

TC609

全国数据标准化技术委员会技术文件

TC609-4-2026-XX

城市全域数字化转型 城市智能中枢 共性组件技术要求

Citywide digital transformation-City intelligent center -Technical requirements for
common components

（征求意见稿）

2026-XX-XX 发布

2026-XX-XX 实施

全国数据标准化技术委员会 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 缩略语	1
5 共性组件分层分类	2
5.1 总体要求	2
5.2 共性组件分层	2
5.3 共性组件分类	2
6 共性组件建设开发	3
6.1 共性组件建设方式	3
6.2 共性组件开发要求	3
7 共性组件目录信息	4
8 共性组件接入要求	4
8.1 共性组件接入要求	7
8.2 共性组件接入指引	7
8.3 共性组件接入流程	8
9 共性组件管理要求	8
9.1 共性组件发布	8
9.2 共性组件下架	9
9.3 共性组件申请	9
9.4 共性组件调用	9
10 安全管控	9
10.1 安全控制	9
10.2 策略控制	10
10.3 应急处置与业务连续性	10
11 运营保障	10
11.1 运营原则	11
11.2 运营组织与职责	11
11.3 运营流程	11
11.4 运营活动	11
11.5 运营评价	11
11.6 运营安全	12
参 考 文 献	14

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。

本文件由全国数据标准化技术委员会（SAC/TC609）提出并归口。

本文件起草单位：北京思特奇信息技术股份有限公司、中国电子技术标准化研究院、浙江省质量科学研究院、合肥市数据资源管理局、南京理工大学、丰图科技（深圳）有限公司、武汉云计算科技有限公司、北京建筑大学、国泰新点软件股份有限公司、中兴通讯股份有限公司、中移雄安信息通信科技有限公司、国家数据发展研究院、华为技术有限公司、宿迁市数据局、贵阳市大数据发展管理局、山东未来集团有限公司、数融智联（徐州）信息科技有限公司、吉林电子信息职业技术学院、南通市数据局、南通市大数据管理中心、南京市玄武区数据局、高颂数科（厦门）智能技术有限公司、江苏省数字化协会、联通（江苏）产业互联网有限公司、国家发展和改革委员会创新驱动发展中心（数字经济研究发展中心）、中国信息通信研究院、四川省大数据中心、数族科技（南京）股份有限公司、苏州数据资产运营有限公司、中电信数政科技有限公司、江苏跨境数据科技有限公司。

城市全域数字化转型 城市智能中枢 共性组件技术要求

1 范围

本文件规定了城市智能中枢共性组件的分层分类、建设开发、目录信息、接入、管理、安全管控、运营保障等技术要求。

本文件适用于城市全域数字化转型背景下城市智能中枢平台共性组件的开发、管理与应用。

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 45402—2025 智慧城市 城市智能中枢 参考架构

GB/T XXXXX—XXXX 城市全域数字化转型 城市智能中枢 能力评价

3 术语和定义

下列术语和定义适用于本文件。

3.1

城市智能中枢 city intelligent center

综合应用新一代信息技术,融合城市多源数据资源,整合状态感知、建模分析、城市运行管理、应急指挥等功能,通过人机交互与协同,提供态势全面感知、趋势智能研判、协同高效处置、调度敏捷响应、平急快速切换等智能化服务,提升城市精准精细治理水平,支撑城市数字化转型的一种复杂系统。

[来源: GB/T 45402—2025, 3.1]

3.2

共性组件 common component

可在多个独立系统或应用中重复使用的模块化部件或技术单元。

注: 共性组件无需针对每个系统或应用进行单独开发。

3.3

资源市场 resource market

聚合云、网、感知、数据、组件、算法模型等数字资源的目录与门户,供用户浏览、申请与体验。

3.4

共性组件接入 common component integration

将组件信息按照规范接入至城市智能中枢平台并完成合规性检查的过程。

4 缩略语

下列缩略语适用于本文件。

API: 应用程序编程接口 (Application Programming Interface)

HTTP: 超文本传输协议 (HyperText Transfer Protocol)

HTTPS: 安全超文本传输协议 (HTTP Secure)

UUID: 通用唯一识别码 (Universally Unique Identifier)

5 共性组件分层分类

5.1 总体要求

共性组件分层分类应确保底层技术组件的通用性和标准化水平,并满足上层业务组件快速响应智慧城市建设需求的能力,主要包括:

- a) 层级划分: 符合 GB/T 45402—2025 中第 5 章的相关要求,对应能力支撑和智慧应用;
- b) 类别划分: 结合共性组件应用需求,按照使用要求、组件形式、技术能力进行分类。

5.2 共性组件分层

5.2.1 能力层

能力层由一系列标准化、可复用技术能力组件构成,该层组件聚焦技术能力封装,不包含特定业务逻辑,通过标准化接口向应用层开放能力,提供统一、高效、可靠的技术支撑,支持跨场景、跨系统的能力复用。

5.2.2 应用层

应用层是面向城市治理、民生服务等具体业务领域,基于能力层组件组合、封装而成的可复用业务功能模块。该层级组件已具备明确的业务属性和场景化功能,能够快速响应和支撑特定业务应用的开发。

5.3 共性组件分类

5.3.1 使用要求分类

组件按照使用要求分为强制类和推荐类两种类型:

- a) 强制类是城市智能中枢应用开发中必须使用的组件,涉及同质功能需求的,不得重复建设;
- b) 推荐类是根据应用实际需求情况可选择使用的组件。

5.3.2 组件形式分类

按照组件的技术实现形态与开放方式分类,分为以下5类:

- a) 接口服务类: 以标准化 API/SDK 形式提供服务的组件;
- b) 智能体类: 具备自主决策、自主执行能力的智能组件;
- c) 模型算法类: 以预训练模型、算法库或标准化算法接口等形式提供的智能化分析组件;
- d) 数据服务类: 以数据接口、数据产品等形式提供数据资源服务的组件;
- e) 其他类: 不满足上述四类特征的组件。

5.3.3 技术能力分类

按照组件的核心技术支撑方向与能力属性分类,分为以下2类:

- a) 基础支撑类组件：提供系统运行必需的通用技术支撑能力，涵盖统一用户中心、统一认证中心、统一证照中心、统一网络资源服务、统一事项中心、统一运维监控、统一视频会商、统一融合调度等组件，保障系统稳定运行与基础服务标准化；
- b) 人工智能类组件：为城市各领域智能化应用提供基础 AI 能力，提供 AI 与大数据驱动的智能决策分析能力，涵盖视频图像智能分析、自然语言处理、通用大模型、语音识别等组件。

6 共性组件建设开发

6.1 共性组件建设方式

6.1.1 新建

指依据城市智能中枢的统一技术架构、标准与规划，从零开始或基于原型设计、开发并部署全新的共性组件。应以统筹建设为主，由省、市级数据主管部门牵头，重点针对城市全域数字化转型中的全局性、基础性需求（如统一认证中心、统一证照中心等）进行开发建设，建成后应纳入“强制类”组件管理，各地、各部门在开展应用系统开发时，有需求的应用系统必须接入使用，不得自建有关组件，以确保城市核心服务的技术标准统一与系统互联互通。

6.1.2 解耦与重构

对城市现有信息系统中已具备的成熟、通用能力进行识别与提取，需完成标准化改造和服务化封装。应将其重构为符合本标准要求的共性组件，纳入“推荐类”组件管理，实现跨部门能力共享，解耦与复用。

6.1.3 外部引入

引入外部成熟的商业化软件、开源项目或平台即服务（PaaS）产品，并进行必要的集成、适配和定制与安全加固，主要包括：

- a) 市场采购：针对 AI 算法、专业领域模型（如环境监测模型、交通预测模型等）等专业技术性强、技术门槛高的需求，可通过政府采购服务等方式，从具备资质的市场主体采购成熟、合规的组件服务；
- b) 自主培育：建立组件创新培育机制，围绕城市治理、民生服务等领域的共性需求，支持科研机构、企业或开发团队开展组件创新研发。

6.2 共性组件开发要求

共性设计开发的主要要求包括：

- a) 先进的架构设计：组件应遵循现代软件工程的最佳实践，如单一职责原则（SRP）、接口隔离原则（ISP）、依赖倒置原则（DIP）等，确保代码的高内聚、低耦合，易于维护和扩展；
- b) 云原生与可运维性：严禁将任何环境相关的配置信息（如数据库地址、密钥等）硬编码在代码中。所有配置必须通过环境变量或平台统一配置中心进行注入。组件必须提供符合平台规范的健康检查接口。同时，必须输出结构化的日志和关键性能指标，以便无缝接入平台的统一监控告警体系；
- c) 标准化接口契约：组件对外提供的所有 API，必须遵循统一的错误码规范。错误码应具备自解释性，能够清晰标识错误来源模块、类型和具体原因，便于调用方进行精确的故障定位和处理；
- d) 版本管理要求：组件须遵循语义化版本控制规范，明确主版本号、次版本号、修订号的变更规则，并保证向后兼容性。

7 共性组件目录信息

组件目录将软件组件作为一种软件产品，组织汇聚在统一目录上进行推荐，供用户选用。组件目录编制工作有利于提升各领域各应用系统的开发效率和质量，实现应用之间的业务协同和数据共享，共性组件目录信息见表1。

表 1 共性组件目录信息

子项	目录信息描述
组件名称	定义:组件的名称 英文名称:name 数据类型:字符串 值域:自由文本 注解:必选项,最大出现次数为1 取值示例:监管全景查询
组件版本	定义:组件的版本 英文名称:version 数据类型:字符串 值域:自由文本 规范:主版本号.子版本号[.修正版本号[.编译版本号]] 注解:必选项:最大出现次数为1 取值示例:5.0.0 build-13124
组件功能领域	定义:描述组件功能领域 英文名称:functionalAreas 数据类型:整型 值域:来自功能领域编码 定义的值 注解:必选项:最大出现次数为1 取值示例:示例1:0代表基础服务 示例 2:1代表政府业务
组件使用要求	定义:组件的使用要求，强制使用或推荐使用 英文名称:useRequirements 数据类型:字符串 值域:来自组件使用要求编码的定义 注解:必选项:最大出现次数为1 取值示例:强制
组件技术领域	定义:描述组件技术领域 英文名称:technicalField 数据类型:字符串 值域:来自技术领域编码 定义的值 注解:必选项;最大出现次数为1取值示例: 示例 1:1代表 API

表1 共性组件目录信息（续）

子项	目录信息描述
是否收费	定义:描述组件是否需要收费 英文名称:isCharge 数据类型:字符串 值域:来自是否收费编码定义的值的组合 注解:必选项; 最大出现次数为1 取值示例:示例 1:1 代表 收费 示例 2:2 代表 不收费
发布地区	定义:组件的发布地市 英文名称:publicRegion 数据类型:字符串值域:来自发布地市编码的定义 注解:必选项; 最大出现次数为1 取值示例:XX市
组件发布范围	定义:描述组件发布的范围 英文名称:publicScope 数据类型:整型值域:来自发布的范围编码定义的值 注解:必选项;最大出现次数为1 取值示例:示例 1:0 代表省域示例 2:1 代表市域
是否托管	定义:描述组件是否需要托管 英文名称:isHosting 数据类型:整型值域:来自是否托管编码定义的值 注解:必选项;最大出现次数为1 取值示例:示例 1:0 代表非托管示例 2:1代表托管
组件简介	定义:简要描述组件的基本介绍 英文名称:remark数据类型:字符串 值域:自由文本 注解:必选项;最大出现次数为1 取值示例:示例1:互联网法人统一身份认证是企业用户提供全面的身份认证能力,包括统一的认证登录服务能力。
组件图标	定义:组件的图标 英文名称:image 数据类型:字符串 值域:来自系统提供的可选图标 注解:必选项;最大出现次数为1 取值示例:平台内置
组件配置环境	定义:组件的体验环境地址 英文名称:demoAddress 数据类型:字符串 值域:无 注解:可选项; 最大出现次数为1 取值示例:http://xx.xx.xx.xx

表1 共性组件目录信息（续）

子项	目录信息描述
组件发布单位信息	定义:描述组件发布者的联系信息 英文名称:releaseCompanyInfo 数据类型:字符串 值域:自由文本 注解:必选项:最大出现次数为1 取值示例:地址:北京市海淀区***
组件提供方信息	定义:描述组件提供方联系信息 英文名称:serviceProviderInfo 数据类型:字符串 值域:自由文本 注解:必选项; 出现次数大于0 取值示例: 地址:北京市海淀区*** 电话:0121-88688888 邮箱:***@qq.com 联系人:***
组件API信息	定义:描述组件 API信息 英文名称: apiInfo 数据类型:结构化对象（含多个字段） 注解:可选项, 出现次数为1 接口名称:必填; 中文/大小写字母/数字/下划线/短划线/括号; 长度≤200; 平台唯一; 接口标识:必填; 小写字母/数字/短划线; 长度≤200; 平台唯一; 接口描述:必填; 长度≤200; 协议支持:必填; 支持 HTTP/1.1、HTTP/2、HTTPS/1.1、HTTPS/2; 目标服务器:选填; 可配置多个 host 与 rank （权重总和=100）; 公开路径:必填; 长度≤200; 不含特殊字符; 转发路径:必填; 长度≤200; 不含特殊字符; 调用频率:必填; ≤2000 次/秒; 转发超时时间:必填; 整数>0; 单位毫秒; 请求内容类型:选填; 默认、xml、json 和 urlencoded; 返回目标类型:选填; 默认、xml、json 和 urlencoded;
组件详情	定义:描述组件宣传推广信息 英文名称:componentDetails 数据类型:字符串 注解:必选项:最大出现次数为1 核心功能:必填, 输入框, 输入框, 250个字符, 中英文(英文含大小写)和数字; 应用场景:必填, 输入框, 输入框, 250个字符, 中英文(英文含大小写)和数字; 特色优势:必填, 输入框, 输入框, 250个字符, 中英文(英文含大小写)和数字; 常见问题:必填, 输入框, 输入框, 250个字符, 中英文(英文含大小写)和数字; 相关资源:功能测试报告、安全测试报告、组件申请指南、性能测试报告上传附件。

8 共性组件接入要求

8.1 共性组件接入要求

8.1.1 安全要求

接入组件应通过平台提供的安全检测，检测范围包括但不限于软件成分分析（SCA）、静态应用安全测试（SAST）、动态应用安全测试（DAST）及依赖漏洞库比对。只有当所有检测项均满足平台设定的最低安全基线要求时，组件方可获准接入。

8.1.2 网络要求

网络要求包括：

- a) 网络区域声明：组件上架时，提供方应在组件目录信息中明确声明其部署的网络区域（如政务外网区、互联网区），并提供准确的服务访问地址（宜使用 DNS 域名而非 IP 地址）；
- b) 访问策略声明：组件提供方应以清单形式提供服务所需的网络访问策略，明确源 IP 地址段、目标端口及协议类型（TCP/UDP），该清单将作为防火墙策略配置的依据；
- c) 健康检查要求：所有服务类组件应提供轻量级的 HTTP 健康检查接口（如/health 或/status），用于组件网关、负载均衡器及运维平台进行存活探测。该接口应能准确反映组件自身及其核心依赖服务的健康状态。

8.2 共性组件接入指引

8.2.1 接入准备

组件提供方在接入前应按以下要求进行准备：

- a) 明确服务能力：根据组件特性，明确可对外提供的能力规格、性能指标，并确认收费模式（免费/收费及计费标准）；
- b) 明确接入方式：若组件提供方属于主管部门授权接入的第三方，应与授权部门确认接入方式，并按管理要求执行托管接入或独立接入；
- c) 完成组件自检：在正式接入前应完成功能、性能及安全自检，并准备相应的功能测试报告、性能测试报告及安全扫描报告。未通过安全自检的组件不得申请上架；
- d) 准备配套文档：提供规范的接口文档（API Docs）及用户操作手册，以支撑申请方进行开发调用。

8.2.2 接入改造

组件完成接入准备后，应根据平台规范进行接口适配改造。所有组件均应适配平台的统一身份认证与API网关标准。涉及二次授权的组件应完成二次授权接口改造，智能体组件应遵循智能体交互接口规范进行改造。

8.2.3 组件部署

组件部署应满足如下要求：

- a) 非托管型组件：由组件提供方根据环境要求自行准备资源并完成部署，确保网络连通并可正常对外提供服务；
- b) 托管型组件：需通过平台部署管理模块上传制品（支持 JAR、WAR、容器镜像等格式）。制品经检测通过后，利用平台自动化能力在准入环境（或测试环境）完成部署。在准入环境通过安全评估、功能及性能测试后，方可发布至生产环境。

8.2.4 安全评估

接入平台的组件需要根据要求在组件接入前对组件进行全方位安全评估，包括软件成分分析检测、安全漏洞扫描。其中接入平台的组件应在接入前完成全方位安全评估，包括：

- a) 软件成分分析：分析软件成分及特征，识别并追踪开源组件的规范性、安全性及潜在缺陷。应支持 Java、C/C++、Python、Go、JavaScript 等主流开发语言的扫描；
- b) 安全漏洞扫描：对运行阶段的组件进行动态检测，模拟攻击行为以分析组件反应，确定安全风险；
- c) 密钥与敏感信息监测：扫描代码或配置文件，检测是否包含硬编码的 API 密钥、密码、Token、私钥等敏感信息。

只有上述安全检测均通过的组件才允许接入。未通过评估的组件需完成整改后重新申请接入。

8.2.5 组件上架

组件发布至资源市场前，须由组件提供方发起上架申请。审核通过后，组件正式上架并将元数据同步至资源目录，由运营人员发布至资源市场，供用户检索与申请使用。

8.3 共性组件接入流程

8.3.1 接口类接入流程

接口类组件是指以API形式提供服务，供应用系统调用的组件。接口类组件接入，均需通过API风险检测，确保接口安全性后方可上架，主要包括：

- a) 托管接入：应先完成组件部署与制品检测，随后进行 API 注册、调试与发布；
- b) 非托管接入：无需部署过程，直接在平台进行 API 注册与接入。

8.3.2 智能体类组件接入流程

智能体组件提供方将具备自主决策、执行能力的智能体部署在本地或政务云上。组件审核通过后，提供方应通过城市智能中枢返回服务访问地址（URL）、管理后台地址及初始访问凭证（如管理员账号或Access Token），供用户后续使用。

8.3.3 模型算法类接入流程

模型算法类组件接入包括模型部署、接口封装和服务发布三个阶段：

- a) 模型部署：将模型文件或算法代码部署至指定运行环境，完成加载与初始验证；
- b) 接口封装：基于平台标准，将模型能力封装为 API，包含输入参数校验、输出结果格式化等；
- c) 服务发布：提交模型描述、调用示例、性能指标等元数据，完成服务注册与发布。

8.3.4 数据服务类接入流程

数据服务类组件接入包括数据源配置、服务封装、权限管控、发布四个环节：

- a) 数据源配置：完成数据库、文件存储或第三方接口的连接配置，确保访问安全稳定；
- b) 服务封装：按平台规范将查询、订阅、交换等功能封装为标准数据 API；
- c) 权限管控：配置数据分级分类标识、访问权限策略及脱敏规则；
- d) 发布：提交服务目录与调用文档，审核通过后完成组件发布上架。

8.3.5 其他类

若组件技术类型不属于上述类别，可选择“其他”类型进行接入，并参照最相近类型的流程执行。

9 共性组件管理要求

9.1 共性组件发布

组件上架发布流程包括组件创建、组件接入、组件上架、组件发布四个关键环节。

- a) 组件创建

- 1) 组件发布单位工作人员在组件管理平台内创建组件，填写组件基本信息（名称、版本、功能领域、使用要求等，参考本标准第7章），并授权组件提供方进行后续开发与接入工作；
 - 2) 组件名称需唯一，避免与现有组件重复，版本号需遵循语义化版本规范。
- b) 组件接入
- 1) 组件提供方完成对组件进行预发布环境部署、网关接入操作，运营人员对组件做功能、性能及安全测试，测试通过后，组件可申请接入；
 - 2) 组件提供方按照本标准8.2节接入指引完成组件接入工作，包括接入准备、接入改造、组件部署、安全评估等；
 - 3) 运营人员对组件进行功能、性能及安全测试，测试通过后，组件可申请接入审核。
- c) 组件上架：组件接入后，运营人员对托管型组件做部署及网关接入，对非托管型组件进行接入信息核验，完成 API 注册与路由配置，通知组件发布单位工作人员发起组件上架申请流程，经主管部门（或组件管理方）审批通过后，组件上架；
- d) 组件发布：已上架组件会推送至资源目录系统，运营人员可对组件做发布操作，组件发布后会在资源门户展现，并支持使用申请。

9.2 共性组件下架

组件下架流程主要包括发起下架申请、下架审批、门户取消发布、网关删除等环节。

- a) 技术落后、存在安全漏洞且组件提供方在规定期限内拒不整改的，由组件审核方发起强制下架；
- b) 组件上架后连续 6 个月无调用记录，且经组件运营方、审核方联合评估确认无保留价值的，执行资源回收式下架；
- c) 组件功能、数据处理方式与新发布的政策法规冲突，无法通过改造符合要求的，由组件审核方发起合规性下架；
- d) 组件提供方可因业务调整、版本迭代等原因主动申请下架，提供数据迁移方案，经审核通过后执行下架。

9.3 共性组件申请

组件申请流程包括组件申请提交流程、组件申请审批流程、应用发布申请查看流程。

9.4 共性组件调用

组件申请，管理者审批通过后，支持可视化的方式直接使用，在个人订单中，点击在线使用。要求包括：

- a) 计量与审计依据：组件调用产生的数据应作为服务计量、费用结算与运营审计的基础，并记录关键调用日志；
- b) 合规性调用约束：调用行为不得用于超出授权范围的场景，且必须符合组件本身声明的数据合规性要求。

10 安全管控

10.1 安全控制

安全控制是外部应用访问组件的安全控制机制的汇总，包括访问控制、接入认证、权限控制、传输安全。要求包括：

- a) 访问控制：当业务应用调用组件时，根据能力使用者状态、应用状态、能力状态、应用来源IP 限制等条件控制业务应用是否可以调用能力；
- b) 接入认证：支持根据用户状态进行接入认证的，只有认证用户的应用才能够进行接入认证，普通用户的应用不能进行接入认证；
- c) 权限控制：权限控制是指应用访问组件时对应用可使用能力的鉴权处理；
- d) 传输安全：传输安全是指对第三方应用和组件管理平台之间的数据进行加密传输和数字签名处理，防止业务数据被篡改和抗抵赖，保证业务数据操作可追溯。

10.2 策略控制

策略控制是指为保证组件的可靠性、可用性、稳定性而采取的服务管理措施，包括流量控制、配额控制、优先级控制，对于托管在组件管理平台中的API接口，应实现策略控制能力。要求包括：

- a) 流量控制：流量控制是指为保证服务的稳定性，对单位时间内访问服务的数量加以控制，防止短时间内服务被大量调用所导致的资源耗尽，造成服务停用或者宕机，当能力使用者调用并发量超过能力的并发调用数量时，平台拒绝调用请求或采取其他应对策略措施。可采用的处理措施示例如表 2 所示；
- b) 配额控制：配额控制是指对能力调用请求次数的管控，按业务需求分为总请求次数控制和成功请求次数控制；
- c) 优先级控制：实现高优先级能力优先处理。在能力新增时，能够对能力优先级进行设定，通过配置管理可以调整能力优先级。

表 2 流量控制处理措施

编号	处理措施名称	指标说明
001	不予控制	对某些合法请求的内部系统调用，即使流量指标超标也无需采取任何流量管控措施
002	抛弃请求	直接抛弃请求，不予响应
003	采用优先级处理	针对优先级高的请求优先响应，优先级低的请求抛弃不予响应
004	触发告警事件	通过触发告警事件通知系统管理员，该措施可以和不予控制、抛弃请求、采用优先级处理三项措施同时使用

10.3 应急处置与业务连续性

应急处置与业务连续性包括：

- a) 应急预案：组件的提供方，应制定《组件服务应急处置预案》，并在组件上架后 15 个自然日内提交至组件运营方备案；预案需包含组件故障定级标准（一般故障、严重故障、重大故障）、故障通知流程（通知对象、方式及时限）、初步处置措施及目标恢复时间；
- b) 熔断与降级：平台应具备组件服务调用熔断、限流及降级能力—当组件调用错误率超过预设阈值时自动触发熔断，暂停新请求；当调用量超出组件承载上限时启动限流；当组件服务不可用时，可触发服务降级；
- c) 组件容灾：组件运营方宜建立同功能组件备选库，对核心业务依赖的组件，至少储备 1 个功能相似的备用组件；当主用组件发生严重故障（超过 2 小时无法恢复）时，应能通过人工审核或系统自动匹配，为已授权调用方推荐备用组件，并提供切换指引。

11 运营保障

11.1 运营原则

明确省、市项目建设过程中组件运营支撑原则，主要包括：

- a) 统一管理：建立省、市两级联动的组件运营管理机制，统一组件接入、审核、发布标准；
- b) 分级运营：按照组件的重要程度和使用范围，划分不同的运营等级和管理权限；
- c) 持续优化：建立组件使用情况监测和反馈机制，推动组件能力持续迭代优化；
- d) 安全可靠：保障组件运行的安全性和稳定性，建立完善的监控和应急机制。

11.2 运营组织与职责

应建立清晰的运营组织体系，明确以下角色的职责：

- a) 组件运营方：负责组件管理平台的日常运行维护、技术服务支持、系统监控、计量计费、用户管理和运营数据分析等工作；
- b) 组件提供方：应承担所提供组件的技术支撑、版本升级、故障修复、性能优化及安全保障责任，并配合运营方完成组件监控、应急处理等工作；
- c) 组件使用方：应遵守组件使用规范，负责组件的合规申请与正确使用，并及时反馈使用过程中发现的问题与优化建议；
- d) 数据主管部门：负责对组件运营状况进行监督、考核与评估，推动运营体系的持续完善。

11.3 运营流程

11.3.1 建设运营

建设运营要求包括：

- a) 规划与需求管理：建立需求征集机制，定期分析评估，确定建设优先级；
- b) 开发与测试：遵循设计开发原则，开展全流程测试；
- c) 上线与推广：按接入规范完成组件上线，制定推广计划。

11.3.2 运营管理

运营管理要求包括：

- a) 目录管理：及时更新目录信息，建立清晰的组件目录结构；
- b) 质量管理：建立质量监控指标，定期评估并优化；
- c) 版本管理：建立规范的版本控制机制，保持向下兼容。

11.4 运营活动

运营过程应覆盖组件全生命周期，主要包括：

- a) 组件目录管理：维护和更新组件服务目录，确保信息准确、分类清晰，建成城市级“共性组件超市”，实现一地上架、多地复用；
- b) 服务支持与请求响应：建立统一的服务请求与事件处理流程，确保用户问题得到及时响应与解决；
- c) 服务监控与持续改进：对组件性能、可用性及业务用量等进行持续监控与分析，定期生成运营报告，并基于数据驱动服务优化；
- d) 变更与发布管理：对组件的版本更新、配置变更等活动进行规范化管理，控制风险，确保服务连续性；
- e) 组件知识管理：积累并维护运营知识库，包括常见问题、解决方案、最佳实践等，提升支持效率。

11.5 运营评价

应定期对省、市的共性组件建设情况、复用率、可靠性进行评估。建立激励与退出机制，促进组件库的优胜劣汰与能力迭代，提升组件库的整体价值。根据GB/T XXXXX-XXXXX《城市全域数字化转型 城市智能中枢 能力评价》，共性组件相关运营评价规则见表3。

表 3 共性组件运营评价指标

指标名称	指标释义	评估规则
共性组件建设情况	评价共性组件建设数量规模情况	指标分数=40%× <i>b</i> <i>b</i> : 共性能力组件建设情况，每建设 1 个组件得 10 分，满分 100 分，共性能力组件包括但不限于统一用户管理、统一认证、统一电子印章、统一电子证照、统一消息通知、统一授权、统一签批等。
共性组件成熟度	评价共性组件建设成熟度	指标分数=40%× <i>b</i> <i>b</i> :共性组件成熟度等级 <i>c1</i> : 基础级，建立了统一的组件目录进行登记管理，对组件资源进行初步归集，能提供标准化的服务能力，得20分。 <i>c2</i> : 发展级，建立了统一的组件技术标准、接口规范和管理流程，组件以服务化形式提供，实现即插即用，得40分。 <i>c3</i> : 协同级，组件成为业务能力单元，能支撑跨领域协同应用，组件在城市内高效复用，得60分。 <i>c4</i> : 融合级，组件与业务场景深度融合，根据业务进行自动推荐、组合并弹性调度，组件之间智能协同，能完成复杂任务，得80分。 <i>c5</i> : 引领级，建成城市级“组件超市”，实现一地上架、多地复用，得100分。
共性组件复用率	评价共性组件在业务系统中的复用情况	指标分数=20%× <i>b</i> ×100 <i>b</i> : 在各个业务系统中统一使用的共性能力组件数量/要求同意使用的共性组件总数量。

11.6 运营安全

11.6.1 安全支撑

安全支撑可从“风险识别、持续监测、应急处置、恢复与评估”四个阶段，进行全生命周期运营保障。要求包括：

- a) 组件安全风险识别：在引入自研组件、第三方组件或开源组件前，需建立安全准入机制，包括来源审查、许可证合规性检查、已知漏洞扫描等；
- b) 组件运行持续监测：建立组件运行情况监测系统，识别组件异常行为，并预测风险，触发系统引入人为干预和分析，决定是否禁用该组件或选用备用组件；
- c) 组件安全应急处置：制定组件运行应急预案，并定期进行应急演练，根据演练情况，及时发现和改进预案；当系统的组件出现问题，影响业务正常运行，启动应急预案，保障业务的连续性；
- d) 组件恢复与评估：对出现问题组件，进行重新设计开发或引入新替代组件，应进行线下测试验证，及线上预运行及评估，确定问题已经解决，再正式上线。

11.6.2 制度支撑

应制定完善的运营管理制度，涵盖组件接入、服务支持、安全管理、考核评估等环节，确保运营工作有章可循。

11.6.3 平台支撑

组件管理平台应具备组件注册、部署、编排、监控、计量、用户管理等技术能力，提升运营自动化与智能化水平。

参 考 文 献

- [1] 关于深化智慧城市发展 推进城市全域数字化转型的指导意见（发改数据〔2024〕660号）
 - [2] 深化智慧城市发展 推进全域数字化转型行动计划（发改数据〔2025〕1306号）
 - [3] GB/T45402—2025 智慧城市 城市智能中枢 参考架构
-