

附件 7

县级安全生产信息化建设技术指导书

国家安全生产监督管理总局

2016 年 12 月

目 录

一、概述	1
二、总体架构.....	1
(一) 综合展现层	3
(二) 应用服务层	3
(三) 应用支撑层	4
(四) 数据资源层	4
(五) 基础设施层	4
(六) 标准规范体系	5
(七) 安全与运维保障体系	5
三、应用系统.....	6
(一) 安全监管类应用系统	6
(二) 应急管理类应用系统	9
(三) 公共服务类应用系统	9
(四) 综合决策类应用系统	10
(五) 行政管理类应用系统	10
(六) 安全生产综合信息门户	11
四、数据资源管理	11
(一) 安全生产监管类数据	12
(二) 应急管理类数据	15

(三) 行政管理类数据	16
(四) 公共服务类数据	17
(五) 其他数据	17
五、应用支撑平台	18
(一) 公共应用支撑服务平台	18
(二) 物联网应用支撑平台	21
(三) 数据共享交换平台	21
(四) 安全生产大数据管理平台	22
六、基础网络系统	23
(一) 安全生产政务外网	23
(二) 安全生产专网	24
七、基础环境.....	28
(一) 机房	28
(二) 安全系统	29
(三) 计算与存储系统	29
(四) 应急通信系统	30
(五) 移动应急平台	30
(六) 容灾与备份系统	30
八、系统运行维护	31

一、概述

当今经济社会各领域，信息已经成为重要的生产要素，渗透到生产经营活动的全过程，融入到安全生产管理的各环节。安全生产信息化就是利用信息技术，通过对安全生产领域信息资源的开发利用和交流共享，提高安全生产管理水平，推动安全生产形势稳定好转。

县级安全监管部门利用市级安全监管部门建设的信息系统以及自行建设的信息系统，为安全监管和应急管理提供有效的技术支撑。但是，县级安全生产信息化建设还存在缺乏顶层设计及制度规范指引，系统建设统筹度不高、覆盖面不全，部分业务系统使用效果不理想、生命周期短，未形成安全生产状况动态掌握机制，对高危企业缺乏有效安全监管手段等问题，信息化建设有待进一步加强。

本文用于指导全国各县级安全监管部门的安全生产信息化建设。

二、总体架构

如图 1 所示，按照全国安全生产信息化总体建设方案的有关要求，建议县级安全生产信息化建设采用多层次架构模型，总体架构划分为综合展现层、应用服务层、应用支撑层、信息资源层和基础设施层五个层次，同时还包含标准规范体系、安全与运维保障体系。



图 1 县级安全生产信息化总体架构图

（一）综合展现层。

通过社交媒体、门户网站、大屏幕、桌面终端、电话传真、便携工作终端和移动通信设备等载体，全方位、多维度、多视角展示安全监管监察、应急救援与社会公共服务应用，实现服务与应用的便捷访问和数据可视化展现。

（二）应用服务层。

应用服务层是县级安全监管相关信息系统业务逻辑的实现层，是资源服务体系的业务实例，是对服务资源进行配置、组织、装配后的产物，其外在表现为信息系统的各种业务功能和接口服务。

应用服务层为县级安全监管部门各类业务提供信息化服务，主要包括安全监管类、应急管理类、公共服务类、综合决策类、行政管理类等五类信息系统，通过安全生产综合信息门户实现综合集成展现。用户包括县级安全监管部门、安委会成员单位、生产经营单位、中介机构以及社会公众等。依照用户权限、职责或设备类型，建议各信息系统分别建立业务端（政府端、企业端、公众端）、维护端、移动端等。

原则上，县级各类应用系统和综合信息门户由县级安全监管部门根据省级和市级安全监管部门的有关要求（如系统建设部署方式）自行开展组织建设（明确提出国家安全监管总局、省级安全监管部门统一建设的应用系统或已经在使用的统建系统除外），优先使用上级已建系统，与上、下级安

全监管部门和安委会成员单位进行数据交换。

（三）应用支撑层。

应用支撑层为应用服务层提供技术支撑，辅助实现应用服务的快速搭建，提供基础与外部数据调用与推送、业务流程与访问权限自定义配置等功能。

应用支撑层由通用及公共使用的基础性软件系统和基础支撑服务组成，主要包括公共应用支撑服务平台、物联网应用支撑平台、数据共享交换平台和大数据管理平台等。用户主要包括县级安全监管部门、安委会成员单位以及平台运行维护保障机构等。

（四）数据资源层。

数据资源层用于存储应用服务层和应用支撑层的相关数据，为信息系统运行和信息共享交换提供数据支撑。

按照县级安全监管部门的业务管理和服务需要，数据资源层主要包括监管执法、应急管理、行政管理、综合决策、公共服务以及共享交换、大数据分析等类别数据，主要以数据库、文件系统及独立文件等形式存储。用户包括县级安全监管部门、安委会成员单位、生产经营单位、中介机构以及社会公众等。

（五）基础设施层。

基础设施层用于提供县级安全生产信息化各类基础硬件资源和设施环境，主要包括计算与存储设备、基础网络、

通信与显示设备、场所与数据采集设备（装备）等，按照逻辑划分为全国安监云平台、政务云平台及传统非虚拟化的信息化基础环境。

全国安监云平台由总局统筹建设并提供云基础设施服务和云应用服务，政务云平台由电子政务部门统筹建设并提供政务云服务。云平台的服务主要包括计算资源服务、存储资源服务、虚拟安全服务和虚拟网络服务等。各县级安全监管部门根据电子政务管理部门、上级安全监管部门有关要求并结合实际，可以将系统部署于政务云平台，也可以部署于国家安监云服务平台。

（六）标准规范体系。

各县级安全监管部门严格遵循国家安全监管总局发布的信息化相关标准规范，推进信息化建设与应用，积极参与全国安全生产信息化标准体系建设和本省安全生产信息化标准规范编制工作。

（七）安全与运维保障体系。

各县级安全监管部门应遵循当地信息化基础条件和安全监管业务特点，遵照国家安全监管总局和电子政务管理部门有关要求，从物理安全、主机安全、网络安全、数据安全及备份恢复、应用安全等方面加强信息安全管理，建立信息安全等级保护工作机制，强化安全生产数据资源保护，保障信息化设施环境和信息系统的整体安全。

各县级安全监管部门应遵照国家安全监管总局和电子政务管理部门有关要求，结合本身实际，建立运维保障制度和运维管理平台，充分利用各类信息化技术支撑保障力量，保障信息化设施环境和信息系统的正常运行。

三、应用系统

（一）安全监管类应用系统。

1. 安全准入类系统。

建设备案登记管理系统。提供第三类非药品类易制毒化学品的经营备案和危化品重大危险源的备案、危险化学品、工贸、烟花爆竹“三同时”监管等业务的网上受理、审查备案、进度查询（发布）与到期提醒等功能。

使用国家安全监管总局建设的危险化学品登记信息管理系统开展危险化学品生产、进口企业的登记工作。

使用安标国家矿用产品安全标志中心网上申办大厅开展矿用产品安全标志的申请、审核、发放与监督管理工作。

2. 事故调查类系统。

（1）事故报送系统。

提供生产安全事故信息填报（接报）、管理、事故报送（快报、续报、专报）、事故统计与统报（含安委会成员单位）以及审核等功能。

（2）事故调查处理系统。

提供生产安全事故立案、取证、分析、报告、案件移送、

整改落实、结案归档的网上信息填报、审核、统计、发布、查询和案例制作与管理等功能。

3. 职业卫生类系统。

(1) 职业卫生监管系统。

提供建设项目职业卫生“三同时”、职业病危害项目申报等业务的网上信息填报、受理、审查备案、进度查询（发布）与提醒等功能。提供职业卫生安全许可业务的网上信息填报、审核审批、进度查询（发布）、证件制作（发证）、证件管理、到期提醒等功能。以上功能模块可以与备案登记管理系统集约整合建设。

(2) 职业卫生执法系统。

提供职业卫生执法计划、执法检查、行政处罚、案件（档案）管理、信息查询以及工作提醒等功能。以上功能模块可以与行政执法系统集约整合建设。

4. 综合协调类系统。

(1) 挂牌督办系统。

面向安全监管部门和负有安全生产监管职责的部门，提供生产安全事故挂牌督办建议、通知和事故案件的网上信息填报、审核、公布、下发、归档管理等功能。

(2) 安全生产目标管理考核系统。

提供安委会成员单位及人员信息管理与维护、考核文书制作、履职信息录入、考核考查与通知公告等功能。

5. 日常监管类系统。

（1）行政执法系统。

提供安全生产行政执法计划、执法检查、行政处罚、案件（档案）管理、信息查询以及工作提醒等功能。以上功能应同时能够在移动终端上使用。

（2）安全标准化达标系统。

提供企业标准化达标的申报、评审、审核、发证以及企业标准化自评等功能。

（3）隐患排查治理系统。

提供企业隐患自查、治理及其整改情况的网上信息录入、状态跟踪、隐患信息公示、记录管理、信息查询、企业（行业、地区）隐患排查治理情况统计报表生成以及隐患挂牌督办等功能。以上功能应同时能够在移动终端上使用。

（4）监管机构和人员管理系统。

提供本级和下级监管机构及其主要人员、直属单位及其主要人员、本地区安全生产专家的基本信息管理与维护、信息查询、统计报表生成等功能。以上功能模块可以与综合办公系统集约整合建设。

（5）安全生产举报投诉系统。

提供安全生产隐患、生产安全事故、安全生产违法行为的在线举报、网上信息录入（采集）、现场情况记录、甄别派发、接报处理、回复反馈、催办督办、办结归档、结果公

式等功能。

（6）企业在线监测联网备查系统。

提供矿山、危险化学品（含重大危险源）等高危行业企业关键设施设备安全参数、视频信号、报警信息的接入、违章行为监控等功能。有条件的可以添加现场三维重建、异常行为自动检测、图像主动抓拍、趋势预测及状态预警等智能分析功能。

（二）应急管理类应用系统。

原则上不自行建设相关应用系统，统一使用省级或市级建设的业务应用系统。

（三）公共服务类应用系统。

1. 政务公开系统。

提供拟公开政务信息的网上编辑、审核、发布、查询和统计等功能。支持“依申请公开”政务信息的网上信息填报、受理、审核审批、进度查询和发布等功能。以上功能模块可以与安全生产综合信息门户或门户网站集约整合建设，公开信息能够通过数据共享交换平台以目录形式进行管理。

2. 在线服务系统。

设置网上办事的服务窗口，提供安全监管有关业务办理信息（职权依据、办理类型、实施机关、范围与流程、申请材料、责任事项与依据、咨询与联系方式、法定期限等）的编辑、审核、发布等功能。建议以上功能模块与安全生产综

合信息门户或门户网站集约整合建设。

3. 互动交流系统。

提供意见征集、网上调查、领导信箱等功能，应列出安全监管部门的咨询电话、技术支持电话、投诉举报电话，可以提供微门户、微博、微信、移动终端应用（APP）链接。有条件的可以提供网上在线咨询、在线投诉举报、在线音视频互动等实时交互功能。建议以上功能模块与安全生产综合信息门户或门户网站集约整合建设。

4. 宣传教育系统。

依托门户网站、微博、微信及客户端，提供安全生产新闻、安全知识、专题讲座、安全文化宣传视频（网络学院）、事故案例等内容的网上编辑、审核、发布、查询和统计等功能，支持网络视频培训。有条件的可以提供网上在线访谈、在线直播、在线新闻发布会等实时功能。建议以上功能模块与安全生产综合信息门户或门户网站集约整合建设。

（四）综合决策类应用系统。

建议直接使用上级安全监管机构建设的综合查询统计系统、安全生产辅助决策系统、政策法规（知识库）管理系统、网络舆情分析系统开展相关工作。

（五）行政管理类应用系统。

建议直接使用上级安全监管机构建设的综合办公系统、机关党建管理系统、纪检监察管理系统、人力资源管理系统、

信访管理系统开展相关工作，有条件的也可以结合自身情况建设以上信息系统。

（六）安全生产综合信息门户。

建设面向安全监管部门、安委会成员单位、生产经营单位、中介机构、社会公众五类用户的安全生产综合信息门户，形成应用系统的集成对外服务窗口。

针对不同类型的用户，建议门户展现为公共服务平台、业务办公平台和辅助决策平台。公共服务平台以公众、企业为主要用户，提供办事服务、政务公开、宣传教育和互动交流等集成访问服务。业务办公平台以安全监管部门为主要用户，提供非煤矿山、危险化学品、烟花爆竹、工贸等行业安全监管执法，职业卫生监管，应急管理服务和行政办公等集成访问服务。辅助决策平台面向安全监管部门内部，提供综合查询统计、大数据辅助决策等集成访问服务。

建议安全生产综合信息门户应与门户网站整合集约建设，也可以与市级综合信息门户整合集约建设。

四、数据资源管理

如图 2 所示，县级安全生产信息资源主要来自于安全生产监管、应急管理、行政管理、综合决策、公共服务等业务产生的数据资源，同时也包括上级安全监管部门共享的安全生产信息资源、电子政务主管部门共享的基础信息资源、安委会成员单位和其他部门共享交换的信息资源、县级安全生

产监管部门共享交换的信息资源、重点企业报送和接入的信息资源等。

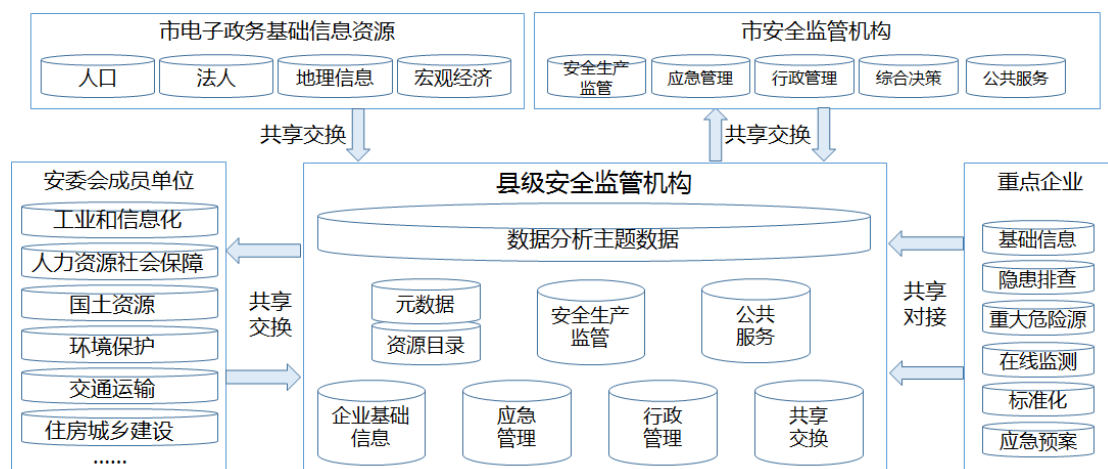


图2 县级安全生产信息资源框架图

（一）安全生产监管类数据。

安全生产监管信息资源包括安全准入、综合协调、职业健康、事故调查、日常监管、安全生产统计六类信息资源。

1. 安全准入。

（1）行政审批：主要包括危险化学品生产企业安全经营许可、烟花爆竹经营（零售）许可等安全生产行政许可等许可申请材料、各环节办理人员、许可证等记录数据或独立文件。

（2）登记备案：主要包括第三类非药品类易制毒化学品生产（经营）备案、危化品重大危险源登记备案、危化安评报告备案、烟花爆竹建设项目“三同时”监管、工贸建设项目“三同时”监管等业务申请材料、各环节办理人员、办理结果（出具文件）等信息数据或独立文件。

2. 日常监管。

(1) 行政执法：主要包括执法计划、检查记录、行政处罚结果、工作提醒等信息数据或独立文件。

(2) 标准化达标：主要包括企业标准化达标的申报、评审、审核、发证，企业标准化自评等业务有关材料、各环节办理人员、办理结果等信息数据或独立文件。

(3) 隐患排查治理：主要包括企业隐患信息及整改记录、事故隐患挂牌督办情况等信息数据或独立文件。

(4) 重大危险源管理：主要包括重大危险源基本信息、备案审核材料、各环节办理人员与办理结果（出具文件）、地图展示等信息数据或独立文件。

(5) 监管机构和人员管理：主要包括安全监管机构、工作人员、安全专家及相关设备设施等信息数据。

(6) 烟花爆竹流向管理：主要包括烟花爆竹批发单位基本情况，烟花爆竹批发单位购、销、回收情况等信息数据。

(7) 举报投诉：主要投诉举报内容、举报时间、受理结果、反馈答复、案件档案等信息数据或独立文件。

(8) 在线监测联网备查：主要包括监测对象（含危险源）基本情况、安全参数记录与实时数据、视频记录与实时数据、报警历史信息等。

3. 事故管理。

(1) 事故报送：生产安全事故首报(快报)、续报（补报）

有关信息，如事故基本情况、举报人、报送人、报送时间、发布时间等。

（2）事故调查：事故调查组成立请示与批复、立案审批材料、调查会议纪要、事故现场勘察报告、事实材料、证人证言、经济损失表、技术鉴定报告、事故调查报告、报告审查请示与批复等记录数据或独立文件。

（3）事故处理：事故案件移送审批材料、形式责任（行政处分）意见材料、整改落实材料、结案审批材料等记录数据或独立文件。

4. 综合协调。

（1）综合协调：主要包括指导、协调和监督县级安全生产主管部门的行业和领域安全监督管理的发文、通告信息，对县级相关部门的考核信息或独立文件，以及横向部门的协调工作动态信息或独立文件。

（2）安委会管理：主要包括安委会成员单位组织架构图、安委会组成人员基本情况等信息。

（3）目标管理考核：主要包括县级安委会组织机构信息、考核文书、履职信息、考核考查、通知公告等信息。

5. 职业健康。

（1）职业卫生监督：主要包括用人单位职业卫生档案、职业病危害项目申报备案材料、各环节办理人员、办理结果等信息数据或独立文件。

(2) 职业卫生执法：主要包括职业卫生执法计划、检查记录、行政处罚结果等信息数据或独立文件。

6. 安全生产统计

《安全生产统计制度》明确的各类统计指标以及辅助日常业务工作的各类汇总数据。

(二) 应急管理类数据。

1. 应急管理。

主要包括应急预案备案和管理信息（材料、各环节办理人员、办理结果）和值守人员信息等。

2. 应急资源。

主要包括各级应急指挥管理机构、应急队伍和救援力量、应急物资设备、应急专家、应急通信资源、应急运输资源、应急医疗资源、应急资金、应急避难场所有关信息等。

3. 应急预案。

主要包括安全监管部门应急预案、专项应急预案、重点防范单位应急预案等。

4. 救援指挥。

主要包含现场采集与交互信息、指挥联络信息、联合指挥协调信息、指挥调度指令信息、事故周边影响信息、人员和财产损失信息、事故衍生灾害信息等。

5. 应急案例。

主要指生产安全事故典型案例，包括案例基本信息和案

例扩展信息，以及与案例相关的图片、音视频等多媒体信息。

6. 培训演练。

主要包括培训演练计划、演练过程记录、演练流程、演练效果评估等信息。

（三）行政管理类数据。

1. 综合办公。

主要包括日常办公相关计划、档案和记录，通讯录、短消息、个人邮件，以数据记录、文档、图片、表格、视频等形式展现。

2. 机关党建。

主要包括党组织、党员、入党申请人员基本信息，党员进出、党费缴纳和使用、党员发展、介绍（证明）信等党组指业务办理记录，党支部动态、党员风采、党的知识（专题教育）等信息以及党员交流互动记录。

3. 纪检监察。

主要包括纪检监察工作有关公文、工作计划、工作记录及总结报告、案件档案、宣传教育材料等。

4. 人力资源。

主要包括招聘、人事在职离职档案、员工履历、劳动合同、奖惩、薪酬、调动、培训、绩效、考勤等信息。

5. 信访管理。

主要包括来访记录、处理状态、回复信息等。

（四）公共服务类数据。

1. 政务公开。

主要包括机构概况、组织架构、部门职能、主要领导情况、人事任免与招聘、财政预算决算、权责清单、政策法规、规划计划、公文（主动公开、依申请公开）、专项工作（警示预警、挂牌督办、事故调查结果、通报曝光、检查执法、安全生产形势分析等）动态、业务办理状态（许可、备案等）、提议提案、部门应急预案等信息。

2. 在线服务。

主要包括业务办理指南、说明、办理状态与结果等信息。

3. 互动交流。

包括在线访谈、意见建议、网上调查、政策解读的记录、反馈等信息或独立文件。

4. 宣传教育。

主要包括安全生产新闻、安全知识、专题讲座、安全文化宣传视频、事故案例，特种作业人员操作资格认定报名材料、考试结果、证书等。

（五）其他数据。

1. 企业基础信息。

主要包括工商注册数据、组织机构代码、地址、法人姓名和联系方式、企业安全管理机构、安全制度、安全人员等信息，来源于各个业务系统采集到的与企业基础相关的信

息，以及共享交换的法人信息。

2. 元数据和目录数据。

用于数据交换和信息资源目录管理的基础数据（属性）、数据交换指标、信息资源描述标识及具体内容等。

3. 数据分析主题数据。

面向数据分析应用的各类主题数据、分析过程中间记录和分析（展现）结果，来源于各应用系统数据的重新整理（抽取、清晰、比对、汇聚）。

4. 地理空间信息。

空间地理基础数据，安全监管与应急管理地理专题数据（图层），三维实景或重建结果等，以矢量图、航拍图或影像图等形式展现。

五、应用支撑平台

（一）公共应用支撑服务平台。

县级公共应用支撑服务平台可以由县级安全监管部门自行组织设计和建设，或直接使用上级平台有关资源，提供数据累、开发类和安全类服务。

1. 数据类服务。

（1）目录服务。

基于信息资源，以网页（Web）服务形式提供目录调用、检索、查询、元数据查询等服务。

（2）信息检索。

为业务系统提供文献资料、互联网信息、基础库、专题库、数据集市等的全文检索服务。

（3）数据交换。

提供纵向与上级安全监管部门以及重点企业，横向与安委会成员单位的数据共享交换。

（4）大数据服务。

为本级安全监管部门统一提供数据分析、模型共享和综合查询的服务调用接口。

2. 开发类服务。

（1）报表服务。

主要为应用系统提供数据分析、展现以及各类图表展现等服务。

（2）地理信息服务。

主要为应用系统提供电子地图服务、符合开放地理空间信息联盟（OGC）标准的网页地图服务（WMS）、网页地理要素服务（WFS）、网页地理覆盖服务（WCS）等。

（3）内容管理服务。

基于安全生产综合信息门户，提供快速定制、个性化配置、基于用户权限的内容访问管理以及门户网站系统管理等服务。

提供功能模块整合、应用接口共享、Web应用聚合和数据集成展现等内容集成功能，功能模块整合实现单点登录的

系统化延伸，应用接口共享提高底层数据整合的处理效率，Web应用聚合实现和数据集成展现分别实现客户端和服务端页面展现结构的平行化组合。

（4）视频服务。

以组件和接口方式为业务系统提供视频资源定位、编解（转）码、播放控制及智能分析等服务。

（5） workflow 服务。

提供标准化的 workflow 引擎和规则引擎配置（控制）、审核、管理与维护服务。

（6）移动应用服务。

面向微门户、微信、微博、短信、APP 等提供各应用系统数据访问和服务调用接口。

3. 安全运维类服务。

（1）统一认证服务。

为各应用系统建立统一的用户管理、认证和授权机制，实现用户“一平台注册、全系统使用”的使用体验。建议采用用户信息集中存储、权限分级管理的模式，实现用户认证、系统登录权限、系统与资源使用权限的有效管理。依照安全监管部组织架构设计用户权限模型，建立身份数据库和用户目录数据库，存储用户的登录信息和用户群组类别，建立用户类型与授权可使用应用系统和数据资源之间的映射关系，并进行定期备份。提供用户账户建立与删除、账户分级、

账户信息（登录密码、姓名、联系地址、联系电话、电子邮件等）编辑与浏览和用户群组设置等功能。建议提供系统功能模块级的用户授权管理，允许临时授权。

在此基础上，针对不同类型不同等级的用户建议采用“用户名/口令”、短信认证、U盾、数字证书等双因素/多因素认证机制，实现用户安全生产综合信息门户单点登录（SSO）的信息加密与访问控制。

（2）日志服务。

及时记录系统（平台）运行中出现的问题和可能存在的隐患，能够对日志进行汇总、查询、统计和分析，用于系统运行监控、整体环境配置、平台数据备份与安全审计等。

（二）物联网应用支撑平台。

对县级安全监管部门的全部物联网应用进行标准化和规范化管理，实现相关物联网信息规范接入和有效整合。主要提供物联信息管理、编码赋码管理、接入设备管理及展示等功能。

物联网应用支撑平台根据省级安全监管部门的有关要求建设，可以直接使用全国安监云平台提供的物联网有关支撑服务。

（三）数据共享交换平台。

根据省级安全监管部门有关要求，自建安全生产数据共享交换平台或使用上级安全生产数据共享交换平台，遵照预

先设定的规则和数据交换标准，实现县级安全监管部门纵向与上级安全监管部门、横向与负有安全监管职责的安委会成员单位信息系统、前端与部分重点企业的DataExchange，并以目录形式开展相关政务信息资源的对内管理与对外服务。

安全生产数据共享交换平台由数据交换系统和信息资源目录管理系统组成。安全生产数据交换系统，用于县本级已建监管监察信息系统之间、本级信息系统与外部其他信息系统之间的数据双向定期交换。安全生产信息资源目录管理系统用于本级安全生产信息资源的对内管理与对外服务。

各县级安全监管部门按照电子政务管理部门、上级安全监管部门有关标准与要求，组织开展数据交换系统和信息资源目录管理系统建设（或应用），建设交换共享数据库。配合完成与上级安全监管监察部门之间数据交换系统建设，配合实现本级信息资源目录与上级目录之间的同步。

平台建设有关内容参见《全国安全生产数据共享交换专项设计》。

（四）安全生产大数据管理平台。

县级安全监管部门直接使用上级大数据管理平台提供的数据查询、报告查询、报表下载等服务，也可以在上级安全监管部门指导下，基于上级大数据管理平台和大数据资源，结合自身业务需要，开展大数据建模、辅助决策和可视化综合展示等应用建设。

六、基础网络系统

（一）安全生产政务外网。

安全生产政务外网主要依托国家和地方政务外网建设。

安全生产政务外网覆盖总局和各级煤监机构、省级监管部门，市级、县级安全监管部 门，通过电子政务外网或基于互联网虚拟专用网络（VPN）技术接入网络。

安全生产政务外网主要承载安全生产监管监察执法类信息传输。

安全生产政务外网网络结构如图 3 所示，采用四级结构，以总局为核心节点，下连各个二级节点（省级安全监管部 门和省级煤监局），核心节点和二级节点组成星型网络；二级节点下连所属的三级节点（市级安全监管部 门和煤监分局），二级节点和所管辖的三级节点组成星型网络；三级节点下连所属的四级节点（县级安全监管部 门），三级节点和四级节点组成星型网络。总局通过国家电子政务外网连接各安委会成员单位。

1. 网络结构。

（1）可以通过县级电子政务外网接入的节点，连接县级电子政务外网，由县级电子政务外网和国家电子政务外网共同提供专网的多协议标记转换虚拟专用网络（MPLS-VPN）通道。

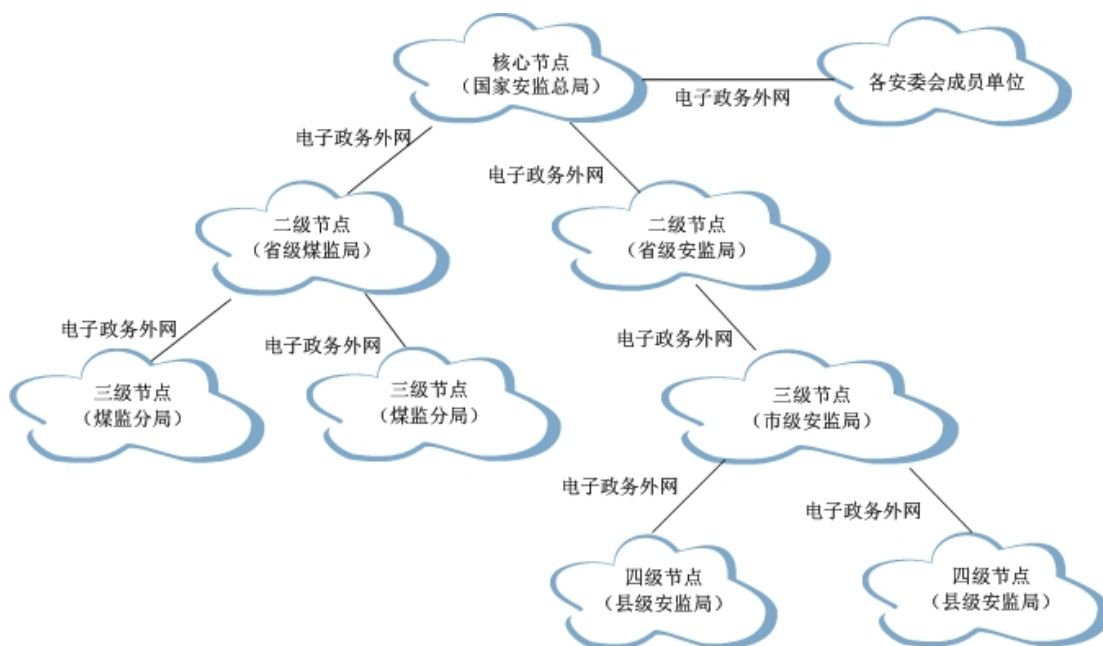


图3 安全生产政务外网结构示意图

(2) 不能通过县级电子政务外网接入的节点，通过专线连接放置在市级级电子政务外网路由器设备直接上联，由市级电子政务外网和国家电子政务外网共同提供专网的MPLS-VPN通道。

2. 网络协议（IP）地址规划。

(1) IP地址分配采用“先区域划分再应用划分”的原则，即先按各县不同的地理区域分配不同的IP地址段，在此IP地址段的基础上再按业务应用划分。特殊的专用系统由国家局统一分配。

(2) 县级IP地址根据市级IP地址段按地理区域划分子网，本地局域网内部IP地址由各县内部制定。

(二) 安全生产专网。

安全生产专网主要依托社会网络资源建设。采用VPN

技术组网，可以依托运营商网络搭建 MPLS VPN 网络。

安全生产专网覆盖所有省、市、县，以及相关安全监管企业。

安全生产专网主要承载企业安全生产音频、视频、监测、预警等信息传输。

如图 4 所示，全国安全生产专网包含 4 类节点，分别是核心节点、骨干节点、汇聚节点和接入节点，这些节点通过专线连接，形成互联互通的安全生产专网。各级安全监管部门、煤矿安监机构、应急救援机构通过专线分别接入当地安全生产专网。煤矿、非煤矿山、危险化学品等生产经营单位按照属地原则接入县级节点，国有重点企业集团按照权属分别接入总局、省、市、县级节点。安全生产专网通过向社会资源租用专线的方式组建逻辑专用网络。

各级生产经营单位通过租用专线的方式接入各级安全监管监察机构，各级安全监管监察机构通过设置专线安全接入区，对企业上传的视频和数据进行交流。

1. 网络设计规范。

(1) 县级网络通过租用电信运营商专线接入安全生产专网。

(2) 县级网络出口应区分专网出口区、互联网出口区和政务外网出口区，保证网络之间的安全隔离。

(3) 县级内部网络采用分区分域建设，同时考虑维持

已有的局域网内部网络结构。

(4) 县级网络核心设备均建议采用双设备，一主一备冗余设置，以保证网络可靠性。

(5) 出口带宽根据实际使用业务需求和业务应用模式计算，并考虑 20% ~ 30% 带宽冗余。

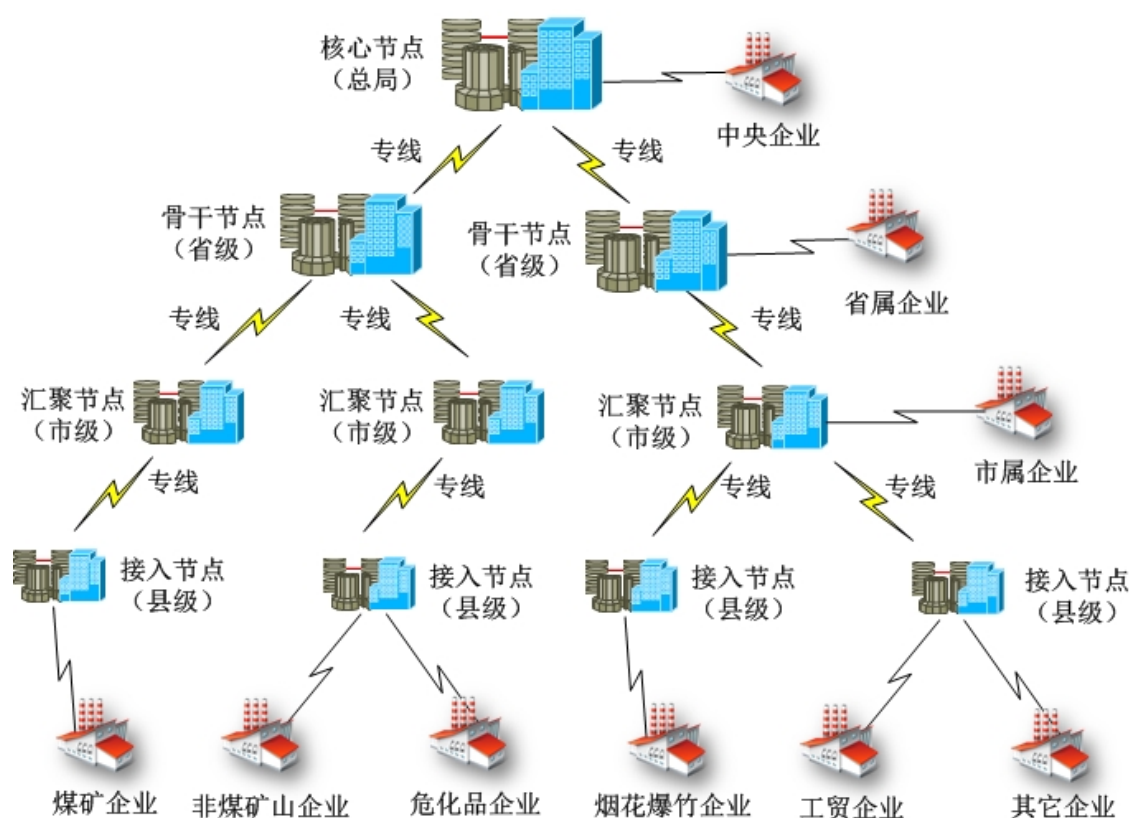


图 4 安全生产专网结构示意图

生产经营单位接入网络建议：

- (1) 可选择租用运营商专线方式接入专网。
- (2) 可选择通过互联网 VPN 方式接入专网。
- (3) 可选择通过无线方式接入专网，包括移动终端接入（配运营商用户身份识别（SIM）卡）、卫星接入等方式。
- (4) 可根据自身情况及当地运营商情况选择。

(5) 接入专网的带宽应满足冗余及应急需求。

2. IP 地址规划。

(1) IP 地址采用双轨制编制方案，直接连接互联网的设备端口应采用公有 IP 地址，其余采用私有 A 类 IP 地址段。

(2) IP 地址分配采用“先区域划分再应用划分”的原则，即先按各县不同的地理区域分配不同的 IP 地址段，在此 IP 地址段的基础上再按业务应用划分，采用可变长子网掩码。

(3) A 类 IP 地址段划分出若干子网 IP 地址段，用于各级网络和网络互联。

(4) 县级网络根据本县及接入企业规模，将市级 IP 地址划分出若干个 C 类地址使用。

(5) 当预分配 IP 地址空间不足时，可向总局网络管理部门另行申请。

3. 网络安全。

(1) 安全生产专网与互联网之间边界防护通过防火墙实现信息交互。

(2) 安全生产专网的边界防护须实现安全的访问控制和入侵防御，阻止来自外部的非授权访问，检测和阻断对安全监管部网络的探测和攻击行为，确保网络边界安全逻辑隔离。

(3) 安全生产专网相同安全域的用户或业务须采用虚

拟局域网（VLAN）、访问控制网络设备的集成式安全技术等手段实现内部用户或业务的安全访问。

（4）应用系统网络内部须采用 VLAN 或防火墙等技术实现不同应用系统的安全隔离，遵循最小化访问原则，确保应用系统间的安全访问，避免内部系统间的无限制访问，防止内部安全事件通过“跳板”方式扩散。

（5）网络设备须具备丰富的集成式安全技术，实现对动态主机配置协议（DHCP）服务器欺骗、IP 欺骗、中间人欺骗和地址解析协议（ARP）欺骗等信息安全事件的预防。

（6）网络须具备对网络流量、应用访问等的统计分析功能，采用网络流（如 NetFlow、Netstream 等）技术实现对网络流量和网络访问的采集分析、监测记录及审计。

（7）网络须具备网络性能保护的能力，避免终端被恶意软件干扰，要求对用户上网行为进行监控，确保网络资源的合理使用和用户对内部应用系统的正常访问。

（8）安全监管部門计算机网络须实现用户 PC 的全面网络准入控制，只有授权的用户才能接入网络，形成安全监管部門全网网络接入、应用系统访问统一的认证体系。网络准入控制方式宜采用中心集中认证方式。

七、基础环境

（一）机房。

结合县级安全监管部門机房建设现状，新建或者利旧已

有机房，内容如下：机房基础设计的高可用性关系到上层业务和数据的安全可靠，县级安全监管部门机房建设参照《电子信息系统机房设计规范》（GB 50174-2008）的要求，按照C级标准化机房设计，同时采用智能化和绿色节能的技术方案和措施，以满足业务部署的要求。

（二）安全系统。

按照上级电子政务外网整体安全规划以及等级保护有关要求，从物理安全、主机安全、网络安全、数据安全以及系统安全等层面进行建设，并依照相关要求完成安全互联规划、设计和实施，配置必要的软硬件设备，配置和调整安全策略，以提供安全保障。

网络安全要求配备防火墙、网闸、数据库安全审计、堡垒机、抗分布式拒绝服务（DDOS）、入侵防御系统、入侵检测系统、Web应用防火墙（WAF）、防病毒网关、网页防篡改、漏洞扫描系统、VPN网关和安全管理平台（SOC）等物理网络安全设备，保护数据中心内部网络架构。

（三）计算与存储系统。

结合县级安全监管部门计算与存储系统建设现状，在县级安全生产政务外网区和安全生产专网区部署应用服务器、数据库服务器，部署县级安全生产信息化业务系统和数据库；也可以直接使用国家安监云、政务云平台的计算和存储资源。

（四）应急通信系统。

整合固定电话、公众移动、卫星等通信方式，建立有线、无线互为补充的应急通信系统，同时实现与上级安全监管部门、本级政府应急通信系统的互联互通。

（五）移动应急平台。

在已有移动应急平台的基础上，结合本地实际，选配中小型移动应急平台、无人机和便携式应急终端等。

（六）容灾与备份系统。

1. 容灾系统。

灾备系统的设计目前可分为自建灾备系统或是利用县级政府建设的灾备中心进行灾备。

（1）自建灾备系统。县级若有条件可在异地自建容灾中心，包括应用级和数据级这两个层面的设计。

- 应用级容灾备份设计。基于应用系统的数据容灾由应用系统来实现远程复制和同步，当数据中心因灾难失效时，容灾备份中心的应用系统恢复运行，迅速接管主中心的业务。

- 数据级容灾备份设计。数据级容灾技术主要适用于数据中心级的海量数据复制。

存储级数据容灾备份将业务数据整合到存储，通过存储间的准同步/异步的方式将数据复制到容灾备份中心。

（2）利用总局及省级、市级灾备中心灾备服务。县级

安全监管部門如果没有条件自建灾备中心，则可利用上级安全监管部門建设或使用的灾备中心开展系统和数据灾备。

2. 备份系统。

本地数据备份主要依托于备份软件，在备份服务器上部署相应备份软件，通过备份软件相关数据备份功能，对业务系统产生的数据进行备份。

安全生产信息化业务数据建议每天进行增量备份，每周或者每月进行一次全备份。具体备份策略需参照实际数据备份需求以及存储空间大小。

八、系统运行维护

如图 5 所示，县级安全监管部門应依託运维管理机构与服务团队，通过安全运维管理信息化平台和基础运维工具，开展各类信息化运维服务，并通过信息化运维管理制度与规范予以保障。安全运维管理信息化平台和基础运维工具可由上级監管部門建设，县级監管部門直接使用。

建立自主运维和市场化运维相结合的信息化运维保障机制，依託上级和本级安全监管部門信息化管理与技术保障机构、第三方技术支持机构建立运维管理机构和服务团队。运维服务团队包括运维服务管理团队、基础设施运维团队、云平台运维团队和应用系统运维团队等。运行运维团队的职责和任务可以参照《国家安全生产信息化通用基础设施专项设计》。

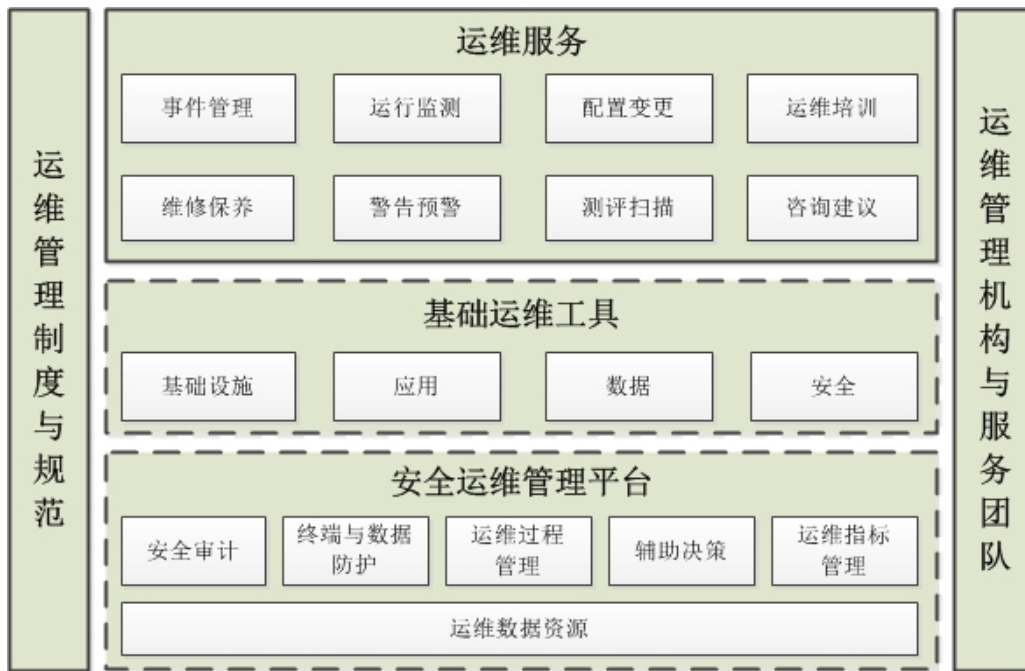


图5 县级系统运行维护框架图

安全运维管理平台提供安全审计、终端与数据防护、运维过程管理（如工单、报告管理）、运维辅助决策和运维指标管理等功能，基础运维工具包括基础设施类、应用类、数据类与安全类工具。运维服务主要包括事件管理（故障申报和应急情况响应）、维护保养（远程、现场）、运行监测、配置变更（或系统上线技术支持）、资产管理、运维培训、故障风险警告与预警、测评扫描（软件、系统、信息安全）和专家咨询建议等。对于专业技术人员短缺的县级安全监管部門，可以委托第三方参与本单位系统运维。

运维管理制度与规范应包括本级安全生产信息化基础设施运维与安全管理、信息系统使用和配置、信息系统安全与运行维护管理等方面的规章制度与规范。