ICS 35.240.01
CCS L 70

DB3205

苏 州 市 地 方 标 准

DB3205/T 1190—2025

县域安全生产监管信息化系统建设与管理要求

Construction and operation requirements of county-level safety production supervision information system

2025-06-23 发布　　2025-06-30 实施

苏州市市场监督管理局　发布

目　　次

前言 II
1　范围 1
2　规范性引用文件 1
3　术语和定义 1
4　系统架构 1
5　系统建设 2
5.1　基础设施 2
5.2　数据库 3
5.3　应用支撑 3
5.4　业务应用 3
5.5　用户 5
6　性能要求 5
7　工作流程 5
7.1　概述 5
7.2　风险库管理 6
7.3　风险点巡查 6
8　管理要求 6
8.1　制度管理 6
8.2　人员管理 6
8.3　运行维护 7
8.4　安全管理 7
8.5　风险管理 7
8.6　监督管理 7
9　评价与改进 7
参考文献 **错误！未定义书签。**

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。

本文件由苏州市应急管理局提出、归口并组织实施。

本文件起草单位：太仓市应急管理局、江苏省质量和标准化研究院、河海大学。

本文件主要起草人：张敏、徐向明、魏俊、管军、王维、凌晨。

县域安全生产监管信息化系统建设与管理要求

1 范围

本文件规定了县域安全生产监管信息化系统的系统架构、系统建设、性能要求、工作流程和管理要求。

本文件适用于县域安全生产监管信息化系统的建设与管理。

2 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件；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。

GB/T 22239 信息安全技术 网络安全等级保护基本要求

GB/T 33000 企业安全生产标准化基本规范

GB/T 36626 信息安全技术 信息系统安全运维管理指南

3 术语和定义

GB/T 33000界定的以及下列术语和定义适用于本文件。

3.1

地标化风险库 landmark risk database

通过对苏州市重点行业进行风险识别、评估和分类后，形成一套包含风险点名称、管理类别、主要事故类型、风险等级、检查事项等字段的标准风险库。

3.2

风险点 risk point

企业在生产经营过程中，依据发生生产安全事故的可能性及其后果的严重程度，判定的带有风险属性的设备设施或生产行为。

3.3

作业票 job ticket

企业在进行危险作业活动时，为了记录和跟踪生产过程中的安全管理工作而按照规定填写的报表。

4 系统架构

县域安全生产监管信息化系统（以下简称“系统”）依托政务云服务器平台、存储设备、移动办公终端、政务外网、互联网资源作为基础支撑，建设包括一企一档、风险库管理、巡查分区管理、任务管理、风险巡查、企业自查、隐患管理、挂牌督办、作业票管理、事故管理、通知公告等功能，形成企业风险画像数据库、风险数据库、巡查自查数据库、法律法规数据库等专业主题库的应用系统，架构详见图1。

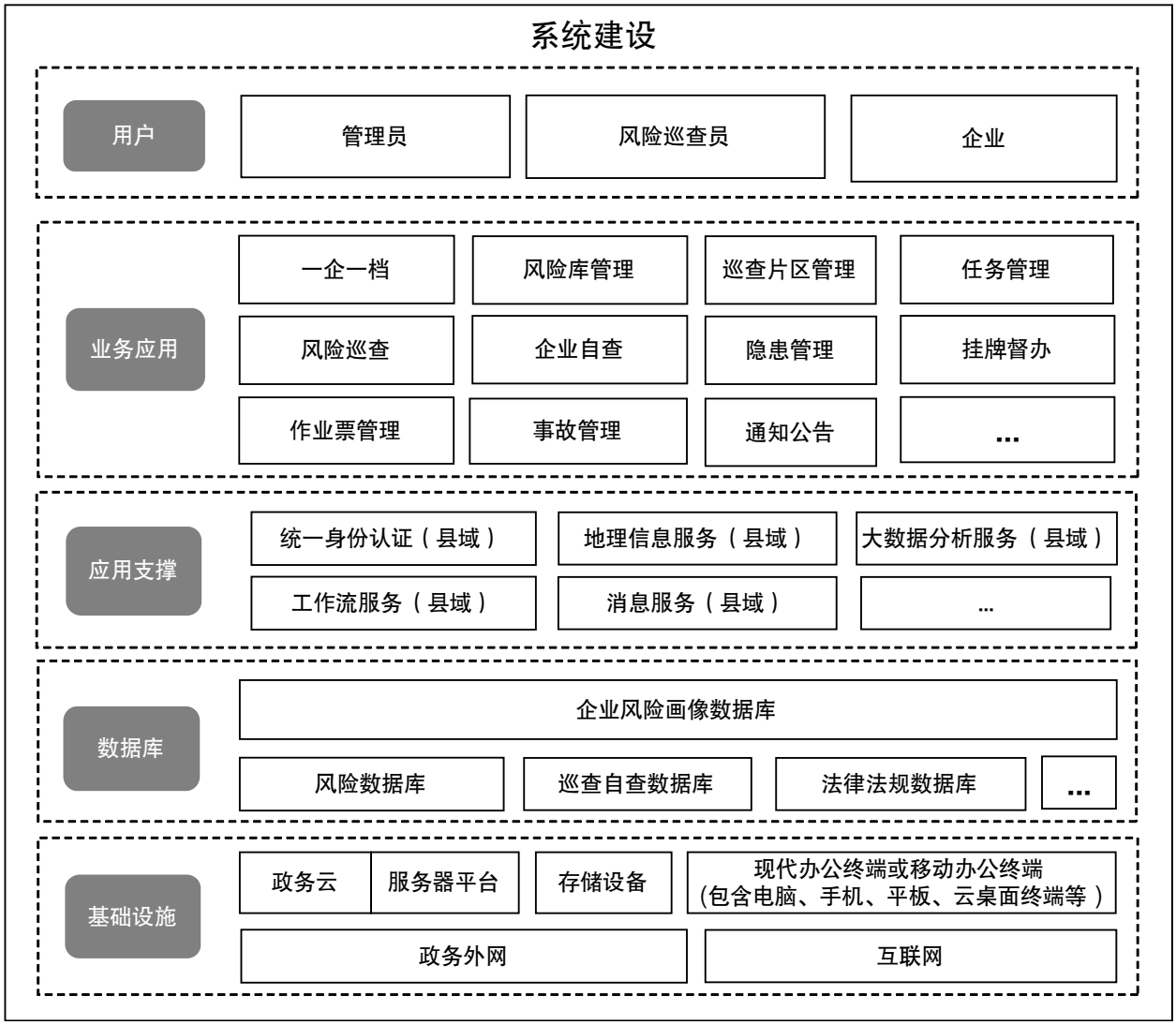


图 1　安全生产监管信息化系统总体架构

5　系统建设

5.1　基础设施

5.1.1　服务器

系统运行应满足国产化适配要求，单台服务器 CPU 核数不宜低于 32 核，内存不宜低于 128G，存储不宜低于 2T。系统运行部署应具有可靠性、实用性、安全性、开放性、先进性、经济性、兼容性和扩展性。

5.1.2　存储设备

应根据当地企业数量计算自查巡查数据及相关附件的存储需求，存储设备容量应大于实际存储需求。

5.1.3　移动办公终端

5.1.3.1 电脑

用于登录系统的PC客户端，配置CPU不宜低于10核；内存不宜低于8G；硬盘容量宜不低于512GB；显示器分辨率宜不低于1920×1080。

5.1.3.2 手机

用于登录系统的移动客户端或微信小程序，配置运行内存不宜低于8G；存储不宜低于128G，操作系统应不低于Android 10.0或HarmonyOS 4.0版本。

5.1.4 网络资源

使用政务外网和互联网等网络资源，为系统建设提供不少于百兆的带宽需求数据的网络支撑。

5.2 数据库

构建安全生产监管信息化各类主题数据库，包括：企业风险画像数据库、风险数据库、巡查自查数据库、法律法规数据库、安全日志数据库等。

5.3 应用支撑

提供业务应用所需的基础服务，包括统一身份认证、地理信息服务、大数据分析服务、工作流服务和消息服务等。

5.4 业务应用

5.4.1 一企一档

支持每个企业建立一套安全生产电子档案，功能包括：企业基础信息、企业特种设备、安全生产投入、安全规章制度、员工信息、工伤信息、应急预案。

5.4.2 风险库

5.4.2.1 管理员对风险库进行动态更新，对风险点进行增、删、改、查、批量导入、批量导出操作，以及启用状态的变更。

5.4.2.2 企业可自定义风险点，经管理员审核后，可转换成为风险库中的标准风险点。

5.4.2.3 企业可基于风险库的风险点进行绑定，关联风险位置；实现风险巡查员根据企业填报的风险位置进行巡查。

5.4.3 巡查片区管理

5.4.3.1 系统具备片区信息维护管理功能，包括：

——片区名称、片区描述、片区类别、片区等级、所属街镇、所属辖区等基础信息的录入；

——基础信息的修改维护；

——查看每一个片区在地图上的位置区域范围情况。

5.4.3.2 系统可根据安全巡查工作需要，添加、修改和删除本片区的风险巡查员。

5.4.3.3 系统可根据区域管辖的安全生产企业，添加、修改和删除网格企业信息。

5.4.4 任务管理

5.4.4.1 管理员可设定安全巡查的任务周期及复查周期，并对巡查情况进行记录。

5.4.4.2　安全巡查的任务由系统下发至风险巡查员及企业，可从区县、乡镇、自定义巡查分区等层级查看企业的自查、巡查记录，并可查看自查任务明细及发现的隐患信息。

5.4.5　风险巡查

风险巡查客户端包括电脑客户端和移动客户端。风险巡查员可通过电脑客户端进行信息核对和信息补录，通过移动客户端对企业进行日常检查，随时上报企业巡检中的隐患信息。风险巡查客户端至少应包含下列功能：

——展示风险巡查员当前周期下需要巡查的企业；

——针对企业名下风险点所对应的检查要点进行巡查操作，发现隐患后即拍即传隐患信息；

——应对基础检查项进行检查，并可在风险位置选项中新增地标化风险库中的风险点；

——查看巡查时发现的隐患，掌握隐患整改进度，并可对企业已整改完成的隐患进行复查，检验企业整改是否合格；

——查看企业基础信息、基础检查项检查结果，并可修改企业基础信息以及重置企业密码，管理员针对风险巡查员在客户端修改企业基础信息以及重置企业密码等行为进行管控与监督。

5.4.6　企业自查

企业客户端包括电脑客户端和移动客户端。企业安全员可通过电脑客户端进行信息查看和信息补录，通过移动客户端对厂区安全生产的风险点进行巡查。企业自身安全风险评估应符合 GB/T 33000 的规定。企业客户端应至少包含下列功能：

——填报风险点管理、企业自查、隐患整改以及个人中心等系统信息；

——通过地标化风险库中的风险点进行自查，手动新增企业自定义的风险点并可关联风险位置；

——查看企业当前周期任务下的检查项，依据风险位置和风险点进行自查操作，发现隐患后即拍即传隐患信息，同时可查看企业周期性自查任务的完成情况；

——对企业自查、网格巡查发现的隐患进行整改操作；

——查看本企业已生成的特殊任务记录及完成情况，针对不同类型的任务，在规定时间内开展检查工作。

5.4.7　隐患管理

5.4.7.1　系统可记录安全巡查时发现的隐患，并反馈给企业。企业可填写隐患整改情况，并记录整改进度。

5.4.7.2　系统对已完成整改的企业发送复查要求，若复查不合格，反馈给企业依据不合格原因进行整改。

5.4.7.3　管理员应能查看隐患上报、隐患整改、隐患复查信息及隐患处置进度。

5.4.8　挂牌督办

5.4.8.1　管理员将拒不整改的企业纳入挂牌督办流程，创建挂牌督办信息单，设定挂牌级别、主要隐患、整改措施等内容，并可对已创建的挂牌督办信息单进行查询、修改、导出等操作。

5.4.8.2　系统向企业发送挂牌督办信息单，企业将整改验收意见上传系统。

5.4.9　作业票管理

5.4.9.1　作业票应有危险作业类型、图片类别、提示文字以及最少上传图片数量等信息。

5.4.9.2　危险作业申请内容包括上报作业计划时间、作业人员资质等，并由企业安全员进行签字确认。企业安全员应可上传作业当天现场监督的作业前、作业中、作业后的照片。

5.4.10 事故管理

5.4.10.1 管理员可录入事故单位、事故原因、事故类型、事故级别、采取措施、死亡人数、经济损失等相关信息。
5.4.10.2 管理员对事故调查进行管理，包括调查组组长、调查组成员等信息以及调查过程中所有的事故资料管理。
5.4.10.3 系统具备安全生产事故统计分析功能。

5.4.11 通知公告

5.4.11.1 系统可按照不同企业类型、不同片区的企业或针对单个以及全部企业/风险巡查员发送通知公告。风险巡查员以及企业在电脑客户端或移动客户端查看收到的通知公告并可及时反馈相关消息。
5.4.11.2 管理员可查看已发布过通知公告的读取情况以及反馈情况。

5.5 用户

5.5.1 管理员

5.5.1.1 管理企业安全档案、指定巡查片区、安排片区风险巡查员。
5.5.1.2 设置巡查任务、下发通知公告、短信提醒等安排巡查工作。

5.5.2 风险巡查员

5.5.2.1 审核管理所属巡查片区内企业档案，核实系统上录入的企业档案信息是否正确完整。
5.5.2.2 协助所属巡查片区下的企业创建系统账号、维护风险数据，确保企业风险点符合实际情况且没有遗漏。
5.5.2.3 定期根据系统下达的检查任务，填报隐患检查及复查情况。

5.5.3 企业

5.5.3.1 维护系统中的企业安全档案、企业风险数据。基于风险画像，定期完成企业自查任务，发现隐患及时整改并填报整改情况。
5.5.3.2 对系统推送的企业特殊任务，按期完成检查工作并上报系统。
5.5.3.3 进行高危特种作业时，遵守作业票管理制度并上报系统。

6 性能要求

系统的主要性能符合下列规定：

——用户并发数不低于100；
——用户注册数不低于1万；
——可用性不低于99.9%，确保7*24 h高效运转；
——数据录入响应时间不大于2 s；
——系统查询响应时间不大于3 s；
——复杂数据分析响应时间不大于5 s。

7 工作流程

7.1 概述

系统的工作流程分为风险库管理和风险点巡查两方面，流程图详见图 2。

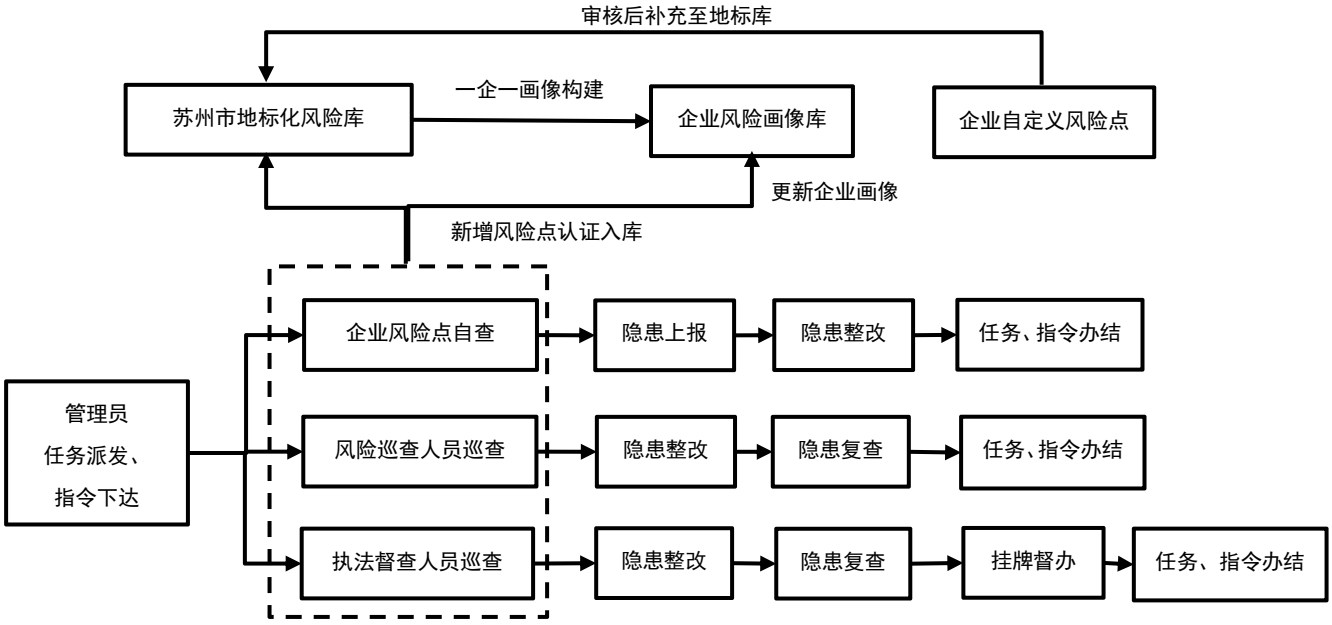


图2　安全生产监管信息化系统工作流程图

7.2　风险库管理

企业、风险巡查人员、执法督查人员依托苏州市地标化风险库精准描绘企业风险画像，形成企业风险画像库。管理员对企业自定义风险点及巡查过程中的新增风险点进行审核，并纳入苏州市地标化风险库，实现动态更新。

7.3　风险点巡查

管理员下达派发任务和指令后，系统将依据苏州市地标化风险库推送自查及巡查要求：

——每 1 个月企业进行风险点自查，依次进行隐患上报、隐患整改，将任务、指令办结情况上传系统；

——每 2 个月风险巡查人员巡查，对发现的隐患进行整改和复查，将任务、指令办结情况上传系统；

——每 3 个月执法督查人员巡查（重点监管企业），对发现的隐患进行整改和复查，并应对发现的相关重大隐患或拒不整改的企业进行挂牌督办或进入执法程序，将任务、指令办结情况上传系统。

8　管理要求

8.1　制度管理

8.1.1　制定系统建设和管理制度，重点完善数字化项目管理、数据管理、硬件设施管理、安全管理等制度。

8.1.2　结合系统建设要求与运行情况，调整优化业务流程，形成工作制度。

8.2　人员管理

依托系统建设与运行情况，结合业务流程，持续完善组织架构和岗位设置，调整岗位职责，优化人员配置。

8.3 运行维护

8.3.1 系统的运行维护应按照 GB/T 36626 的规定执行。
8.3.2 应确定专职运维人员、成立专门的信息化部门或委托专业机构，负责系统的运行维护和信息管理工作。
8.3.3 宜探索建立健全分级分类数据管理机制。

8.4 安全管理

8.4.1 系统应建立统一的安全体系，从物理、网络、系统、信息和管理等方面保证系统安全，通过权限管理、日志管理等多种技术手段，保障系统安全、高效、可靠运行。
8.4.2 系统应通过软件测评和安全测评，按照 GB/T 22239 的要求进行安全管理。

8.5 风险管理

8.5.1 应对系统建设组织开展内部评审、发布、宣贯，且过程记录完整、可读。
8.5.2 应建立完善的信息系统管理风险评估与控制程序，包括但不限于风险识别、风险定级、风险处置、风险例外处置策略。
8.5.3 应配合业务主管部门、监管部门对系统内部风险管理落实情况组织开展监督检查工作。

8.6 监督管理

8.6.1 应定期对企业的安全生产自查情况进行监督检查，督促企业落实安全生产有关规定。
8.6.2 应依据风险巡查员工作职责，监督风险巡查员工作完成情况，汇总企业安全巡查工作信息。

9 评价与改进

9.1 应建立自评自查、监督评价、问题投诉和申诉处理机制，在系统应用界面宜设置用户评价、投诉建议等功能。
9.2 应根据自评自查、监督评价、投诉反馈等信息，汇总分析系统运行的不足并制定相应的预防措施，实现系统服务持续改进。

参 考 文 献

[1] GB 17859-1999 计算机信息系统安全保护等级划分准则
[2] GB 18218-2018 危险化学品重大危险源辨识
[3] GB/T 23694-2013 风险管理术语
[4] GB/T 36626-2018 信息安全技术 信息系统安全运维管理指南
[5] 江苏省工业企业安全生产风险报告规定（江苏省人民政府令第140号）