ICS 35.240.50
CCS L70

团　　体　　标　　准

T/ZIUR XXXX—2026

工业物联网平台 工业设备数据接入规范

Industrial Internet Platform—Specification for Industrial Equipment Data Access

（征求意见稿）

XXXX－XX－XX 发布　　XXXX－XX－XX 实施

浙江省产学研合作促进会　　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XXX提出。

本文件由浙江省产学研合作促进会归口。

本文件起草单位：XXX。

本文件主要起草人：XXX。

工业物联网平台 工业设备数据接入规范

1 范围

本文件规定了工业物联网平台的设备数据接入的总体要求、设备接入、数据格式与编码、数据字典、数据安全、测试与验证。

本文件适用于工业物联网平台的工业设备数据接入工作。

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 3100～3102 量和单位

GB/T 7408.1 日期和时间 信息交换表示法 第1部分：基本原则

GB/T 11383 信息处理 信息交换用八位代码结构和编码规则

GB/T 18391.1 信息技术 元数据注册系统（MDR）第1部分：框架

GB/T 22239 信息安全技术 网络安全等级保护基本要求

GB/T 30269.401 信息技术传感器网络 第401部分：协同信息处理：支撑协同信息处理的服务及接口

GB/T 33560 信息安全技术 密码应用标识规范

GB/T 35273 信息安全技术 个人信息安全规范

GB/T 38639 系统与软件工程 软件组合测试方法

GB/T 39400 工业数据质量 通用技术规范

GB/T 47019 工业互联网平台 工业设备接入数据字典

GB/T 47021 工业互联网平台 体系架构

GB 50311 综合布线系统工程设计规范

YD/T 4982 工业企业数据安全防护要求

YD/T 6209 工业互联网标识解析 体系架构

3 术语和定义

GB/T 11457界定的以及下列术语和定义适用于本文件。

3.1

架构 architecture

系统在组件层面的基本组织结构表现，包括系统内部组件之间的关系、组件与外部的关系以及决定设计和演进的原则。

[来源：GB/T 47021，3.1]

3.2

元数据 metadata

定义和描述其他数据的数据。

[来源：GB/T 18391.1，3.2.16]

3.3

布线 cabling

能够支持电子信息设备相连的各种缆线、跳线、接插软线和连接器件组成的系统。

[来源：GB 50311，2.1.2]

3.4

网络安全 cybersecurity

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 22239，3.1]

4 总体要求

4.1 基本原则

4.1.1 可靠性原则

应具备抗干扰、容错能力，减少数据丢失、传输中断等异常情况，保障数据接入的连续性。

4.1.2 可扩展性原则

应支持接入设备类型、数量的扩展，适配工业物联网平台功能升级及业务场景的延伸需求。

4.1.3 易用性原则

应简化设备接入配置流程，降低设备接入门槛。

4.1.4 安全性原则

设备接入身份、数据传输过程应进行安全防护，防范非法接入、数据篡改等安全风险。

4.1.5 经济性原则

在满足接入需求的前提下，应优化接入方案，降低设备改造、接入部署及运维的成本。

4.2 体系架构

4.2.1 工业设备数据接入体系架构应参考 GB/T 47021 的规定，分为接入层、传输层、适配层三个核心层级，各层级职责清晰、协同工作。

4.2.2 接入层作为设备与平台的连接入口，应支持多种接入方式和通信协议，负责工业设备的数据采集、身份标识与初始校验。

4.2.3 传输层应负责数据从接入层到适配层的稳定传输，提供数据加密、路由转发、流量控制等功能，保障数据在传输过程中的完整性与安全性。

4.2.4 适配层应实现数据格式转换、协议适配、数据清洗等功能，将不同设备、不同格式的数据统一转换为平台可识别、可处理的格式，支撑数据后续处理与应用。

4.2.5 体系架构各层级应具备模块化设计特性，支持各模块的独立升级、替换，提升架构的灵活性与可维护性，适配不同工业场景的接入需求。

4.3 接入流程

工业设备数据接入应遵循标准化流程，主要包括设备注册、身份认证、接入协商、数据传输、状态监控、注销退出六个环节：

——设备注册环节：设备应向工业物联网平台提交注册申请，提供设备标识、设备类型、厂商信息、能力参数等基础信息，完成注册信息的录入与审核；

——身份认证环节：平台应采用密码认证、密钥认证等方式，对注册设备进行身份校验，未通过认证的设备不得接入平台；

——接入协商环节：设备与平台应协商确定通信协议、数据传输频率、数据格式、加密方式等接入参数，形成接入协议，确保数据传输的一致性；

——数据传输环节：设备按照协商的接入参数，向平台传输采集的数据，平台对接收的数据进行实时接收、解析与临时存储，同步反馈接收状态；

——状态监控环节：平台应实时监测设备接入状态、数据传输状态，及时发现设备离线、数据异常等问题，并记录相关日志；

——注销退出环节：设备需退出平台接入时，应向平台提交注销申请，平台注销设备接入权限，清理设备相关注册信息与接入记录，完成接入闭环。

4.4 性能指标

4.4.1 工业设备数据接入的性能指标应满足工业场景实际需求，主要包括并发接入能力、数据传输延迟、数据传输成功率、设备接入响应时间等，具体要求见表 1。

表 1 工业设备数据接入性能指标要求

性能指标名称	单位	要求值	说明
并发接入设备数	台	≥10000	支持同时接入的工业设备最大数量，可根据平台规模扩展
数据传输延迟	ms	≤500	从设备采集数据到平台接收完成的时间，实时性要求高的场景≤100ms
数据传输成功率	%	≥99.9	单位时间内成功传输至平台的数据量与总数据量的比值
设备接入响应时间	ms	≤1000	从设备提交接入申请到平台反馈接入结果的时间
数据丢失率	%	≤0.1	单位时间内丢失的数据量与总传输数据量的比值
系统稳定性	小时	≥720	连续无故障运行时间，每月累计故障时间≤1小时

4.5 兼容性要求

4.5.1 接入系统应兼容不同类型、不同厂商的工业设备，包括传感器、控制器、执行器、智能仪表等，支持设备型号的扩展与更新。

4.5.2 应兼容多种工业通信协议，包括 MQTT、Modbus、OPC UA 等常用协议，可通过协议适配模块实现不同协议的转换与兼容。

4.5.3 应兼容不同的数据格式，能够对设备输出的二进制、ASCII、JSON 等多种格式数据进行解析与转换，统一适配平台数据规范。

4.5.4 宜兼容不同版本的工业物联网平台，支持平台版本升级过程中数据接入的连续性，不影响设备正常数据传输。

4.5.5 应兼容工业现场常见的网络环境，包括以太网、无线网络（5G、Wi-Fi、LoRa）等，适应不同工业场景的网络部署需求，符合工信部工业控制系统网络安全防护指南相关要求。

5 设备接入

5.1 接入方式

5.1.1 有线接入

5.1.1.1 有线接入方式适用于工业现场网络稳定、设备固定的场景，主要包括以太网接入、RS485 总线接入、RS232 总线接入。

5.1.1.2 以太网接入应采用 TCP/IP 协议，支持 1000Mbps 及以上传输速率，接线规范应符合 GB/T 50311 的规定，保障数据传输的稳定性。

5.1.1.3 RS485 总线接入适用于短距离、多设备连接场景，传输距离宜控制在 1000 米以内，支持 32 个及以上设备同时接入，采用差分传输方式抗干扰。

5.1.1.4 RS232 总线接入适用于单设备、短距离接入场景，传输距离不宜超过 15 米，主要用于小型控制器、智能仪表等设备的接入。

5.1.2 无线接入

5.1.2.1 无线接入方式适用于设备移动、现场布线困难的场景，主要包括 5G、Wi-Fi、LoRa、NB-IoT 等接入方式。

5.1.2.2 5G 接入适用于实时性要求高、数据传输量大的场景，支持低延迟（≤10ms）、高带宽、广连接。

5.1.2.3 Wi-Fi 接入适用于工业现场局部区域设备接入，支持 IEEE 802.11b/g/n/ac 标准，传输速率≥150Mbps，覆盖范围宜控制在 100 米以内。
5.1.2.4 LoRa 接入适用于低功耗、远距离、低速率的场景，传输距离可达 3000 米以上，支持大量设备并发接入，适用于传感器等低功耗设备。
5.1.2.5 NB-IoT 接入适用于低功耗、广覆盖、低速率的场景，支持深度覆盖，功耗低，适用于工业现场偏远区域设备的接入。

5.2 通信协议

5.2.1 工业设备数据接入应采用标准化通信协议，优先选用国家、行业标准协议，确保协议的通用性与兼容性。
5.2.2 协议传输过程中应采用加密算法对数据进行加密处理，可选用 AES-128 及以上加密算法，防止数据传输过程中被篡改、窃取，符合 GB/T 33560 的规定。
5.2.3 平台应具备协议适配能力，可通过协议网关实现不同协议的转换，支持协议版本的兼容与升级。

5.3 接口规范

5.3.1 工业设备数据接入接口应分为南向接口和北向接口，南向接口用于设备与平台的连接，北向接口用于平台与上层应用的连接，接口定义应规范、统一。
5.3.2 南向接口应支持多种接入方式和通信协议，接口参数应包括设备标识、数据类型、传输频率、加密方式等，接口格式应标准化，便于设备接入与适配。
5.3.3 北向接口应采用 RESTful API 接口规范，支持 HTTP/HTTPS 协议，接口应具备身份认证、权限控制功能，防止非法访问。
5.3.4 接口应支持数据批量传输与实时传输两种模式，批量传输适用于非实时性数据，实时传输适用于实时性要求高的数据，传输模式可根据业务需求配置。
5.3.5 接口应具备错误处理能力，当数据传输失败、接口异常时，应返回明确的错误代码与错误信息，便于运维人员排查处理，错误代码定义应统一、规范。
5.3.6 接口应支持版本管理，当接口功能升级时，应保留旧版本接口的兼容性，避免影响现有设备与应用的正常运行。

5.4 设备标识

5.4.1 工业设备接入应采用唯一的设备标识，确保设备的可识别性与可追溯性。
5.4.2 设备标识应采用分层结构，主要包括厂商代码、设备类型代码、设备序列号三部分，总长度宜为 16-32 位，可采用数字、字母组合形式。
5.4.3 厂商代码由行业主管部门统一分配，用于标识设备厂商，长度宜为 4-8 位；设备类型代码用于标识设备类型，长度宜为 4 位；设备序列号由厂商自行分配，确保同一厂商、同一类型设备的序列号唯一。
5.4.4 设备标识应固化在设备中，不可修改，可通过设备固件、硬件标签等方式存储，便于平台读取与校验。
5.4.5 平台应建立设备标识管理体系，记录设备标识对应的设备信息、接入状态、运维记录等，实现设备标识的全生命周期管理。
5.4.6 设备标识应支持与工业互联网标识解析体系对接，可通过标识解析获取设备的详细信息，提升设备管理的智能化水平，符合 YD/T 6209 的规定。

5.5 即插即用

5.5.1 工业设备应具备即插即用功能，设备接入工业物联网平台时，无需人工手动配置复杂参数，可自动完成注册、认证、接入等流程。
5.5.2 设备应支持自动发现功能，能够自动搜索工业物联网平台的接入节点，获取接入地址、通信协议等基础参数，完成接入准备。
5.5.3 平台应具备设备自动识别能力，能够根据设备发送的标识信息、能力参数等，自动识别设备类型、厂商、型号等信息，完成设备注册与参数配置。
5.5.4 设备接入后，应自动同步设备状态、能力参数等信息至平台，平台根据设备类型自动分配数据

采集策略、传输参数等，实现设备的快速接入与正常运行。

5.6 自描述机制

5.6.1 工业设备应具备自描述能力，能够向工业物联网平台提供设备自身的详细信息，包括设备标识、设备类型、厂商信息、能力参数、数据采集范围等。
5.6.2 自描述信息应采用标准化格式，可采用 JSON、XML 等格式存储与传输，信息内容应完整、准确，便于平台解析与识别。
5.6.3 自描述信息应包括静态信息与动态信息，静态信息包括设备型号、厂商、硬件版本等固定信息，动态信息包括设备运行状态、数据采集频率等可变信息。
5.6.4 设备应在接入时主动向平台提交自描述信息，当设备参数发生变更时，应及时更新自描述信息并同步至平台，确保平台获取的设备信息准确、最新。
5.6.5 平台应具备自描述信息解析能力，能够根据设备提交的自描述信息，自动适配数据采集、传输、处理策略，无需人工干预，提升设备接入的智能化水平。

6 数据格式与编码

6.1 数据分类

工业设备接入数据应根据数据性质、用途进行分类，分类应清晰、合理，便于数据的存储、处理、分析与应用：

——设备状态数据：涵盖运行状态、故障状态、能耗状态等，用于设备状态监控与故障诊断；
——运行参数数据：涵盖温度、压力、流量、转速、电压、电流等，用于设备运行优化与性能分析；
——事件告警数据：涵盖告警类型、告警级别、告警时间、告警描述等，用于告警通知与故障排查；
——控制指令数据：涵盖指令类型、指令参数、执行状态等，用于设备远程控制与操作；
——设备属性数据：涵盖设备标识、厂商、型号、硬件版本、软件版本等，用于设备管理与身份识别，分为静态属性与动态属性两大类。

6.2 数据结构

6.2.1 工业设备接入数据应采用标准化的数据结构，数据结构应包括数据头、数据体、数据尾三部分，各部分字段定义规范、统一，便于平台解析与处理。
6.2.2 数据头应包含数据标识、设备标识、数据类型、数据长度、时间戳等基础信息，用于数据的识别与定位，具体字段要求见表 2。

表 2 数据头字段定义

字段名称	字段类型	字段长度（字节）	说明
数据标识	字符串	8	唯一标识一条数据，采用字母+数字组合
设备标识	字符串	16-32	对应设备的唯一标识，符合6.4条要求
数据类型	整数	1	0－设备状态数据，1－运行参数数据，2－事件告警数据，3－控制指令数据，4－设备属性数据
数据长度	整数	4	数据体的长度，单位为字节
时间戳	字符串	20	数据产生的时间，格式符合7.4条要求

6.2.3 数据体应包含具体的业务数据，根据数据类型的不同，数据体字段应有所差异，字段名称、类型、长度应标准化，确保数据的一致性与可读性。
6.2.4 数据尾应包含校验码、数据结束标识等信息，校验码用于验证数据传输过程中的完整性，防止数据被篡改，可采用 CRC32 校验算法。

6.3 数据编码

6.3.1 工业设备接入数据应采用标准化的编码方式，编码应具备可读性、可解析性、可扩展性。
6.3.2 文本类型数据应采用 UTF-8 编码方式，符合 GB/T 11383 的规定，确保中文、英文、数字等字符的正常显示与传输。
6.3.3 数值类型数据应采用二进制编码或十进制编码，二进制编码适用于数据传输效率要求高的场景，十进制编码适用于可读性要求高的场景，编码格式应统一。
6.3.4 二进制数据编码应采用大端序或小端序，同一平台内编码顺序应统一，避免数据解析错误，大端序适用于网络传输场景，小端序适用于本地存储场景。
6.3.5 复杂数据结构应采用 JSON 或 Protobuf 编码方式，JSON 编码适用于可读性要求高、数据量适中的场景，Protobuf 编码适用于数据量较大、传输效率要求高的场景，符合 ProtoJSON Format 相关规范。

6.4 时间戳格式

6.4.1 工业设备接入数据的时间戳应符合 GB/T 7408.1 的规定，采用公历日期和时间表示。
6.4.2 时间戳格式应采用“YYYY-MM-DD HH:MM:SS.SSS”格式，其中 YYYY 表示年份（4 位），MM 表示月份（2 位），DD 表示日期（2 位），HH 表示小时（24 小时制，2 位），MM 表示分钟（2 位），SS 表示秒（2 位），SSS 表示毫秒（3 位）。
6.4.3 时间戳应基于协调世界时（UTC）或本地时间，同一平台内时间标准应统一，若采用本地时间，应明确时区信息，避免时间混乱。
6.4.4 设备采集数据时，应同步记录数据产生的时间，时间戳精度应不低于毫秒级，确保数据的时间准确性，满足实时监控与数据分析需求。
6.4.5 时间戳应嵌入数据头中，与数据同步传输，平台接收数据后，应根据时间戳对数据进行排序、归档，便于数据的时间维度分析。

6.5 数据单位

6.5.1 工业设备接入数据的单位应符合 GB 3100～3102 的规定，采用国际单位制（SI）。
6.5.2 数据单位应与数据值同步传输，嵌入数据体中，平台接收数据后，应根据数据单位对数据进行解析、转换。
6.5.3 当数据单位发生变更时，设备应及时同步单位信息至平台，平台应支持单位的动态适配。

6.6 数据质量要求

6.6.1 工业设备接入数据的质量应满足完整性、准确性、一致性、时效性、唯一性要求，确保数据能够支撑平台的后续处理、分析与应用，符合 GB/T 39400 的规定。
6.6.2 数据应完整无缺失，关键字段缺失率≤1%，非关键字段缺失率≤5%，缺失数据应标注缺失原因，便于后续补充与处理。
6.6.3 准数据值应真实反映设备实际运行状态与参数，数值错误率≤1%，误差范围应符合设备自身精度要求，可采用双重校验和阈值报警。
6.6.4 同一设备、同一类型的数据在不同时间、不同传输环节的格式、单位、精度应统一，跨系统共享字段格式一致性≥99%，无矛盾、无冲突。
6.6.5 数据从产生到平台接收完成的时间应符合 5.4 条性能指标要求，实时性数据延迟≤100ms，非实时性数据延迟≤500ms，数据更新频率应匹配业务需求。
6.6.6 数据应具有唯一标识，无重复数据，重复记录率≤0.5%，尤其是设备标识、数据标识等关键信息，应确保唯一性。
6.6.7 平台应具备数据质量检测能力，实时监测数据质量，对不符合要求的数据进行标记、预警，并记录数据质量异常日志，便于运维人员排查处理。

7 数据字典

7.1 数据字典结构

7.1.1 工业设备数据接入数据字典结构应符合 GB/T 47019 的规定，采用分层分级结构。
7.1.2 数据字典应分为顶层、中层、底层三个层级，顶层为数据大类，中层为数据子类，底层为具体

数据项，各层级间存在明确的从属关系。

7.1.3 顶层数据大类应对应第 6 章数据分类，包括设备状态数据、运行参数数据、事件告警数据、控制指令数据、设备属性数据五大类，与前文数据分类保持一致。

7.1.4 中层数据子类应基于顶层大类进一步细分，例如设备属性数据可细分为静态属性数据、动态属性数据，运行参数数据可细分为电气参数、机械参数等。

7.1.5 底层数据项为数据字典的核心单元，应包含数据项标识、数据项名称、数据类型、数据单位、取值范围等基础信息。

7.2 元数据定义

7.2.1 元数据定义应遵循 GB/T 18391.1 的规定，确保元数据的规范性、统一性与可理解性。

7.2.2 元数据应定义数据字典各层级的描述信息，包括数据大类元数据、数据子类元数据、数据项元数据，覆盖数据的全生命周期描述需求。

7.2.3 数据大类元数据应包含大类标识、大类名称、大类描述、数据来源、创建时间、更新时间等属性，用于描述数据大类的核心信息。

7.2.4 数据子类元数据应包含子类标识、子类名称、所属大类标识、子类描述、数据范围等属性，明确子类与大类的从属关系及自身范围。

7.2.5 数据项元数据是元数据定义的核心，应包含以下核心属性，可根据业务需求适当扩展：

——数据项标识：唯一标识数据项，采用字母+数字组合，长度宜为 8-16 位；

——数据项名称：简洁明了描述数据项含义，名称应规范、统一，避免歧义；

——数据类型：明确数据项的类型，包括字符串、整数、浮点数、布尔值等，与第 7 章数据格式要求一致；

——数据单位：符合 GB 3100～3102 的规定，无单位数据项应标注“无”；

——取值范围：明确数据项的合法取值区间，包括最小值、最大值、枚举值等，确保数据有效性；

——数据精度：明确数值型数据的精度要求，例如保留小数点后 2 位，无精度要求的标注“无”；

——描述说明：详细说明数据项的含义、用途、采集方式等，便于用户理解与使用。

7.2.6 元数据定义应避免歧义，同一数据项的元数据描述应统一，跨数据子类的同类数据项，元数据属性宜保持一致，提升数据字典的一致性。

7.3 属性描述方法

7.3.1 数据字典各层级属性描述应采用标准化方法，结合文字描述、代码标识、表格补充的方式。

7.3.2 文字描述应简洁严谨，用词规范，避免模糊表述，长度控制在 50 字以内，明确属性的核心含义与要求，不使用冗余表述。

7.3.3 代码标识应采用标准化编码规则，编码应具有唯一性，可采用分层编码方式，体现属性的从属关系，例如数据项标识可包含大类编码、子类编码、自身编码。

7.3.4 数值型属性应采用量化描述，明确具体数值或区间，避免定性描述，确保属性描述的可操作性。

7.3.5 枚举型属性应列出所有合法取值，每个取值应附带简要说明，明确取值的含义，便于用户理解与应用。

7.3.6 属性描述应结合数据字典的应用场景，针对工业设备接入特点，重点描述数据项的采集要求、传输要求、解析要求，与第 5 章、第 6 章内容保持衔接。

7.3.7 对于复杂数据项的属性描述，可采用表格补充的方式，清晰呈现属性的各项参数，提升描述的直观性，示例见表 3。

表 3 复杂数据项属性描述示例表

数据项标识	数据项名称	属性名称	属性描述
OP-001	设备运行温度	取值范围	0-100℃，超出范围视为异常数据
OP-001	设备运行温度	数据精度	保留小数点后1位
OP-001	设备运行温度	数据单位	℃（摄氏度），符合GB/T 3102.4-1993

7.4 约束条件

7.4.1 数据字典的约束条件应针对数据项、元数据、结构三个层面制定，确保数据字典的规范性、完整性与一致性。
7.4.2 数据项约束条件应明确数据项的必填性、取值约束、格式约束，是数据采集、传输、解析的核心依据，不得随意违反。
7.4.3 必填性约束分为必选、条件必选、可选三类，核心数据项应设为必选，非核心数据项可设为可选或条件必选。
7.4.4 取值约束应明确数据项的合法取值范围，数值型数据应明确最小值、最大值，枚举型数据应明确所有合法枚举值，超出约束范围的数据应视为无效数据。
7.4.5 格式约束应与第 6 章数据格式与编码要求保持一致，明确数据项的格式、长度、编码方式，例如数据项标识长度宜为 8-16 位，采用 UTF-8 编码。
7.4.6 元数据约束条件应明确元数据的完整性、一致性要求，元数据属性不得缺失核心字段，同一数据项的元数据描述应统一。
7.4.7 结构约束条件应明确数据字典的分层分级规则，各层级的从属关系应清晰，不得出现跨层级、跨大类的混乱关联，数据子类应隶属于唯一数据大类。
7.4.8 约束条件可根据工业设备类型、业务场景的变化进行调整，但调整应遵循标准化流程，经审核确认后更新，确保约束条件的严肃性。

7.5 扩展机制

7.5.1 数据字典应具备灵活的扩展机制，支持数据大类、子类、数据项及元数据的扩展，适配不同类型工业设备的接入需求。
7.5.2 扩展机制应遵循“兼容原有、适度扩展”的原则，扩展后的内容应与原有数据字典结构、元数据定义、约束条件保持兼容，不影响原有数据的正常使用。
7.5.3 数据大类扩展应结合工业设备接入的新场景、新需求，新增大类需经标准化审核，明确大类标识、名称、描述等元数据，确保与原有大类无冲突。
7.5.4 数据子类扩展可基于现有数据大类，根据设备类型、业务需求细分，新增子类应明确所属大类、子类标识、描述等信息，保持与大类的从属关系清晰。
7.5.5 数据项扩展应针对具体业务需求，新增数据项需符合元数据定义要求，明确各项属性及约束条件，与同类数据项的描述方式保持一致。
7.5.6 元数据扩展可根据数据项的特性，新增元数据属性，新增属性应具有通用性、必要性，避免冗余，新增后应同步更新相关约束条件。
7.5.7 扩展流程应规范化，包括扩展申请、审核、实施、更新四个环节，扩展申请应说明扩展原因、扩展内容，审核通过后方可实施扩展。
7.5.8 扩展后的内容应及时更新至数据字典，同步更新附录 A 的数据字典示例，通知相关使用方，确保数据字典的统一性与时效性。
7.5.9 扩展内容应建立版本管理机制，明确扩展版本、扩展时间、扩展内容，便于追溯与回滚，当扩展内容不再适用时，可按流程进行删除或修改。

8 数据安全

8.1 接入安全

8.1.1 身份认证

8.1.1.1 身份认证可采用密码认证、密钥认证、数字证书认证等方式，优先选用密钥认证或数字证书认证，提升认证安全性。
8.1.1.2 设备应存储唯一的认证凭证，认证凭证应加密存储，不得明文传输，凭证有效期宜设置为 1-3 年，定期更换。
8.1.1.3 平台应建立认证凭证管理体系，对凭证的生成、分发、更换、注销进行全生命周期管理。

8.1.1.4　未通过身份认证的设备，平台应拒绝其接入，记录认证失败日志，明确失败原因，便于运维人员排查处理。

8.1.2　设备准入

8.1.2.1　平台应建立设备准入机制，只有符合本标准要求、通过身份认证、完成注册的设备，方可接入平台，符合 YD/T 4982。
8.1.2.2　设备准入应审核设备标识、厂商信息、设备类型、自描述信息等内容，审核不通过的设备，应反馈审核意见，禁止接入。
8.1.2.3　平台应实时监测接入设备的状态，对非法接入、伪造身份接入的设备，应立即切断连接，采取隔离措施，并记录相关日志。
8.1.2.4　宜建立设备接入白名单机制，仅允许白名单内的设备接入平台，进一步提升接入安全，白名单应定期更新、审核。

8.2　传输安全

8.2.1　设备与平台之间的数据传输应采用加密方式，加密算法应符合 GB/T 33560 的规定，优先选用 AES-128 及以上加密算法。
8.2.2　传输过程中应采用完整性校验机制，可采用 CRC32、SHA-256 等校验算法，验证数据传输过程中是否被篡改、丢失。
8.2.3　通信协议应具备安全防护能力，禁止使用明文传输协议，MQTT、OPC UA 等协议应启用加密传输功能，关闭不必要的端口与服务。
8.2.4　数据传输应采用专用通道，可通过 VPN、工业防火墙等设备隔离，避免与公共网络直接连接，防范网络攻击。
8.2.5　平台应监测数据传输状态，当发现传输异常时，应及时告警，通知运维人员处理，并尝试重新传输数据。
8.2.6　传输日志应完整记录数据传输的时间、设备标识、数据量、传输状态、加密方式等信息，日志留存时间不少于 6 个月，符合 GB/T 22239 的规定。
8.2.7　宜采用数据分片传输方式，对大量数据进行分片加密传输，提升传输安全性与效率，分片传输应确保数据的完整性与顺序性。

8.3　存储安全

8.3.1　敏感数据应采用加密存储，加密算法与传输加密算法保持一致，密钥应单独存储、定期更换。
8.3.2　存储设备应具备访问控制、数据备份、故障恢复能力，防止数据丢失、泄露、篡改，存储介质应符合国家相关安全标准。
8.3.3　应建立数据备份机制，定期对存储的数据进行备份，备份频率应根据数据重要性设定，核心数据备份频率不少于每日 1 次。
8.3.4　备份数据应存储在安全的存储介质中，可采用本地备份与异地备份相结合的方式，异地备份距离应符合安全要求，确保备份数据可恢复。
8.3.5　存储数据应建立生命周期管理机制，根据数据重要性设定存储期限，过期数据应按规范进行销毁，销毁过程应确保数据无法恢复。
8.3.6　存储日志应记录数据的存储、访问、修改、删除等操作，日志留存时间不少于 6 个月，便于数据追溯与安全审计。

8.4　访问控制

8.4.1　平台应建立严格的访问控制机制，遵循最小权限原则，对不同角色的用户分配不同的访问权限。
8.4.2　访问角色应分为管理员、运维人员、普通用户等，不同角色的访问权限应明确界定，禁止越权访问，具体权限分配见表 4。

表 4　访问角色与权限分配表

访问角色	核心访问权限	权限说明

管理员	全权限访问，包括用户管理、权限分配、数据管理、系统配置	负责平台整体管理，权限最高，需严格管控
运维人员	设备管理、数据监测、日志查看、故障处理	负责设备接入运维，无用户管理、权限分配权限
普通用户	数据查看、设备状态监测	仅具备基础查看权限，无修改、删除权限

8.4.3 用户访问时应进行身份认证，采用账号密码、动态口令等认证方式，认证通过后方可访问对应权限的内容。
8.4.4 应定期对用户访问权限进行复核，及时调整、注销过期权限、闲置权限，防止权限滥用，复核周期不少于每季度 1 次。
8.4.5 访问日志应记录用户访问时间、访问角色、访问内容、操作行为等信息，日志留存时间不少于 6 个月，便于安全审计与异常排查。

8.5 隐私保护

8.5.1 工业设备接入过程中涉及的隐私数据，应符合 GB/T 35273 的规定，加强隐私保护。
8.5.2 隐私数据主要包括设备运维人员信息、现场人员信息、敏感设备位置信息等，应明确隐私数据范围，建立隐私数据清单。
8.5.3 应建立隐私数据访问控制机制，仅授权人员可访问隐私数据，访问过程应记录日志，明确访问时间、访问人员、访问内容。
8.5.4 隐私数据不得随意泄露、传播、篡改，不得用于与工业设备接入无关的用途，确需共享的，应经授权并采取加密措施。
8.5.5 应定期对隐私数据保护情况进行检查，排查隐私泄露风险，发现问题及时整改，确保隐私数据的安全性。
8.5.6 过期隐私数据应按规范进行销毁，销毁过程应确保数据无法恢复，留存销毁记录。
8.5.7 宜建立隐私保护应急机制，当发生隐私数据泄露时，应立即启动应急响应，采取补救措施，通知相关人员，并上报相关主管部门。

9 测试与验证

9.1 测试环境

9.1.1 工业设备数据接入测试环境应模拟工业现场实际场景。
9.1.2 测试环境应包括硬件环境、软件环境、网络环境三部分，各部分配置应满足测试需求，确保测试结果的真实性、可靠性。
9.1.3 硬件环境应包含工业设备、网关、服务器、测试终端等设备，设备型号、参数应覆盖常见工业设备类型，与实际接入设备一致。
9.1.4 服务器配置应满足平台运行及测试需求，CPU、内存、存储容量应适配并发接入测试、数据传输测试等场景，确保测试过程无卡顿。
9.1.5 软件环境应包含工业物联网平台软件、数据采集软件、测试工具软件，软件版本应与实际部署版本一致，无额外插件、补丁影响测试。
9.1.6 网络环境应模拟工业现场网络，支持以太网、5G、LoRa 等多种接入方式，网络带宽、延迟、丢包率应可调节，模拟不同网络场景。
9.1.7 测试环境应具备隔离性，与生产环境严格隔离，防止测试过程影响生产环境的正常运行，测试环境应配备安全防护设备。
9.1.8 测试环境应保持稳定，温度、湿度、电压等环境参数应符合设备运行要求，避免环境因素影响测试结果。

9.2 测试内容

测试应包含以下内容，全面验证工业设备数据接入的合规性、可靠性、安全性，符合GB/T 38639的规定：

——总体要求测试：验证接入过程的基本原则、体系架构、接入流程、性能指标、兼容性是否符合本标准第 4 章要求；
——设备接入测试：验证接入方式、通信协议、接口规范、设备标识、即插即用、自描述机制是否符合本标准第 5 章要求；
——数据格式与编码测试：验证数据分类、数据结构、数据编码、时间戳格式、数据单位、数据质量是否符合本标准第 6 章要求；
——数据字典测试：验证数据字典结构、元数据定义、属性描述方法、约束条件、扩展机制是否符合本标准第 7 章要求；
——数据安全测试：验证接入安全、传输安全、存储安全、访问控制、隐私保护是否符合本标准第 8 章要求，重点测试加密、认证功能；
——并发接入测试：验证平台并发接入设备的能力，测试不同并发量下平台的运行状态、数据传输成功率、延迟等性能指标；
——异常测试：模拟设备离线、网络中断、数据异常、非法接入等场景，验证平台的容错能力、告警能力、恢复能力；
——兼容性测试：验证平台对不同类型设备、不同通信协议、不同网络环境的兼容能力，确保设备接入的通用性；
——长期运行测试：模拟设备长期接入运行场景，测试平台的稳定性、数据存储的可靠性，运行时间不少于 72 小时。

9.3 测试方法

9.3.1 测试方法应标准化、可操作，结合黑盒测试、白盒测试、压力测试、模拟测试等方式，确保测试结果准确、可重复。
9.3.2 总体要求测试采用文档审查与现场测试相结合的方式，审查体系架构文档、接入流程文档，现场验证性能指标、兼容性。
9.3.3 设备接入测试采用实际设备接入测试方式，选取不同类型、不同厂商的设备，通过多种接入方式接入平台，验证接入功能的合规性。
9.3.4 数据格式与编码测试采用数据采集与解析测试方式，采集设备传输的数据，验证数据格式、编码、时间戳、单位等是否符合要求。
9.3.5 数据字典测试采用文档审查与实例验证相结合的方式，审查数据字典文档，选取典型数据项验证元数据定义、约束条件的合规性。
9.3.6 数据安全测试采用工具测试与模拟攻击相结合的方式，使用安全测试工具检测加密、认证功能，模拟非法接入、数据篡改等攻击场景。
9.3.7 并发接入测试采用压力测试工具，模拟不同数量的设备同时接入平台，记录平台的并发接入能力、数据传输延迟、成功率等指标。
9.3.8 异常测试采用模拟场景测试方式，人为模拟设备离线、网络中断、数据异常等情况，观察平台的告警、容错、恢复能力，记录相关日志。
9.3.9 兼容性测试采用多设备、多协议、多网络测试方式，选取不同型号设备、不同通信协议、不同网络环境，验证平台的兼容能力。
9.3.10 测试过程中应详细记录测试数据、测试结果，每个测试项目应重复测试 3 次以上，确保测试结果的稳定性、可靠性。

9.4 验证标准

9.4.1 总体要求验证应符合本标准 4.1-4.5 条及 GB/T 47021 的规定，性能指标应满足表 5-1 的规定。
9.4.2 设备接入验证应符合本标准 5.1-5.6 条及 GB/T 30269.401 的规定，即插即用接入时间≤1000ms。
9.4.3 数据格式与编码验证应符合本标准 6.1-6.6 条及 GB/T 39400 的规定，数据格式解析成功率≥99.8%，数据质量符合相关指标。
9.4.4 数据字典验证应符合本标准 7.1-7.5 条及 GB/T 47019 的规定，数据项元数据完整率 100%，约束条件符合率 100%。
9.4.5 数据安全验证应符合本标准 8.1-8.5 条及 GB/T 22239 的规定，加密算法合规，无数据泄露、非

法接入情况。

9.4.6 并发接入验证应符合平台并发接入设备数≥10000 台，数据传输延迟≤500ms，数据传输成功率≥99.9%，符合表 5-1 性能指标要求。

9.4.7 平台应能及时发现异常并告警，告警响应时间≤100ms，异常恢复后数据传输正常，无数据丢失。

9.4.8 平台应兼容至少 3 种接入方式、5 种以上通信协议、10 种以上不同类型工业设备，接入无异常。

9.4.9 平台应连续无故障运行时间≥72 小时，数据存储无丢失、无篡改，设备接入状态稳定，无异常离线情况。