|  |  |
| --- | --- |
| ICS | 35.240.99 |
| CCS | L 67 |

团体标准

T/CASMES XXXX—XXXX

智能辅助决策平台

Intelligent decision support platform

（征求意见稿）

XXXX - XX - XX发布

XXXX - XX - XX实施

中国中小企业协会  发布

目次

[前言 II](#_Toc206496087)

[1 范围 1](#_Toc206496088)

[2 规范性引用文件 1](#_Toc206496089)

[3 术语和定义 1](#_Toc206496090)

[4 界面设计 1](#_Toc206496091)

[5 组成 2](#_Toc206496092)

[6 功能 2](#_Toc206496093)

[7 性能 5](#_Toc206496094)

[8 接口 6](#_Toc206496095)

[9 调试和评估验收 6](#_Toc206496096)

[10 安全管理 6](#_Toc206496097)

[11 运维 7](#_Toc206496098)

[12 持续改进 8](#_Toc206496099)

1. 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。

本文件由浙江锦智人工智能科技有限公司提出。

本文件由中国中小企业协会归口。

本文件起草单位：浙江锦智人工智能科技有限公司、富盛科技股份有限公司、北京中科领虹科技有限公司。

本文件主要起草人：许翠玲、黄丽丽、张洋、魏衍召、石璐。

智能辅助决策平台

* 1. 范围

本文件规定了智能辅助决策平台的界面设计、组成、功能、性能、接口、调试和评估验收、安全管理、运维和持续改进。

本文件适用于协助政府部门应对重大事件的智能辅助决策平台的建设和管理。

* 1. 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 20269 信息安全技术 信息系统安全管理要求

GB/T 20270 信息安全技术 网络基础安全技术要求

GB/T 20271 信息安全技术 信息系统通用安全技术要求

GB/T 20272 信息安全技术 操作系统安全技术要求

GB/T 20273 信息安全技术 数据库管理系统安全技术要求

GB/T 20979—2019 信息安全技术 虹膜识别系统技术要求

GB/T 22239—2019 信息安全技术 网络安全等级保护基本要求

GB/T 25000.51 系统与软件工程 系统与软件质量要求和评价(SQuaRE) 第51部分：就绪可用软件产品(RUSP)的质量要求和测试细则

GB/T 28827.1 信息技术服务 运行维护 第 1 部分：通用要求

GB/T 28827.2 信息技术服务 运行维护 第 2 部分：交付规范

GB/T 28827.3 信息技术服务 运行维护 第 3 部分：应急响应规范

GB/T 29765 信息安全技术 数据备份与恢复产品技术要求与测试评价方法

GB/T 35273 信息安全技术 个人信息安全规范

GB/T 44588 数据安全技术　互联网平台及产品服务个人信息处理规则

GB/T 45574 数据安全技术 敏感个人信息处理安全要求

GB/T 41479 信息安全技术 网络数据处理安全要求

GM/T 0054 信息系统密码应用基本要求

* 1. 术语和定义

本文件没有需要界定的术语和定义。

* 1. 界面设计

平台界面设计应简洁明了，简单易用，应能使平台用户快速找到所需功能和信息。

平台各个模块的界面风格和操作习惯应一致。

平台应能适应计算机、平板电脑、手机等不同终端设备，在不同分辨率和屏幕尺寸下应能良好显示效果。

* 1. 组成

智能辅助决策平台由以下部分组成：

1. 综合管理平台：实现统一用户、权限管理；
2. 知识中心：对陈述性知识和程序性知识进行统一管理；
3. 审批中心：对任务进行审批、管理；
4. 数据资源中心：对各类数据资源进行采集、处理、统一管理；
5. 资源服务管理平台：对资源进行信息管理、调配、使用情况监测和分析；
6. 人员画像系统：对人员信息进行全面刻画；
7. 四侦合一应用系统：提供统一研判、分析平台，实现跨部门合作；
8. 挂图作战指挥处置系统：提供灾害应急管理和指挥处置服务；
9. 线索研判盯办系统：对多个线索进行自动分析、比对、关联、挖掘等，并将线索信息汇总用于研判；
10. 指令支持业务系统：实现指令下达、执行和反馈的全过程管理；
11. 应急指挥调度中心系统：监控和管理突发事件和紧急情况，协调应急资源和响应行动；
12. 作战预案管理平台：协助用户指定和管理各种应急预案；
13. 领导驾驶舱：将数据通过可视化方式呈现；
14. 指令闭环管理系统：进行指令传递、落实、反馈和闭环管理。
    1. 功能
       1. 工作台管理

工作台可展示登录用户的待办信息、通告通知、值班信息、警务日历、用户统计、平台使用情况、应用全览、通用应用、个人应用等内容。

* + 1. 全域布控

对发现的涉稳人员进行布控，包括：

1. 临时布控：可设置涉稳人员身份证、手机号、车牌、人像等任一信息，其余信息自动关联，任一信息触网即可产生预警；在布控时自动推荐其亲属、同户、房产及关系人车辆等信息，可选择同时进行布控；
2. 群体预警：安排群体布控，设置布控方向和预警规则；
3. 审批任务：对临时布控任务进行审批操作；
4. 布控预警：展示通过布控平台产生的预警信息；
5. 布控人员管理：展示已布控的人员信息。
   * 1. 人力情报

上传情报奖励信息。

* + 1. 标签目录

包括标签统计、标签检索、标签预览、标签管理、标签画像等功能。

* + 1. 维稳研判
       1. 情报时空关联分析

利用时空研判算法，结合涉及时间和地点的信息，对情报线索和案事件进行时空分析，揭示事件发生的时间模式、地点关联性等。

基于地址空间维度，将情报线索和案事件进行聚合，将相关的信息进行关联分析，通过人、时间等维度对信息进行关联，发现不同线索和案事件之间的联系和共同点。

* + - 1. 多人轨迹分析

对多个人员的轨迹数据进行综合分析和挖掘，揭示活动关联性和行为模式。

* + - 1. 活动规律分析

对个人活动轨迹数据进行处理和分析，识别出其经常的住宿地点、工作位置和落脚点信息。

* + - 1. 车辆关联分析

对车辆的出行时间、轨迹、落脚点等维度进行分析，发现车辆的活动规律。

* + - 1. 要素融合分析

对个人的金融活动数据和交易轨迹进行分析和关联，实现人员与其金融活动的分析。

* + - 1. 实时事件态势分析

以时空维度对可防性事件进行挖掘分析，并对具体事件的处置过程进行跟踪和监控。

对事件撒点、事件上图展示、事件类型特点等进行多维度分析。

* + - 1. 历史涉稳事件全景态势分析

通过运用统计学和数据挖掘技术，对历史事件数据进行以下分析：

1. 热点分析：识别特定时间段和地区的热点问题；
2. 冰点分析：识别特定时间段和地区的冰点问题；
3. 防控弱点分析：识别防控工作中的薄弱环节和需要改进的方面；
4. 四时段象限分析：将事件发生的时间与事件性质进行分类，统计和分析不同时间段下的事件发生模式和防控需求；
5. 事件类型统计分析：统计和分析不同类型事件出现的频率和趋势。
   * + 1. 关系分析

根据搜索的分析对象，分析其不同亲密度（亲密、频繁、偶尔）下的电话通联等数据。支持分析多个对象的共同联系人。

* + - 1. 群体分析

对恶性事件制造群体的特征、行为、关系等进行分析，了解群体的结构、动态、规律等，通过分析将表面无关联、弱关联的案事件涉案人员整合为一个群体。

* + - 1. 多维研判

支持多种搜索方式，支持搜索历史智能推荐，并允许用户灵活选择搜索范围。

支持基于单个实体进行扩展，找到跟实体相关联的数据；也可选择多个实体，同时进行扩展。

支持可视化数据关联分析操作，在实体关系网中，实时进行关系分析、路径推演、共同关系查询等，并通过可视化交互方式，获取有价值的数据。

支持通过时间轴从时间序列的维度对多维研判进行分析，观察关联关系网络及事件在时间维度的分布及统计情况。

支持用户将每一步数据关系和挖掘的临时结果保存为照片，并可随时查看或修改。

支持通过关系推演找到目标人物。

支持多种布局算法，可根据研判场景，选择适合的布局方式，以便直观了解实体之间的关系。

支持通过输入多个关键信息，基于时间轴的轨迹查询进行轨迹比对的可视化展示。

* + - 1. 再次犯罪研判

对犯罪人员进行再次犯罪研判。将经常性犯罪群体可能聚众再次作案的嫌疑推送给社区民警。

* + - 1. 综合查询

支持根据要素、关键词对数据进行检索，并可由用户设置检索的数据范围。

支持身份证号码、手机号码、电子邮箱、网络身份账号等常见要素的精确和模糊检索。

支持记录同一操作用户的搜索历史。

支持数据弹性扩展。

对查询范围内的每类数据定义不同类型的展示界面，包括列表中数据的展示内容以及数据的详情页面，并能对数据项设置展示格式、图标、链接等属性。对于有附件的数据，支持附件的下载、预览。

* + 1. 智能接出警
       1. 警情展示

通过警情列表查看一定时段内警情的事件状态、呼入时间、事发地址、联系电话和出警单位、上级案由、案由、接警员、案件等级等信息，警情列表中警情状态和警情数量应实时更新。

* + - 1. 接警

包括：

1. 当报警电话呼入，坐席电话振铃时，受理台界面自动显示呼叫相关信息；
2. 接警过程中，接警员可根据报警人描述的实际报警地址，向地图台发起二次地图定位；
3. 接警员可根据实际需要，手工选择合适的警种，以相应的接警单格式记录警情；
4. 若接警员接听到与之前某一个警情补充的报警电话，可将此接警单作为补充报警保存，并将此接警单与此警情相关的上一个接警单进行关联；
5. 当出现非电话报警时，可通过辅助接警手工生成接警单；
6. 接警时，选择案由可自动匹配微预案。
   * + 1. 转警

接警员在发现来话的警情非自己能受理的警种类型或者非本单位的警情时，可将当前受理的警情转发至对应单位。

* + - 1. 出警调度

调度出警人员、车辆、时间等信息。

* + - 1. 坐席管理

通过监控界面显示所有在线的座席，坐席详情界面可显示坐席通话数量和违规数量等信息。

监控各接出警坐席的坐席状态、违规操作。

若发现坐席状态异常，可对其进行强制释放。

* + - 1. 特殊名单管理

支持加入、删除、修改黑名单、红名单和骚扰信息。

* + - 1. 地图台操作

对地图进行对地图的放大、缩小、漫游、查询定位、测距、测面积、图片输出、辖区图层查看等操作。

* + 1. 警务处理情况调查

统计接出警自动回访、人工回访的结果和满意度。

* + 1. 报表生成

生成接出警月报、接出警回访报表。

* + 1. 图上指挥调度

以文字、曲线图、饼状图、柱状图为展现形式，配合报警类别、反馈类别、辖区单位、时间区间、关键字为条件进行搜索，统计出相关警情数据进行分析研判。

* + 1. 勤务管理

包括：

1. 查看勤务任务列表；
2. 对勤务进行排班；
3. 监督检查不同单位的应撞线人数和排班人数；
4. 查询统计勤务情况；
5. 总览勤务相关数据，可切换下属单位查看下属单位总览概况。
   1. 性能

平台正常情况下访问容量最大并发用户数应不少于 500。

平台操作界面平均响应时间应不超过 2 s，数据传输平均响应时间应不超过 5 s，调度控制指令、任务消息派发与反馈平均响应时间应不超过 30 s。

平台应用的虹膜身份识别技术应符合 GB/T 20979—2019 中第 7 章的要求。

平台软件应符合 GB/T 25000.51 的规定并具备软件升级能力。

平台应具有重要数据的备份方案，数据备份应符合 GB/T 29765 的相关规定。平台发生故障时，利用备份数据恢复时间应小于 30 min。

平台平均故障间隔时间应大于 720 h，平均故障修复时间应不超过 2 h。

平台应按 GB/T 35273、GB/T 44588、GB/T 45574 的规定，处理个人隐私信息时，保护个人信息安全。

平台应具有可扩展性和开放性，应提供硬件冗余配置方案，易于升级与扩容。

* 1. 接口

平台接口宜通过计算机网络采用数据服务总线或接口方式实现数据传输。

平台接口应具备以下特性：高吞吐量、数据分片、数据复制、多客户端接入、低传输延迟、数据一致性、服务能力可扩展。

接口信息传输速率应满足平台功能要求。

* 1. 调试和评估验收

应在系统安装完成后进行调试。

调试前应具备下列条件：

1. 平台软件已按设计要求安装完毕；
2. 已制定调试和试运行方案；
3. 根据使用说明书校验功能的正常工作及数据实时性、准确性。

平台建成后应在第三方功能、性能、安全测试和网络安全等级保护测评后，进行初步验收，初步验收通过之后，转入试运行。

平台连续、安全、稳定试运行 1 个月后，组织竣工验收。验收不合格的应限期整改，整改完毕后进行试运行、复验，直至验收合格。

* 1. 安全管理
     1. 一般要求

平台的安全管理宜按照 GB/T 20269、GB/T 20270、GB/T 20271、GB/T 20272、GB/T 20273 相应规定执行。

* + 1. 网络安全

平台网络安全等级保护应符合 GB/T 22239—2019 中第三级安全要求。

平台不应承载高于其安全保护等级的业务系统。

平台应建立安全防护机制，对网络进行 24 h 不间断监控，能检测到网络攻击行为。

平台网络应保障数据的完整性、持续性、不可篡改性。

* + 1. 运行环境安全

应使用正版、稳定的服务器版操作系统，定期升级系统补丁，加强对密码的分级管理措施。

数据库应采用科学的管理方法，对数据进行分区分库存储；数据库系统的密码和权限应分级管理。宜使用数据库备份软件，定期对数据库中的数据进行备份。

应使用主流应用服务器软件，应用服务器软件宜安全性高、稳定性好。

应安装正版高性能杀毒软件，制定安全措施，定期升级病毒库，防止病毒感染。

* + 1. 数据安全

平台应对数据进行基础的安全检测。

平台应能检测到重要数据在传输过程中完整性受到破坏，并在检测到完整性错误时采取必要的恢复措施。

平台应对数据进行分类分级安全保护，并对数据进行加密存储。

数据处理应符合 GB/T 41479 的要求。

平台应采用加密协议或其他有效措施实现数据传输保密性。

* + 1. 访问控制

应由授权主体配置访问控制策略，结合密码、短信验证、指纹等多因素安全认证方式，并限制默认账户的访问权限。平台密码应用应符合 GM/T 0054 的规定。

应授予接警员、出警员、班长等不同用户为完成各自承担任务所需的最小权限，限制不同用户对系统和数据的访问权限。

* + 1. 安全审计

平台应对可审计事件生成审计记录，如平台用户的登录、平台用户的操作、时间类型等。

平台应采用技术手段，保证审计数据完整性、保密性和不可篡改性。

平台应对审计记录进行保护、备份。

除具有明确访问权限的授权管理员外，其他用户应不具备审计日志的访问权限。

* 1. 运维
     1. 运维人员

平台应安排专人进行管理，配置专职安全管理人员并明确各系统角色权限、责任和风险。

平台应具备用户分层分类功能，满足不同用户不同权限的需求。

技术运维人员应有从事平台运维的能力。

平台运维人员应遵从安全管理规定，定期进行安全意识教育和培训。

* + 1. 运维安全

运行维护基本要求应符合 GB/T 28827.1 的要求，运行维护的交付应符合 GB/T 28827.2 的要求，运行维护的应急响应符合 GB/T 28827.3 的要求。

应根据警务需求和系统安全分析确定系统的访问控制策略。

应定期进行漏洞扫描，对发现的系统安全漏洞及时进行修补。

应建立系统安全管理制度，对系统安全策略、安全配置、安全审计等方面做出具体规定。

应依据操作手册对系统进行维护，详细记录操作日志，不允许进行未经授权的操作；应定期对运行日志进行分析，及时发现异常行为。

应建立健全的数据对接维护机制，设置专人负责数据对接运维工作，并定期整理信息。

运维人员账号应实行权限管理，定期修改账号密码。

* + 1. 运维制度

应建立运维管理的工作机制，制定以下制度：

1. 日常运维管理制度，包括运维操作规程、人员日常操作管理等；
2. 运维过程管理制度，包括运维各个环节管理、操作流程等。

应建立运维管理制度制定、发布、维护和更新的机制，定期修订和完善运维管理制度。

* + 1. 应急处置

应制定平台运行异常应急恢复方案，定期组织演练。应急恢复方案应包括网络、硬件设备、软件系统等异常情况的处置方案和应急操作手册，确保平台安全高效运行。

宜聘请专业人员定期对平台进行巡检，发现问题应及时处理。

* 1. 持续改进
     1. 反馈评价机制

宜建立平台反馈评价机制，将用户的反馈意见作为进一步改进平台的参考依据。

* + 1. 改进机制

宜定期组织专家或第三方机构对平台运行情况进行评价，根据其提供的服务效果实行有针对性的改进。

