ICS xx.xx.xx
CCS XX

团 体 标 准

T/KCH XXX—2022

智慧城市物联网支撑平台 功能规范

Functional Specifications Of Smart City IOT Support Platform

（征求意见稿）

2022-XX-XX 发布 2022-XX-XX 实施

杭州市科技合作促进会 发 布

目　　次

前　言

本标准按照 GB/T1.1-2020《标准化工作导则第 1 部分：标准的结构和编写》规则起草。

本标准为首次制订。本标准由杭州市科技合作促进会提出并归口。

本标准的某些内容可能涉及专利，本标准的发布机构不承担识别这些专利的责任。

本标准起草单位：浙江千问科技有限公司、集思蔚来（杭州）科技有限公司、杭州佳迈科技有限公司。

本标准起草人：王伊薇、谭清端、林君柳、吴宇青、陈钢、黄剑辉、孙伟 、陈贤明。

在本标准实施过程中，如发现需要修改或补充之处，请将意见和有关资料发邮件给归口单位杭州市科技合作促进会，以便修订时参考，邮箱：irobotinfo@qq.com。

引　言

智慧城市是一个有机结合的大系统，涵盖了更透切的感知、更全面的互连，更深入的智能。物联网是智慧城市中非常重要的元素，它侧重于底层感知信息的采集与传输，城市范围内泛在网方面的建设。

通过智慧城市物联网支撑平台实现海量碎片化传感设备、物联感知应用统一接入与集成，可大大降低物联感知应用开发、集成、运维管理的难度，从而助力物联感知业务场景的发展与推广。通过平台实现物联感知数据的统一接入、存储、共享与利用，防止新的数据孤岛发生，可为城市大脑分析提供有效的海量城市数据资源。

编号 T/KCH-XXX-2022

智慧城市物联网支撑平台 功能规范

1. 范围

本标准规定了智慧城市物联网支撑平台的通用术语和定义、基本功能与要求。
本标准适用于智慧城市物联网支撑平台设计、开发及应用。

2. 规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件，仅注日期的版本适用于本文件。凡是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。
《智慧城市 数据融合 第1部分：概念模型》（GB/T 36625.1-2018）

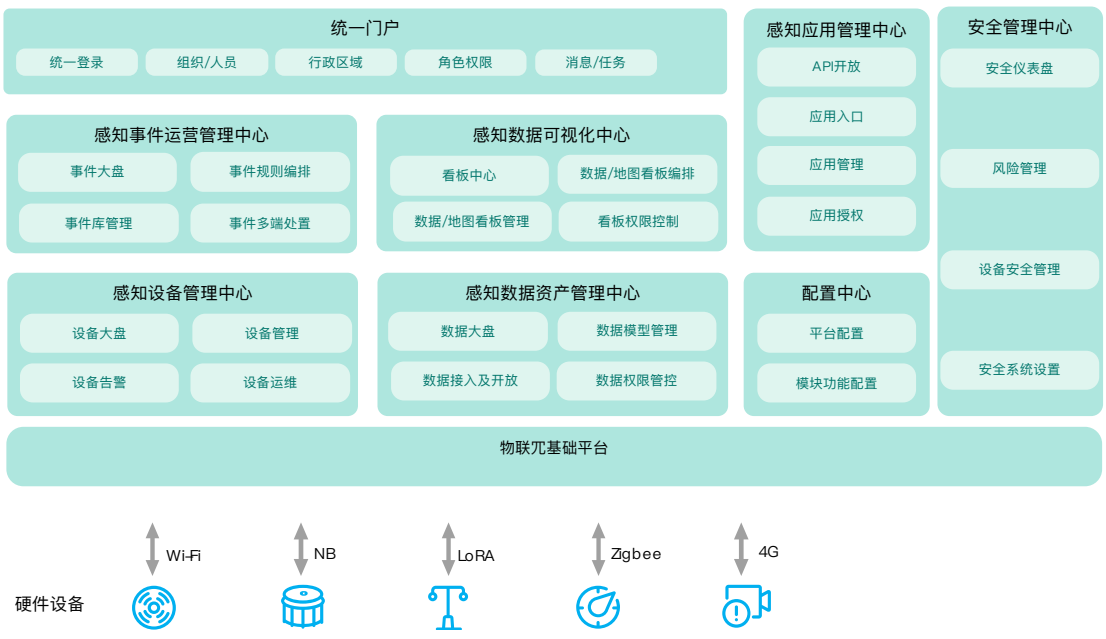
3. 术语和定义

下列术语和定义适用于本标准。
《智慧城市—术语》

4. 概述

智慧城市物联网支撑平台是基于物联网技术，支撑智能化运营管理的统一工作平台，主要包括感知设备管理中心、感知事件运营中心、感知数据资产管理中心、感知数据可视化中心、感知应用管理中心、安全管理中心、配置中心、统一门户等主要核心能力。

5. 功能架构



城市物联网平台是基于物联网技术，支撑智能化运营管理的统一工作平台，主要包括感知设备管理

中心、感知事件运营中心、感知数据资产管理中心、感知数据可视化中心、感知应用管理中心、安全管理中心、配置中心、统一门户等主要核心能力。

6. 物联网平台

6.1. 物联网基础平台

6.1.1. 设备接入管理

物联网设备接入。

通过2/3/4G、NB-IoT、LoRa等不同网络设备接入方案，解决多元异构网络设备接入管理问题。

需提供MQTT、CoAP等多种协议的设备SDK，既满足长连接的实时性需求，也满足短连接的低功耗需求。

开源多种平台设备端代码，提供跨平台移植，支持基于多种平台做设备接入。

6.1.2. 设备通信管理

设备可通过物联网平台与云端进行双向通信。物联网平台提供了设备与云端的上下行通道，为设备上报与指令下发提供稳定可靠的支撑。

服务端和设备端通过Topic来实现消息通信。为了方便海量设备基于海量Topic进行通信，简化授权操作，物联网平台要支持Topic类（Topic是针对设备的概念，Topic类是针对产品的概念）。产品的Topic类会自动映射到产品下的所有设备中，生成用于消息通信的具体设备Topic

Topic类是一个Topic模版配置，编辑更新某个Topic类后，可能对产品下所有设备使用该类Topic通信产生影响。

除物联网平台预定义的Topic，可以根据业务需求，平台支持自定义Topic。

6.1.3. 设备运行管理

提供完整的设备生命周期管理功能，支持设备注册、功能定义、数据解析、在线调试、远程配置、远程维护、实时监控、分组管理、设备删除等功能。

对设备进行抽象，利用设备物模型对设备的属性、事件和服务进行描述，使得能够软硬件分离，简化应用开发。

提供设备上下线变更通知服务，方便实时获取设备状态。提供数据存储能力，方便用户海量设备数据的存储及实时访问。

提供设备影子缓存机制，将设备与应用解耦，解决不稳定无线网络下的通信不可靠痛点。

6.1.4. 边缘计算接入

边缘计算平台，物联网平台能力在边缘端的拓展。它继承了物联网平台安全、存储、计算、人工智能的能力，可部署于不同量级的智能设备和计算节点中，通过定义物模型连接不同协议、不同数据格式的设备，提供安全可靠、低延时、低成本、易扩展、弱依赖的本地计算服务。同时，可以结合大数据、AI学习、语音、视频等能力，打造出云边端三位一体的计算体系。

6.1.5. 设备安全接入

1) 身份认证

提供芯片级安全存储方案及设备秘钥安全管理机制，防止设备密钥被破解。安全级别很高。

提供一机一密的设备认证机制，降低设备被攻破的安全风险，适合有能力批量预分配ID密钥烧入到每个芯片的设备。安全级别高。

提供一型一密的设备预烧，认证时动态获取设备证书，适合批量生产时无法将设备证书烧入每个设备的情况。安全级别普通。

2) 通信安全

支持TLS（MQTT\HTTP）、DTLS(CoAP)数据传输通道，保证数据的机密性和完整性，适用于硬件资源充足、对功耗不是很敏感的设备。安全级别高。

支持TCP(MQTT)、UDP(CoAP)上自定义数据对称加密通道，适用于资源受限、功耗敏感的设备。安全级别普通。

支持设备权限管理机制，保障设备与云端安全通信。

支持设备级别的通信资源（TOPIC等）隔离，防止设备越权等问题。

6.2. 感知设备管理中心

6.2.1. 设备空间管理与可视化展现

基于接入平台的各种类型感知设备的地理位置和实时数据构建出城市级的综合设备运行态势的可视化大盘。通过设备大盘可以实时监测当前区域内所有感知设备的空间分布、设备整体运行关键指标及统计数据（类型占比、区域占比），并可以查看单点设备的实时数据或进行视频流直播，通过一张图实现城市感知设备资产的全局洞察。

6.2.2. 设备关键指标分析与展示

分析城市感知设备的总量，在线率、激活率是重要的考核指标，用来判断城市范围感知设备的整体运行情况。

6.2.3. 设备全生命周期管理

平台提供了设备创建、接入、部署、运维、删除的全生命周期管理。首先通过新增设备，完成设备入网凭证的统一颁发，设备供应商将设备入网凭证及平台域名烧录到固件中设备才能连接到城市平台，从而保障设备连接的安全可靠。设备的基本信息可以在根据实际需求进行编辑（包括设备所属的权属机构，部署区域、详细地址、经纬度坐标等等）。

平台同时提供设备信息的批量修改工具，一方面可以根据设备的现场部署情况填写设备部署信息模版表格，将设备部署信息一次性导入到平台。一方面可以根据实际管理需求给设备批量打标，实现各种个性化的管理需求。设备的实时数据和历史数据通过安全可靠的加密通道传输到平台，平台提供设备实时数据（属性和事件）和历史数据（属性和事件）的存储及查看功能。对于摄像头类设备，平台目前只支持视频拉流的直接播放功能，不支持存储回看功能。

同时针对实际业务需求，平台提供多维度的设备检索方式来快速定位到具体设备，当前支持设备ID、类型、型号、供应商、部署区域、权属机构、通讯方式、设备状态、标签类型等维度进行具体设备或某一类设备的检索功能。

6.2.4. 设备监控与告警管理与展现

管理与展现基于对设备资产中设备本身的运行状态的监控产生的告警记录，方面用户在统一看到与处置所有相关的设备告警。

6.2.5. 设备固件升级

远程维护是针对感知设备完成实施部署后，通过远程在线的方式进行设备的维护管理，提升感知资产的运维效率，目前主要提供远程的固件升级功能。由于设备资产的权属归属于相应的政府机构，所以固件的升级需要得到业主方的认可和授权，设备供应商可以通过相应API对设备进行升级，但是升级计

划需要得到相应权限人员的审批，审批通过之后会自动生成设备的升级任务，用户可以在平台查看升级的进度、影响的设备范围等具体信息，以此对升级的情况进行评估。

6.3. 感知数据资产管理中心

6.3.1. 数据接入管理

物联感知设备的数据会自动沉淀到平台的感知设备管理中心，而在实际业务需求中依然会存在很多非感知设备的数据（比如五常的实时气象数据、市区所有室内停车场的基本数据等），这些数据通过平台提供的数据接入功能来完成数据汇聚，目前支持API对接、文件上传和数据库对接三种方式。

对于更新频率较低的数据模型，建议采用文件导入的方式来进行数据接入。在具有某个数据模型的数据读写权限的情况下，可以按照平台提供的数据模板，将数据录入到文件中，通过文件完成数据的批量导入。平台会对数据格式进行校验，校验通过后进入审批环节，审批通过后数据会自动导入到对应的数据模型中。

而对实时性，更新频率要求较高的数据，建议采用API的方式完成数据接入，将数据及时更新到对应的数据模型中。实际操作时需要预先在平台上创建应用，然后在应用授权中选择可以写入的数据模型及数据相关的API调用，然后在数据模型的权限管理时选择授权给对应的第三方应用。

对于可以获取到数据库信息的数据模型，可以直接配置数据库相应信息，数据会自动同步到对应的数据模型中。

6.3.2. 数据管理

数据管理是数据资产管理平台最重要的功能之一，在数据管理页面，平台使用者可以搜索到整个平台的数据模型，根据不同的模型权限对数据进行管理，也可申请相应的数据模型权限。数据管理权限类型分为5种，分别是模型管理、数据管理、数据读写、数据只读以及无权限，不同的数据管理权限可进行不同级别的数据操作。

在数据管理的主页面上可以点击新建模型来创建一个新的模型，同时也可以点击查看详情进入的模型详情。模型详情页可查看模型的详情信息，包括所属部门、创建人、创建时间、最近访问时间、最近变更时间、模型权限、权限有效期、数据最近变更时间、访问记录，数据概况以及模型字段详情。模型对应有如下操作，申请权限、数据接入、数据开放、编辑模型、权限管理、删除模型以及查询数据。不同模型权限对应了不同的操作权限。

数据模型（Data Model）是数据特征的抽象，类似于数据库中的表。数据模型中需要定义具体的数据字段名、字段类型、字段约束条件、是否脱敏等信息。字段的定义可以手动输入，也可以直接从已有数据库中同步对应的表结构。数据模型的管理包括数据模型的创建、删除、编辑等功能。

6.3.3. 数据开放管理

数据本身是一种资产，资产的特性是要通过流动，在关键的人手里才能产生巨大的价值，但这个流动必须是可控可视的，平台提供了可视化数据权限、数据清洗、数据脱敏、数据申请、数据审批等管控工具，实现数据开发管理。

数据开放应具备对数据流通的规则定义、流通过程的管理和API接口的开放、API接口封装以及API接口权限几部分。

6.3.4. 数据资产统计分析与展示

对城市数据管理者提供了数据资产各个维度的统计与抽象，城市数据管理者可以在数据大盘上看到数据多个维度的统计，包括总量统计、总量变化趋势、访问排行榜以及各级部门之间的占比。

6.3.5. 感知数据可视化管理

数据可视化编排是基于城市数据开放汇聚的物联感知数据、社会开放数据、政府存量数据，围绕数据呈现，进行数据基于GIS、图表等数字呈现手段等可视化配置编排工具，直观呈现数据的看、查、管、用，将元数据直接映射到流程，以政府管理流程的输入驱动数据、算法、流程的自学习和自优化。

1) 数据可视化展示

地图可视化：将城市资产（主要是指物联网相关部件、政府存量数据、社会开放数据）的空间位置信息，通过GIS平台以二维方式显示资产空间分布，并进行空间相关的分析及计算。

图表可视化：基于图表形式，对城市感知设备、数据资产、事件等信息进行可视化展示，为城市管理、运营调度、辅助决策提供数据支撑。

2) 数据可视化配置

可视化编排包括地图可视化配置引擎与图表可视化配置引擎两大功能：

地图可视化配置引擎：基于城市默认地图底图，结合地图可视化引擎，支持用户自主定义物联网及城市相关数据、事件与空间位置的标绘和关联。

图表可视化配置引擎：支持基于数据可视化引擎，对相关数据通过图表形式进行可视化展示，系统支持对可视化图表进行个性化定制。

6.4. 事件运营中心

6.4.1. 事件可视化管理

实现城市事件可视化展示、事件态势感知、事件多维统计分析的管理仪表盘。通过事件可视化展示的城市事件统一视图，城市管理者可以进行统一的组织和指挥调度。事件可视化展示通过基于GIS，形成城市可视化管理平台，使城管、环保、水务等部门基于该仪表盘实现对城市事件的监控、处置、调度、跟踪等：

6.4.2. 事件配置管理

城市物联网平台通过城市事件采集与上报，可实现日处理超过百万城市事件（安全、交通、水务、环境…），如何让城市管理者更加高效、智能、正确、及时的处置海量城市事件？城市运营中心通过事件配置管理模块，通过对上报事件进行类型定义、严重级别判定、基于规则管控，实现城市事件进行梳理、过滤、智能配置，使城市管理者能够针对重要、严重、紧急的事件，进行有效的针对性的分级分时处置。针对重要性严重级别低的事件，可以自动隔离和甚至智能解决。

6.4.3. 事件信息管理

通过事件的关键数据统计、统计图表和具体事件列表的方式展示城市事件的综合概况。

通过事件列表提供了查看事件记录的详情，处置预案，处置进度，以及执行处置操作的功能。可以根据事件的不同维度进行搜索和过滤，如事件编号、事件名称、事件类型等，以方便快速地定位到具体时间。

可以直观地看到已触发事件的详情，包括事件发生的概述、等级、处置方案、及处置流程操作，对事件的查看和处置需要有权限控制，有权限的用户才能查看和处置。

6.4.4. 事件触发规则管理

事件触发规则管理是城市事件借助物联网设备/数据进行基于规则编排或结果计算出来可以用于执行的事件触发逻辑的管理列表，主要用于管理平台所有定义好的事件清单，方便管理人员可以了解当前平台可以解决问题的城市事件全貌。

6.4.5. 事件处置流程管理

事件处置流程管理是事件处置触发后的处置预案及流程配置、管理与启动，同时实现事件处理流程中的状态呈现。

运营管理过程中，基于事件的工作流模型，根据事件的类型和严重程度，自动启动相应的工作流程，并且能够监控工作流程的状态；

工作流管理可应用到系统的所有事件处置过程中，管理者随时可以了解当前工作的执行情况，将处置任务准确传递到相关的责任人，保证事件能够及时完成，信息传递也可以通过邮件、站内信、手机短信方式进行推送；

应用工作流可以按事件规则连接所有业务部门，完成计划、审批、执行、反馈相关环节，实现信息传递，并能够跟踪流程执行情况，发现任务执行环节中存在的问题，及时进行改进。

事件处置流程管理可以确保能够以统一视图，进行统一的组织和指挥调度，实现城市事件标准化、流程化、智能化处置。

6.4.6. 事件处置规则引擎

规则引擎服务是物联网管理平台提供的标准服务之一，能够为开发者以及上层应用提供规则管理、规则定义和规则的运行环境。通过规则引擎服务，可以满足不同业务场景下的事件处置流程自动化运行需求，例如配置触发条件和联动规则，如告警触发等，实现设备间的互联互通和消息推送等能力。通过规则引擎实现跨业务部门的应用联动，实现城市多业务系统实现数据共享、任务分发、工作协同。

6.4.7. 事件统计分析

未来更好的运营与管理城市，城市管理者需要了解城市事件发生的概况、事件特征、发生概率、发展趋势。事件统计分析系统是通过统计分析，并以多维图表与列表的方式展示城市事件的概况，从而帮助城市管理者对城市状况以及发展趋势做出判断。

6.5. 感知应用管理中心

6.5.1. 应用集成

城市感知设备需要被丰富的应用调用后才能产生最终的业务效果，而平台作为设备的统一接入层，需要向应用开放对应的设备数据及管控通道。这些开放能力，需要通过有效的授权模型来保证其合法性。应用集成重点通过不同的API调用完成。API的资源授权会在应用权限管理中进行统一操作。

6.5.2. 应用管理

提供基本的新增应用、编辑应用基本信息及应用配置功能，并支持多维度（类型、名称、状态）的应用检索功能。

提供统一的入口，对应用的名称、类型、图标、访问地址、供应商和功能描述等进行管理。

6.5.3. 应用监控

支持通过状态来控制应用中心中的应用可见性，可以在后台设置应用上线、下线。应用中心中展示当前用户可以访问的应用，可以直接免登跳转到相关应用的页面，其中允许访问哪些应用为可见、哪些不可见，可以在角色权限中配置。

如果某个应用完成配置，调试验证完成，那么可以通过在系统中直接启用 / 停用应用，并直观显示系统启用和停止的状态。系统的启停的权限，可以通过在后台配置中完成。

6.5.4. 应用权限管理

基于平台沉淀的统一设备资产、数据资产、事件、任务、消息、人员、组织机构、角色权限、行政区域等，对不同的应用授权不同的可访问资源及API来实现在统一资源的基础上不同应用本身的权限控制。

6.6. 物联网安全管理中心

6.6.1. 安全仪表盘

1) 风险统计

设备风险统计部分包括受影响设备的数量，发现漏洞的数量，阻挡威胁的事件数，以及待修复设备的总量。

2) 设备安全等级统计

通过设备发布时的安全检测结果，平台可以统计出所有接入设备的安全机制的实践等级，可以展示出符合各安全等级的设备比例状况。各个安全等级又详细展示出具体安全方案分类下详细的设备比例。

3) 设备异常事件时间线

以事件轴的方式展现在一段时间内每一个采样时间点上异常事件的数量和受影响设备的数量，可以直观的反映设备安全运行状况的历史记录，便于发现潜在的风险，在事件密集的时间段可能是侵入发生和传播的时候，可以帮助缩小需要仔细排查的范围。

6.6.2. 风险管理

1) 系统异常

展示单个设备每一个异常的内容、行为以及时间点，借助端网云的安全能力，系统异常又细分为：系统对象异常、应用行为异常、网络行为异常。

安全运营人员可以进行相依的处理，包括忽略、阻止、允许。

2) 组件漏洞

直观的反映了每一型号产品对比安全运营中心漏洞库的扫描结果，如果发现相匹配的漏洞，安全运营人员可以根据漏洞的内容上传相应的补丁或者系统镜像，然后部署到该型号产品。

3) 安全日志

安全日志提供设备取证和其他安全操作的历史记录的列表和查看的功能，方便了解设备周期取证的执行结果，和单个设备是实际响应情况。在复查设备侵入事件时可以帮助作为缩小调查范围。

6.6.3. 设备安全管理

1) 设备安全发布

基于端网云的安全能力，安全运营中心可以自动感知该型号设备，并显示在安全发布页面，设备开发者只需保持设备正常运行一段时间以获取当前产品运行时再多个安全维度上的行为基线，评估设备的安全实践的等级供设备开发者参考修正。设备开发者可以发布该基线，作为后续设备运行时的安全监控的参考基线。

同时根据设备行为基线的检测结果，平台自动优化安全策略部署到设备端，进一步保证设备的安全性。设备厂商可以根据设备的典型运营场景，设置是否要对优化过的安全策略进行锁定，一旦锁定，任何不符合策略的行为将被自动阻止，否则会产生相应的风险预警提示安全运营人员，进行核实。

2) 设备安全状态

在设备安全发布后，针对每一型号设备的汇总状态和取证周期的设备需要在状态管理界面完成。安全运营人员可以在该界面进行设备管理，状态查询和调整安全设置。

6.6.4. 安全系统设置

系统设置提供平台相关事件的通知设置。安全运营人员可以根据实际要求选择需要通知的事件，并设置一个邮件地址实时接收相应的通知邮件。

6.7. 物联网平台配置中心

6.7.1. 应用管理

城市感知设备的供应商不仅提供硬件，通常还会提供解决方案（应用），而应用可以访问的设备范围，可以访问的API的资源授权都是会在应用管理中进行统一操作。

6.7.2. 组织人员管理

主要实现行政区域、机构与人员、行政区域、角色权限等平台基础功能的配置。

6.7.3. 平台样式配置

主要实现平台登录页面、整体样式、可视化展示样式的定义配置。

6.7.4. 消息配置

对平台向外部发送消息的渠道（包括短信、邮件）进行统一管理维护。

6.8. 物联网平台统一门户

6.8.1. 个人中心

登录用户支持在个人中心中修改姓名、手机号码、邮箱，所属机构和角色由于由管理员创建用户账号的时候分配。

6.8.2. 任务中心

任务中心为平台用户提供任务管理工具，实现对用户所有任务进行统一管理，并实现任务查询、任务详情、任务处置等功能。

6.8.3. 消息中心

消息中心提供平台内沟通机制，包括系统自动发送的信息以及用户相互沟通信息，可点击通知标题查看通知详情，可以对通知消息进行批量操作。

6.8.4. 应用中心

平台通过集成不同的应用（软硬件解决方案）来解决城市治理中各个细分领域（市政、水务、出行、环境、安防等）的问题，通过将ISV应用和城市平台API进行集成，解决应用管理割裂，应用中的数据烟囱、账号烟囱、设备烟囱的问题。

应用中心面向用户提供统一的应用入口，通过统一权限、单点登录，实现对应用的统一门户集成。