（网络地址转换）
ＰＡＢＸ	Private Automatic Branch eXchange（专用自动交换分机）
ＰＫＩ	Public Key Infrastructure (公钥基础设施)
ＰＳＴＮ	Public Switched Telephone Network (公众电话网)
PVC	Permanent Virtual Circuit（永久虚电路）
ＴＣＰ／ＩＰ	transmission Control Protocol/Internet Protocol （传输控制协议/互联网络协议）
ＴＥＴＲＡ	TErrestrial Trunked RAdiao（陆上集群无线电）
UDDI	Universal Description ， Discovery ， and Integration(统一描述，发现和集成)
ＶＬＡＮ	Virtual Local Area Network（虚拟局域网）
ＶＰＮ	Virtual Private Network（虚拟专用网络）
VOD	Video on Demand（点播图像）
VOIP	Voice Over IP（IP语音）

4 总体框架

4.1 北京市应急指挥系统的组织体系

北京市建设市区两级应急指挥系统(见图1)，市应急指挥中心规划、组织、协调、指导、检查各专项应急指挥部和各区县应急指挥中心的突发公共事件预防和应对工作。各专项应急指挥部遵从相关预案和行业规定，建立和完善突发公共事件管理与应急系统，指挥调动突发事件应急处置队伍。区县应急指挥中心主要完成属地管理原则所赋予的各项任务。

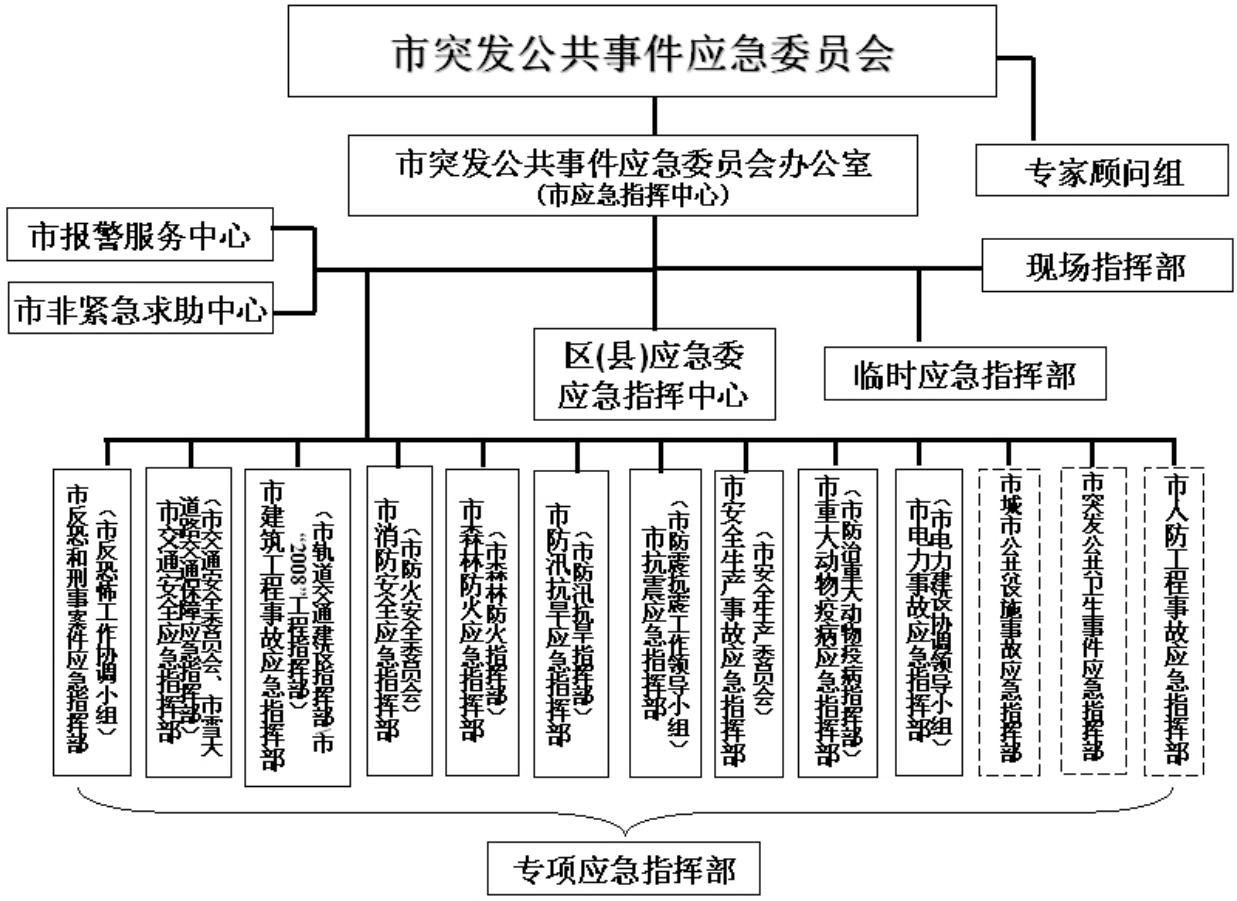

图1　应急指挥系统的组织体系

4.1.1　北京市突发公共事件应急委员会

简称市应急委（下同）。由该委员会负责统一领导全市突发公共事件的应对工作。委员会下设专项应急指挥部和以相关委办局为依托临时成立的处置突发公共事件现场指挥部。

4.1.2　市应急指挥中心

北京市突发公共事件应急委员会下设办公室（简称市应急办，下同），作为日常办事机构，挂市应急指挥中心牌子。市应急指挥中心备有指挥场所和相应的设备，作为突发事件发生时市应急委的指挥平台。

4.1.3　突发公共事件专项应急指挥部

为应对某类突发公共事件成立的跨部门综合应急管理机构。如市防汛抗旱应急指挥部、市安全生产事故应急指挥部等。

4.1.4　相关委办局

与突发事件的预测、预警、处置、善后、保障等各环节有关的市属各委办局，包括主责部门、预测部门和协作部门。

4.1.5　应急专业处置队伍

由相关委办局或企业组织的基本抢险救援队伍。同一支应急专业处置队伍在不同事件中，其可以分别做为主责处置队伍或应急救援队伍，两种角色是根据不同应急预案来确定的。公安、交警、消防、急救等专业处置队伍是骨干应急救援队伍。

4.2　北京市应急指挥系统的业务体系

4.2.1　事件等级

为了有效处置各类突发公共事件，依据突发公共事件可能造成的危害程度、波及范围、影响力大小、人员及财产损失等情况，由高到低划分为特别重大（Ⅰ级）、重大（Ⅱ级）、较大（Ⅲ级）、一般（Ⅳ级）四个级别。

4.2.1.1 特别重大突发公共事件（Ⅰ级）

指突然发生，事态非常复杂，对北京市公共安全、政治稳定和社会经济秩序带来严重危害或威胁，已经或可能造成特别重大人员伤亡、特别重大财产损失或重大生态环境破坏，需要市委、市政府统一组织协调，调度首都各方面资源和力量进行应急处置的紧急事件。

4.2.1.2 重大突发公共事件（Ⅱ级）

指突然发生，事态复杂，对一定区域内的公共安全、政治稳定和社会经济秩序造成严重危害或威胁，已经或可能造成重大人员伤亡、重大财产损失或严重生态环境破坏，需要调度多个部门、区县和相关单位力量和资源进行联合处置的紧急事件。

4.2.1.3 较大突发公共事件（Ⅲ级）

指突然发生，事态较为复杂，对一定区域内的公共安全、政治稳定和社会经济秩序造成严重危害或威胁，已经或可能造成较大人员伤亡、较大财产损失或生态环境破坏，需要调度个别部门、区县力量和资源进行处置的事件。

4.2.1.4 一般突发公共事件（Ⅳ级）

指突然发生，事态比较简单，仅对较小范围内的公共安全、政治稳定和社会经济秩序造成一定危害或威胁，已经或可能造成人员伤亡和财产损失，只需要调度个别部门或区县的力量和资源能够处置的事件。

4.2.1.5 各类突发事件的具体分级指标

按照国家总体应急预案、国家专项应急预案和各部委的部门预案的相关规定执行。

4.2.2 北京市应急指挥系统的应急联动

4.2.2.1 应急联动机制

北京市突发公共事件应急委员会、北京市应急指挥中心、各专项应急指挥部、相关委办局和区县应急指挥中心在特别重大（Ⅰ级）、重大（Ⅱ级）、较大（Ⅲ级）和一般（Ⅳ级）事件发生后的应急联动机制遵照京政发[2005]17号文第4条执行。

突发公共事件应急预案启动后，事件具体处置的指挥调度职能由各专项应急指挥部执行，调度相关处置队伍和应急救援队伍分别按照各自职责和业务范围，密切配合，具体负责突发公共事件的预防、处置和善后等工作。

市应急指挥中心按法定程序和权限对各区县应急指挥中心、各专项应急指挥部和相关委办局行使跨部门的组织协调。

4.2.2.2 应急联动信息流程

应急指挥系统信息进入的渠道有多种形式（见图2）。各专项应急指挥部所拥有的专业监测系统所获辖区内外信息，经分析整理后按规定报送市应急指挥中心，并按照突发公共事件发生、发展的等级、趋势和危害程度，及时向市应急指挥中心提出相应的预警建议。

以语音、网络和短信等方式发送的各类公众报警信息，由市紧急报警服务中心负责将先期处置指令直接下达到骨干应急救援队伍和区县应急指挥中心，并通报各相关专项应急指挥部。

各专项应急指挥部在处置突发公共事件过程中的信息管理应遵循京政发[2005]17号文第6条执行。

咨询类信息由非紧急求助中心（市政府便民电话）负责协调相关委办局解决，对打入市非紧急求助中心的紧急类事务，通过热线转接到市报警服务中心处理。

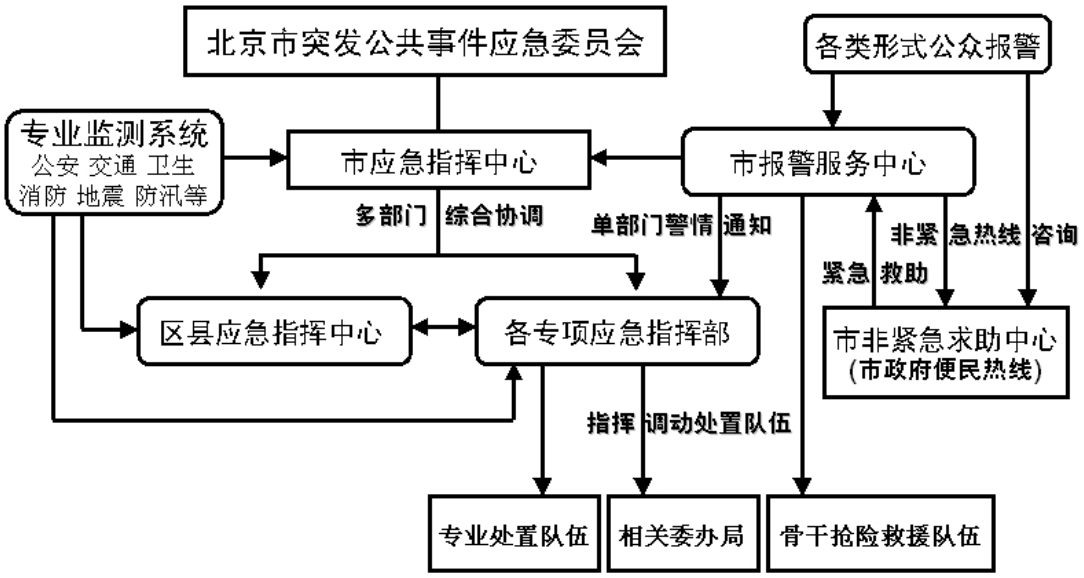

图2　应急指挥联动信息流程参考模型

4.3　北京市应急指挥系统的技术支撑体系

4.3.1　应急指挥系统的技术参考模型

由网络基础设施、基础信息资源、应用基础支撑平台、应急指挥系统、安全体系和技术标准与管理共同组成应急指挥技术支撑体系（见图3）。

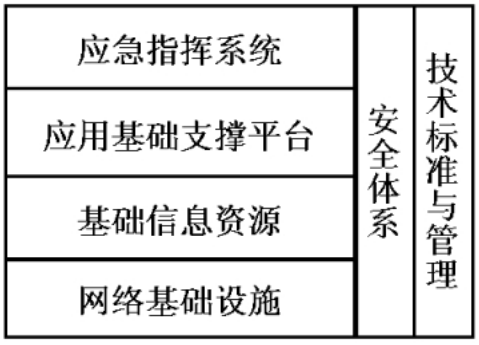

图3　应急指挥技术参考模型

4.3.2　应急指挥系统的技术支撑体系逻辑结构

北京市应急指挥系统技术支撑体系的逻辑结构如图4所示。

该体系以北京市统一规划建设的有线和无线政务专网进行信息传输，使用全市统一建设的基础数据库和共享数据库，共享各专项应急指挥部和相关委办局生产的各类业务数据库，通过市应急指挥系统应用基础支撑平台进行信息交换而构成。各专项应急指挥部和区县应急指挥中心的应用系统，使用北京市电子政务外网门户，向北京市突发公共事件委员会及其他应急管理部门提供个性化的辅助决策服务，利用英特网向公众提供应急信息服务。

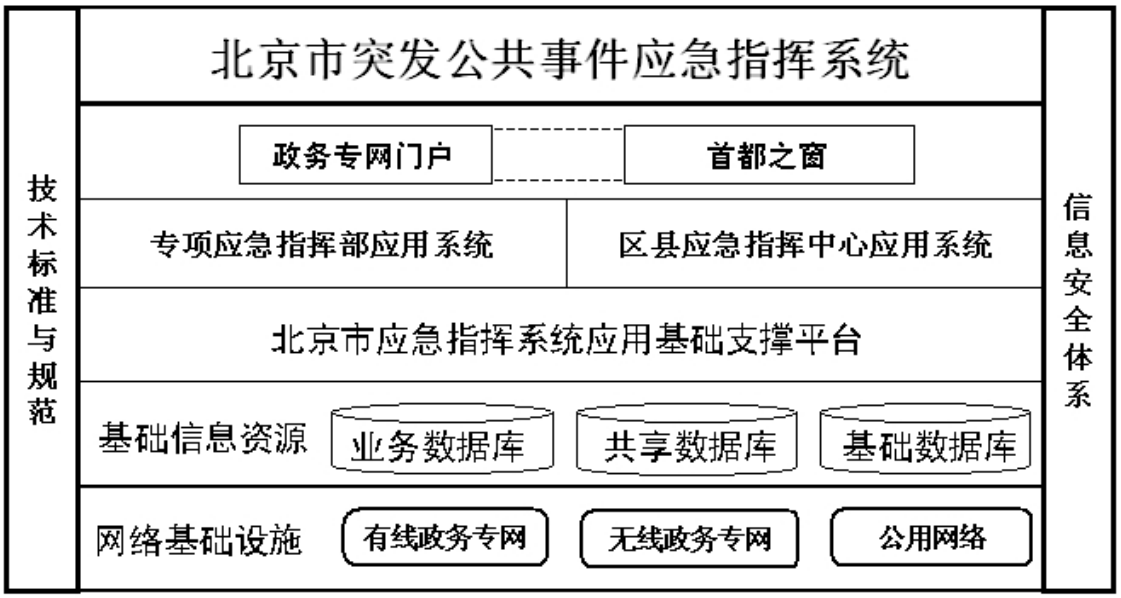

图4　北京市应急指挥系统技术支撑体系逻辑结构图

4.4　应急指挥中心模型

4.4.1　固定指挥中心

4.4.1.1　固定指挥中心功能

北京市应急指挥中心、区县应急指挥中心及专项应急指挥部均以固定指挥中心形式建设。固定指挥中心在使用有线通讯、无线通讯、网络基础设施、空间管理系统等技术条件下，依托各专业监测网络、视频监控系统、视频会议系统等模块，实现信息获取、信息分析、应急现场信息存储、情景再现、视音频会议召开、指令下达、信息发布等功能。上述功能为突发公共事件处置决策提供事件动态监视、跟踪评估与应急对策会商支持，使决策者对发生在辖区范围内的突发事件能够“看得见、听得清、信息准、反应快”，确保“指令下得去，情报上得来”。系统应具有良好的扩展性。

在未启动应急预案时，固定指挥中心负责从相关渠道接收各类事件信息。

4.4.1.2　固定指挥中心技术构成

固定应急指挥中心应包括图像监控和大屏幕显示系统、有线通信系统、无线通信系统、计算机网络设备和集成、综合指挥席设备和集成、会议系统集成、综合保障系统集成、功能应用软件等。

4.4.2　移动指挥中心

4.4.2.1　移动指挥中心功能

移动指挥中心作为处理重大事件时现场指挥部的技术保障手段之一，是各专项应急指挥部应急系统的补充和延伸。可以移动指挥中心为基础组建现场指挥部，当固定指挥中心无法满足针对突发事件的信息收集、指令下达等功能时，移动指挥中心接替固定指挥中心的职能。它以800MHz数字集群、卫星、微波、GSM、GPRS、CDMA等作为传输手段，实现话音、图像、数据资料的无线实时传输。移动指挥中心可以从相邻基站接入区县应急指挥中心或市应急指挥中心。

4.4.2.2　移动指挥中心技术构成

移动应急指挥中心技术模块如图5所示，移动指挥中心必须至少但不限于包括指挥应用系统、视频会议系统、视频显示系统等，分别设置与数字集群通信系统、移动基站、各种信息系统、各种无线通信网络和视频传输系统的接口。

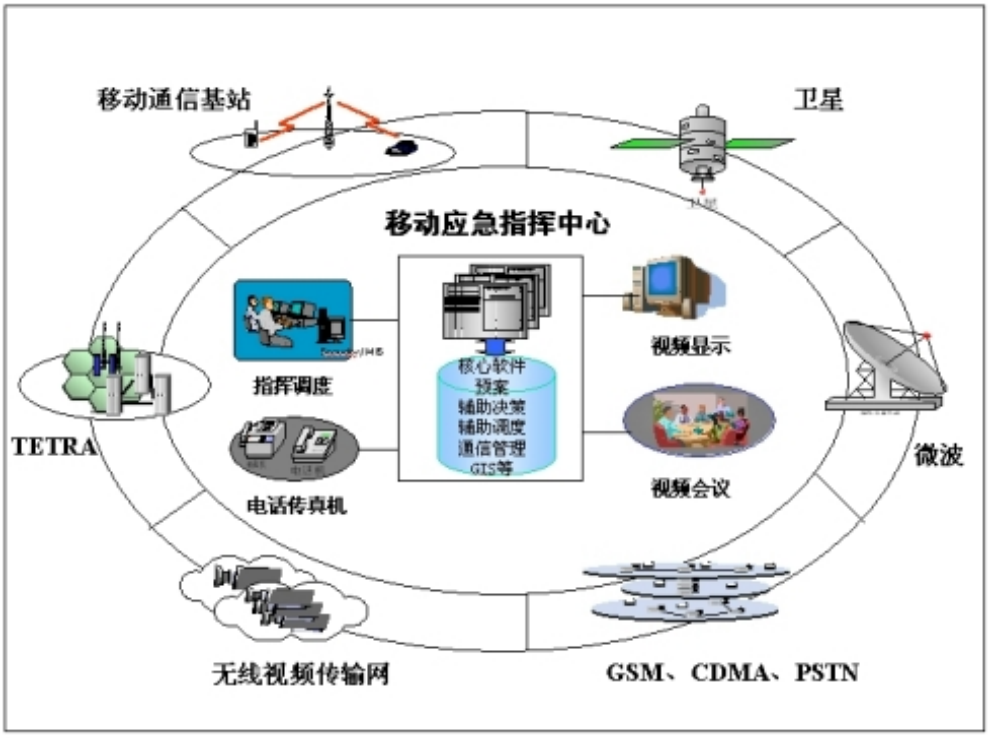

图5　移动应急指挥中心技术模块图

4.4.2.3　移动指挥中心的基本保障要求

移动指挥中心必须至少但不限于具备以下基本要求：

□　使用环境：

环境温度（指挥舱外）：　-20℃～+46℃
相对湿度（温度在40℃时）：　95%～98%
地面风速：　＜20米/秒
降雨：　＜50毫米

□　展开/撤收时间：

行驶状态转指挥工作状态时间：　15分钟
指挥工作状态转行驶状态时间：　10分钟

□　指挥准备时间：

正常状态（指挥舱内温度0℃～+40℃）：10分钟
紧急准备状态：　5分钟

□　系统可靠性：

平均无故障时间：　50小时
平均故障修复时间：　0.5小时

□　配备可供系统工作2小时的后备蓄电设备

□　配有自备发电机组并可保障系统连续工作

□　指挥舱载车道路通过能力：

可正常通过土路和碎石路路面。
在碎石路面以25公里/小时的速度行驶200公里，指挥系统设备无故障。

4.4.2.4　移动指挥中心的通信要求

在特定地点为移动指挥中心预留接入点，实现的连接方式如下：

□　与TETRA移动收发基站的连接：TETRA空中接口；

- TETRA移动收发基站与TETRA数字集群交换机的连接：通过卫星通信链路、微波链路、无线宽带IP链路相连；
- 与无线视频传输网络的连接：通过无线宽带IP网络实现；
- 与GSM、CDMA的连接：通过通信终端的方式连接。

5 应急指挥系统应用基础支撑平台

应急指挥系统应用基础支撑平台依托于北京市电子政务应用基础支撑平台，连接市应急指挥系统、各个区县/专项应急指挥系统的开放性基础设施。它提供各类信息资源/服务的跨部门共享、交换与整合。

该平台能够屏蔽基础信息资源和共享专业信息/服务资源的分布性和异构性，利用应急指挥系统的统一目录体系，能够在异构环境中获取相应信息资源或调用相应功能服务资源，以服务于上层应用。

5.1 应急指挥系统应用基础支撑平台体系结构

应急指挥系统应用基础支撑平台由基础组件层和核心服务层构成，其体系结构如图6所示。

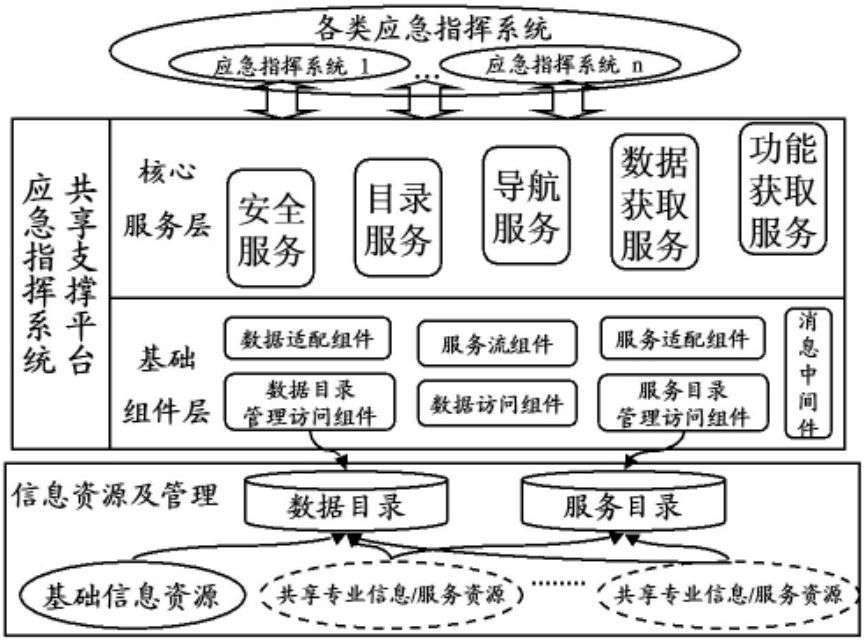

图6 应急指挥系统应用基础支撑平台体系结构

5.2 基础组件层

基础组件层通过标准的目录管理体系，通过信息资源发现系统和信息资源获取系统，实现了信息资源/服务的发现、获取、转换和集成，屏蔽了数据及系统的异构性和分布性,并在逻辑上形成了核心服务层，为上面各类专项应急指挥系统和区县应急指挥系统提供统一信息服务和功能支撑。

基础组件层由数据目录管理访问组件、服务目录管理访问组件、数据访问组件、数据适配组件、服务适配组件、服务流组件和消息中间件组成，其功能特点和交互方式的应符合《北京市电子政务总体技术框架（试行）》。

5.3 核心服务层

核心服务层能够以web服务和API两种形式的标准接口为上层应用提供安全服务、目录服务、导航服务、数据获取服务和功能获取服务等基础性服务。这些服务的基本功能和建设规范均应符合《北京市电子政务总体技术框架（试行）》。

5.4 服务模式

按照《北京市电子政务总体技术框架（试行）》的要求，应急指挥系统应用基础支撑平台应根据用户（应用系统）的不同需求，提供以下几种服务模式：

- □ 信息代理模式
- □ 信息导航模式
- □ 服务代理模式
- □ 服务导航模式
- □ 安全通道模式

5.5 原则性要求

应急指挥系统共享支撑平台的建设应遵循《北京市电子政务总体技术框架（试行）》的要求，统一规划、设计与建设应急指挥系统共享支撑平台；平台所提供功能应充分体现各子系统的普遍性需求，并能为各子系统提供规范的共性服务，从而实现标准统一，避免重复性建设。

应急指挥系统两级应用基础支撑平台如图 7 所示。与应急指挥系统相关的各市级委办局、区县应急指挥系统、专项应急指挥系统应分别建立节点服务器与市级中心服务器连接，并通过市级平台实现信息资源和应用系统的互连互通、交换与共享。同样，与区县应急指挥系统相关的各区县委办局也需要建设节点服务器与本区县中心服务器连接。

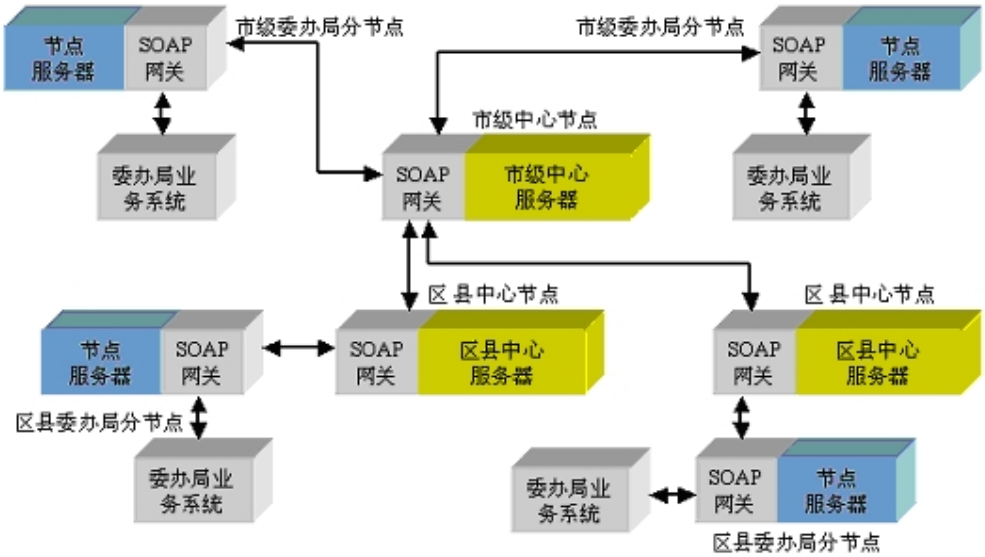

图7 应急指挥系统两级应用基础支撑平台

6 专项应急指挥系统

6.1 专项应急指挥系统的业务逻辑

专项应急指挥系统建立专项应急数据中心，采集的突发公共事件数据按照专业技术规范直接报送到该数据中心，数据中心存放相关的指挥调度信息。数据中心根据突发公共事件等级设置不同的数据存取和查询权限，专项应急系统根据事件等级对应的管理权限，进行突发公共事件数据的分流，向北京市应急指挥中心、区县应急指挥中心、现场指挥部、北京市报警服务中心、国家相关部委和国务院应急办提供应急信息服务。

专项应急指挥系统实现针对某类突发公共事件的监测、预警、上报、处置、恢复重建以及教育、培训和演习全过程的处置和管理。专项应急指挥系统的逻辑架构如图8所示：

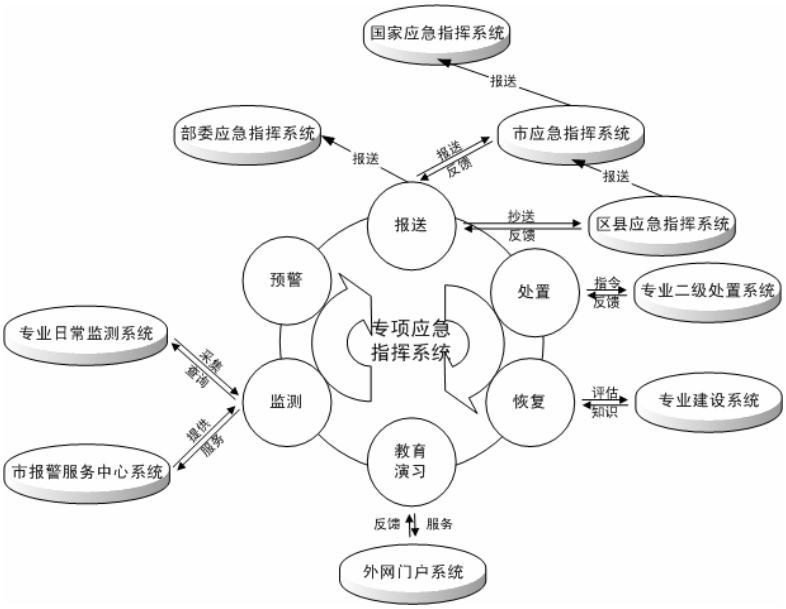

图8　专项应急系统的逻辑架构

6.1.1　监测

专项应急指挥系统对突发公共事件的监测，是建立在相关委办局专业监测系统基础之上的，同时可以接收市报警服务中心系统和其它系统传送的突发公共事件报警信息，实现对突发公共事件的全面监测。

6.1.2　预警

专项应急指挥系统根据采集到的数据和系统设置的预警模型实现对不同等级突发公共事件的预警。

6.1.3　报送

专项应急指挥系统根据事件等级采用直报方式，向专项应急指挥部、区县应急指挥中心、市应急指挥中心、各部委应急指挥部上报或抄送突发公共事件信息。

6.1.4　处置

专项应急指挥系统按照预案规定直接进行突发公共事件的应急指挥调度，通过专项二级、三级等应急指挥系统实现应急资源的指挥调度，通过现场信息的采集得到突发公共事件处置结果的反馈并及时调整和修改预案。根据突发事件的等级，为现场应急指挥部提供应急指挥服务，为市应急指挥中心提供应急组织协调服务。

不同类别委办局的具体应急业务类型，包括主责部门、预测部门、保障部门，具有各不相同的指挥调度系统模型。两种调度模式在不同的突发公共事件条件下应能够进行切换或者同时具备。预测部门如果不需要设置应急指挥中心的，在保障应急行动的前提下，可以不建设应急指挥调度系统功能。系统根据调度模型实现调度处置功能。

6.1.4.1　主责部门应急指挥调度模型

处置主责部门的应急指挥调度模型，其应急指挥调度系统建立在主责委办局日常的管理系统基础之上，应满足对本专项内各个专业应急资源的指挥调度的要求；对非主责委办局的应急资源通过系统资源的整合实现统一的指挥调度；对外部其它应急资源的指挥调度，由专项应急指挥部通过北京市应急指挥中心或区县应急指挥中心协调后纳入本系统，由专项应急指挥中心统一指挥调度。指挥调度系统采用分级指挥调度的模式，在各个专项指挥调度系统下设各个专业二级指挥调度系统，二级指挥调度系统通常也采用两级或多级指挥调度模式，专业指挥调度机构直接指挥调度现场应急处置，并将处置结果进行直接反馈。

6.1.4.2　保障部门应急指挥调度模型

处置保障部门的应急指挥调度模型，其应急指挥系统应能够接收专项指挥系统要求进行配合应急处置的指挥命令，在接到配合应急处置的指挥命令后，根据专项应急指挥系统的要求对本专业应急资源进行指挥调度，并将指挥调度的现场信息及时反馈给专项指挥系统。

6.1.5 恢复

专项应急指挥系统根据评估对突发事件的事件程度和影响范围进行评估；根据恢复建设模型，为恢复建设提供决策支持。

6.1.6 教育、培训和演习

专项应急指挥系统通过模拟演习达到对应急参与人员的日常培训和演习的目的，通过统一的门户系统向广大的民众进行突发公共事件的预防、处置知识的宣传和教育。

6.2 专项应急指挥系统基本要求

专项应急指挥系统由专项应急事务处置的主责委办局负责建设，其它相关委办局协助工作。建设过程中参照本文件确立的参考模型。

6.2.1 专题资源整合要求

专项应急指挥系统应实现专项应急指挥部内部各委办局相关应急专题资源的整合。每个委办局可以面向专项应急系统提供专题资源服务，整个专项应急系统可以统一面向外部系统提供专题资源服务，提供服务的方式遵循信息服务标准。

6.2.2 不同突发事件间协作要求

以现有各专业技术规范要求的格式提供各突发事件涉及的专业数据的现状信息，现状信息包括空间位置信息和属性信息。同时提供不同突发公共事件对本专业设施的影响和本专业应该采取的应对措施，每个专项应急系统应能够接收统一的协作指令，配合进行本专项应急资源的调度和指挥。

6.2.3 突发公共事件上报处理要求

不同的专项突发公共事件上报数据格式，遵循现有的专业技术规范，要求按各个专项统一的上报格式进行数据上报，有关上报数据格式参见各个专项的相关行业标准。

专项应急指挥系统应能够满足不同频度的上报要求，能够支持按指定时间、按天、按周、按月、按季度、按年的定时上报形式，以及随时的不定时上报形式。

数据上报应采用直报的形式并根据突发公共事件等级进行分级报送，在报送的过程中，根据北京市市区两级突发公共事件指挥平台，形成市、区两级管理的原则进行信息分流报送。

6.2.4 数据交换和信息共享要求

专项应急指挥系统通过统一的应用基础支撑平台与区县应急指挥系统进行数据交换和信息共享。

专项应急指挥系统通过统一的应用基础支撑平台实现各专项应急系统之间的数据交换和信息共享。

6.3 专项应急指挥系统技术参考模型

专项应急指挥系统建立在网络基础设施、信息资源、基础应用共享支撑平台之上，并有完整的安全体系和遵照有关的技术标准。

专项应急指挥系统应具备但不仅限于下列子系统，包括：信息采集系统、监测预警系统、信息报送系统、指挥调度系统、恢复重建系统，以及视频监控系统、视频会议系统、通讯控制与调度系统、内容管理与发布系统、协同办公系统、数据整合与分析系统、事件专家知识管理系统、应急预案管理系统、应急模拟培训系统、基于空间的辅助决策分析系统、安全管理系统、网络管理系统、维护系统等功能模块。

专项应急指挥系统技术参考模型如图9所示。

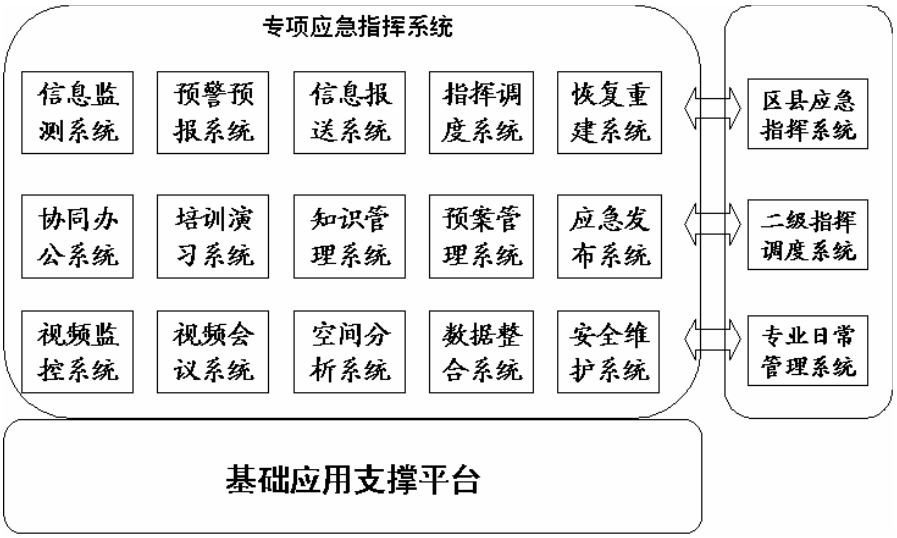

图9　专项应急指挥系统技术参考模型

6.4　专项应急系统功能/服务

6.4.1　突发公共事件监测功能

专项应急系统应具有突发公共事件监测的功能，能从日常管理的系统数据中、日常管理作业流程中、各种监测数据中发现突发公共事件隐患的功能，能利用各种数据挖掘工具，进行突发公共事件信息的挖掘分析，实现早发现、早报告、早处置，将突发公共事件消灭在萌芽状态。

6.4.2　突发公共事件预警功能

专业应急指挥系统要根据本专业特点建立各种突发公共事件预测预警模型，由日常管理系统不断为模型输入参数，一旦模型计算结果出现异常情况时，系统必须能够通过预先设定的途径进行报警，并宜自动通过电话、传真、Email、短信等方式提醒应急工作相关人员。

6.4.3　突发公共事件信息上报

专项应急按相关专业行业管理的业务模式，实行突发公共事件信息直报制度。突发公共事件一旦发生，系统必须能够自动地根据已经配置好的报送流程，根据事件等级的不同，直接报送到不同的应急机构，同时，根据不同的事件等级将信息报送或抄送市、区（县）应急指挥中心。信息报送业务逻辑模型如图10所示：

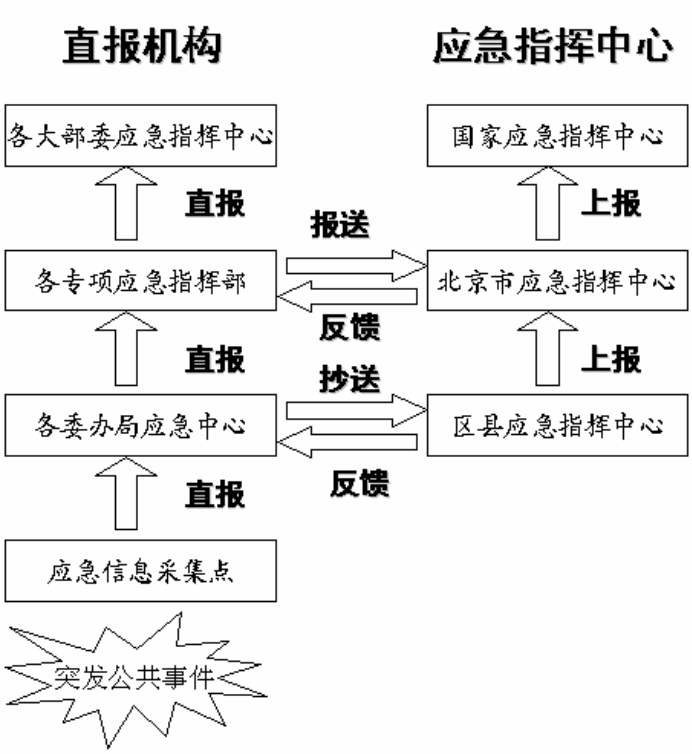

图10　专项应急信息报送业务逻辑参考模型

突发公共事件信息上报格式按现行的专业技术规范执行，能自动形成。

6.4.4　突发公共事件处置功能

应急处置是各个专业部门的责任。系统应提供各类突发公共事件处置预案的管理功能，包括预案的电子化、可执行化。提供针对本专业的应急处置方案，以及与应急处置相关的、需要其它专业配合的方案。通过处置系统直接指挥调度应急资源，直接连接二级、三级以及现场指挥调度系统下达调度指令，采集现场信息，反馈处置结果信息，根据现场信息及时调整和修改处置方案，充实预案库。

专项应急指挥系统应具备接收各级应急指挥中心调度指令和各种反馈的应急处置信息的功能，并根据统一调度指令，对突发公共事件进行处置。

6.4.5　资源调度分配功能

专项应急指挥部根据突发公共事件等级和预案，对应急资源采用统一调度的模式。专项应急指挥系统通过系统资源整合实现对主责单位的应急资源、保障单位的应急资源以及其它应急资源集中管理和统一调度。

由于各个专项应急指挥部涉及的不同专业的应急资源具有不同的调度权限，应急资源的调度指令应根据调度权限逐级下达。应急资源的现场调度情况，应通过系统直接反馈到专项应急指挥部，各专项应急指挥部根据现场情况及时进行预案的调整。

各个专业应急系统应该具备应急资源分配功能，能够设置本专业应急资源的空间分布、资源属性以及分配和调度方式。

6.4.6　会商与决策支持功能

系统应能够支持协同办公、空间分析、知识管理等功能，并基于视频监控和视频会议系统，在预警、预报、信息发布、指挥调度等功能中支持会商，提供决策支持。

6.4.7　信息发布功能

各个专项应急指挥系统必须支持应急信息的发布及发布内容的管理。在发布方式上，应支持空间信息的Web发布。系统应开发信息服务功能，宜利用Web服务技术实现专业应急信息的服务功能。

6.4.8　恢复重建功能

专项应急指挥系统的灾后重建应具备但不仅限于下列功能。

—— 事件录入功能

能够把各类事件信息（包括文字信息、数据信息、图片信息、录象信息、空间位置信息等）录入系统，便于系统进行事件分析。

—— 事件分布分析功能

能够将各种事件以空间信息为基础进行事件分布分析，以地理信息系统为依托，显示各类事件分布图。

—— 恢复重建模型分析功能

能够辅助管理灾后恢复工作，计算各类工作量，调度各种灾后恢复资源。各个专项应急指挥系统要提供恢复重建的模型分析功能，利用突发公共事件评估模型，对突发公共事件的危害进行评估。系统应能通过评估和模拟对各种重建方案作出评估，以便确定最优的恢复重建方案。系统确定的恢复重建方案通过统一的应用基础支撑平台为区县指挥中心提供决策依据。

6.4.9 平时管理功能

各专项应急指挥系统是建立在日常专业应用系统之上的，平时管理功能主要是实现各专业对应突发公共事件因子的管理和监测。

6.4.10 教育培训演习功能

专项应急指挥系统应具备仿真演习的功能，能通过仿真演习对应急工作人员进行培训和演练。

专项应急指挥系统能够通过统一的外网门户系统，建立专业应急教育培训版块，为广大的民众提供应对突发公共事件的基础知识教育，提高广大民众应对突发公共事件的能力。

7 区县应急指挥系统

区县应急指挥系统是以区域综合减灾为目标，各区县负责建设和维护的系统。平时为区县应急机构提供信息服务；在突发公共事件处置中，支持区县应急机构在市应急委领导下，参与特别重大和重大突发公共事件相关的应急工作，负责指挥本行政区域内各类较大和一般突发公共事件的应对工作。系统应由专门人员进行日常维护。

区县所属委办局应根据实际需要建设和维护以应急专业监测、信息报送、专业处置为主的业务系统。向市专项应急指挥部和区县应急指挥中心提供监测数据，报送事件信息；接受区县应急指挥中心的指令，具体负责属地突发公共事件的先期处置和善后工作的实施，提出处置建议、反馈执行结果；接受现场指挥部的统一指挥实施突发公共事件处置。

区县所属委办局专项应急指挥系统应遵循相关市专项应急指挥部的技术体系，可完善和建立电子政务系统，不宜建单独的指挥调度系统。

7.1 区县应急指挥系统基本要求

区县应急指挥系统应满足如下要求：

7.1.1 区县内资源整合要求

以全市统一的空间信息平台为基础，整合属地相关的基础信息数据和各种专业监测数据资源。

7.1.2 区县间协作要求

各区县应急指挥系统之间共享地图、人口等基本信息和应急相关信息。

7.1.3 突发公共事件上报处理要求

根据应急预案要求，为上级系统提供及时、准确、规范的数据。

7.2 区县应急指挥系统接口关系

在两级管理、分类指挥、综合协调、逐级提升的突发公共事件处置体系中，区县应急指挥系统位于第二级，是区县级指挥机构的信息管理系统，其在整个应急指挥系统的位置如图11所示。

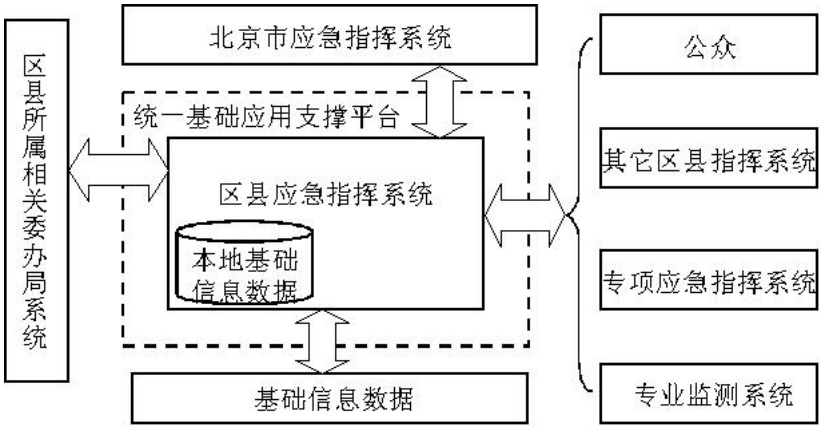

图11　区县应急指挥系统在整个应急指挥系统中的位置

7.3　区县应急指挥系统业务流程

区县应急指挥系统应适应如下业务处理流程：

7.3.1　预警处理

区县应急指挥系统日常运行中接收由专业监测系统和专项应急指挥系统发来的各种数据，根据所获得的相关数据和系统设置的预警模型实现对突发公共事件的预警，向市应急指挥中心提出相应的预警建议。

7.3.2　先期处置

启动区县专项应急预案，指挥所属相关委办局、社区和志愿者应急队伍，对属地发生的突发公共事件先期处置，包括：成立或协助成立现场指挥部；开展先期救援；组织、动员、帮助群众开展防、减、救灾行动。

7.3.3　现场指挥

专业处置队伍到达之后，作为属地现场指挥系统，汇集事件相关数据，协助市专项应急指挥系统进行事件处置，还应负责治安维护，交通保障，社会动员，人员疏散，群众安置等辅助工作。

7.3.4　善后工作

负责突发公共事件处置结束之后的各种善后工作，包括：损害核定，现场恢复，实施灾损补偿和事后恢复等工作。

7.3.5　宣传教育和培训演习

区县应急指挥系统日常运行状态下，开展突发公共事件的宣传教育，组织所属相关委办局、社区和志愿者应急队伍和群众进行培训和演习。

7.4　区县应急指挥系统数据流程

区县应急指挥系统向市应急指挥系统报送相关数据、接受市应急指挥系统的指挥指令并反馈执行结果。向区县所属相关委办局发送指挥调度指令并接收反馈。协调实施本辖区内跨街道（乡镇）、跨专业的应急。通过首都之窗或其他新闻媒体向群众发布公告、接受建议。从相关专业监测系统获取共享数据。

本地只建设和维护区县应急预案和应急相关的本地必要基础信息，其余数据宜应通过应用基础支撑平台从相关单位获得。对于目前无法通过共享方式得到的基础信息数据，可本地建设和维护，但应遵循相关专项应急指挥系统的技术体系和数据规范。

7.4.1　基础信息数据

共享基础信息数据库应由全市统一规划建设和维护，并提供给区县应急指挥系统使用。

7.4.2　监测数据

应由各专业监测业务系统向区县应急指挥系统提供。包括应急基础信息、视频、影像等监测数据。

7.4.3　指挥数据

区县应急系统接受市应急指挥系统的指挥数据；与专项应急指挥系统及其它区县应急指挥系统之间交换相关指挥信息；向本区县委办局各业务系统下达指挥数据。

7.4.4 反馈数据

区县应急系统向市应急指挥系统反馈指令执行结果；与专项应急指挥系统及其它区县应急指挥系统之间交换相关反馈数据；接受本区县委办局各业务系统的反馈数据。

7.5 区县应急指挥系统功能模块

区县应急指挥系统一般由事件处理、事件分析和数据交换三个层次构成，事件处理包括分预案管理、预警、处置和善后，事件分析包括各种数据的整合显示、分析、评价、会商和决策，为事件处理提供必要的信息，数据交换解决区县应急指挥系统与市应急指挥系统、本地事件处理单位、相关专项指挥系统、其他区县指挥系统之间通过应用基础支撑平台的数据共享问题。区县应急指挥系统功能模块参考模型见图12，系统应包含以下功能模块：

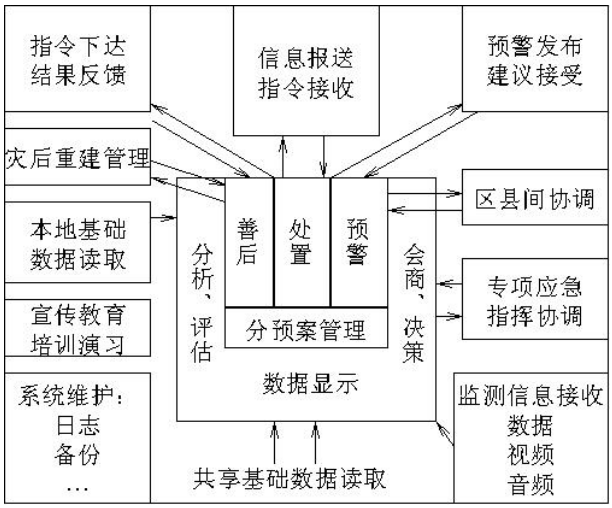

图12 区县应急指挥系统功能模块参考模型

7.5.1 监测信息接收

从相关专业监测系统中获取数据、视频、音频等监测数据。

7.5.2 基础数据获取

从共享基础信息库和本地基础信息库中读取所需基础信息。

7.5.3 应急协调

与相关的专项应急指挥系统、或其他区县指挥系统实现数据交互，达到协调指挥的目的。

7.5.4 数据整合显示

将从指挥部获得的监测信息与从本地获得的各种基础信息整合并实现图形化的综合显示。

7.5.5 数据分析评估

应对整合后的数据进行分析和挖掘，评估突发公共事件的等级。

7.5.6 会商决策

通过视频会商方式，提供决策支持。

7.5.7 区县预案管理

区县预案的定期更新、维护。

7.5.8 事件预警

对于较大和一般事件，发布相关预警信息、进入事件处置。一旦事态扩大，在进行先期处置的同时向市应急指挥中心提出相应预警建议，向事件可能波及的地区通报有关情况，必要时可通过媒体向社会发出预警。

7.5.9 事件信息上报

应按照标准数据格式向市级指挥系统报送相关信息，包括：对相关指令的执行情况、事态的最新进展。同时应将情况及时通报给各相关单位。对于较大以上的突发公共事件，应立即上报北京市应急指挥中心。

7.5.10 事件处置

区县指挥系统指挥所属相关委办局、社区和志愿者应急队伍实施先期处置，市属专业处置队伍到达之后进行协调和配合工作，执行上级指挥中心的指令，反馈相关结果，提出相应建议提供支持；区县现场指挥部负责事件的处理和上报，包括预案管理，决策支持，调度指挥和事件跟踪。

7.5.11 调度分配

根据预案实施应急资源分配和指挥调度，下达指令并接收反馈信息。

7.5.12 信息发布

向社会公众公布预警信息、动员令及事件信息，按照标准格式提供发布草稿，经过批准后，发布渠道需要支持因特网发布、短信发布、语音电话发布、电视发布、广播发布。

7.5.13 宣传教育

系统应利用网络等多种技术手段，面向公众、面向属地社区和农村进行突发公共事件的宣传教育。包括区县突发公共事件历史情况统计、本地多发性突发公共事件的处理和防护措施、本地相关部分和责任人、相关政策法规和管理公告等信息。

7.5.14 灾后重建

区县应急指挥中心要对突发事件损害核定工作提供支持，负责事件情况、人员补偿、征用物资补偿、重建能力、可利用资源评估数据的收集整理，为补偿计划和事后恢复计划提供数据支持，并跟踪落实情况。

7.5.15 系统维护

系统日常维护管理、日志信息处理、定期备份，本地应急管理基础信息数据的定期更新。

7.5.16 演习和培训

定期、不定期的演习和培训。

8 基础应急信息资源建设及管理

8.1 基础应急信息资源建设总体框架

北京市应急指挥系统的基础信息资源建设宜依托政府各部门已有及规划建设的各类基础信息资源。其总体架构应包括：基础数据库、共享数据库、业务数据库及信息资源目录等内容，应急指挥系统基础信息资源总体架构如图 13 所示：

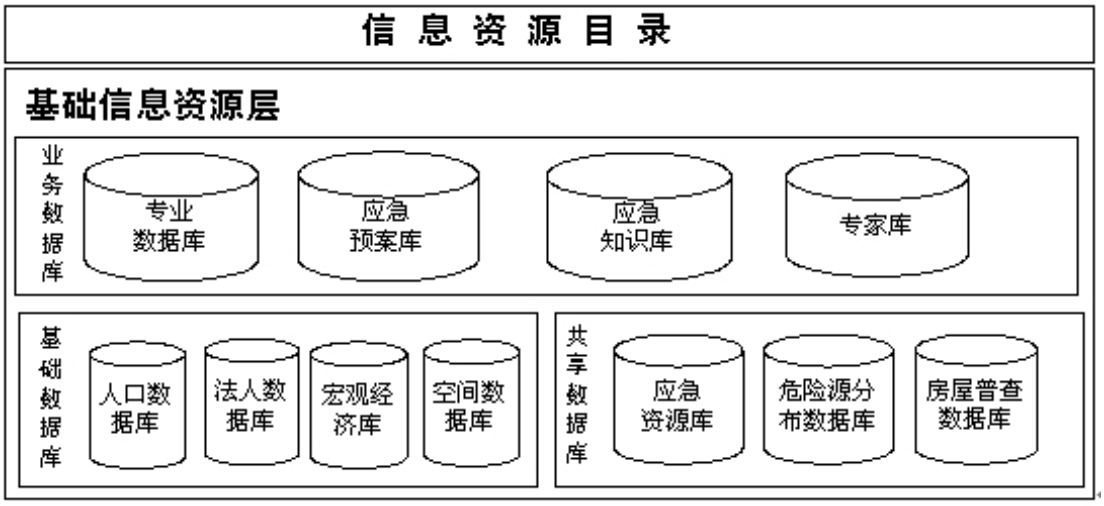

图13 应急指挥系统基础信息资源总体架构图

8.1.1　基础信息资源

北京市应急指挥系统基础信息资源由基础数据、共享数据、业务数据三部分组成。其中，基础数据库包括人口基础数据库、法人单位基础数据库、宏观经济基础数据库和空间地理基础数据库四大基础数据库；共享数据库是应急指挥系统中各委办局、区县相关子系统需共同建设或共享使用的数据库，包括安全隐患分布数据库、应急资源数据库、建筑物分布数据库等。业务信息资源库是指专项应急指挥部内涉及的信息资源，包括本专业领域的专业数据库、应急预案库、知识库、专家库等数据库。

北京市应急指挥系统的基础信息资源建设必须按照全市统一规划、统一建设，在统一的技术标准和架构下建设，避免在应急指挥系统建设过程中产生新的“信息孤岛”，避免重复建设。

8.1.2　信息资源目录

北京市应急指挥系统的信息资源目录建设应遵照《中共北京市委办公厅北京市人民政府办公厅关于加强政务信息共享工作的若干意见》，由市信息办配合市应急指挥中心统一规划，实行数据的分布式存储、集中式管理的共享模式，在市应急指挥中心建设、存储、提供应急指挥系统基础信息资源总目录，各应急指挥管理机构存储和提供相关的应急信息资源分目录。其中，信息资源的分类参照《面向公共服务的政务信息分类规范》，结合应急指挥系统中各类信息资源的特点，来具体实施。

北京市应急指挥系统中信息资源目录总体结构如图14所示。

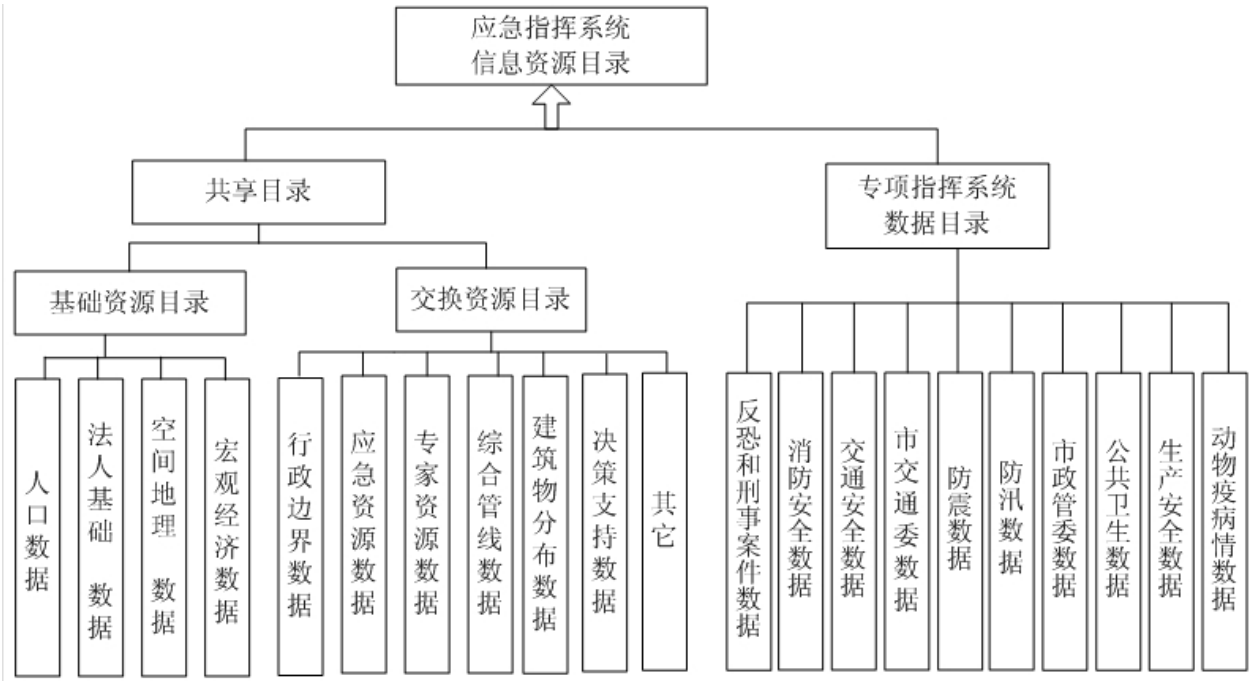

图14　应急指挥系统中信息资源目录总体结构

8.2　基础信息资源主要建设内容

8.2.1　基础数据库建设

根据京信发[2004]1号文中的要求，在北京市应急指挥系统中使用全市统一规划、统一建设的人口基础数据库、法人基础数据库、宏观经济基础数据库和空间地理基础数据库。

8.2.1.1　人口基础数据库建设

人口基础信息主要分为市民基础信息和业务专用信息两类。人口数据基础库建设应参照《市民基础信息数据元素目录规范》，其中数据项至少应包含身份证号码、姓名、性别、出生年月日，出生地、民族6项。

8.2.1.2　法人基础信息数据库

法人基础信息数据库是指将相关的法人单位基础信息，按照法定的统一方式进行汇总、整理和更新，并依法给相关政府部门提供共享信息的数据库系统。法人基础库中数据项至少应包含标识码、注册名称、地址、性质、法人代表身份证号码与姓名6项。

8.2.1.3 宏观经济基础数据库

宏观经济基础数据库应在全市统一规划组织下，应充分利用各委办局已有资源来建设。

8.2.1.4 空间地理基础数据库

应急系统建设所使用的空间地理基础数据库至少应由电子地图数据库、遥感影像数据库、地址数据库和政务信息图层数据库等四个数据库构成。其中，电子地图数据库应以北京市测绘院提供的北京市测绘基础电子地形图和国家测绘局与总参测绘局生产的电子地形图为基础建设，其更新数据精度：市区地图数据实地精度控制在1米以内，各比例尺数据叠加时精度控制在5米以内；郊区地图数据精度控制在10米以内。

8.2.2 共享数据库建设

8.2.2.1 应急资源数据库建设

应急资源数据库包括通信保障资源数据库、现场救援和工程抢险装备保障资源数据库、应急救援队伍资源数据库、交通运输保障资源数据库、医疗卫生保障资源数据库、物资保障资源数据库等。应急资源数据库建设应建立数据维护更新机制，并结合相应的应急预案库来建设。

1)现场救援和工程抢险装备保障资源数据库

现场救援和抢险装备与物资信息数据库涉及到移动卫星通讯设备、电视直播设备、大型运输设备、救灾专业直升机、核、生物、化学等有毒有害物质的监测、检验等特种大型设备和工程抢险特殊装备等设备，涉及保证突发事件应急处置所需的医疗救护设备、救治药品、日常生活用品等救灾物资的储备。全市各类应急管理主管部门都应按照统一格式标准，在其中明确装备的类型、数量、性能和存放位置、责任人及其通讯方式等。

2)应急救援队伍资源数据库

应急救援队伍数据库涉及人防、消防、医疗、地震、防汛、矿山、建设工程、市政等专业骨干救灾队伍数据。应急队伍数据库建设内容应包含先期处置队伍、增援队伍的组织保障方案、各类抢险救援队伍的部署和配置信息，特种救援装备情况、通信和交通工器材具情况以及各类专家等情况。

3)交通运输保障资源数据库

北京市突发公共事件交通保障动态数据库应建立各级各类公路、铁路、地铁、空港及有关交通设施、装备的基础档案，明确各类交通工具的数量、分布、功能、使用状态、维护责任人等基础信息。

4)医疗卫生保障资源数据库

医疗卫生保障资源动态数据库建设内容主要涉及北京市卫生机构基本情况、人力资源情况、大型医疗设备基本情况、卫生机构运营情况、卫生机构基础建设情况等。

5)物资保障资源数据库

北京市应急指挥中心统一组织协调，各专项应急指挥部根据应急预案中对不同种类突发公共事件物资需求，建设物资保障资源数据库。

8.2.2.2 安全隐患分布数据库

安全隐患分布数据库应统一协调各部门的安全隐患数据采集、存储、管理与更新机制，形成全市共享的安全隐患管理信息系统。该系统应包含基础信息、辅助信息管理、危害对象及危害程度预测、预案操作流程自动化、指挥调度安排等功能。

8.2.2.3 建筑物分布数据库

建筑物分布数据库应实现北京市现有建筑物分布信息的动态管理，实现人工难以完成的统计、查询及定位工作，为灾害评估、应急决策提供分析依据。

8.2.3 业务数据库建设

业务数据库由专业数据库、应急预案库、专家库和知识库构成。

8.2.3.1 建设内容

1）专业数据库建设

专业数据库是在全市范围内，根据管理职能由各相关委办局建设的，是应急指挥系统的基础信息资源，为资源共享、整合奠定基础。

2)应急预案库建设

应急预案库宜包括指挥机构的组成和职责；事件监测与预警；事件信息的收集、分析、报告、通报制度；应急监测和处置机构及其任务；事件的分级和应急响应工作方案；事件预防、现场控制，应急设施、设备、救灾物资和技术的储备与调度等。

已经制定的应急预案建议按照应急系统建库规范，将预案电子化。

3)专家库建设

专家库包括为应急指挥系统所需相关行业、领域专家的基本情况、研究领域、研究成果、特长、通讯联络等信息资料。各级应急管理机构都宜建立专家库，并及时更新维护。

4)知识库建设

知识库为应急指挥辅助决策提供支持,该库由行业专家经验、相关专业知识、事件历史资料和相关辅助决策模型等构成。

知识库设计应注意对库中知识的调用、检索和查询效率；知识的一致性维护和完整性检查、知识库的体系结构定义等环节。

知识库由各建库单位负责维护、管理等工作。

8.3 应急信息资源共享机制

8.3.1 各应急指挥机构内部信息的纵向整合

各专项应急指挥部按统一的标准和规范，新建或改造数据库，重构数据库中的数据格式。对各区县和相关委办局内部的信息资源整合，由建库单位负责，市信息办提供信息资源整合规范和技术支持。

8.3.2 各应急指挥机构间的横向整合及数据共享

在各应急指挥机构内部信息资源纵向整合的基础上，为满足应急联动需求，需要遵循下列原则，在各系统间进行信息资源共享的横向整合。

—— 建立统一的数据共享交换机制

各相关部门协同工作，遵循相关标准，进行信息资源的访问和共享。发生信息共享请求时，系统需要对请求者的身份和访问权限进行验证。

—— 明确数据共享方式、范围

参考《中共北京市委办公厅北京市人民政府办公厅关于加强政务信息共享工作的若干意见》。

—— 处理好地理坐标转换问题

应急指挥系统中原则上应采用统一的平面坐标系。

8.4 信息资源管理标准

8.4.1 信息资源管理标准框架

信息资源管理标准框架如图15所示：

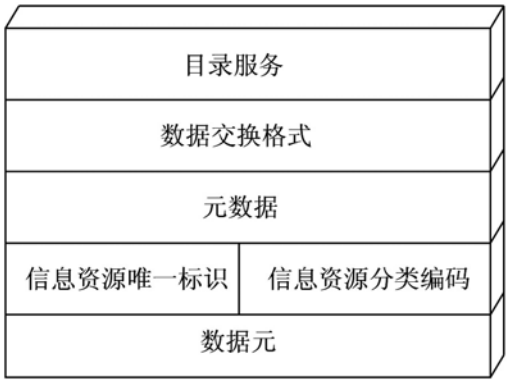

图15　信息资源管理标准框架

8.4.1.1　数据元

应急指挥系统中数据元是指应急系统中涉及的所有数据单元，应在对各应急指挥系统业务流程分析的基础上，进行数据元的提取。数据元标准化规则及其属性方法应按照GB/T18391.1-2002的规定执行。

8.4.1.2　信息分类与编码

应急指挥系统中信息分类与编码应在GB 7027-2002、GB/T 20001.3-2001第3部分的基础上，按照《面向公共服务的政务信息分类规范》的原则，对各类信息进行分类与编码。

8.4.1.3　元数据

应急指挥系统中应增加元数据描述信息，核心元数据标准应参考《政务信息资源目录体系》中关于信息资源核心元数据参考标准制定；同时，可根据各业务系统中信息资源特点，建立相应的扩展元数据描述。

元数据系统建设应包括元数据采集系统、发布系统、管理系统、标准转换系统组成。其中，元数据采集系统要依据一定的元数据标准进行元数据采集和入库，元数据发布系统提供内容元数据的网关注册和发布。元数据管理系统提供元数据查询、修改功能。

元数据应以XML表示，并以DTD或XML Schema对XML文档的结构进行定义。应急指挥系统中的信息资源目录建设以元数据技术为基础，分资源目录和服务目录两部分建设。其中，资源目录建设基于HTTP、Web Services提供服务；服务目录基于Web Services、UDDI技术实现。

8.4.2　信息资源交换

应急指挥体系中的信息资源交换应通过建立信息资源交换平台完成。信息资源交换平台建设按照国家标准《政务信息资源交换体系》执行。

9　网络基础设施

9.1　总体要求

通信网络是实现应急指挥信息传输的基础，是融合数据、语音和视频的多种信息流的承载平台，保证所有信息采集、信息获取节点和通信终端的通信连接。

北京市应急指挥系统通信网络基于北京市有线政务专网、北京市无线政务专网建设，充分利用现有网络资源，避免重复建设，统一接口标准，整合多种通信方式，建立跨部门、多手段、多路由的通信网，构建安全、可靠、稳定的应急指挥系统通信网络传输体系，实现情报搜集、指挥调度、图像传输、电视会议、视频监控等应急指挥业务。利用电信运营商的公用通信网络，建立备份和紧急保障措施，确保应急指挥系统通信网络的畅通。

公用网络指以互联网为代表的各种社会公用网络资源，这些资源是有线政务专网的有益补充，是政府面向公众和企业提供服务的重要途径。

9.2　北京市有线政务专网

北京市有线政务专网（以下简称有线政务专网）是连通全市各级政务部门的高速宽带信息网络，实现政务部门间内部网的高速互连，以市委、市政府两个办公厅为枢纽的北京市党政机关办公业务资源网，为应急指挥系统提供网络连接，实现H.323视频会议、VoIP语音、VOD视频点播、OA办公系统、领导辅助决策等多种数据信息流的传输，是建设市应急指挥系统的重要基础设施。

有线政务专网分为政务内网和政务外网。

政务内网是相对封闭的政务信息网络平台，主要承载市级党政机关办公系统，它的边界为市委、市政府，市级部委办局，区县委、区县政府等单位，与政务外网在接入层物理隔离。

政务外网与是相对开放的多种政务应用系统的支撑平台，主要承载的业务是各部委办局的各类纵向业务系统及跨部门的横向共享信息系统。与因特网在用户接入端逻辑隔离。

政务外网由市级政务专网和区县级政务专网组成。区县级专网是有线政务外网在各个区县的延伸。根据各区县的实际情况而建立的专用网络平台，应符合京信息办[2001]26号的规定。它覆盖本区县所有的政府相关单位，并与市级政务专网实现互连，为本区县开展电子政务提供网络基础。各区县级平台主要承载政务系统的政务外网业务。

9.2.1 应急指挥系统网络连接

9.2.1.1 区县应急指挥系统网络连接原则

1)按京信息办[2001]26号文规定，进行网络调整与修改，使用全市统一规划的有线政务专网IP地址，并为区县应急指挥系统规划专用IP地址。

2)采取规范的安全连接方式和隔离手段，保证区县平台与有线政务专网的连接方式安全可靠。

3)各区县应对网络管理提出规范化要求，从系统功能、人员职责和义务等方面做出明确规定。

9.2.1.2 专项应急指挥系统网络连接原则

专项应急指挥系统网络可根据现有应急指挥系统建设情况，采取下列技术与有线政务专网进行整合。

1)对尚未建成完善数据传输网络的应急指挥系统，应依托有线政务专网构建应急指挥系统网络。在有线政务专网覆盖不到的范围，可以利用其他网络资源来构建。

2)网络带宽要满足实际业务数据量的需求，并能保证H.323视频会议业务的传输。

3)新建专项应急指挥系统网络，需使用全市统一规划的有线政务专网IP地址，同时按电子政务专网的接入规范，连接有线政务专网，使本应急指挥系统网络能与市级应急指挥系统网络全程全网连通。

4)对于已有数据传输网络的应急指挥系统，应充分考虑这些已建系统的实际情况，力争使这些系统最少改动或不做改动。为实现专项应急指挥系统网络的相关功能，应在应急指挥系统网络和有线政务专网的边界处设置网络连接点。

9.2.1.3 各应急指挥系统网络不再单独考虑备份迂回路由，由有线政务专网管理部门统一设计。

9.2.2 接口标准

9.2.2.1 物理接口

区县级专网的核心网络交换设备与专网接入设备的互联接口为：100M快速以太网或1000M光纤以太网。为区县应急指挥系统设置单独的VLAN，应符合802.1Q的规定。

专项应急指挥系统网络与有线政务专网互联时，采用与相关委办局接入有线政务专网一致的接口方式，即各专项应急指挥系统网络通过专网接入设备实现与有线政务专网的互联，物理接口采用100M快速以太网方式。

9.2.2.2 IP 地址

区县应急指挥系统使用有线政务专网的IP地址，即单独分配的应急指挥系统网络专用IP地址，以保证区县应急指挥系统与相关委办局及各专项应急指挥系统网络横向互通。

待建或在建各级应急系统网络的IP地址应使用有线政务专网IP地址，避免IP地址混乱使用，造成网络冲突。

对已运行的各级应急指挥系统网络，为使这些系统最少改动或不做改动，通过NAT地址转换技术或服务器双网卡技术，实现各级应急指挥系统IP地址与有线政务专网IP地址的一致性。

9.2.2.3 路由协议

各级应急指挥系统在本系统内部交换数据时，应按照本系统网络平台的总体技术方案，采取相应的路由协议，但在对市级应急指挥平台进行路由交换时，应采用静态路由协议。

9.2.3 网络管理

应急指挥网络应纳入有线政务专网的管理体系，通过有线政务专网的日常运行维护管理，来保障应急指挥网络在平时的连通性和可用性。当应急指挥系统启动时，为保障网络在紧急状态下的高可靠性和高可用性，将提升应急指挥网络的管理保障级别，增加人员、设备等管理力量的投入。

9.2.3.1 网络资源管理

市级专网运行维护单位负责对市级专网所属网络设备及基础设施的管理。区县级政务专网运行维护单位负责区县级政务专网的管理。市应急指挥中心、区县应急指挥中心和各专项应急指挥部分别负责对各自所属网络设备及基础设施的管理，并将网络资源信息汇总给市政务专网管理单位。

9.2.3.2 网络运行和维护管理

网络运行和维护管理采用市、区（县）两级管理方式。

市级专网运行维护单位负责市级专网的运行维护，区县级政务专网运行维护单位负责区县级政务专网的维护。市应急指挥中心、区县应急指挥中心和各专项应急指挥部的维护部门负责各自网络的运行维护。

9.2.3.3 网络互连管理

应急指挥传输网络的IP地址应遵循京信息办[2002]57号文件，不符合规定IP地址编码规范的网络和节点不允许接入有线政务专网，拒绝在有线政务专网内部互访。

9.2.4 有线政务专网与因特网连接

9.2.4.1 有线政务专网内系统只有特定服务向因特网用户开放，因特网用户访问有线政务专网内系统时必须采取安全隔离措施。

9.2.4.2 通过因特网访问有线政务专网内信息系统的用户，应进行用户身份认证和用户访问策略，确保用户身份的真实性、合法性。

9.2.4.3 对有线政务专网内用户访问因特网实行有效控制，对进出因特网的 IP 地址进行过滤、审计，对访问内容实行分级控制。

9.2.4.4 通过对拨号连接的监控来防止用户擅自接入因特网。

9.2.5 有线政务专网与公用网络互联

有线政务专网的建设应依托于本地电信运营商的网络资源来扩大接入覆盖面，对有线政务专网新增用户且现有专网未覆盖的节点，可通过电信运营商的网络来提供接入，并在突发公共事件时提供通信保障。

9.2.6 应急指挥系统网络备份

应急指挥系统的业务数据主要通过有线政务专网来传送，一旦有线政务专网出现故障，会导致业务数据的中断。应急平台网络建设时，应租用公众运营商德电路作为应急指挥系统的备用网络线路，进行双路由备份，通过网络切换，将指挥信息通过备用线路进行传输，达到保证应急指挥系统需要的数据交换的目的。

9.2.6.1 网络切换

有线政务专网出现故障时，参与应急指挥系统的各节点应立即切换到备份线路上，实现指挥信息在备份网络上的传输，且应在应急指挥系统软件上建设快速切换的通道，即在有线政务专网网络及其路由出现故障之后，能将通信通道迅速切换到备份网络中去，满足应急指挥系统快速响应的要求。

9.2.6.2 数据传输

在使用公用网络传输数据时，采用数据加密，以及安全操作系统、入侵监测内核、身份认证、访问控制和安全审计等多种安全技术，对传输数据类型、内容等进行检查和过滤，提供可信任的专用信息交换服务。

9.2.6.3 视频会议系统的网络

为保证视频会议的质量，应将视频传输和数据传送电路分开，IP网络连接采用不同的路由器端口；ATM连接可采用不同的PVC。局域网内，视频会议和数据通信采用不同的VLAN。

9.3 有线语音通信系统

9.3.1 有线语音系统组成

有线语音通信包含一般话音通信、VoIP话音通信和多方话音通信，其组成主要包括程控交换机、录音系统、电话分配系统、自动应答系统、电话数据获取系统、有线调度系统和电话会议系统等。

9.3.2 程控交换机

程控交换机应实现如下功能：语音互通、有线指挥调度、进行全程或有选择录音、实现多方会议和电话会议功能等，与PSTN的连接满足中国一号信令和中国七号信令标准的要求。

9.3.3 录音系统

在应急指挥系统中需要对每一重要环节如应答、调度、会议等进行语音记录。录音系统应具备各类接口，包括：模拟接口、数字用户接口、数字中继接口、数字监听/会议板接口、网络接口；具有大容量存储器，多方式查询，统计分析等功能，同时具备与语音交换机系统进行信息交换的能力。

9.3.4 电话分配系统

电话分配系统对所有来电进行有效分配和对应急值守人员进行管理。具有分组定义、优先级设置等功能，可按电话类型、空闲时间、组特点进行来话分配。其中CTI作为语音部分与数据部分的结合点，是程控交换机与数据网络的接口，实现交换机与计算机网络的交互、传递信息、数据与语音的同步等。应具丰富的函数库，并可通过中间件完成二次开发，实现计算机对交换机进行控制。

9.3.5 自动应答系统

自动应答系统系统应支持文字转语音、自动查询、数据库连接、来电显示、传真等功能，应具有与CTI系统互通和图形化的管理操作界面、提供在线更改语音流程功能。

9.3.6 有线调度系统

有线调度系统应具有多语音通道和录音接口，包含外拨呼叫、输入呼叫、语音设备、组共享线、线路转换、会议、电子电话簿、电子信箱、外部用户通知等内容。

9.4 无线应急指挥调度系统

以北京市无线政务专网为主，各应急管理机构调度通信均以虚拟网方式接入北京市无线政务专网，与原有的模拟集群通信网实现互通，构建无线应急指挥调度系统。

9.4.1 构建原则

各应急管理机构应按照以下原则构建无线应急指挥调度系统：

——　系统性:无线应急指挥调度系统的建设规划设计，应注重设备的整体性和有机性。

——　科学性:合理设计系统的整体结构，保证系统结构和工作运行符合现代化应急指挥的要求。

——　可靠性:可靠性体现在设备可靠、数据可靠、网络可靠和软件可靠。系统必须具备自检功能和故障弱化功能。

——　实时性:系统要满足实战要求，具有处置突发公共事件的快速反应和联动的能力。

9.4.2 数字集群设备要求

通信终端设备应采用符合中华人民共和国电子行业标准SJ/T 11228－2000A的通讯设备。

9.4.3 北京市无线政务专网

北京市无线政务专网是基于Tetra技术体制的800MHz数字集群通信网，为应急指挥系统的领导、调度人员和现场工作人员进行语音、数据及视频交互提供无线通信保障，是北京市应急指挥系统的无线通

信支撑平台。北京市无线政务专网主要包括数字集群交换机、发射接收系统、调度系统、网络管理设备等。北京市无线政务专网的基本连接图如图16所示。

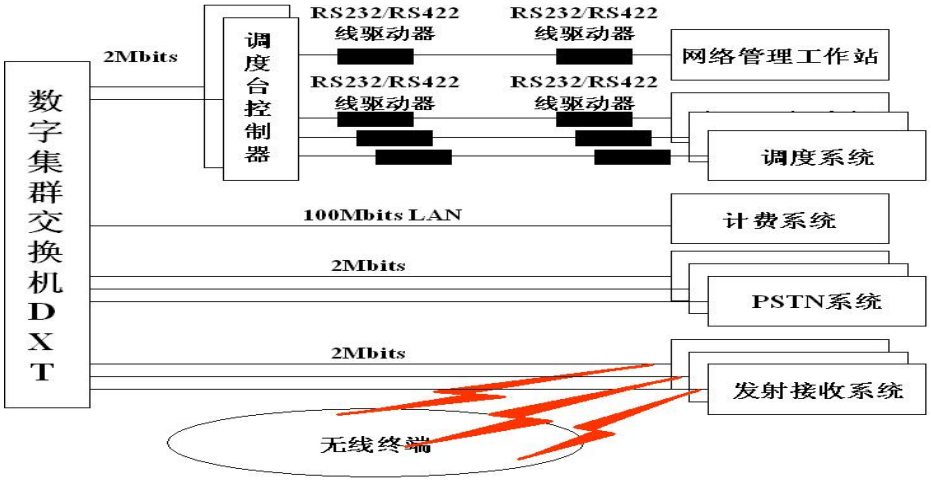

图16　北京市无线政务专网的基本连接图

北京市无线政务专网可提供如下作用：

——　提供虚拟组网、群组通信及数据通信等功能。

——　提供紧急呼叫、用户优先级、动态重组、限时通话、快速呼叫建立、直通等专业指挥调度通信业务功能。

——　可实现全市统一的、分层的指挥调度通信。

——　通过动态重组技术，可实现多部门的快速联动应急响应。

——　直通和故障弱化功能，可保障各种环境下应急指挥通信的连续性。

9.4.4　无线应急指挥调度系统框架结构

在北京市无线政务专网上构建无线应急指挥调度支持平台，实现“信息交互，统一协调，分级指挥，一致行动”的应急联动机制。为无线应急指挥调度系统框架结构如图17所示。

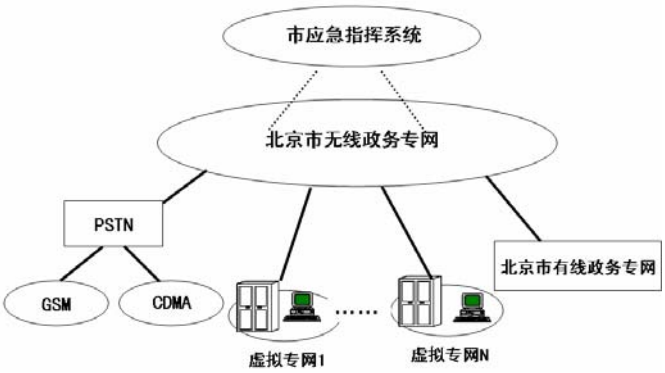

图17　无线指挥调度系统框架结构

9.4.4.1　接口连接方式

与各应急指挥系统PABX的连接：采用E1线与数字集群交换机连接，每条E1线按30路话路计算，采用中国一号信令或中国七号信令。

与PSTN的连接：采用E1线与数字集群交换机连接，每条E1线按30路话路计算，采用中国一号信令或中国七号信令。

与有线政务专网的连接：提供以太网100M接口，采用TCP/IP协议。

通过PSTN与中国移动的GSM移动通信网，中国联通的GSM移动通信网，以及中国联通的CDMA移动通信网连接。

与模拟集群通信网通过第三方调度台实现连接。

目前与指挥调度台之间可选用以下三种的连接方式：

1）调度台控制器连接方式（见图18）。

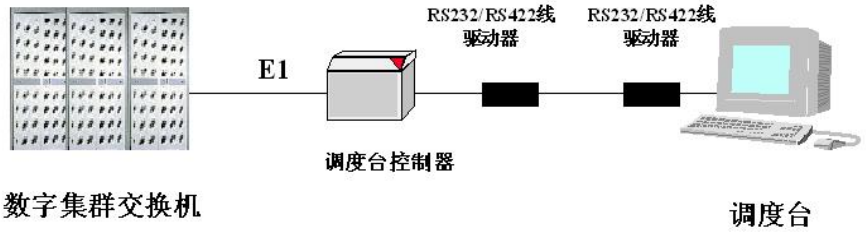

图18　调度台控制器连接方式

2）独立调度台连接方式（见图19）：

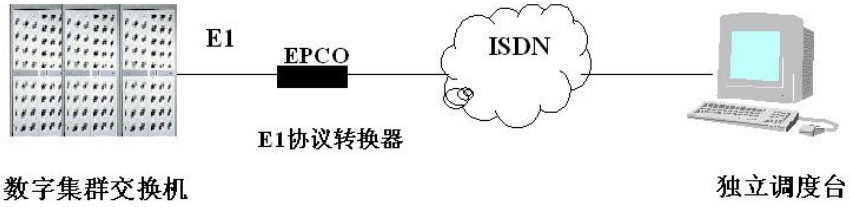

图19　独立调度台连接方式

3）网络连接方式（见图20）：

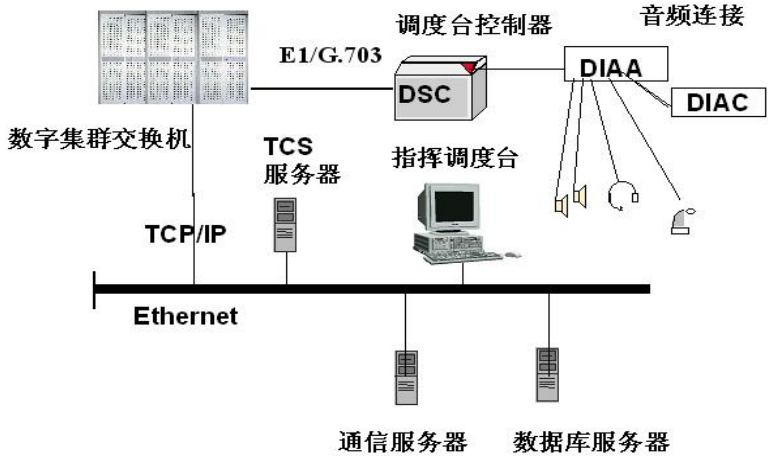

图20　网络连接方式

9.4.4.2　无线应急指挥调度系统

1）调度体系

调度体系由无线政务专网管理部门与应急管理部门一起，根据应急工作的组织结构、工作流程确立。详细结构如图21所示。

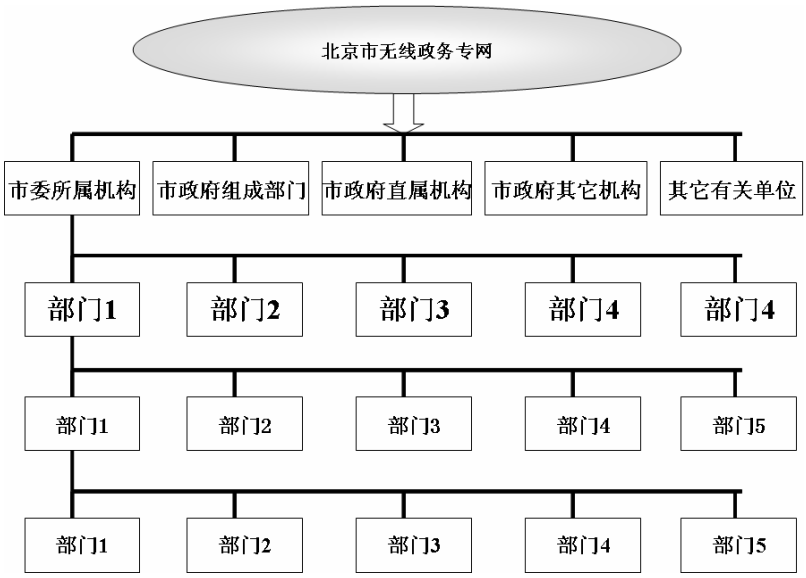

图21　虚拟网组织块结构图

2）虚拟网与指挥调度台

根据应急指挥系统的分层结构，进行相应的虚拟网规划和调度台等级确定。在虚拟网规划体系中，上一层调度台仅对其管理的组织块具有系统定义的通信和管理权限，实现分类分级的管理结构。每个组织都在各自的虚拟网中独立工作;全面控制各自享有的资源;用户接入权力和编码与组织结构联系起来;各组织可以接入自己的PABX专网和单位内部互联网。应急指挥调度通信系统指挥调度台逻辑结构如图22所示。

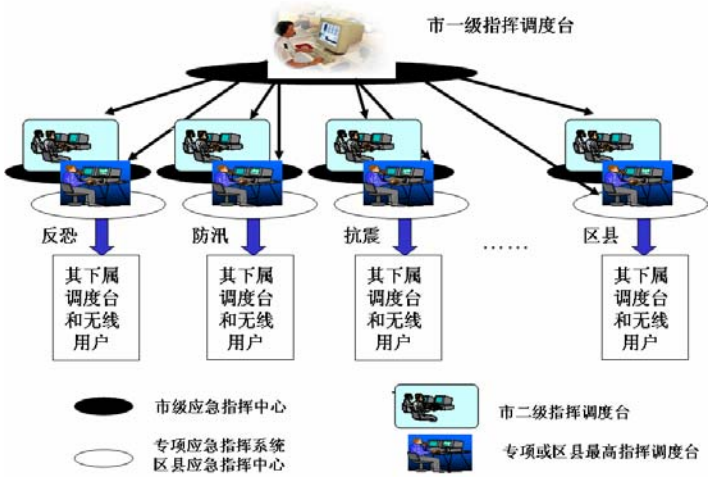

图22　应急指挥调度通信系统指挥调度台逻辑结构

市应急指挥中心、市委办公厅、市政府办公厅是北京市无线政务专网体系的核心，统一组织协调市委、市政府所属机构、各专项应急指挥部和各区县开展应急无线通信工作。市应急指挥中心调度台具有无线应急指挥调度系统中最高的通信调度权限;专项应急指挥部和区县应急指挥中心调度台指挥调度其所负责范围内的无线用户，具有次级的通信调度权限；移动应急指挥中心由与其相关的管理单位级别确定其指挥调度权限。

市应急指挥中心指挥调度台的功能：

——通信调度功能——单呼、组呼、广播呼、发起或接收来自PABX/PSTN的呼叫、紧急呼叫、数据通信、接收/发送状态信息、接收/发送中文短数据信。

——管理功能——无线用户管理、通话组管理等。

——其他功能——动态重组、强插强拆、环境侦听。

专项应急指挥部和区县应急指挥中心调度台的功能：

依据相关的调度权限，以及用户的具体需求进行功能设置。各设立一个值守通话组，由各专项应急指挥部和区（县）应急指挥中心或值班部门负责值守。

3）号码资源

根据北京市无线政务专网的号码资源状况，按照一定的规则由无线政务网管理单位协助分配。

4）通话组和呼号设计

无线应急指挥调度系统通话组和呼号设计分两种：

——与市级应急指挥中心有关的通话组和呼号设计

应根据京办字〔2005〕1号文为基础确定相应的通话组。

——与其它应急指挥中心有关的通话组和呼号设计

为自用组，应结合本指挥中心应急机制，依据实际工作需要自行编制，但不能与京办字〔2005〕1号文重复。

每个无线终端除设置自用通话组外，还需设立全市统一的勤务组以满足应急工作的要求，勤务组由市突发公共事件应急指挥机构统一调配使用。在确定通话组之后，依据统一分配的号码资源，通过有管理权限的调度台完成编码工作。

4）优先级设计

优先级共分为十级，其中十级最高。通话组的优先级与个人用户的优先级可以在一至十级范围内选择。各部委办局和各区（县）值守组的通话组优先级定为八级,其中的个人用户优先级定为七级或八级。

9.4.5 应急替代

可利用卫星移动通信系统作为无线应急指挥调度系统的备份系统，但应有加密手段。

9.5 视频会议系统

视频会议系统建设应依托有线政务专网、利用成熟技术、统一建设标准，以保障在日常或应急状态下各系统之间的远程互动决策。

9.5.1 原则性要求

应急指挥视频会议系统应按照以下原则构建：

——采用分散建设、集中管理的模式，即各个单位可以按照本要求自行建设视频会议系统，同时应支持各级会议管理系统的统一调度；

——管理兼容性：该系统应是一套完整的、可交互的、多点间的视频会议系统，既能实现市应急指挥中心、各专项应急指挥部及区县之间的会议调度和管理，又可实现各专项应急指挥部及区县的内部会议调度和管理；

——系统兼容性：利用有线政务专网，并与已有的系统进行良好的兼容，满足应急状态与日常使用的需要；

——系统安全性：该系统应能获取应急指挥相关的信息资源，并保证其安全传输；

——系统实用性：必须满足日常多媒体办公应用，同时实现日常的多点视频会议、点对点个人视频通信、VOIP、电话会议等多媒体办公需求；

——网络的扩展性:拥有良好的扩充性,必须满足北京市应急指挥复杂的用户需求和网络发展需要。

9.5.2 总体方案与会议模式

9.5.2.1 总体方案

北京市应急指挥视频会议系统应分为市和专项（区县）两级建设，市应急指挥中心牵头建设市级视频会议系统,各专项应急指挥部和区县分别建设二级视频会议系统,各级会议系统主要由会议管理系统、MCU、终端等部分组成。其中市级会议管理系统包括顶级业务管理系统和顶级GK，用于管理和调度市级视频会议设备;二级会议管理系统包括二级业务管理系统和二级GK,用于管理和调度二级视频会议设备。

各级会议管理系统之间逻辑关系:顶级业务管理系统和二级业务管理系统通过协作实现视频业务的开展，顶级业务管理系统能够对二级业务管理系统进行管理和消息转发，并汇总二级系统上报数据，包

括会议列表、接入端业务请求、用户信息等。召开全市范围会议，需要相关二级业务管理系统协同管理。二级业务管理系统完成多元化用户接入，并提供业务功能接口，包括基于Web的用户自主操作接口，主要的业务功能包括：用户信息查询、会议预约、会议操作、故障申告等。对于需要全市业务管理系统完成的业务功能，由各专项（区县）业务管理系统将业务功能请求上传到全市业务管理系统完成。应急通信视频会议系统整体逻辑如图23所示，应急通信视频会议系统网络连接如图24所示。

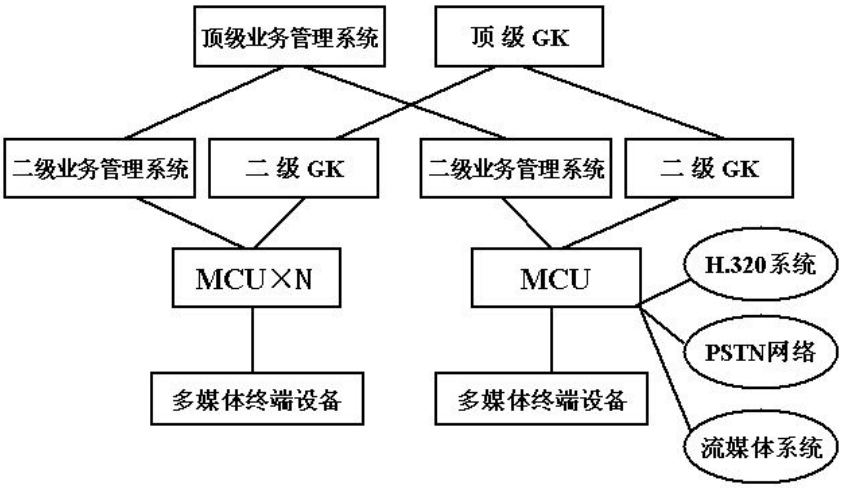

图23　应急通信视频会议系统整体逻辑图

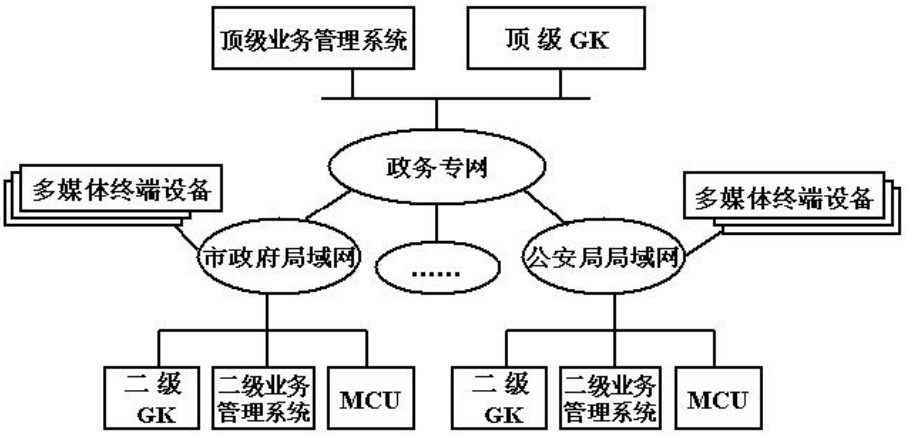

图24　应急通信视频会议系统网络连接图

各专项（区县）应急指挥部自行配置MCU和终端数量，并建设可以独立运作的业务管理和GK调度系统，以保障跨MCU及不同品牌产品之间实现会议自动调度和管理。各专项（区县）应急指挥部的组网如图25所示：

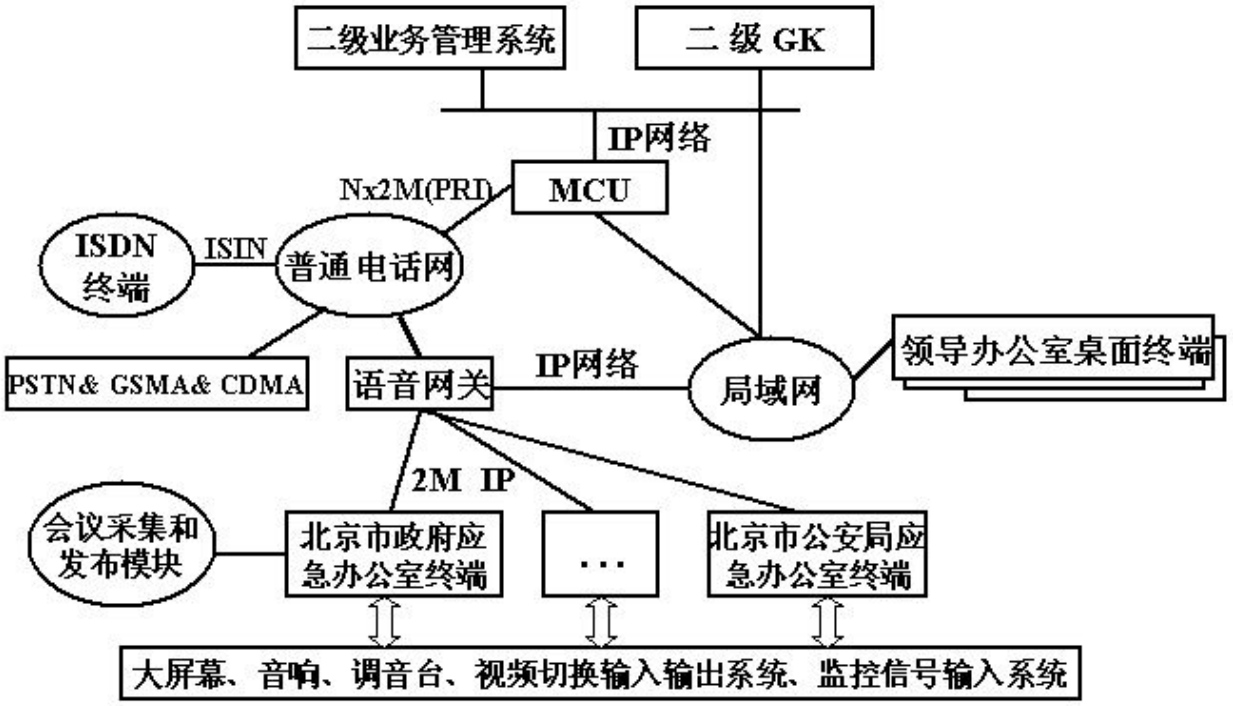

图25　应急通信视频系统各专项应急指挥部及区县组网图

9.5.2.2　会议模式

会议模式分以下几钟：

大型会议:由市政府会议室控制终端发起会议，召集相关各专项（区县）应急指挥部进入会议，领导可直接在办公室利用桌面终端参加会议；

小型会议:各级领导利用桌面终端发起会议，召集相关人员进入，召开小型会议；

IP视频通话:各级领导之间可任意呼叫，进行视频通话；

混合工作方式:会议室大型会议、领导间的小型会议、领导之间的视频通话可以同时进行。

9.5.3　硬件部分技术要求

9.5.3.1　MCU 技术要求

1）系统：符合H.323、H.320技术标准、支持100路以上终端以384K以上速率接入，采用嵌入式操作系统，全部硬件化；

2）网络：支持IP等网络接入；

3）视频协议：支持H.261、H.263、H.264；

4）音频协议：支持G.711、G.722、G.728，支持4路以上混音；

5）混速：支持召开384K、512K、768K、1920K等多种速率的混合会议；

6）稳定性：支持系统热备份、单板热插拔、电源备份；

7）业务支撑模式：支持通过终端定义和召开、控制会议；

8）其他：支持H.243会议控制、支持会议密码保护、支持多画面同屏、支持会议主席管理，应满足16个以上的系统同时召开会议。

9.5.3.2　会议室终端的技术要求

1）系统标准：H.323、H.320；

2）视频

协议：支持H.261、H.263、H.263+、H.264

显示模式：单一远端窗口、画中画、电视机＋VGA同时显示远地图像＋第三方内容

功能：双视频流，支持摄像机加计算机胶片叠加的双视频流发送；

3) 音频

协议：G.711、G.728、G.722

音频输入：外置话筒、线路电平输入

其他：采用先进技术，实现声音无误码、不失真的传送和接收；

4) 网络

类型：支持IP等网络接入

带宽：支持2M带宽终端接入；

5) 业务支撑模式

支持终端发起会议，并直接实现对会议的自动控制。

9.5.3.3 可视电话终端技术要求

1）系统标准：H.323

2）视频编码：H.261、H.263、263+

3）音频编码：G.723.1、G.711、G.728

4）图像分变率：有效像素大于30万

5）网络：

类型：支持IP等网络接入

带宽：不小于384 kbps

6）功能：

—— 业务：支持终端会议召集和会议控制

—— 带宽调整：带宽自适应、预设参数人工选择

—— 用户呼叫：手工拨号、快速拨号、电话簿拨号

—— 其他：内置双网口，可以实现 PC 和可视电话的共同使用。

9.5.4 会议管理系统技术要求

对业务管理系统和GK调度系统作出要求。

9.5.4.1 原则性要求

—— 顶级业务管理系统应负责协调全市会议的召开，二级业务管理系统应负责各专项（区县）应急指挥部会议的召开。

—— 业务管理系统应完成对 MCU 的统一控制、统一资源调度和管理，并通过与 MCU 的交互，完成对视频业务全流程的管理、调度和控制。包括用户管理、业务管理、会议管理、视频资源管理、网络管理等功能。

—— 业务管理系统必须提供用户 Web 操作接口，使用户可以通过 Web 自主进行业务相关的操作，包括用户信息查询、会议预约、会议控制、故障申告等。

—— GK 调度系统必须对全网 IP 设备进行统一注册、地址解析，完成会议的统一调度。

9.5.4.2 业务管理系统技术要求

业务管理系统应完成视频会议系统的管理功能，是视频会议调度的核心单元，作为业务的开展点，应具有完整的业务管理系统结构。主要功能包括：

—— 用户管理：提供面向用户的接口，采用 Web 界面，负责用户认证、用户信息管理、操作员管理等；

—— 业务管理：负责对业务相关的操作进行处理和实现，包括务开户销户、会议预约、会议控制、用户信息查询和修改、故障申告等；

—— 网络管理：负责对网络设备的管理；

—— 视频设备的管理：包括配置管理、性能管理、安全管理和故障管理；

—— 系统管理：包括业务管理系统服务器管理、数据库管理、数据备份等；

6)会议管理：会议管理是视频会议的控制中心，应具有会议调度、会议召集、会场控制、会议资源管理等功能。会议管理还包括数据会议的管理，即数据会议的召集、数据会议的功能控制等；

7)视频资源管理：负责提供对MCU的统一接口，进行相关的资源管理，包括对MCU的控制管理、MCU资源状态管理等功能。视频资源管理可以看作是管理支撑层面向MCU的执行模块。

9.5.4.3 GK 组网技术要求

—— 负责管理所属区域内端点的地址解析和注册认证，防止非法端点的注册，完成视频业务的地址解析和计费信息的采集。

—— 应支持 H.323、H.225、RAS 协议和 Radius 协议；

—— 顶级 GK 负责管理二级 GK，上下级 GK 之间配置快速路由寻址，实现跨 GK 的地址解析和消息的转发；

—— 应提供和业务管理系统的接口，完成用户认证、终端发起会议等功能；

—— 应提供网络管理的接口，完成配置、统计、故障查询、告警等功能；

—— 应提供计费采集，并向业务管理系统传递计费信息；

—— 应满足可靠性、安全性的要求，支持用户的密码认证功能。

9.6 图像监控系统

9.6.1 设计原则

图像监控系统建设应以北京市公安局图像监控系统为骨干体系，通过整合利用现有图像监控资源，同时对一些重点区域的覆盖盲区进行增、扩建，以保障在日常或应急状态下指挥中心对图像监控资源的实时调度。

应遵循以下原则构建：

—— 集中式管理

—— 网络化设计

—— 分布式共享

—— 拓扑型扩展

—— 规范化接口

9.6.2 总体方案和系统框架

9.6.2.1 总体方案

该系统应整合利用各专项（区县）应急指挥系统的图像监控资源而组成大型监控网络，通过公安局图像监控系统整合资源，向市应急指挥中心传送图像监控资源，并保障其实时调用的需求。每一个子系统必须实现各级系统间的互联互通，并根据自身业务需求分级再向下设多级监控系统。

图像监控系统总体框图如图26所示。

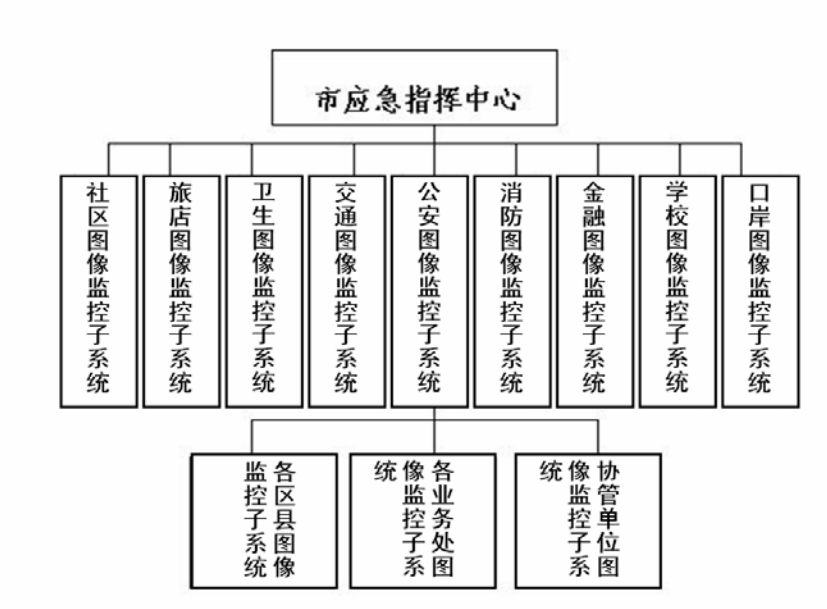

图26　总体框图

1）市应急指挥中心：作为最重要的用户，应具有调用、切换和控制任何子系统内的监控图像资源的功能。

2)公安图像监控中心：是整个系统的核心，级别与权限为最高，应做好本地监控系统的建设和发展，同时必须协调与其他各子系统的联网互通。

3）各专项应急指挥部图像监控子系统：应按照地域、业务等需求分级建设图像监控系统，为应急管理决策机构提供直观、适时的图像资源。

4）各区县图像监控子系统：应根据实际需求建设一定规模的本地图像监控系统，满足与骨干系统和同级系统之间的互连。

9.6.2.2　模拟监控系统框架

模拟监控系统建设必须符合《公安图像监控系统建设技术规范》规定。

模拟电监控系统应采集安装在前端摄像机的图像信号，经过传输链路送到远端控制室进行显示。模拟监控系统传输方式如图27所示。

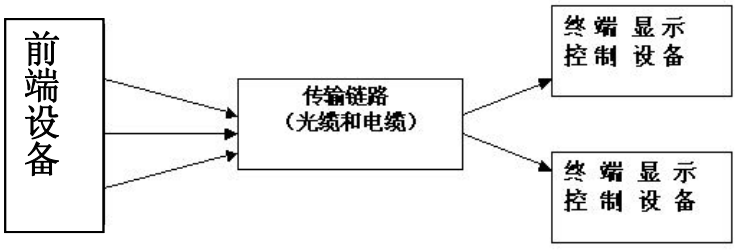

图27　模拟监控系统传输方式图

系统主要由三部分组成即前端摄录像设备、传输设备、终端显示控制设备。

1）前端摄录像设备应由摄像机、云台、防护罩、解码器等设备组成，应完成对前端监控区域的信号采集；

2）传输设备应完成图像信号的传输，一般近距离采用电缆传输，若超过300米时，应采用光缆借助光端机来传输，在开路视频监控系统中，可以把微波作为传输介质利用制高点基站或卫星来进行远距离传输；

3）终端显示控制设备应在专用的监控机房中完成，包括监控主机及附属设备，切换矩阵、操作键盘、大屏幕监视器、控制操作台等设备，负责完成对系统内图像的控制、调用，同时应具备向其他部门提供监控资源的功能。

9.6.2.3 数字监控系统框架

数字监控系统建设应符合BJ/Z 0001—2003。

数字监控系统应把前端采集到的图像监控信号进行压缩编码，然后通过计算机数字宽带网络进行适时传输，应满足网络上的所有终端用户对所需监控图像进行切换、控制的需要。数字监控系统如图28所示。

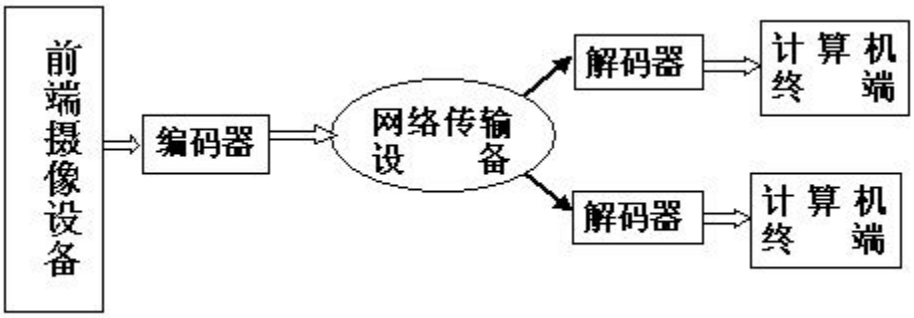

图28 数字监控系统图

系统主要由三部分组成即前端摄录象设备、编解码设备、网络传输设备。

1）前端摄象设备应采集监测区域的图像，同时接收控制指令，完成相应的动作；

2）编解码设备应对采集到的视频信号进行压缩编码和解压复原，完成模拟信号与数字信号之间的转换；

3）网络传输设备应完成对整个传输网络进行管理配置，保障系统可靠运行。

9.6.2.4 综合型监控系统框架

综合型监控系统包括模拟监控系统和数字监控系统。它必须兼容模拟和数字的图像数据，通过网络实现与其他系统监控资源的交换共享或向上级指挥中心传输实时图像，完成异地监控系统的融合互通。综合型监控系统如图29所示。

图29 综合型监控系统方案图

系统由三部分组成：模拟/数字监控子系统、传输网络、用户终端。

9.6.3 系统建设主要内容

9.6.3.1 摄像前端

组成：摄像机、镜头、云台、防护罩、解码器、电源等辅助设备。

9.6.3.2 传输链路

传输方式：图像监控信号的传输应有闭路和开路两种方式。

传输介质：同轴电缆、平衡对称电缆、光缆。

光端机：完成视频信号的光电转化，包括光发射机和光接收机。

9.6.3.3 显示终端

图像监控系统的终端设备必须位于专门的机房内，设备应根据机房的功能、规模不同进行相应选配。以下是监控系统必备设备：

1）监控主机：应局有管理配置整个监控系统的功能。主机的好坏直接影响到系统的稳定性，所以应由高档的多媒体计算机和处理器构成，同时必须具有较高的可扩展性、可编程性、可兼容性。

2）附属设备：

—— 控制键盘：操作前端设备。

—— 控制主机：根据主机指示向前端解码器发出控制信令。

—— 切换矩阵：完成输入输出的控制切换。

—— 字符叠加器：根据需要对回传图像进行标识。

3）显示设备

监视器是常用的终端显示设备。监视器的选择应根据整套系统的技术性能指标及使用目的来选择，应与系统的摄像机一致，屏幕的大小应根据控制中心的面积和监视人数进行选择，监视器的清晰度应相当于或高于摄像机的清晰度，以充分发挥摄像机的性能。监视器的数量应与摄像机数量成适当比例，对于重点部位监视器与摄像机的比例一般不小于1：3，非重点部位不小于1：8。

9.6.4 保密措施

在系统技术上必须进行以下三个方面设置：系统进入时的权限认证、网络优先等级设置、视频传输加密。

9.6.4.1 用户登陆

—— 操作员使用键盘时先进行密码、口令验证

—— 用户的身份等级必须经过系统主机的认证

9.6.4.2 认证手段

—— 姓名、密码：使用时必须输入姓名、密码

—— 指纹：使用时必须配套指纹系统，对生理特征实行检测

—— I 网卡：使用时必须利用网卡确定身份

9.6.4.3 网络等级

—— 优先权设置

根据系统用户的不同，必须对一个或多个联网系统内的下属子系统设置等级；对于同一个监控系统，等级高的享有调用、控制优先权，同时可锁控等级低的系统操作。

—— 操作键盘等级设置

为保障系统正常运行，必须对不同的操作键盘进行等级设置，特别是限定其对本地系统内或其他系统监控图像的访问级别。

—— 本地系统控制优先

对于几个联网内的监控系统，应履行本地系统对监控图像调用优先的原则，其他系统的调用应在征得本地系统同意后才能得到释放。

9.6.4.4 视频传输加密

无论是模拟传输线路，还是数字化传输网络，必须提高加密举措，防止重要图像信息外泄，特别是开路利用微波传输图像的监控系统，必须在载波中加密。

9.6.5 系统联网扩展性

9.6.5.1 系统自身扩展

—— 监控前端数量的扩展

每一个监控系统的建设均应具有无限的可扩展性，尤其是随着监控情况的不断变化，需要增建相应的摄像前端以及系统主机的相应增容，可扩展性是衡量一个监控系统优劣的重要指标。

——　监控系统向下级子系统的扩展

每一个监控系统除了自身的扩展外，还必须具备向下级连的功能。对于构建一个同时满足日常和应急状态下需要的大型智能化图像监控系统，必须采取分散建设、集中管理的方法来实施。要求各级子系统所建的监控系统必须具有向下扩展系统的功能。

——　与报警系统的联动

每个监控系统不但必须完成对重点区域的部控、监视任务，还应能与周边报警系统进行联动，起到对监视区域的安全防范作用。

9.6.5.2　与其他监控系统的互连

图像监控系统不是独立、封闭意义上的单一系统，而是综合多个不同区域或不同职能监控系统的集成，要求建设的监控系统必须具有广泛的互连兼容性，它是建设完整的城市图像监控网络的必备前提。

10　安全体系

10.1　安全体系结构

北京市应急指挥系统安全保护体系对应系统层次结构，划分为三个保护范围，即：网络和基础设施保护，系统边界和计算环境保护，应急指挥应用安全保护。应急指挥网络平台以北京市电子政务专网平台为基础构建。应急指挥系统安全体系结构如图30所示。

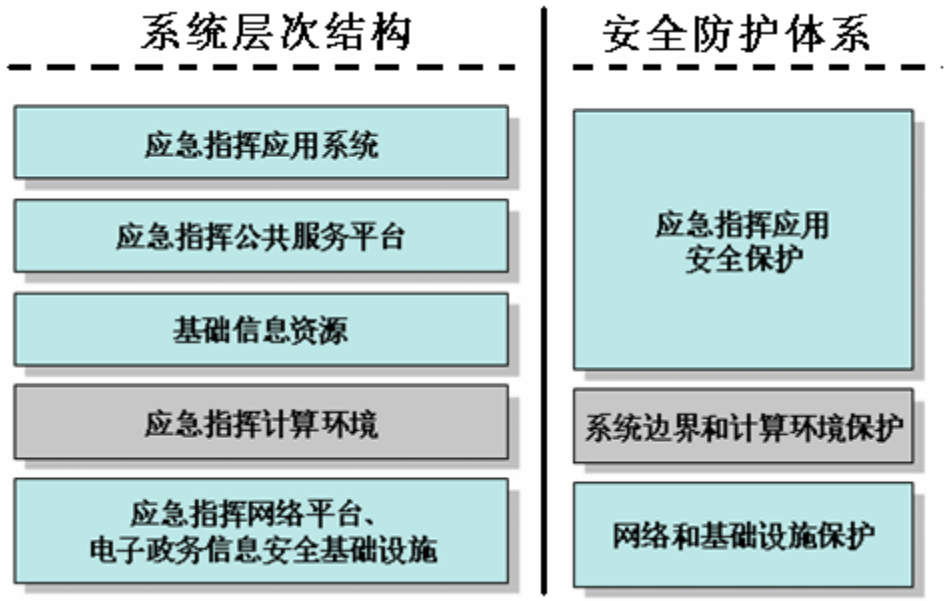

图30　应急指挥系统安全体系结构

应急指挥系统计算环境指由相关单位内部的信息处理、传输与存储设备，以及运行在这些设备之上的各种信息系统构成。应急指挥系统边界是应急指挥系统子网与其它网络连接的边界。应急指挥系统子网内的系统通过系统边界与外部的系统交换信息。

应急指挥应用系统的安全保护包括基础信息资源、应急指挥公共服务平台和应急指挥应用系统的安全保护三方面内容。

10.2　信息安全基础设施

应急指挥系统的安全保障应依托北京市统一的信息安全基础设施，为全市提供统一的安全支撑环境，为信息交换和共享提供安全保障。北京市信息安全基础设施主要包括：公钥基础设施、信息安全应急响应基础设施、信息安全容灾备份与灾难恢复基础设施、信息安全测评基础设施。

建设北京市应急指挥系统，应依托公钥基础设施的数字证书服务，以PKI技术为基础，构建统一信任体系。

北京市信息安全应急响应基础设施负责提供信息安全风险评估、信息安全应急响应支援和信息安全技术支持等安全服务。

北京市信息安全容灾备份与灾难恢复基础设施为北京市应急指挥系统提供统一的系统备份与灾难恢复服务，保护信息系统和数据的可用性。在灾难发生的情况下，保障应急指挥的连续性。

北京信息安全测评基础设施负责信息安全系统和信息安全产品的安全测评，以评价系统是否达到相应等级的安全保护要求。测评结果是信息安全产品选型和信息系统是否可投入运行的重要依据。

10.2.1 公钥管理基础设施

PKI技术是采用证书管理公钥，通过第三方的可信任机构，把用户的公钥和用户的其它标识信息，如名称、e-mail、身份证号等捆绑在一起，用以在网上验证用户身份的安全技术。采用建立在PKI基础之上的数字证书，通过把要传输的数字信息进行加密和签名，保证信息传输的保密性、完整性和可用性，从而保证信息在传输之中的安全。

PKI作为一种安全应用，通过发布密钥和证书，帮助各部门建立和维护安全域。在安全域内，PKI管理加密密钥和证书的发布，并提供诸如密钥管理、证书管理和策略管理等。PKI也允许一个单位通过证书级别或直接交叉认证等方式来同其他安全域建立信任关系。

标准的PKI体系的结构如图31所示。

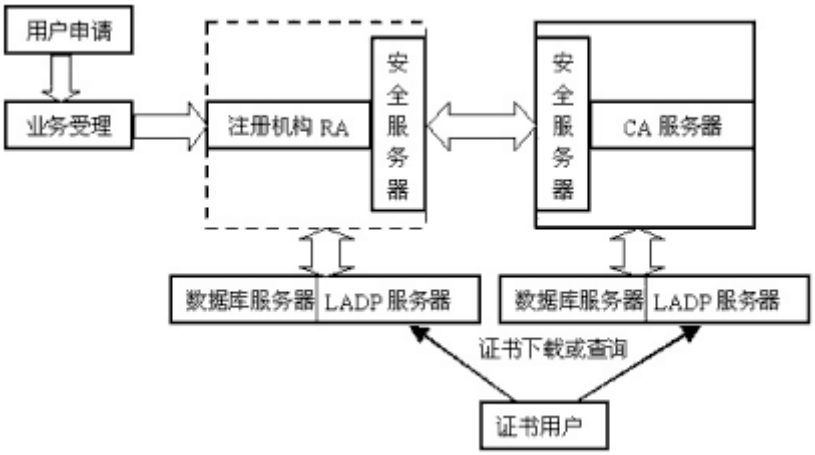

图31 标准 PKI 体系的结构图

10.2.2 信息安全应急响应基础设施

信息安全应急响应是对信息安全事件按一定的程序进行处理，其主要任务是尽可能减小事件发生的范围和数量、防止事件升级、迅速恢复系统以及事后的分析审计等。

在通常的安全保障模型中，安全保障的主要环节包括防护、监测、抑制和恢复这几个主要部分。北京市信息安全应急支援基础设施作为北京市信息安全保障体系的重要组成部分，依托北京市信息安全应急支援社会网络，对电子政务用户提供安全监控、安全预警、应急支援、信息通报、事件分析、顾问咨询等安全服务，如图32所示。

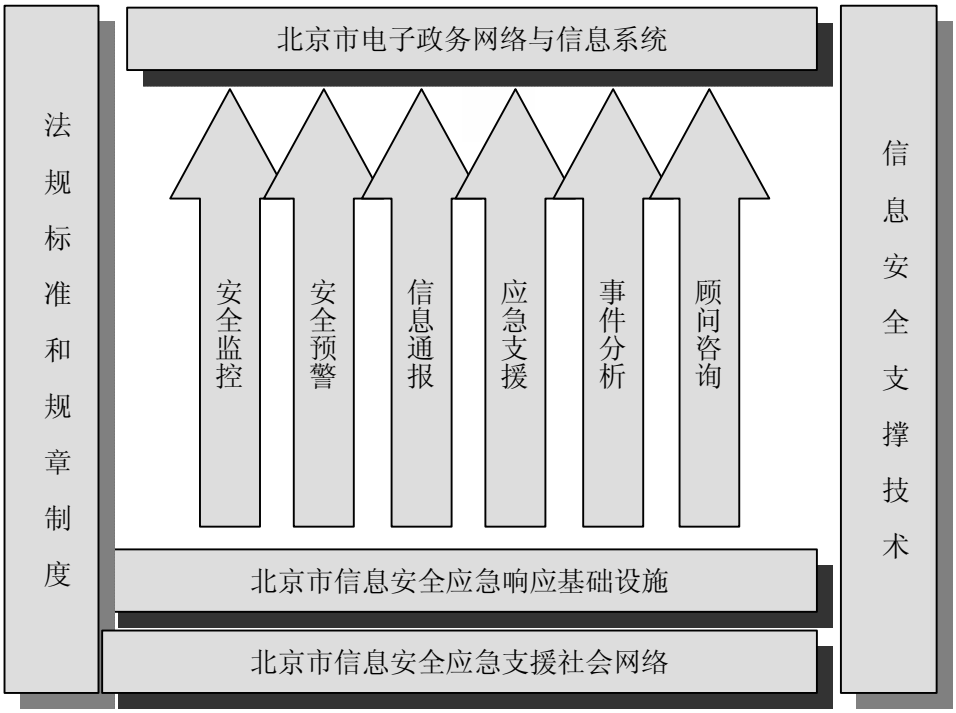

图32　信息安全应急支援基础设施

北京市信息安全应急响应基础设施是在北京市网络与信息安全协调小组的统筹规划、组织协调和监督检查下建立的旨在保障北京市电子政务及其他重要信息系统正常运行的基础设施。北京信息安全服务中心是应急支援工作的具体实施部门，承担北京市应急响应基础设施的建设和运维工作。

信息安全应急支援社会网络是北京市信息安全应急支援的重要储备力量。北京市各科研机构、高校、企业和政府部门等依照相关的规定，在北京市信息安全应急响应基础设施的统一组织协调下组成北京市信息安全应急支援社会网络。

各项信息安全应急响应工作的开展需遵从相关的法律法规和规章制度。

10.2.3　信息安全容灾备份与灾难恢复基础设施

容灾备份与灾难恢复又称灾难备份与恢复，是指利用技术、管理手段以及相关资源，确保已有的关键数据和关键业务在灾难发生后，在确定的时间内可以恢复和继续运营的过程。容灾备份与灾难恢复防范的灾难包括地震、水灾等自然灾害以及火灾、战争、恐怖袭击、网络攻击、设备系统故障、人为破坏等无法预料的突发事件。

容灾备份与灾难恢复工作的主要目标是：提高抵御灾难和重大事故的能力，减少灾难打击和重大事故造成的损失，确保重要信息系统的数据安全和作业持续性。

如图33所示，根据不同的需求，信息安全容灾备份与灾难恢复基础设施（简称容灾中心）可为应急指挥系统提供同城异地的介质级、数据级和应用级容灾备份与灾难恢复服务。介质级容灾备份是指将重要的系统和数据信息先备份在磁带、光盘、缩微胶片等存储介质上，然后定期或不定期地以人工转运的方式将存储介质在容灾中心进行异地保存；数据级容灾备份是指将重要的系统和数据信息通过在线电子传输的方式，远程备份或复制到容灾中心的存储设备上；应用级容灾备份是在数据级容灾备份的基础上，在容灾中心预先配置可支撑原系统运行、并可接替原系统对外提供服务的主机、信道和信道切换设备和相关软件系统的备份方式。

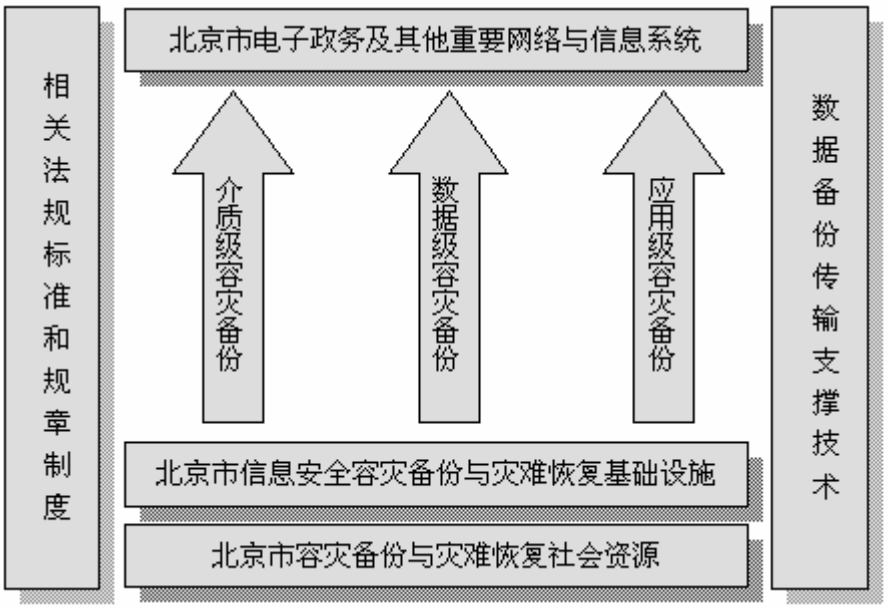

图33　北京市异地容灾备份基础设施

该基础设施在北京市网络与信息安全协调小组的统筹规划、组织协调和监督检查下建立，旨在为北京市电子政务以及其他重要信息系统抵御灾难事件打击、确保系统和业务恢复提供服务保障。北京信息安全服务中心负责该基础设施的建设和运维。

容灾备份与灾难恢复工作的开展需要遵从相关的法律法规和规章制度。数据备份及传输技术是容灾备份的基础支撑技术。

在北京市提供专业化外包服务的商业化容灾中心和企事业单位自建的容灾中心是全市容灾备份与灾难恢复体系的有机组成部分，可为全市各类信息系统提供不同层次和不同级别的容灾备份与灾难恢复服务。

10.2.4　安全测评基础设施

信息安全测评是信息安全保障的重要环节和支撑手段，是推动适度安全、整体安全、统一安全策略的有效方法和途径。

信息安全测评基础设施的主要业务范围包括：开展网络与信息系统安全等级测评、安全风险评估以及信息安全工程项目验收；开展信息安全产品检测，为北京市信息安全产品政府采购目录提供技术依据；开展信息安全测评相关培训和咨询服务；协助信息安全主管部门对北京市电子政务及其他重要信息系统实行信息安全检查。

信息安全测评主要依据DB11/T 171-2002《党政机关信息系统安全测评规范》、DB11/T 145-2002《政务公开网站通用安全技术要求》、《关于本市各级党政机关网络与信息系统开展安全等级保护工作的通知》（京信息办函[2004]72号）等实施。

10.3　安全保护技术要求

北京市应急指挥系统是北京市公共突发事件的总体指挥和协调系统，其受到破坏时，会对系统所承载的业务带来极其严重的损失和破。依照京信息办函[2004]72号的相关要求，北京市应急指挥系统的安全等级应不低于4级，本技术指导性文件将北京市应急指挥系统的安全等级定为4级。

10.3.1　网络和基础设施安全保护技术要求

10.3.1.1　总体要求

为保障北京市应急指挥系统整体安全，其涉及到的各应急指挥系统在网络层次，均应采用相同级别的安全策略。

应急指挥网络平台安全保护应满足DB11/T 171-2002安全类型Ⅳ的相关安全技术要求和安全管理要求。

10.3.1.2 物理安全

物理安全保护范围包括：应急指挥网络通信骨干网基础设施,包括有线、无线通信线路，各级节点机房环境及网络设备等和网络基础服务系统。应当保护计算机系统设施，通信网络设施免受自然事件造成的破坏、人为操作失误及各种计算机犯罪行为导致的破坏。机房和物理环境保护遵循GB2887-89和GB9361-88。

10.3.1.3 信道安全

市应急指挥网络平台的核心链路传输应采用ATM虚电路的安全传输技术，为各应用系统提供安全的虚拟专网服务。

区县应急网络平台，如果租用电信或其它企业的线路，应尽可能采用专用设备，不能采用专用设备的，应采用VPN技术保护通信的安全。

无线通信，应采用基于加密技术的信道安全保护措施。

针对各应用系统对安全性的不同要求，可以采用相应的加密技术和设备，对信息进行加密传输。

10.3.2 系统边界和计算环境安全保护技术要求

应急指挥系统的系统边界和计算环境安全保护，应符合DB11/T 171-2002安全类型Ⅳ的相关安全技术要求和安全管理要求。

10.3.2.1 安全隔离

指挥系统所涉及的各单位信息网络与因特网,应急指挥网络与本单位其他业务网络之间应采取相应的安全隔离措施进行边界保护。

拔号接入包括直接通过远程访问服务器接入和通过因特网ISP服务接入两种方式。拔号用户接入需要对用户进行身份认证，认证协议必须保证用户身份信息不在网络上以明码形式传输。应采用相应的保密措施，以保证敏感数据的机密性与完整性。

10.3.2.2 检测与监控

通过采用IDS等设备，建立有效的检测与监控系统，及时发现网络和系统入侵等安全事件，实施有效的响应。

10.3.2.3 物理安全

计算环境物理安全是计算环境信息安全保护的基础。应加强对机房和主机设备、通信线路和设备、信息媒介等的物理安全保护。遵循标准同10.3.1.b。

10.3.2.4 虚拟子网划分

应急指挥网络子网内部,应当根据部门或者使用群体不同等实际情况,划分相应的虚拟子网(VLAN),通过VLAN的划分对不同的系统和用户进行隔离。

10.3.2.5 关键主机保护

对系统中的关键主机，可以采取以下安全保护措施加强安全保护：对于计算环境中的关键服务器，单独划分虚拟子网，其所在的网段与其他子网互连的接口应当采取隔离和监控措施；采用基于防火墙、入侵监测、安全扫描工具来确保关键主机的安全。加强对于关键主机的操作和访问行为的安全审计。

10.3.2.6 操作系统安全

服务器操作系统和数据库系统的安全等级应符合DB11/T 171-2002规定的Ⅳ类以上安全类型的安全技术要求。对于应急指挥网络中使用的各种操作系统，均需采用安全扫描工具定期检查操作系统的安全隐患，并及时进行安全修补。

10.3.2.7 数据库安全

数据库系统的安全等级应符合DB11/T 171-2002规定的Ⅳ类以上安全类型的安全技术要求,并及时进行安全修补。

10.3.2.8 病毒防范

病毒防范主要包括预防病毒、检测病毒、清除病毒等功能。应急指挥网络平台接口边界设备要采取相应的病毒防范措施，防止系统遭受病毒和恶意代码攻击。

10.3.2.9 计算环境可用性

根据系统安全类型，为保证计算环境的可用性，应建立相应的容错、备份和恢复机制。备份可以采用冗余备份、系统备份和数据备份。重要系统应当依托北京市异地容灾备份中心建立备份和灾难恢复机制，保证数据和系统的安全性与可用性。

10.3.2.10 通过公共网络进行应急指挥的安全保障技术要求

当专用应急指挥网络出现故障而使用公共通信网络进行应急指挥时，相关网络与信息系统的安全隔离、检测与监控、物理安全、虚拟子网划分、关键主机保护、操作系统安全、数据库安全、病毒防范、计算环境可用性等参照以上要求执行。此外，还应在各通信实体之间建立可信信道，确保应急指挥信息的保密性、完整性不受威胁。

10.3.3 应急指挥应用系统安全保护技术要求

应急指挥应用系统安全保护，应符合DB11/T 171-2002安全类型Ⅳ的相关安全技术要求和安全管理要求。应急指挥应用系统实现以下基本的安全功能要求。

10.3.3.1 安全审计

各子系统应明确说明每一审计点的审计内容与范围。审计点为应用平台系统、数据库系统和应用系统。在系统的设计和实施方案中应明确说明审计数据的来源。在应急指挥系统的设计和实施方案中应明确说明审计数据的预处理和后处理。

10.3.3.2 通信

通信在实体之间进行，应急指挥系统中的通信实体包括：用户、进程、主机。

应用平台通信应利用标准网络应用协议实现，通信实体应当使用标准协议提供的标识方式进行身份标识，并提供对通信的双方实体的通信行为不可抵赖性的保证。

10.3.3.3 可信路径/信道

应在通信实体之间建立不会对信息的保密性、完整性构成威胁的信息传输信道。

10.3.3.4 密码支持

在应急指挥系统中使用密码技术，应严格按照国家密码主管部门的要求进行使用和管理。

10.3.3.5 用户数据保护

应急指挥系统的用户数据存储在服务器、单机以及备份媒体上，应当保证这些数据的保密性、完整性和可用性。

10.3.3.6 标识与鉴别

在应急指挥系统中，“用户标识”在不同的应用系统、不同的层次中可能采用不同的形式，而相应的用户管理方式、标识方法和鉴别机制也可能不同。应对系统中存在的所有用户进行标识和鉴别。

应急系统的身份认证采用集中统一策略，系统最终用户的身份认证采用统一的电子政务数字证书为身份认证的基础。所有的身份认证均由应急门户网站统一完成。

10.3.3.7 安全管理

应急系统的访问控制采用分布式的基于角色的访问控制策略。各用户所对应的角色，可以由应急系统总体组根据统一规定来分配。各角色所能够访问的资源，则由各子系统分别定义。

10.3.3.8 安全功能保护

应急指挥系统中，安全管理主要包括：安全功能的配置管理、安全事件的管理和安全功能的故障管理等。

10.3.3.9 系统访问

应保证公共应用平台系统、应用系统建立用户会话过程的安全。

参考文献

[1]. GB 2887-89 计算站场地技术条件
[2]. GB 9361-88 计算站场地安全要求
[3]. GB/T 18391.1-2002 信息技术 数据元的规范与标准化第1部分:数据元的规范与标准化框架
[4]. DB11/T 337-2006 政务信息资源目录体系
[5]. DB11/T 240-2004 市民基础信息数据元素目录规范
[6]. DB11/Z 359-2006 面向公共服务的政务信息分类规范
[7]. 《中共北京市委办公厅北京市人民政府办公厅关于加强政务信息共享工作德若干意见》