ICS 03.220.50
CCS V60

T/CCAATB

中 国 民 用 机 场 协 会 团 体 标 准

T/CCAATB 0032—2022

民用机场物联网平台建设指南

Construction Guidance for Civil Airport Internet of Things Platform

2022-09-26 发布　　2022-10-26 实施

中国民用机场协会　发布

目　　次

前　言

本文件按照GB/1.1—2020给出的规则起草。

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。

本文件由北京首都国际机场股份有限公司提出。

本文件由中国民用机场协会归口。

本文件起草单位：北京首都国际机场股份有限公司、中国信息通信研究院、浙大网新系统工程有限公司。

本文件主要起草人：张立斌、陈红泉、张玄弋、罗松、张健、张领、任杰、钟娟娟、张玉、柳迹恒。

本文件为首次发布。

民用机场物联网平台建设指南

1 范围

本文件给出了民用机场的物联网平台总体架构、功能和接口描述。

本文件适用于民用机场物联网平台的设计和建设。

2 规范性引用文件

下列文件对于本文件的引用是必不可少的。凡是注日期的引用文件，仅所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。

GB/T 22239-2019 信息安全技术 网络安全等级保护基本要求

GB/T 34080.1-2017 基于云计算的电子政务公共平台安全规范 第一部分 总体要求

GB/T 36478.3-2019 物联网信息交换和数据共享 第 3 部分：元数据术语

GB/T 36620-2018 面向智慧城市的物联网技术应用指南

GB/T 37025-2018 信息安全技术 物联网数据传输安全技术要求

GB/T 37032-2018 物联网标识体系 总则

GB/T 38624-2020 物联网 网关 第 1 部分 面向感知设备接入的网关技术要求

YD/T 2437-2012 物联网总体框架与技术要求

3 术语与缩略语

3.1 术语

下列术语适用于本文件。

3.1.1

规则引擎 rule engine

嵌入在应用程序中的组件，实现了业务决策与应用程序代码相分离，并使用预定义的语义模块编写业务决策；接受数据输入，解释业务规则，并根据业务规则做出业务决策。

3.1.2

规则节点 rule node

规则引擎中处理传入消息、实体生命周期事件等的基本单元。

3.1.3

规则链 rule chain

相连规则节点的逻辑单元。

3.1.4

边缘计算 edge computing

在靠近物或数据源头的一侧，采用网络、计算、存储、应用核心能力为一体的开放平台，就近提供服务。

3.1.5

外部系统 external system

与物联网平台存在数据对接关系，从物联网平台获取或推送数据给物联网平台的机场其他系统。

3.1.6

外部应用 external application

通过调用物联网平台提供的接口实现应用功能的机场其他应用。

3.1.7

物联网数据 internet of things data

感知数据以及与感知对象关联的数据的统称。

[来源：GB/T 36478.1-2018]

3.1.8

物联网网关 internet of things gateway

具有数据存储能力、计算能力和协议转换能力，可通过接口分别与物联网平台和传感器进行通信的实体。

3.1.9

网络安全 cyber security

通过采取必要措施，防范对网络的攻击、侵入、干扰、破坏和非法使用以及意外事故，使网络处于稳定可靠运行的状态，以及保障网络数据的完整性、保密性、可用性的能力。

[来源：GB/T 22239-2019]

3.2 缩略语

下列缩略语适用于本文件。

IoT 物联网 （Internet of Things）

LoRa 一种工作于非授权频段的远程、低功耗无线物联网通信技术，LoRa 是 Long Range 的缩写

MQTT 消息队列遥测传输协议（Message Queuing Telemetry Transport）

NB-IoT 窄带物联网（Narrow Band Internet of Things）

CoAP 受限应用协议（Constrained Application Protocol）

GIS 地理信息系统（Geographic Information System）

SSH　安全外壳协议（Secure Shell）

SSL　安全套接层（Secure Sockets Layer）

JSON　JavaScript 对象表示法（JavaScript Object Notation），一种轻量级的数据交换格式

4　架构与规范

4.1　概述

物联网是通信网和互联网的拓展应用和网络延伸，它利用感知技术与智能装置对物理世界进行感知识别，通过网络传输互联，进行计算、处理和知识挖掘，实现人与物、物与物信息交互和无缝对接。

物联网平台是一个集成了设备通讯、设备管理、数据流转、数据存储和数据共享等能力的平台。向下对设备提供接入管理能力，向上对物联网应用提供基于设备采集的低延迟数据和以设备为对象进行管理控制的通用能力，协同大数据、云计算等技术共同组成智慧机场的基础部分。

物联网平台技术框架体系宜采用成熟先进的物联网、移动互联等技术，可无缝融合各已建或新建的传感采集、安防监控、工业控制、融合通讯及设备管理等系统，使得各系统之间形成数据共享、智慧联动的有机整体。

4.2　系统架构

按照物联网分层架构思路进行设计，自下而上将平台分为设备感知层、边缘接入层、网络传输层、连接管理层、数据管理层和核心功能层六个层级。平台系统架构如图 1 所示。

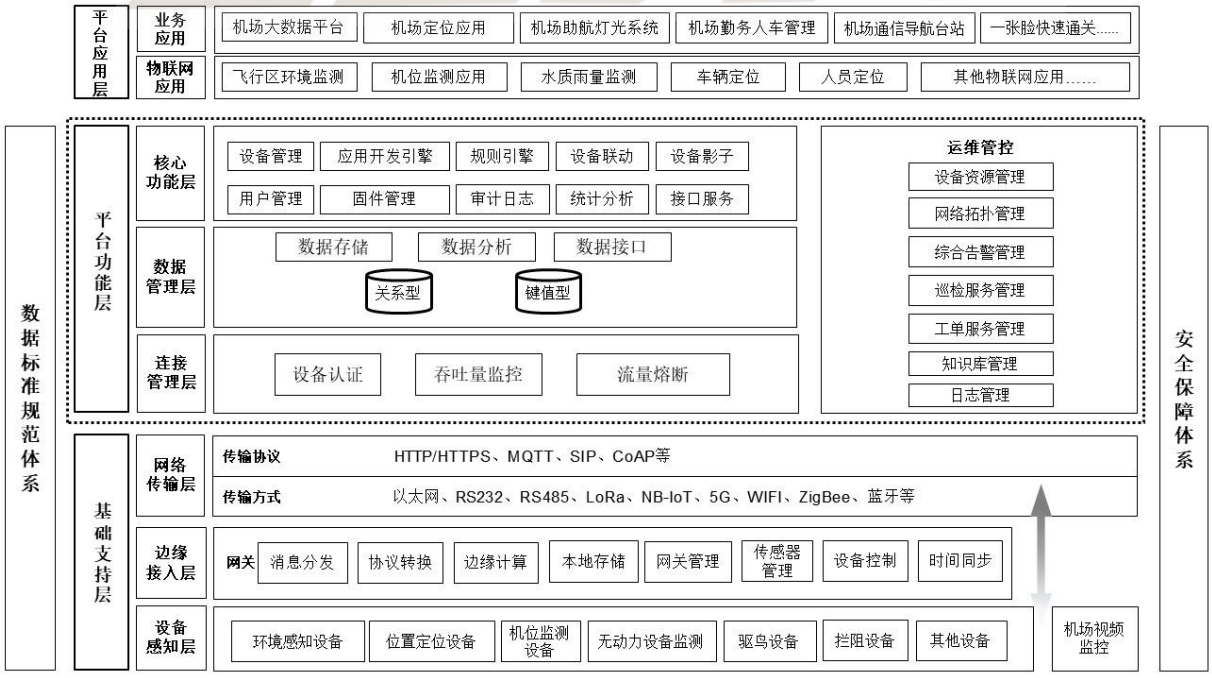

图 1 平台系统架构

设备感知层、边缘接入层和网络传输层是物联网平台的基础支撑层，连接管理层、数据管理层和核

心功能层是物联网平台自身具备的功能层。

在整个物联网平台架构之外，可定义一个由平台提供应用接口支撑的平台应用层。平台应用层包括物联网应用和业务应用两部分。平台应用层可通过物联网平台提供的标准接口服务或按照物联网互联互通技术标准，实现应用的定制开发或与物联网平台的对接。

各个层级之间宜独立灵活部署，整个平台宜采用冗余架构建立相应容错机制，保证系统稳定可靠。

4.2.1 基础支撑层

4.2.1.1 组成

基础支撑层为平台运行提供支撑和保障，包括设备感知层、边缘接入层和网络传输层三个子层级。

4.2.1.2 设备感知层

设备感知层是指可以获取感知对象信息的硬件设备的实体集合，具体可以包括电子标签、视频监控设备、环境感知设备、定位设备（包括基站和节点）、专用设备和机场其它设备。

所有设备的物联网编码可参照《GB/T 37032-2018 物联网标识体系 总则》及相关规范标准。涉及专用设备为机场使用的用于专门用途的特种设备，例如驱鸟设备、安防设备等。该类设备宜满足机场相关管理规定。设备部署时宜考虑一定的冗余量，对于安装在重要区域或监控重要指标的设备，宜同时部署两台或以上设备，保证当其中一台设备故障时不对业务产生严重影响。

传感设备接入物联网平台的技术说明详见本文件第 7 章节：设备接入接口。

4.2.1.3 边缘接入层

边缘接入层用于连接设备感知层，宜具备设备接入和数据预处理能力，同时可包含消息分发、网关管理、传感器管理、协议转换、边缘计算、本地存储、控制下发、时间同步等功能。除具备一定运算能力的智能设备以及视频监控设备外，其余需接入平台的设备宜通过边缘网关来实现与物联网平台的互联互通。（智能设备以及视频监控设备可通过网络传输层直接接入平台）。

a) 消息分发：将数据分发给外部系统，分发的规则能够配置；
b) 网关管理：支持对网关进行统一管理，包括在线状态检测和接入控制；
c) 传感器管理：支持对传感器进行集中管理，支持在线状态监控；
d) 协议转换：支持设备私有协议和平台标准协议之间的转换；
e) 边缘计算：具备在边缘端对数据进行加工处理的能力；
f) 本地存储：当边缘端离线的情况下，能将数据保存到本地；
g) 设备控制：使用控制命令与设备交互，实现对设备的远程控制；
h) 时间同步：为设备提供时间同步服务，保证设备与平台之间的时间一致性。

4.2.1.4 网络传输层

网络传输层是边缘接入层与平台应用层之间通讯路由的抽象集合，实现基础支撑层与平台功能层之间连接，包括传输方式和传输协议两部分。

a) 传输方式包括有线和无线两种方式：

——有线网络接入方式包括：以太网、RS485、RS232 和 USB 连接等；

——无线网络接入方式包括：5G、NB-IoT、WIFI、LoRa、ZigBee、1.8GHz 频段行业专网和蓝牙连接等，应根据机场具体情况，选用相应的无线网络接入方式。

b) 传输协议包括：HTTP/HTTPS、MQTT、SIP、CoAP 等。

4.2.2 平台功能层

4.2.2.1 概述

平台功能层为核心功能模块的集合，包括连接管理层、数据管理层和核心功能层三个子层级，以及贯穿各层级全过程的运维管理功能模块。

4.2.2.2 连接管理层

连接管理层是管理接入物联网平台的各种设备和通道的功能集合，对连接到物联网平台的设备和网络的连接类型、连接状态等进行管理，保证终端、平台网络通道的稳定。

连接管理层宜包括设备认证、吞吐量监控两项功能，可具有流量熔断功能：

a) 设备认证功能对接入物联网平台的设备提供安全认证，宜支持的安全认证方式包括：令牌（Token）认证、用户名密码认证、私有证书认证等，支持的设备认证方式宜根据设备类型、安全等级等进行不同配置，并能够根据认证技术的发展进行相应升级。

b) 吞吐量监控功能指对接入物联网平台设备的数据吞吐量进行监控，监控的内容可包括但不限于：

——设备连接状态监控；

——设备单位时间消息数量监控；

——设备单位时间报文大小监控。

c) 对于单设备的吞吐量监控结果和全部接入设备的吞吐量统计情况能够输出给核心功能层进行处理。

d) 流量熔断是使设备在单位时间消息发送数量大于某个阈值时，主动断开该设备连接的功能，宜支持在一段时间内禁止设备连接，并生成流量超限告警。

4.2.2.3 数据管理层

数据管理层是数据库、文件系统等数据存储实体的软硬件集合，宜支持数据存储、数据分析和数据接口等功能，实现对物联网数据的统一管理。

a) 数据存储宜根据不同数据类型和实际需求提供不同的存储方式。针对物联网中主要为结构化数据和按时间排序的数据，宜分别提供关系型数据库和键值型数据库。

——关系型数据库：宜支持扩容，可用于存储各类复杂的业务关联数据、配置数据、周期性统计数据等；

b) ——键值型数据库：宜支持分布式扩容，可用于处理设备上传的带时间标签的采集数据，支持大量设备高并发高频次访问和读写数据，保证系统实时访问性能。数据分析宜具备常规数据查

询检索与统计分析能力，可支持长时间大规模离线数据的挖掘分析能力和流式数据分析能力。

c) 数据接口功能指提供可访问的数据接口，并提供统一的数据对接协议。

4.2.2.4 核心功能层

核心功能层是实现平台各种基础能力的实体集合。平台的核心功能宜包括用户管理、设备管理、规则引擎、设备联动、统计分析、审计日志和接口服务等功能模块，可集成应用开发引擎、固件管理、设备影子、审计日志、接口服务。核心功能层宜采用容器技术（注：一种内核轻量级的操作系统层虚拟化技术），保障应用服务的稳定和安全。

a) 用户管理：宜支持对访问系统的用户账号及权限的维护；宜支持用户组的设置，不同用户组的用户可设置具备不同的权限。

b) 设备管理：包含设备的基础管理及查看设备信息功能，可包括但不限于：

——基础管理包括添加设备、分配设备、删除设备和管理凭证等，添加的方式宜支持单个添加和批量添加；

——支持用户查看和控制授权范围内的设备相关信息，宜包括设备属性、数据、警告、事件、关联和日志等；

——设备版本的批量升级；

——定位和查看工作状态异常的设备。

c) 应用开发引擎：支持用户对物联网应用的个性化开发，具体功能宜包括但不限于：

——根据设备类型和所属区域定制各类可视化界面，并将其分配给具体用户；

——可视化界面可包括信息查询类、设备控制类、地图定位类、告警提醒类等应用界面；

——允许指定的用户或者全部用户访问和控制应用。

d) 规则链库：具体功能宜包括但不限于：

——对设备的内部逻辑（包括实时数据处理、日志处理、告警处理）等数据流的可视化规则进行编排；

——通过规则链处理实时数据、告警数据、属性数据、日志管理等；

——通过规则链定义告警产生、清除以及告警日志记录的规则。

e) 固件管理：宜支持对设备固件包的管理。

f) 统计分析：具体功能宜包括但不限于：

——对设备信息进行图形化展示；

——设备使用概览、设备区域分布、关键指标趋势分析、时间周期性故障告警分布以及数据服务等各类统计分析功能。

g) 设备联动：具体功能宜包括但不限于：

——基于规则预置的多设备协同工作；

——根据设备上传的消息，通过用户设置的规则，自动产生并下发到其它设备的消息。

h) 设备影子：具体功能宜包括但不限于：

——支持对设备状态、属性、指令的缓存，保证连接中断期间平台对设备的修改在连接恢复后能同步到设备。

i) 审计日志：具体功能宜包括但不限于：

——支持对平台各类操作的记录，包括用户登录注销、对业务数据的增删改查、设备运行警告等；

——支持按时间范围及关键字查询日志。

j) 接口服务：提供一系列标准 API 接口，包括但不限于设备接入、数据分析、边缘计算、开发服务、规则引擎等。

4.2.2.5 运维管理

运维管理是对平台业务及系统运行过程的维护和保障，宜支持基础组件自动化运维、设备运维告警、日志管理等功能。

a) 基础组件自动化运维：宜支持在基础组件出现异常失效时自动重启。

b) 设备运维告警：宜支持对设备运行状态的实时告警。

c) 日志管理：宜支持对系统运行日志的监控。

4.2.3 平台应用层

平台应用层是指由物联网平台基于应用开发引擎和规则引擎提供数据和功能支撑的应用的集合。平台应用层包括物联网应用和业务应用两部分。通过平台提供的标准接口服务或按照物联网互联互通技术标准，实现应用的定制开发或与物联网平台的对接。

4.3 平台接口关系

外部系统、设备/网关、外部应用和平台应用等在与物联网平台进行对接时，可按照物联网相关接口技术说明进行。物联网平台接口关系如图 2 所示。

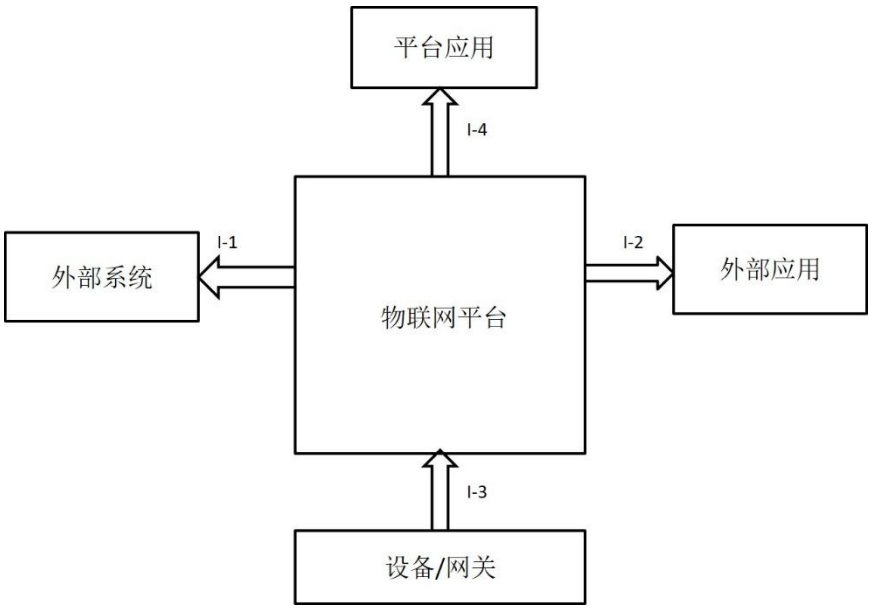

图 2 物联网平台接口关系

I-1：平台互联互通接口。实现物联网平台与外部系统之间的数据交换，接口具体描述见第 5 章节：平台互联互通接口。

I-2：开放调用接口。物联网平台将自身能力、数据封装为接口方法供外部应用调用，以实现不同业务的不同需求。接口具体描述见第 6 章节：开放调用接口。

I-3：设备接入接口。物联网平台针对接入设备软硬件能力不同、所处网络环境不同等情况，提供不同方式实现设备接入。接口具体描述见第 7 章节：设备接入接口。

I-4：平台应用接口。物联网平台用户可通过物联网平台自身的应用组件，定制发布各类物联网应用。接口具体描述见第 8 章节：平台应用接口。

4.4 接入数据说明

物联网平台与较多第三方系统进行数据对接，在保障第三方系统对接数据的规范化的同时，需保证当下的业务的灵活性不受影响，因此第三方系统接入数据的格式宜符合如下格式：

a) 数据有效负载可使用 JSON 格式字符串，字符集编码可使用 UTF-8；

b) 字段名称可使用驼峰命名法。

数据的具体字段定义及格式参见附录 A。

4.5 安全管理说明

平台的安全包含系统运行物理环境的安全性、服务器/云平台及网络的安全性、操作系统的安全性、应用系统的安全性及应用数据的安全性、网关和感知设备的安全性等。设计时宜根据《GB/T 22240 信息安全技术 网络安全等级保护定级指南》确定系统的安全保护等级，之后根据相应等级按照《GB/T 25058 信息安全技术 网络安全等级保护实施指南》进行实施。实施完成后，系统需通过相应安全等级保护测试要求。

4.6 设备标识规范

设备标识规范包括物联网平台中设备编码、IP 地址的分配规则和使用的规范；对于物联网应用中所使用的标识格式及映射的规范；为物联网平台上标识相关应用部署提供统一的标识分配和管理的规范。

4.6.1 设备编码

4.6.1.1 编码原则

针对物联网平台的大规模的设备接入，参考以下标准，制定物联网平台接入设备的编码原则：

a) 宜符合物联网中实体标识和机场行业中编码规范标识设备的要求，如唯一性、系统性和规范性；

b) 编码宜反映设备分类信息，如设备类属和类别等；

c) 信息结构应简单、稳定，能唯一标识设备，保障编码的简单、经济、可靠，同时具备可扩展性

等。

4.6.1.2 分类编码

可将机场设备分类编码分为物品分类编码、物品标识编码和物品属性编码三类：

a) 物品分类编码：物品分类编码就是物品分类的代码化表现方式。分类编码宜采用产品总分类；
b) 物品标识编码：物品标识编码是物品的唯一身份 ID 代码。主要是为了避免自然语言的二义性；
c) 物品属性编码：物品属性编码是对物品属性的唯一的、通用的代码化表示。从应用的角度看，物品属性编码宜包括物品固有属性编码、物品贸易属性编码和物品流通属性编码等。

4.6.1.3 编码方法

根据机场对设备管理的要求，结合对机场现有设备类型和设备数量估算，设计合理的编码长度和编码采用的字符集。

4.6.2 设备 IP 地址

机场物联网网络规划过程宜包含连接不同网段的各种主要网络设备的信息，并用相应的网络地址标注各网段。设备 IP 地址的取值宜支持 IPv4，可支持 IPv6 的取值规则。在设备 IP 地址分配设计上，需充分估算所需的 IP 地址数量，做好 IP 地址的合理规划和分配，保障每一个设备的 IP 地址的唯一性。

5 平台互联互通接口

5.1 数据推送方式

物联网平台宜支持将数据提供给外部系统，宜支持的方式有消息中间件、REST API、电子邮件等。其中常用的消息中间件有 Kafka、MQTT、RabbitMQ 等。使用以上方式将数据推送给外部系统，外部系统使用相应的服务接收数据。

平台与外部系统数据推送方式如图 3 所示。

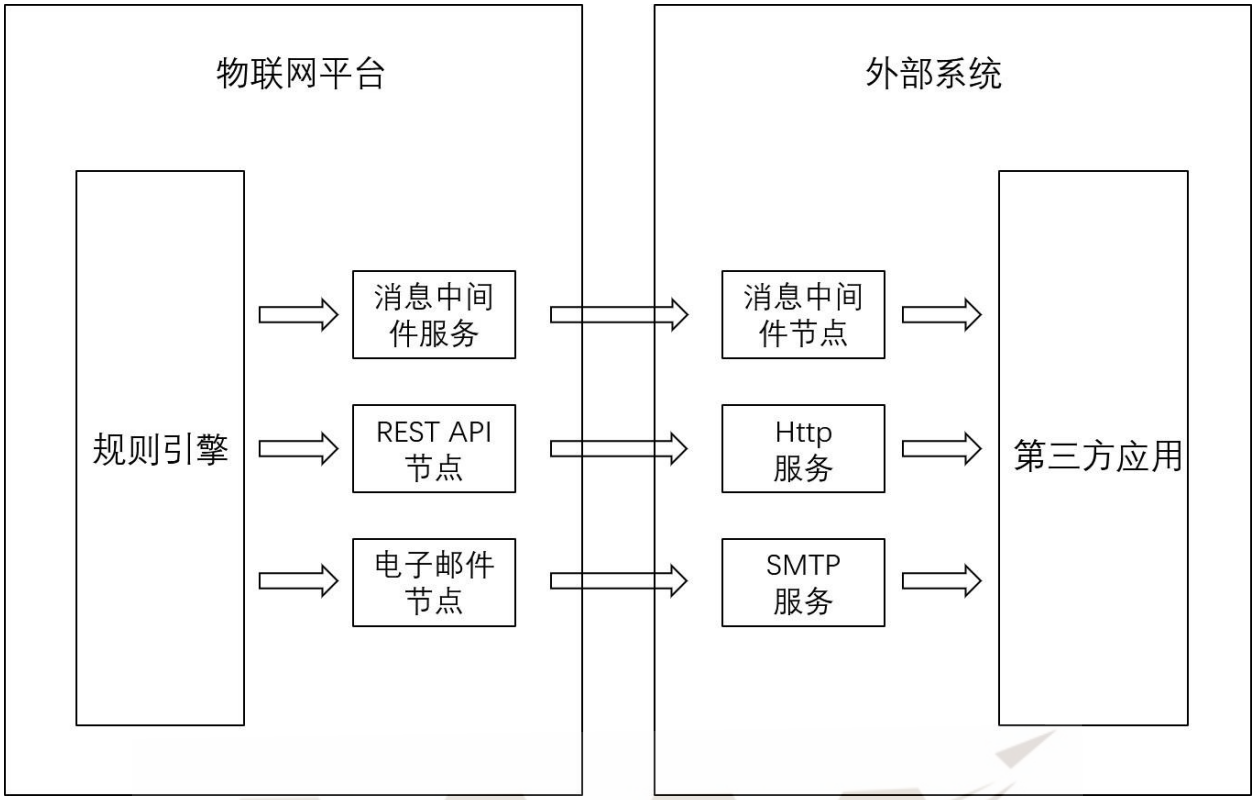

图 3 对外数据推送方式

5.1.1 消息中间件方式

物联网平台通过消息中间件的方式提供数据给外部系统时，宜由物联网平台定义好中间件相关参数，外部系统参照指定参数对接。

如采取 Kafka 方式，宜由物联网平台提供 Kafka 服务，并定义相应的主题，之后物联网平台作为生产者发布数据，外部系统作为消费者消费数据。接口宜具备以下功能：

a) 主题：主题由物联网平台定义，不同业务或设备类型宜加以区分；

b) 接入安全认证：Kafka 服务宜提供接入安全认证，可支持用户名密码或安全证书方式；

c) 数据缓存：数据能在 Kafka 服务中缓存，缓存策略宜支持根据最大大小或最长保留时间进行设置；

d) 流量限制：宜根据业务需要和硬件性能控制数据发送频率，保证流量不超出系统负载上限。

如采取 MQTT 方式，需要定义主题、身份认证信息等。物联网平台作为生产者，外部系统作为消费者，通过 MQTT 服务实现数据推送。MQTT 服务可由物联网平台或外部系统提供。

如采用 RabbitMQ 方式，需要定义交换器、路由键、身份认证信息等，物联网平台作为生产者，外部系统作为消费者，通过 RabbitMQ 服务实现数据推送。RabbitMQ 服务由物联网平台或外部系统提供。

5.1.2 REST API 方式

如采用 REST API 方式，需要定义调用地址和方法，外部系统作为服务端提供服务供物联网平台调

用。

5.1.3 发送电子邮件方式

如采用发送电子邮件方式，需要定义邮件服务器地址、认证信息等，外部系统作为邮件服务器接收邮件。

5.2 推送数据说明

物联网平台宜支持通过规则引擎对数据进行处理加工的能力。在规则引擎中可使用不同功能的规则节点组成规则链来实现复杂的处理流程。物联网平台可把规则链中流转的数据分为消息类型（msgType）、元数据（metadata）和消息负载（msg）三部分，这三部分合称数据体。数据体是规则链中进行流转的数据的基本单位。

在规则链中流转的数据体的类型称为消息类型。消息类型用字符串表示，可根据消息来源、用途等定义不同类型。

在消息流转的过程中，可根据消息的上下文对消息进行过滤和处理，规则节点在处理消息的过程中可附加一些上下文信息。这些上下文信息可保存在元数据（metadata）中。

元数据中保存的内容格式使用 JSON 字符串格式。不同功能的规则节点可在流出的元数据中附加不同的内容。

数据的实际内容可保存在消息负载中，使用的格式为 JSON 字符串格式。消息负载的内容根据消息来源的不同主要分为两类：一类是来自于接入物联网平台的设备上传的消息；另一类来自于规则节点产生的消息。

6 开放调用接口

6.1 概述

开放调用接口是提供给外部应用调用物联网平台提供的能力和数据的接口(如用户注册、设备添加、设备控制等)，外部应用可以使用该接口实现定制化应用开发。

6.2 平台能力开放接口

物联网平台宜提供友好的浏览页面，利用 HTTP/HTTPS 协议交互物联网平台与外部应用之间的操作指令、数据信息。外部应用的各种操作都宜支持通过调用 Web 界面实现，数据格式宜用字符串的形式传到服务器。

6.3 调用接口说明

平台对外提供的能力开放接口可通过 HTTP/HTTPS 等接口方式供外部应用开发调用。为了保证 API 调用的安全性等因素，外部系统需要通过相应的安全认证。

7 设备接入接口

7.1 接入方式

物联网平台针对待接入设备软硬件能力不同、所处网络环境不同等情况，可提供直接接入平台或通过网关接入平台两种接入方式。

7.2 设备接入认证方式

设备凭证用于设备在接入物联网平台时的身份标识和安全验证。物联网平台基于设备资源能力和网络情况的不同可提供以下两种设备凭证：

7.2.1 设备访问令牌

适用于设备资源和网络开销受限情况下设备的通用凭据。该方式基于访问令牌的身份验证在未加密或单向 SSL 模式下使用。

物联网平台使用随机生成的不短于 20 个字符长度的字符串作为默认访问令牌。该令牌提供给设备以便设备在接入物联网平台时作为身份认证信息。

7.2.2 设备安全证书

适用于加密网络连接、高安全性要求接入认证方式。该方式宜符合 TLS 和 PKI 标准。基于安全证书的身份验证可用于双向 SSL 模式。

物联网平台对于硬件资源较充足的设备可提供遵守 X.509 标准的安全证书并生成密钥文件供设备接入时进行安全认证。

7.3 设备接入性能

物联网平台宜根据预计接入规模，对设备数据流量进行估算，从而分配资源。典型民用机场设备的数据更新频率根据设备类型不同，可以从每秒 1 条到每小时 1 条，因此在计算时可参考附录 A 提供的经验值：

表 1 物联网平台流量阈值参考表

接入设备数	10 万	100 万	1000 万
单个设备每秒平均消息数	0.1	0.1	0.1
单个设备每分钟平均消息数	6	6	6
平台总体每秒平均消息数	1 万	10 万	100 万
平台总体每分钟平均消息数	60 万	600 万	6000 万

7.4 网关接入

直接接入物联网平台的网关，宜具备以下功能：

a) 支持物联网平台指定的连接方式；

b) 支持自定义的协议转换，能将消息格式映射为物联网平台可解析的格式；

c) 支持物联网平台提供的安全认证方式。

8 平台应用接口

8.1 概述

平台应用接口是平台用户用于定制发布个性应用的应用组件，该组件由物联网平台自身提供，平台应用接口见 I-4（平台应用技术接口说明）。

8.2 平台应用特征

物联网平台应用宜具备以下功能：

a) 支持通过控件接入符合条件的各类设备数据，并可定制各类可视化界面；

b) 支持应用的权限管理，设置应用的访问范围；

c) 支持应用导出/导入；

d) 可提供预设应用以方便用户使用：如设备管理、告警查看、电子地图等。

8.3 应用控件说明

平台应用可通过使用控件为平台用户提供可视化的多种展示方式。宜支持控件的增加、编辑、删除、查询等操作。

物联网平台宜提供包括且不限于以下控件：

a) 报警控件：对于实时和历史模式下特定设备的警报可视化；

b) 列表或卡片：以列表方式显示数据；

c) 图表：以时间轴的窗口可视化历史或实时数据；

d) 控制控件：显示控制类按钮的状态以及发送控制指令；

e) 数字仪表盘：用于可视化温度，湿度，速度和其他整数或浮点值；

f) 模拟仪表盘：与数字仪表相似，但样式不同；

g) 实体管理界面：按实体类型或者实体名称对设备进行管理；

h) 地图控件：可视化设备地理位置以及跟踪实时和历史的设备（人、物）路线；

i) 输入控件： 可对实体属性信息进行维护。

9 安全防护技术

9.1 概述

物联网平台安全防护技术是指包括物理环境、数据承载、业务部署支撑、网关和感知终端等方面的安全技术。

9.2 物理环境安全

物联网平台的物理环境安全宜符合国家标准 GB 50174 与 GB 50462 的规定，并参考 GB/T 22239-2019 中的相应级别物理安全要求。

9.3 数据传输安全

数据传输安全宜实现以下功能：

a) 宜通过采用 VPN（虚拟专用网络）、数据传输加密等技术，实现从物联网平台承载业务系统数据传输通道的安全；

b) 宜采用 SSH 、SSL 等方式为物联网平台内部的维护管理提供数据加密通道，保障管理信息安全；

c) 宜采用加密或其他有效措施实现虚拟机镜像文件、系统管理数据、鉴别信息和重要业务数据传输保密性；

d) 宜采用校验技术或密码技术保证重要数据在传输过程中的完整性，在检测到完整性错误时可采取一定的恢复措施；

e) 宜能够支持国家密码管理机构要求的通信加解密算法和签名验签。

9.4 业务部署支撑安全

9.4.1 通用应用服务软件

通用应用服务软件宜实现以下功能：

a) 提供自主访问控制功能，依据安全策略控制用户对文件、数据库表等的访问；

b) 提供安全通道保障供业务系统选择使用；

c) 能够对一个业务应用占用的资源分配最大限额；

d) 将物联网平台所部署应用的认证、账号、授权组件化；

e) 对物联网平台所部署应用系统进行审计；

f) 支持双向认证；

g) 业务系统试运行前宜经过安全检查与安全扫描，通过后再接入物联网平台；

h) 业务运营期间应定期对业务系统承载的物联网平台资源进行检查和审核；

i) 业务系统运行中不宜存在业务功能以外的数据调用。

9.4.2 应用开发环境

应用开发环境宜实现以下功能：

a) 业务应用系统的开发环境资源访问宜受控；

b) 业务应用系统的开发环境宜在经过认证授权后才可接入物联网平台进行测试；

c) 业务系统的物联网平台开发接口宜经过安全测试；

d) 业务系统的接口宜开放，能够进行代码审查；

e) 宜支持业务系统组件式开发，各个组件均能进行独立的安全检测；

f) 宜提供业务系统的安全威胁扫描。

9.4.3 数据库安全环境

数据库安全环境宜实现以下功能：

a) 数据库宜建立严格用户认证机制；

b) 数据库宜限制用户只能进行经过授权的操作；

c) 提供数据库加解密引擎池，并可配置数据项、数据隔离等的数据加密要求，支持基于用户角色的关键业务数据的加密存储服务；

d) 物联网平台所承载数据的数据库系统宜支持行、列级的细颗粒度加解密，并对高碰撞性字段进行加解密，支持主流数据库的加解密；

e) 数据库加解密宜对应用系统提供完善、灵活的集成接口，并对数据持久层提供良好的支持；

f) 使用虚拟化技术构建高性能的数据库加解密组件，避免大数据量的数据库加解密而影响数据库性能；

g) 支持单实例多用户的数据加密、隔离要求。

9.5 网关和感知终端安全

9.5.1 网关安全管理

物联网网关宜实现基本的安全管理功能，包括用户身份鉴别、数据加密传输等功能。

a) 用户身份识别宜支持账号密码方式，宜支持安全证书、加密锁等其他方式；

b) 物联网网关宜支持对其所传送的数据进行加密处理；

c) 物联网网关受到攻击（如漏洞扫描或拒绝服务攻击）时，宜具有能够自动记录攻击的发起地址、攻击时间以及攻击类型等关键信息，生成实时报警信息，宜具有一定的阻断能力。

9.5.2 感知终端安全管理

9.5.2.1 范围

感知终端的安全管理包括物理安全、接入安全、通信安全、设备安全和数据安全等。

9.5.2.2 物理安全

a) 产品选型宜有质量认证证书并通过相应产品类别的标准要求；

b) 宜能满足安装环境的防护要求；

c) 供电宜稳定可靠；

d) 宜具有防破坏、盗窃措施。

9.5.2.3 接入安全

a) 宜具有唯一身份标识，支持身份鉴别如：基于网络身份标识的鉴别、基于 MAC 地址的鉴别、

基于通信协议的鉴别等；

b) 宜具有访问控制功能，如禁用端口、支持设置网络访问策略等。

9.5.2.4 通信安全

a) 使用无线方式通信的感知终端宜满足机场和国家电磁环境相关规定；

b) 宜具有数据完整性校验和通信延迟及中断的处理机制。

9.5.2.5 设备安全

a) 有操作系统的感知终端宜支持用户登录管理、能控制远程或本地访问。宜具有记录运行情况和相应操作的功能；

b) 宜能够自检出已定义的故障并告警，宜具有一定的故障自动处理能力。

9.5.2.6 数据安全

a) 宜保证数据的实时性和有效性。

附 录 A 接入数据字段

（资料性）

名称	字段	是否必需	说明	例子
时间戳	ts	否	毫秒形式的 Unix 时间戳，如果上传时没有该字段，物联网平台会以接收时间作为时间戳赋给该消息。	"ts": "1590475693000"
设备编号	deviceId	是	设备唯一标识，在设备接入时由物联网平台分配给设备。	"deviceId": "2945097634435667"
数据内容	values	是	以键值对方式存储有效数据的字典集。	"values": {"standId": "101","standStatus": 0}

接入字段示例

```
[
  {
    "ts": 1590475693000,
    "deviceId": "12345678",
    "values": {
      "longitude": 114.984208,
      "isConnect": true,
      "name": "device1"
    }
  }
]
```