ICS 35.200
CCS L 65

T/ZPP

团　　体　　标　　准

T/ZPP 146—2025

物联网设备数据接口规范

Specification for data interface of internet of things devices

2025－06－27 发布　　2025－06－30 实施

浙江省品牌建设促进会　　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》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。

本文件由杭州赛普特信息科技有限公司提出。

本文件由浙江省品牌建设促进会归口。

本文件起草单位：杭州赛普特信息科技有限公司、杭州觉起科技有限公司、浙江雨林电子科技有限公司、浙江永康五金生产力促进中心有限公司、永康市新时代实业有限公司、杭州协能科技股份有限公司、中科润禾(杭州)信息技术有限公司、杭州智海合达科技有限公司、杭州创新易软件有限公司、杭州半云科技有限公司、浙江净禾智慧科技有限公司、杭州易泰达科技有限公司、浙江六久科技有限公司、杭州宇泛智能科技股份有限公司、品茗科技股份有限公司、杭州文拓智能科技有限公司、湖州深蓝计算机科技发展有限公司、杭州迈的智能科技有限公司、杭州美帮网络科技有限公司、杭州聚达物联科技有限公司、宁波中铖信息科技有限公司、宁波市科技园区明天医网科技有限公司、浙江希杰金属科技有限公司、浙江群安安全生产技术咨询有限公司、浙江中杭电子有限公司、杭州市西湖区数据资源服务中心、宁波满坐数字技术有限公司、杭州峻偕科技有限公司、杭州仁盈科技股份有限公司、浙江数汉科技有限公司、杭州威灿科技有限公司、浙江达摩网络科技有限公司、杭州乐湾科技有限公司、浙江固微科技有限公司、杭州信雅达泛泰科技有限公司、浙江融健科技有限公司、杭州长勺智能科技有限公司、浙江友华工程咨询有限公司。

本文件主要起草人：冯益君、马小飞、沈云波、徐李斌、冯文明、吴红宇、吴懿红、朱明、汪晖、陈细平、朱新荣、方卫中、陈招华、吴振涛、余志飞、陈思、殷金旗、黄龙、叶茂允、姚俊山、俞琦莺、蔡昌伟、江成飞、刘德志、钟少春、潘黎明、孙腾龙、项方云、祝骅、汪家斌、蔡华满、胡顺扬、楼静斐、王启宏、陈锦帅、蒋钰霏、王吉国、白伟龙、鲍银涛、陈秋骥、陈骧、陈勇、戴琦、方宇、冯倩、高晓明、韩芳、韩剑波、胡欣鹏、吴桂林、吴彩霞、翁日君。

物联网设备数据接口规范

1 范围

本文件规定了物联网设备数据接口的术语和定义、总体架构要求、数据格式要求、通信协议要求、安全要求。

本文件适用于物联网设备数据接口。

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 35319 物联网 系统接口要求

3 术语和定义

下列术语和定义适用于本文件。

3.1

物联网设备 internet of things devices

通过传感、通信及数据处理能力接入网络，并与其他实体进行数据交换的物理或虚拟实体，包括传感器、执行器、网关及边缘计算节点。

3.2

遥测数据 telemetry data

设备周期性采集并上报的物理量测量值，例如温度、湿度或电压，通常以时间序列形式存储。

4 总体架构要求

4.1 系统分层架构

4.1.1 感知层

4.1.1.1 感知层应支持异构设备的接入，包括但不限于传感器、执行器及边缘计算节点。

4.1.1.2 设备应遵循统一的数据采集格式和通信协议，宜支持动态注册与发现机制。

4.1.1.3 数据接口可扩展适配多种物理层协议，例如有线以太网、无线 LoRa 或 NB-IoT。

4.1.1.4 物联网系统接口应符合 GB/T 35319 的有关规定。

4.1.2 网络层

4.1.2.1 网络层应提供可靠的数据传输通道，宜支持多协议代理转换功能。

4.1.2.2 网络层应实现数据路由优化，可依据场景需求选择集中式或分布式组网模式。

4.1.2.3 对于低功耗设备，宜采用轻量级传输协议以减少能耗。

4.1.3 平台层

4.1.3.1 平台层应具备数据汇聚、存储及分析能力，宜提供标准化的北向接口供上层应用调用。

4.1.3.2 平台应支持设备管理功能，包括状态监控、固件升级及配置下发。可引入微服务架构以实现功能模块的灵活扩展。

4.2 接口拓扑结构

4.2.1 星型拓扑

4.2.1.1 星型拓扑应作为基础部署模式，设备应通过单一中心节点接入系统。

4.2.1.2　中心节点应实现协议转换与数据聚合功能，宜支持负载均衡机制以应对高并发场景。

4.2.2　网状拓扑

4.2.2.1　网状拓扑可应用于设备间应直接通信的场景，例如工业现场控制网络。

4.2.2.2　设备应支持动态路由协议，宜具备自组织与自修复能力。该模式应确保数据传输的实时性与可靠性。

4.2.3　混合拓扑

4.2.3.1　混合拓扑可结合星型与网状结构的优势，边缘节点宜承担局部数据预处理职责。

4.2.3.2　系统应支持拓扑模式的动态切换，可基于网络质量或业务优先级调整连接策略。

4.3　跨平台兼容性

4.3.1　操作系统适配

4.3.1.1　接口协议应独立于操作系统，宜提供跨平台开发工具链。

4.3.1.2　设备厂商应确保驱动层兼容主流操作系统内核，例如 Linux、Windows 及 RTOS。

4.3.2　协议互操作性

4.3.2.1　系统应支持主流物联网通信协议，包括 MQTT、CoAP 及 HTTP/2。宜定义协议映射规则，实现不同协议间的语义互通。

4.3.2.2　数据接口可适配私有协议扩展，但需通过标准化封装确保兼容性。

4.3.3　数据模型一致性

4.3.3.1　设备数据模型应遵循统一元数据规范，宜引用行业通用本体库定义语义关系。

4.3.3.2　异构平台间交换数据时，应通过中间件实现模型转换与校验。

4.4　安全架构要求

4.4.1　分层防护机制

系统应实施分层安全策略，感知层宜采用轻量级加密算法，网络层应强制启用传输加密，平台层应部署访问控制与审计系统。

4.4.2　身份认证

设备接入时应完成双向身份认证，宜采用证书与动态令牌结合的认证方式。可引入设备指纹技术增强身份唯一性验证。

4.4.3　数据完整性

4.4.3.1　关键数据传输应包含数字签名，宜支持端到端完整性校验。

4.4.3.2　数据存储时可启用加密保护，密钥管理应符合国家密码行业标准。

4.5　可扩展性要求

4.5.1　接口扩展

4.5.1.1　系统应支持接口功能的模块化扩展，宜定义标准插件接口规范。

4.5.1.2　新增功能模块时，应确保不影响既有接口的兼容性。

4.5.2　规模扩展

架构设计应适应设备规模动态变化，宜采用分布式部署方案以支撑百万级设备并发。可引入边缘计算节点分担平台层负载。

4.5.3　协议演进

4.5.3.1　接口协议应支持版本平滑升级，宜通过语义化版本号标识变更等级。

4.5.3.2　重大版本更新时应提供过渡期兼容方案。

4.6　容错与可靠性

4.6.1　故障隔离

系统应实现分层故障隔离机制，单点故障不应导致整体服务中断。宜采用冗余设计保障关键节点可用性。

4.6.2　数据可靠性

4.6.2.1　传输层应提供消息确认与重传机制，宜定义服务质量分级策略。
4.6.2.2　平台层应实现数据持久化存储，可采用多副本机制防止数据丢失。

4.7　性能基线要求

4.7.1　时延敏感场景

对于工业控制等低时延场景，端到端传输时延应小于100 ms。宜采用数据预取与缓存机制优化响应速度。

4.7.2　高吞吐场景

视频监控等高频数据场景应支持批量数据传输模式，可启用数据压缩与分片传输技术。

4.7.3　资源受限场景

低功耗设备应优化接口协议开销，宜采用二进制编码替代文本格式。可选择性关闭非关键功能以节约资源。

5　数据格式要求

5.1　数据结构要求

5.1.1　数据格式应支持结构化与非结构化数据混合承载，结构化数据宜采用 JSON 或 XML 格式，非结构化数据可采用二进制流封装。
5.1.2　结构化数据应包含以下基础字段：
——数据类型：应明确区分遥测数据、事件告警或控制指令；
——数值单位：应采用国际单位制或行业约定计量单位；
——数据质量：宜包含信号强度、采集精度等元信息。
5.1.3　嵌套数据结构深度应不超过五层，单条数据载荷长度宜控制在 1 MB 以内，超长数据应启用分片传输机制。

5.2　压缩与加密

5.2.1　数据压缩算法应根据场景选择：
——文本数据宜采用 GZIP 或 Brotli 算法；
——二进制数据可选用 Zstandard 或 LZ4 等低延迟算法；
——图像与视频数据应遵循行业标准压缩格式。
5.2.2　加密数据应明确标注加密算法与密钥版本。加密后的数据载荷应包含初始化向量与认证标签。
5.2.3　压缩与加密处理顺序应遵循“先压缩后加密”原则，避免重复压缩已加密数据。

5.3　数据字典与语义标注

5.3.1　设备厂商应提供标准数据字典，字典条目应包含以下内容：
——字段名称与数据类型；
——取值范围与精度参数；
——语义描述与关联本体 URI。
5.3.2　动态生成的扩展字段应通过注册机制纳入字典管理，注册请求宜通过平台 API 自动提交。

5.3.3 语义标注应支持多语言描述，至少包含中文与英文版本，标注内容可嵌入数据包或通过元数据服务独立发布。

5.4 数据校验规则

5.4.1 格式校验应包括：

——语法正确性验证，例如 JSON 格式完整性检查；

——数据类型匹配性校验，例如数值型字段不得包含字符；

——取值范围合规性校验，例如温度值不得超出传感器量程。

5.4.2 语义校验应符合下列要求：

——本体一致性验证，例如单位与物理量维度匹配；

——上下文关联性校验，例如同一设备的位置数据不得超出现实移动速度范围。

5.5 实时数据流格式

5.5.1 流式数据应包含时间窗口标记，窗口大小可配置为 1 s~10 min，窗口重叠率宜小于 20%。

5.5.2 数据流宜采用轻量级封装格式，例如 Apache Avro 或 MessagePack，包头应包含流 ID、时间戳序列及校验和。

5.5.3 实时数据优先级应分为三级：

——紧急事件数据应立即推送，端到端时延应小于 50 ms；

——常规监测数据可批量聚合后传输；

——历史回溯数据允许延迟处理。

5.6 批量数据传输

5.6.1 批量数据文件应采用标准容器格式，例如 ZIP 或 TAR 包，压缩比宜达到 50%以上。文件内部应包含元数据索引文件。

5.6.2 批量传输应支持断点续传功能，分片大小宜设置为 1MB~10 MB，分片哈希值应通过 SHA-256 算法生成。

5.6.3 批量数据包应附加全局唯一标识符，命名空间宜选择设备厂商域名。

5.7 数据版本管理

5.7.1 数据格式版本号应采用语义化版本规则，主版本号变更表示不兼容性修改，次版本号表示功能扩展。

5.7.2 设备应通过协议握手过程声明支持的数据格式版本，平台应兼容最近三个次版本的数据格式。

5.7.3 版本弃用应提前六个月发布公告，过渡期内新旧版本应并行支持，平台可提供自动转换服务。

5.8 扩展性与自定义

5.8.1 厂商可扩展私有数据字段，但扩展字段命名应添加厂商前缀。

5.8.2 自定义数据格式应在公共注册库备案，备案信息应包括格式说明文档与解析工具下载链接。

5.8.3 私有数据与标准数据的转换应由边缘节点或平台中间件实现，转换规则应通过 JSON Schema 或 XML XSLT 定义。

6 通信协议要求

6.1 传输层协议

6.1.1 系统应支持 TCP 与 UDP 两种传输层协议，TCP 宜用于可靠性要求高的场景，UDP 可适用于实时性优先的应用。

6.1.2 TCP 连接应实现心跳保活机制，心跳间隔宜配置为 30 s~300 s，超时重连次数应可动态调整。

6.1.3 UDP 传输应支持数据包校验与乱序重组功能，宜在应用层实现简单重传机制以提升可靠性。

6.1.4 低功耗设备可采用轻量级传输协议，例如基于 UDP 的 CoAP 或专有 LPWAN 协议，但应确保与标准协议的互通性。

6.2 应用层协议

6.2.1 MQTT 协议

6.2.1.1 应支持 MQTT 5.0 及以上版本，保留字段的使用应符合 OASIS 标准。
6.2.1.2 宜启用遗嘱消息与会话保持功能，QoS 等级应根据数据类型动态选择。
6.2.1.3 可扩展自定义主题命名空间，但主题层级结构应遵循“设备类型/区域/功能”逻辑划分。

6.2.2 CoAP 协议

6.2.2.1 观察模式应支持多客户端订阅同一资源，资源更新通知时延应小于 500 ms。
6.2.2.2 块传输功能可启用以支持大数据分片传输，块大小宜适配网络 MTU 值。

6.2.3 HTTP/2 协议

6.2.3.1 应启用头部压缩与多路复用特性，单个连接宜并发处理至少 100 个请求。
6.2.3.2 服务器推送功能可选择性启用，推送内容应与客户端请求语义关联。
6.2.3.3 长轮询模式应设置超时阈值，默认值宜为 60 s。

6.2.4 LwM2M 协议

6.2.4.1 对象模型应遵循 OMA 标准定义，设备管理接口应包含固件升级与远程配置功能。
6.2.4.2 宜支持 JSON 与 TLV 两种数据序列化格式，可依据网络带宽灵活切换。
6.2.4.3 安全模式应强制启用 DTLS 1.2 以上版本，预共享密钥与证书认证方式可并存。

6.3 服务质量分级

6.3.1 应定义三级服务质量策略：
——QoS 0（至多一次）：适用于周期性遥测数据，允许有限丢包；
——QoS 1（至少一次）：用于指令下发与告警，需确保送达确认；
——QoS 2（恰好一次）：适用于计费或关键控制指令，需实现事务性传输。
6.3.2 消息优先级宜划分为 0~7 级，其中：
——0~2 级用于后台同步等非实时任务；
——3~5 级用于常规监测数据；
——6~7 级保留给紧急事件与实时控制指令。
6.3.3 流量整形机制应防止网络拥塞，令牌桶算法参数宜根据网络带宽动态调整。

6.4 安全通信机制

6.4.1 传输层安全

6.4.1.1 TLS 1.3 应作为标准加密协议，密码套件宜禁用弱加密算法。
6.4.1.2 DTLS 1.2 可适用于 UDP 协议，但应定期更新预置证书链。
6.4.1.3 会话恢复机制应限制恢复时间窗口，默认值宜为 24 h。

6.4.2 身份认证

6.4.2.1 设备接入应强制双向认证，证书颁发机构应符合国际可信根证书列表。
6.4.2.2 宜支持 OAuth 2.0 设备流授权模式，令牌刷新周期应不超过 7 天。
6.4.2.3 临时设备可采用预置短期凭证，凭证有效期宜小于 72 h。

6.4.3 数据隐私

6.4.3.1 敏感字段应进行端到端加密，加密密钥生命周期应不超过 90 天。
6.4.3.2 匿名化处理宜在边缘节点完成，脱敏后的数据应移除设备指纹信息。
6.4.3.3 数据流经第三方节点时，应通过代理重加密技术保护隐私。

6.5 协议适配与兼容性

6.5.1 协议网关应实现多协议转换功能，例如将 MQTT 消息转换为 CoAP 请求，转换过程应保留原始

语义信息。
6.5.2　私有协议扩展应提供标准适配器，适配器应开放接口定义与测试工具集。
6.5.3　协议版本升级时，旧版本客户端应至少保留 6 个月兼容期，平台可提供协议降级转换服务。

6.6　性能优化要求

6.6.1　头部压缩

6.6.1.1　HTTP/2 应启用 HPACK 压缩，MQTT 宜采用属性别名缩短报文长度。
6.6.1.2　二进制协议可定义紧凑字段编码规则，例如变长整数表示法。

6.6.2　数据分片

6.6.2.1　单条消息载荷超过 1 MB 时应强制分片，分片序号与总片数应包含在元数据中。
6.6.2.2　分片重组超时时间宜设置为消息 RTT 的三倍。

6.6.3　本地缓存

6.6.3.1　断网期间设备宜缓存未发送数据，缓存队列深度应可配置。
6.6.3.2　平台应支持增量数据同步，避免重复传输历史数据。

6.7　网络适应性设计

6.7.1　弱网环境应启用以下优化措施：
——降低心跳频率至最低可行值；
——压缩算法切换为低计算复杂度模式；
——优先传输关键数据字段，延迟非必需元数据。
6.7.2　多网络切换场景应实现无缝漫游，会话迁移时延应小于 200 ms，IP 地址变化不应中断业务流。

7　安全要求

7.1　设备身份认证

7.1.1　设备在接入网络前应完成双向身份认证机制，认证过程应基于非对称加密算法，例如采用 X.509 数字证书或国密 SM2 算法。
7.1.2　临时接入设备或资源受限设备可采用预共享密钥方式，但密钥分发过程应通过加密通道完成，预置密钥生命周期宜限制在 72 h 内，过期后应重新授权。
7.1.3　设备唯一标识应具备防篡改与防伪造特性，宜通过硬件安全模块或可信平台模块固化标识，不应通过软件手段修改标识信息。
7.1.4　认证失败时应记录详细日志，连续失败超过 5 次可触发临时锁定机制，锁定时间宜按指数退避原则递增。

7.2　数据机密性保护

7.2.1　数据传输过程应强制启用端到端加密，传输层协议宜采用 TLS 1.3 或国密 TLCP 协议，弱密码套件如 DES 或 MD5 应明确禁用。
7.2.2　静态数据存储时应使用强加密算法，例如 AES-256-GCM 或 SM4-OFB 模式，加密密钥应与设备身份解耦，密钥管理应符合国家商用密码标准。
7.2.3　密钥生命周期管理应实现自动化轮换机制，根密钥存储应依赖硬件安全单元保护，临时会话密钥有效期宜不超过 24 h。
7.2.4　加密算法选择应兼顾性能与安全性，低功耗设备可采用轻量级加密方案，但应通过国家密码管理部门认证。

7.3　访问控制与权限管理

7.3.1　设备应实现基于角色的访问控制模型，角色权限至少划分为管理员、操作员及观察员三级，权限分配应遵循最小特权原则。

7.3.2 敏感操作接口应实施多因素认证，例如结合动态口令与生物特征验证，关键指令下发前需二次确认。
7.3.3 动态授权宜采用 OAuth 2.0 或 OpenID Connect 框架，令牌作用域应精确限定设备功能与数据访问范围，令牌有效期宜不超过 1 h。
7.3.4 访问策略变更应触发实时生效机制，权限回收时应终止当前会话并清除相关缓存。

7.4 数据完整性保障

7.4.1 控制指令、固件升级包及配置数据应附加数字签名，签名算法宜采用 ECDSA 或 SM2，哈希函数应使用 SHA-256 或 SM3。
7.4.2 数据存储完整性可通过哈希链或 Merkle 树结构实现，数据篡改检测到后应自动隔离并触发告警通知。
7.4.3 传输层应防范重放攻击，数据包应包含时间戳与递增序列号，历史序列号缓存窗口期宜设置为 24 h。
7.4.4 数据校验失败时应记录详细错误信息，并支持自动修复或人工介入流程，原始错误数据应保留取证副本。

7.5 固件与软件安全

7.5.1 固件升级包应由厂商私钥签名，升级流程应验证签名合法性，验签失败时应终止升级并回滚至安全版本。
7.5.2 固件回滚机制应限制版本降级范围，仅允许回退至最近两个安全版本，防止利用历史漏洞实施攻击。
7.5.3 运行时内存保护应启用地址空间随机化、堆栈保护及代码签名验证，动态加载的第三方库应审核签名合法性。
7.5.4 设备应定期上报软件版本与补丁状态，未修复已知高危漏洞的设备应限制部分功能使用。

7.6 安全日志与审计追踪

7.6.1 设备应记录以下安全事件日志：
——身份认证成功与失败事件；
——敏感配置变更与权限调整操作；
——异常流量模式或协议违规行为；
——加密密钥生成与轮换记录。
7.6.2 日志条目应包含精确时间戳、事件类型、源设备标识及操作结果，时间同步误差应小于 500 ms。
7.6.3 审计日志应集中存储于防篡改区域，访问日志应通过独立认证通道，日志保留周期宜不少于 1 年。
7.6.4 日志分析系统应支持自动化异常检测，例如通过机器学习模型识别潜在攻击行为。

7.7 物理安全与防篡改

7.7.1 关键设备应集成防拆机传感器，物理外壳非法开启时应触发密钥清零及存储数据自毁流程。
7.7.2 调试接口如 JTAG 或 UART 应默认禁用，启用时应通过硬件跳线或授权指令激活，并记录操作日志。
7.7.3 存储介质应实现全盘加密，设备报废时应自动执行多次覆写擦除，确保数据无法通过物理手段恢复。
7.7.4 硬件设计应避免侧信道攻击泄露敏感信息，例如电源分析与电磁辐射防护措施。

7.8 漏洞管理与应急响应

7.8.1 设备厂商应建立公开漏洞披露渠道，高危漏洞修复补丁宜在发现后 30 天内推送至全部设备。
7.8.2 设备应支持远程热修复能力，应急模式下可动态关闭非核心服务，降低受攻击面。
7.8.3 供应链安全应纳入管理体系，第三方组件应提供软件物料清单，并定期更新漏洞扫描报告。
7.8.4 安全事件响应流程应包含事件分级、遏制措施与根因分析，重大事件应在 24 h 内启动处置。

7.9 隐私保护与合规性

7.9.1 个人可识别信息应进行假名化或匿名化处理，假名生成算法应不可逆且无法关联原始数据。
7.9.2 数据收集范围应遵循最小化原则，生物特征等敏感信息应获得用户明示授权，授权记录应永久保存。
7.9.3 数据跨境传输应符合国家法律法规，隐私政策变更应提前 30 天通知用户并重新获取同意。
7.9.4 用户数据访问请求应支持合规导出与删除功能，删除操作应彻底清除所有副本及备份。

7.10 安全生命周期管理

7.10.1 设备全生命周期应覆盖安全需求分析、设计、测试、部署及退役阶段，各阶段应输出对应安全文档。
7.10.2 生产环节应实施安全烧录与密钥注入流程，禁止出厂设备携带测试用临时凭证。
7.10.3 设备退役时应自动触发数据销毁程序，并生成不可逆的退役证明供审计查验。