ICS
点击此处添加中国标准文献分类号

团　　体　　标　　准

T/××× ××××—××××

综合能源物联系统通用技术规范

General technical specification for integrated energy IOT system

（征求意见稿）

202X—XX—XX 发布　　202X—XX—XX 实施

中国能源研究会　发　布

目　　次

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》给出的规则编制。

本文件由中国能源研究会提出并解释。

本文件由 XXXX 归口。

本文件起草单位：

本文件主要起草人：

本文件首次发布。

本文件在执行过程中的意见或建议反馈至中国能源研究会标准化委员会。

综合能源物联系统通用技术规范

1　范围

本标准规定了综合能源物联系统的基本原则、系统架构、系统功能要求、系统接口要求、系统性能要求、安全防护要求和验收。

本标准适用于综合能源物联系统的设计、使用和验收。

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 信息系统安全等级保护基本要求

GB 17859 计算机信息系统安全保护等级划分准则

DL/T 645 多功能电能表通信协议测试方法

3　术语和定义

下列术语和定义适用于本文件。

3.1

产品　products

设备的抽象，通常指一组具有相同功能的设备。

3.2

设备　device

归属于某个产品下的具体设备。设备可以直接连接物联网平台，也可以作为子设备通过网关连接物联网平台。

3.3

网关　gateway

能够直接连接物联网平台的设备，且具有子设备管理功能，能够代理子设备连接云端。

3.4

实时监控　real-time monitoring

对产品下的设备以及网关、子设备的实时数据的监控。

3.5

设备监控　device monitoring

对产品下的设备的实时数据的监控。

3.6

规则链 rule chain

规则节点及其关系的逻辑组。

3.7

规则节点 rule node

规则链的基本单元，包含一组规则操作。

3.8

规则操作 rule action

规则节点的基本组成部分，用于实现具体的数据处理、转换、过滤和响应功能。

3.9

规则触发 rule trigger

定义了规则链执行的条件和触发方式。

3.10

规则变量 rule variable

规则链的上下文信息，用于保存规则链执行过程中的状态和数据。

3.11

远程升级 OTA

通过互联网对物联网设备进行固件升级、配置更改和故障排除等操作的方式。

3.12

权限控制 RBAC

是一种访问控制机制，它将权限分配给角色，而不是将权限直接分配给用户。在这种机制下，用户被分配到角色上，而角色被授予相应的权限。这种权限分配可以基于用户的工作职能、职位或其他属性。

3.13

接口 API

是一种编程接口，允许应用程序之间交换信息。

3.14

标准化接口 REST

是一种软件架构风格、设计风格，而不是标准，只是提供了一组设计原则和约束条件。它主要用于客户端和服务器交互类的软件。基于这个风格设计的软件可以更简洁。

3.15

发布/订阅模式的通信协议 MQTT

是一种轻量级的、基于发布/订阅模式的通信协议，常用于物联网（IoT）应用程序中。MQTT 的设计目标是在受限的网络环境中实现可靠的、低带宽消耗的消息传递。

3.16

远程过程调用协议 RPC

是一种远程过程调用协议，用于在网络上进行分布式计算。它允许应用程序通过网络调用远程的函数或方法，就像调用本地函数一样。RPC 的目的是使分布式系统的通信变得更加透明和易于使用。

3.17

约束应用协议 CoAP

是一种专为受限设备设计的应用层协议，适合在受限的网络环境中使用，例如低带宽、低功耗的无线传感器网络。

3.18

浏览器双向通信协议 Websocket

它实现了浏览器与服务器全双工通信，能更好的节省服务器资源和带宽并达到实时通讯，它建立在 TCP 之上，同 HTTP 一样通过 TCP 来传输数据。

3.19

基于浏览器的自定义回调函数 Webhook

是一种 Web 编程的概念，用于在特定事件发生时自动触发一些自定义操作。它是一种反向 API，即由第三方应用程序或服务向指定 URL 发送 HTTP 请求，而不是由人手动发送请求。

4 基本原则

4.1 综合能源物联系统的设计、建设应融合智能化、去中心化、综合化等能源新业态的实际需求，完善综合能源物联系统数据介入与安全防护的规范，为综合能源服务发展提供基础支撑。

4.2 应遵循标准化原则，满足安全性、可靠性、互联性及可扩展性的要求，实现各项功能的模块化设计。

5 系统架构

物联网综合管控平台提供了可靠的设备接入、设备管理、规则链引擎、远程控制、OTA 升级、安全保障、数据分析与可视化、告警管理、RBAC 权限、平台集成及 API 等功能，使 物联网应用程序的开发和管理变得更加简单和高效且易于扩展，同时支持多协议多维度的数据接入方式，系统架构见图 1。

图 1 系统架构

6 系统功能要求

6.1 设备接入

6.1.1 设备接入模块主要定义设备连接协议和数据交互方式，包括设备接入认证、设备接入管理、设备指令下发等功能,设备接入模块应当支持多种设备接入协议，包括消息队列遥测传输协议（Message Queuing Telemetry Transport,MQTT）、受限制的应用协议（Constrained Application Protocol,CoAP）、超文本传输协议（Hypertext Transfer Protocol,HTTP）、远程过程调用（Remote Procedure Call,RPC）等，用于连接不同类型的设备。

6.1.2 设备接入认证

6.1.2.1 宜支持设备接入认证机制，确保只有经过认证的设备才能连接到平台。

6.1.2.2 宜采用基于令牌的认证机制，设备需要在连接到平台之前获取认证令牌，然后将认证令牌作为设备身份标识符发送给平台。

6.1.3 设备接入管理

宜支持管理员在平台上注册和管理设备接入，包括设备认证、设备绑定、设备授权等，以确保设备接入的安全性和可控性。

6.1.4 设备接入数据格式

宜支持多种数据格式，包括 JSON、Protobuf 等。

6.1.5 设备接入数据上传

6.1.5.1 宜支持设备向平台上传数据，包括设备状态、传感器数据等。

6.1.5.2 宜支持设备数据上传的批量处理，以提高数据上传的效率。

6.1.6 设备指令下发

6.1.6.1 宜支持向连接到平台的设备下发指令，以控制设备的行为。

6.1.6.2 宜支持通过 MQTT 的发布订阅机制进行设备指令下发。

6.2 设备管理

6.2.1 设备管理模块主要定义设备的注册、管理、配置、升级等功能，包括设备注册、绑定、属性管理、元数据管理、分组管理、监控和日志管理等，以帮助管理员对连接到平台的设备进行高效管理和监控，实现设备的智能化管理和运维。

6.2.2 设备注册

宜支持管理员在平台上注册新设备，为设备创建唯一的标识符，并设置设备属性和元数据。

6.2.3 设备绑定

6.2.3.1 宜支持将设备绑定到特定的组织、租户、设备组等实体上，以实现设备的分类和管理。

6.2.3.2 宜支持将设备授权给不同的用户和角色，以实现设备访问控制。

6.2.4 设备属性管理

6.2.4.1 宜支持对设备的属性进行管理，包括添加、删除、更新等操作。

6.2.4.2 设备属性可以用于描述设备的特征、状态、位置等信息，以便后续的设备监控和数据分析。

6.2.5 设备元数据管理

6.2.5.1 宜支持对设备的元数据进行管理，包括添加、删除、更新等操作。

6.2.5.2 设备元数据用于描述设备的详细信息，如设备类型、生产日期、厂商信息等，以帮助设备管理和监控。

6.2.6 设备分组管理

6.2.6.1 宜支持设备分组，以实现设备的分类和管理。

6.2.6.2 设备分组可以根据不同的属性、位置、状态等进行划分，方便后续的设备监控和数据分析。

6.2.7 设备监控

6.2.7.1 宜提供设备监控功能，支持实时查看设备的状态、属性、数据等信息，以及设备的连接状态、在线时间等。

6.2.7.2 设备监控可以帮助管理员及时发现设备故障、异常等问题。

6.2.8 设备日志管理

宜提供设备日志管理功能，可以记录设备的运行日志、错误日志等信息，方便后续的故障排除和问题分析。

6.3 规则链引擎

6.3.1 规则链引擎模块主要定义数据处理流程和规则运算方式，包括规则节点、规则操作、规则触发、规则部署等功能，以实现设备数据的实时处理、分析和响应。规则链引擎由多个规则节点组成，每个规则节点包含一组规则操作，用于处理、转换、过滤和响应设备数据。规则链可以根据用户需要自定义构建，支持串联、并联等多种组合方式，以实现复杂的数据处理和分析场景。

6.3.2 规则节点

宜提供多种类型的规则节点，包括数据转换节点、过滤节点、计算节点、通知节点、Webhook 节点等。

6.3.3 规则操作

宜提供丰富的规则操作，包括数学计算、字符串处理、时间转换、数据转换、数据聚合、邮件通知、短信通知、推送通知等。

6.3.4 规则触发

宜支持多种类型的规则触发，包括数据到达触发、定时触发、手动触发、Webhook 触发等，支持根据用户需要自定义触发条件和触发方式。

6.3.5 规则变量

宜提供丰富的规则变量，包括设备属性、设备元数据、设备数据、系统变量等，支持根据用户需要自定义规则变量。

6.3.6 规则链部署

宜提供灵活的规则链部署方式，支持将规则链部署到指定的设备、设备组、租户等实体上，以实现不同层级的数据处理和分析。

6.4 远程控制

6.4.1 远程控制模块主要定义远程设备控制的方法和接口，包括设备远程操作、参数配置、设备状态查询等。远程控制模块应当实现服务器对设备的精准控制，支持设备主动向服务器发送请求通知。

6.4.2 宜支持两种类型的远程控制调用：设备发起的远程控制调用和服务端发起的远程控制调用。

6.4.3 宜开放应用程序编程接口（Application Programming Interface,API），包括 MQTT RPC API、CoAP RPC API、HTTP RPC API，支持从设备上运行的应用程序发送和接收远程控制命令。

6.5 OTA 升级

6.5.1 OTA 升级模块主要定义设备的固件升级方法和流程。

6.5.2 准备升级

6.5.2.1 宜支持创建升级包和升级任务。

6.5.2.2 OTA 升级包包含新固件或软件的文件。

6.5.2.3 OTA 升级任务定义升级的设备、升级包和升级方式等信息。

6.5.3 设备连接和验证

6.5.3.1 宜支持设备连接到系统，并验证升级任务的完整性和可用性。

6.5.3.2 宜支持使用 JWT（JSON Web Token）令牌进行身份验证和授权。

6.5.4 升级包下载和安装

6.5.4.1 宜支持设备下载升级包，安装并重启设备。

6.5.4.2 宜支持设备通过系统提供的 REST API 或 MQTT API 实现 OTA 升级。

6.5.5 升级日志和状态

宜提供 OTA 升级任务的状态和日志记录功能，以便管理员和用户了解升级过程和结果。

6.5.6 升级错误处理和回滚

宜提供升级错误处理和回滚功能，以确保设备的稳定性和可靠性。

6.5.7 升级规则引擎

宜提供 OTA 升级规则引擎，可以根据设定的规则自动触发 OTA 升级任务。

6.6 安全保障

6.6.1 安全保障模块主要定义系统的安全策略和安全控制方法，包括用户认证、访问控制、数据加密、攻击防范等功能。

6.6.2 访问控制

6.6.2.1 宜支持访问令牌（Access Tokens）鉴权模式。

6.6.2.2 宜支持基于角色的访问控制（Role-based Access Control,RBAC），允许管理员为不同的用户和组设置不同的权限和角色，以实现对设备、数据和功能的访问控制。

6.6.3 数据加密

6.6.3.1 系统宜使用安全套接字层（Secure Sockets Layer,SSL）/传输层安全（Transport Layer Security,TLS）协议对数据进行加密传输，以保护数据在传输过程中的安全性。

6.6.3.2 系统宜支持设备端到云端的 MQTT SSL、HTTP SSL、CoAP 数据包传输层安全性协议（Datagram Transport Layer Security,DTLS）等协议，保证设备与云端之间的数据传输的安全性。

6.6.4 数据备份和恢复

6.6.4.1 系统宜支持数据备份和恢复功能，确保在系统故障或数据丢失时能够及时恢复数据。

6.6.4.2 系统宜支持配置定期备份，或手动备份数据，以保障数据的安全性和完整性。

6.6.5 日志审计

宜支持系统操作日志和设备事件日志的记录和审计功能，以便管理员跟踪和分析系统和设备的操作情况，及时发现异常情况。

6.6.6 安全认证

宜支持开放授权 2.0 协议（Open standard for Authorization 2.0,OAuth2.0）、轻量目录访问协议（Lightweight Directory Access Protocol,LDAP）等多种认证方式，允许用户使用自己的账户和密码登录，以保障系统的安全性。

6.7 数据分析与可视化

6.7.1 数据分析与可视化模块主要定义数据的分析和展示方式，包括数据可视化、数据查询、数据分析、时序数据分析、实时数据监控、数据导出和数据可视化定制等功能，帮助用户对设备数据进行分析和展示。

6.7.2 数据可视化

宜提供多种数据可视化方式，包括折线图、柱状图、饼图、仪表盘等，直观展示设备数据的趋势和状态。

6.7.3 数据查询

宜提供数据查询功能，根据用户的需求查询设备数据，并以图表或表格等形式展示查询结果。

6.7.4 数据分析

宜提供数据分析功能，对设备数据进行分析，包括聚合、统计、过滤、排序等操作，并以图表或表格等形式展示分析结果。

6.7.5 时序数据分析

应提供时序数据分析功能，对设备数据进行时间序列分析，并以图表或表格等形式展示分析结果。

6.7.6 实时数据监控

宜提供实时数据监控功能，实时监控设备数据，并以图表或表格等形式展示监控结果。

6.7.7 数据导出

宜提供数据导出功能，将设备数据导出为 CSV、Excel 等格式，以方便用户进行后续的数据处理和分析。

6.8 告警管理

6.8.1 告警管理模块主要定义告警的生成、传递和处理方式，包括告警规则设置、告警级别管理、告警信息推送等功能。

6.8.2 告警规则设置

宜支持用户创建告警规则，设置告警条件和触发动作。

6.8.3 告警通知管理

6.8.3.1 当告警触发时，应将告警信息发送给指定的用户或组织。

6.8.3.2　宜支持用户管理告警通知的方式和接收人员，包括添加、删除、编辑告警通知等。

6.8.4　告警事件处理

6.8.4.1　当告警触发时，应支持用户查看和处理告警事件。

6.8.4.2　告警事件包括告警触发时间、设备信息、告警类型、告警等级等详细信息。

6.8.4.3　宜支持用户对告警事件进行处理和关闭。

6.8.5　告警历史记录查询

6.8.5.1　宜支持用户查询历史告警事件，包括告警触发时间、设备信息、告警类型、告警等级、告警状态等详细信息。

6.8.5.2　宜支持根据时间范围、设备、告警类型等条件进行查询。

6.9　RBAC 权限

6.9.1　RBAC 权限模块主要定义系统的权限管理方法和接口，包括用户角色管理、权限分配等功能。

6.9.2　用户和租户管理权限

宜支持管理员创建和管理用户和租户，并为它们配置不同的角色和权限，如超级管理员、管理员、普通用户等。

6.9.3　数据模型管理权限

宜支持管理员创建和管理设备类型、遥测数据、属性和事件模板等，为用户和租户提供数据模型的管理能力。

6.9.4　规则链和规则节点管理权限

宜支持管理员创建和管理规则链和规则节点，为用户和租户提供规则引擎的管理能力，实现设备数据的分析和处理。

6.9.5　消息路由管理权限

宜支持管理员配置消息路由规则，将设备上传的消息路由到指定的规则链中，为用户和租户提供设备消息的管理能力。

6.9.6　设备管理权限

宜支持管理员创建和管理设备，为用户和租户提供设备的管理能力。

6.9.7　仪表盘管理权限

宜支持管理员创建和管理仪表盘，为用户和租户提供数据可视化的管理能力。

6.10　平台集成及 API

6.10.1　平台集成及 API 模块主要定义系统与其他平台或应用程序之间的接口和协议，包括开放的 REST API 、MQTT API、CoAP API、Websocket API、Admin API。

6.10.2　REST API

6.10.2.1　宜支持多种类型的身份验证和授权方式，如 OAuth 2.0 协议。

6.10.2.2　宜支持通过 HTTP 请求进行调用，使用 JSON 格式进行数据交互。

6.10.2.3　宜支持以下操作：

6.10.2.3.1　设备管理，创建和管理设备、获取设备信息、查询设备遥测数据和属性等。

6.10.2.3.2　规则链和规则节点管理，创建和管理规则链和规则节点，编辑规则链和规则节点逻辑等。

6.10.2.3.3　RPC 调用，向设备发送命令或请求，并获取设备的响应数据。

6.10.2.3.4　历史数据查询，查询设备遥测数据和属性的历史记录。

6.10.2.3.5　事件查询，查询设备生成的事件记录。

6.10.3　MQTT API

6.10.3.1　宜支持通过 TCP 或 Web Socket 连接到系统。

6.10.3.2 身份验证和授权使用 JWT 令牌。用户需要在访问 MQTT API 前获取有效的 JWT 令牌，并将其嵌入到 MQTT 连接中。

6.10.3.3 宜支持以下操作：

6.10.3.3.1 设备注册，设备使用 MQTT 连接到系统，并进行身份验证和注册。

6.10.3.3.2 遥测数据上传，设备上传遥测数据和属性到系统。

6.10.3.3.3 RPC 调用，设备向系统发送命令或请求，并获取平台的响应数据。

6.10.3.3.4 OTA 升级，设备通过 MQTT API 下载和安装 OTA 升级包。

6.10.4 CoAP API

6.10.4.1 身份验证和授权使用 JWT 令牌。用户需要在访问 CoAP API 前获取有效的 JWT 令牌，并将其嵌入到 CoAP 连接中。

6.10.4.2 宜支持以下操作：

6.10.4.2.1 设备注册，设备使用 CoAP 连接到系统，并进行身份验证和注册。

6.10.4.2.2 遥测数据上传，设备上传遥测数据和属性到系统。

6.10.4.2.3 OTA 升级，设备通过 CoAP API 下载和安装 OTA 升级包。

6.10.5 Websocket API

6.10.5.1 身份验证和授权使用 JWT 令牌。用户需要在访问 WebSocket API 前获取有效的 JWT 令牌，并将其嵌入到 WebSocket 连接中。

6.10.5.2 宜支持以下操作：

6.10.5.2.1 遥测数据订阅和推送：设备订阅遥测数据和属性的更新，并推送遥测数据和属性到系统。

6.10.5.2.2 事件订阅和推送：设备订阅事件的更新，并推送事件到系统。

6.10.6 Admin API

6.10.6.1 使用 REST API 的方式进行调用，使用 JSON 格式进行数据交互。

6.10.6.2 身份验证和授权使用 OAuth 2.0 协议，需要获取有效的 OAuth 2.0 令牌才能访问 Admin API。

6.10.6.3 用于管理员对平台进行管理和配置。

6.10.6.4 宜支持以下操作：

6.10.6.4.1 用户和租户管理，创建和管理用户和租户，配置用户和租户的权限和角色等。

6.10.6.4.2 数据模型管理，创建和管理设备类型、遥测数据、属性和事件模板等。

6.10.6.4.3 规则链和规则节点管理，创建和管理规则链和规则节点，编辑规则链和规则节点逻辑等。

6.10.6.4.4 消息路由管理，配置消息路由规则，将设备上传的消息路由到指定的规则链中。

6.10.6.4.5 日志和监控管理，查看系统日志、性能监控和调试信息，配置日志和监控策略等。

7 系统接口要求

7.1 接口规范

7.1.1 宜采用基于 HTTP/HTTPS 协议的 REST 架构，接口内容可包括业务信息约定、时间与日期规定、数据请求测试方式、公共信息规格、响应码规则约定、数据交换安全与标准等。

7.1.2 宜采用基于 MQTT 协议，规范统一网关接入流程、通信标准及数据结构。

7.2 数据采集量类型

宜按照业务类型对数据采集量进行划分，包括配电系统、锅炉系统、空调系统、供暖系统、热水系统、储能系统、充电桩、光伏发电系统等。

7.3 通信协议

宜支持 HTTP/HTTPS、MODBUS、OPC、WEBSOCKET、MQTT、WEBSERVICE 等，宜参考 DL/T 645 协议。

8 系统性能要求

8.1 宜最大同时连接数、每秒处理的消息数、并发下指令数、系统可靠性、平台可扩展性等。

8.2 系统最大连接数

表 1 设备最大同时连接数

规格	指标
平台支持连接数	业务正常情况下，支持连接数 > 100 万，连接持续 8 小时不中断
单服务节点连接数	业务正常情况下，支持连接数 > 10 万，连接持续 8 小时不中断
CPU 平均占用率	业务高峰时 < 85%
内存平均占用率	业务高峰时 < 85%

8.3 每秒处理消息数

表 2 每秒处理消息数

规格	指标
平台每秒处理消息数	业务正常情况下，每秒处理消息数 > 20 万，每条消息 100 字节
单节点每秒处理消息数	业务正常情况下，每秒处理消息数 > 2 万，每条消息 100 字节
CPU 平均占用率	业务高峰时 < 85%
内存平均占用率	业务高峰时 < 85%

8.4 并发下达指令数

表 3 并发下达指令数

规格	指标
并发下达指令数	业务正常时间 1 分钟内，批量下发指令设备数 > 10 万
CPU 平均占用率	业务高峰时 < 85%
内存平均占用率	业务高峰时 < 85%

8.5 系统可靠性

表 4 系统可靠性

规格	指标
稳定性	(1) 在承受最大并发用户数持续运行 2 小时的情况下： 系统运行平稳，业务失败率不超过 0.1%；CPU 平均占用率低于 80%；内存占用率没有明显增长且 1 小时后内存恢复初始值。 (2) 在承受 80%的最大并发用户数持续运行 4 小时的情况下： 系统运行平稳，业务失败率不超过 0.1%;CPU 平均占用率低于 80%;内存占用率没有明显增长且 1 小时后内存恢复初始值。 (3) 网络局部中断可靠性，支持网络出现局部中段情况下，仍保持平台稳定，数据新线重传，具备断线重传。

自监控性	系统应具备自监控能力，能够对重要的进程和服务的运行状态、重要操作、故障修复等进行记录、监控和告警，能够提供这些组件的监控接口。
健壮性	系统应建立大并发或超载业务情况下保护机制，确保系统稳定运行:高并发量情况下的可靠性承载应用的 N 个节点的服务集群中，单个服务节点能承担系统设计最大并发的/(N-2)。

8.6 平台可扩展性

表 5 平台可扩展性

规格	指标
可扩展性	(1)支持云上资源调配动态弹性扩展，以满足不同数量设备的接入需求。 (2)支持基于组件或功能模块的功能、性能扩展，系统原有组件无需更改。

9 安全防护要求

9.1 系统安全防护等级划分应符合 GB 17859 的规定，并应符合 GB/T 22239 相应等级保护要求。
9.2 系统和电网侧系统交换信息时，应按中华人民共和国国家发展和改革委员会令第 14 号执行。
9.3 系统采用公共互联网传输信息时，应根据终端类型在通信协议的应用层、网络层和传输层采用相应的安全协议。
9.4 系统应采用基于角色控制方式访问用户数据,并具备禁止非授权访问和拷贝日志记录等防护措施，防止数据泄露。

10 验收

10.1 系统验收前应通过试运行。
10.2 系统应经过具备软件检测资质的第三方机构测试合格。
10.3 系统验收应包括以下工作内容：

a) 编制验收大纲；
b) 检查验收资料；
c) 进行系统测试；
d) 形成验收报告。