ICS 35.110
CCS L79

# 团　　体　　标　　准

T/ZIUR XXXX—XXXX

# 电子制造领域嵌入式物联网设备通用技术要求

General Technical Requirements for Embedded IoT Devices in Electronic Manufacturing Field

（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××××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：

本文件主要起草人：

# 电子制造领域嵌入式物联网设备通用技术要求

## 1 范围

本文件规定了电子制造领域嵌入式物联网设备的术语和定义、基本要求、硬件通用技术要求、嵌入式系统要求、通信与接入技术要求、数据采集与交互要求、信息安全技术要求、设备管控要求、检验、测试与验收要求。

本文件适用于电子制造场景中，具备数据采集、联网传输、智能管控功能的嵌入式物联网设备的设计研发、生产制造、集成部署、运行管控及检验测试等活动。

## 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 4208.1 外壳防护等级（IP代码）
GB/T 5226.1 机械电气安全 机械电气设备 第1部分：通用技术条件
GB/T 17626.5 电磁兼容 试验和测量技术 浪涌（冲击）抗扰度试验
GB/T 22033 信息技术 嵌入式系统术语
GB/T 33745 物联网 术语
GB/T 34989 连接器 安全要求和试验
GB/T 35273 信息安全技术 个人信息安全规范
GB/T 35313 模块化存储系统通用规范
GB/T 36468 物联网 系统评价指标体系编制通则
GB/T 38619 工业物联网 数据采集结构化描述规范
GB/T 38624.1 物联网 网关 第1部分：面向感知设备接入的网关技术要求
GB/T 38637.1 物联网 感知控制设备接入 第1部分：总体要求
GB/T 40684 物联网 信息共享和交换平台通用要求
GB/T 41782.1 物联网 系统互操作性 第1部分：框架
GB 50311 综合布线系统工程设计规范
DB33/T 2579 审计数据归集规范

## 3 术语和定义

下列术语和定义适用于本文件。

3.1

**物联网 internet of things(IoT)**

基于感知控制设备，通过通信网络，使物理实体、人、系统和信息资源相连接，响应和处理物理和虚拟世界信息的基础设施。

[来源：GB/T 33745，3.1.1]

3.2

**嵌入式系统 embedded system**

置入应用对象内部，起信息处理或控制作用的专用计算系统。

[来源：GB/T 22033，2.001]

3.3

**嵌入式物联网设备 embedded IoT device**

集成嵌入式系统，具备数据采集、联网传输、智能控制能力，部署于电子制造场景的终端设备。

3.4

**物联网网关 IoT gateway**

具有数据存储能力、计算能力和协议转换能力等，能将一个或多个邻近网络以及网络中的物联网设备相互连接，并连接到一个或多个接入网络进行通信的物联网系统的一类实体。

[来源：GB/T 38624.1，3.1，有修改]

3.5

**边缘计算 edge computing**

将计算、存储能力部署在靠近感知控制设备或数据源头的网络边缘侧的计算架构。

[来源：GB/T 33745，3.1.13]

3.6

**固件 firmware**

被写入非易失程序存储器内的专用软件。

[来源：GB/T 22033，2.032]

## 4 基本要求

### 4.1 总体架构

4.1.1 电子制造领域嵌入式物联网设备应采用分层架构进行设计，整体划分为硬件层、嵌入式系统层、感知执行接口层与应用层，各层级边界清晰、功能独立，架构设计宜满足模块化扩展需求。

4.1.2 设备架构应具备本地数据处理与云端协同能力，可在终端侧完成数据预处理、协议转换等工作，并能够安全对接物联网平台。

4.1.3 架构可根据电子制造不同生产场景进行功能裁剪与配置适配，满足产线检测、现场管控、物料管理等差异化使用需求。

4.1.4 架构设计应兼顾运维便利性，预留状态监测、故障定位以及远程程序升级的相关接口。总体架构图见图 1 所示。

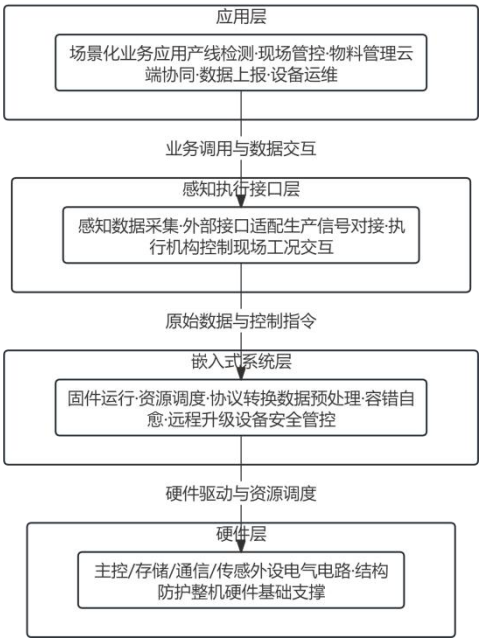


**图 1 总体架构图**

### 4.2 基本原则

设备设计、研发、生产与应用应遵循以下原则：

a) 合规性原则：设备全流程应遵守国家、行业现行法规与技术规范，满足设备安全、电磁兼容等基础要求；

b） 可靠性原则：设备适配电子制造现场长期运行工况，关键功能模块宜采用冗余设计，降低故障发生概率；
c） 安全性原则：设备应建立完整防护机制，落实身份认证、访问控制、数据保护等要求，防范非法接入与信息泄露风险；
d） 兼容性原则：硬件接口、通信协议及数据格式宜采用行业通用规范，保障设备与各类系统、终端互联互通；
e） 低功耗原则：在保障性能的前提下，优化电路与程序逻辑，合理控制设备运行及待机功耗；
f） 实用性原则：技术方案应贴合电子制造实际应用场景，兼顾技术指标与规模化落地需求。

### 4.3 环境适应性要求

4.3.1 设备在正常工作状态下，可在-40 ℃至 70 ℃区间内稳定运行；非工作存储状态下，耐受温度范围应达到-55 ℃至+85 ℃。
4.3.2 设备经受温度变化影响时，各项功能不应出现异常，相关试验可按照现行电工电子产品环境试验相关规范执行。
4.3.3 湿度环境下，设备工作时相对湿度范围应控制在 10 %RH～95 %RH，运行过程中不应出现凝露现象。设备长期处于湿热环境中，外壳、内部元器件及电路应无腐蚀、短路等问题。
4.3.4 电子制造现场存在的振动、机械冲击等外力作用，不应造成设备结构损坏、部件松动或功能失效。针对高频振动、短时冲击等工况，设备结构与硬件布局宜做加固处理。
4.3.5 设备外壳应具备防尘、防水能力，常规使用场景下防护等级应不低于 IP54；粉尘、油污较多的严苛生产场景中，设备防护等级宜提升至 IP65，外壳防护性能判定可依据外壳防护等级相关标准执行。
4.3.6 设备部署于工业电磁环境中时，应具备良好的抗电磁干扰能力，自身产生的无线电骚扰也应符合限值要求，避免对周边电子设备造成影响。

### 4.4 可靠性与稳定性要求

4.4.1 设备应支持全天候连续运行，在长期不间断工作过程中，不应出现无故死机、自动重启、数据中断等故障。
4.4.2 当设备出现软件异常、网络临时中断等问题时，应具备自诊断与自恢复能力，可在短时间内自行修复故障、恢复正常运行状态。
4.4.3 设备采集、传输及存储的业务数据，应保证真实完整，数据传输过程中丢包现象应控制在合理范围之内，重要业务数据宜进行备份留存。
4.4.4 电网电压小幅波动、网络信号不稳定等非正常工况下，设备核心业务功能应保持正常，各项性能指标不应出现大幅偏差。
4.4.5 设备全生命周期内，核心硬件与主体性能应保持稳定，长期使用后不应出现明显的性能衰减，固件程序可正常完成迭代更新。

## 5 硬件通用技术要求

### 5.1 核心硬件配置要求

5.1.1 主控单元应根据电子制造现场的数据处理、逻辑控制、协议解析等实际负荷合理选型，硬件运算、存储能力应匹配设备既定功能需求。
5.1.2 存储单元，包括含内存、固态存储等的读写性能、容量及使用寿命应满足设备全生命周期使用要求。
5.1.3 固态存储器件选型与测试可参照 GB/T 35313 中的具体要求。
5.1.4 通信模组应适配电子制造场景主流联网方式，无线、有线通信模块的信号接收、传输能力应满足现场组网与数据交互需求，模块工作稳定性应符合工业级应用要求。
5.1.5 各类传感、采集类硬件单元，采样精度、响应速度应符合设备预设技术指标，长时间连续工作状态下性能不应发生明显偏移。

### 5.2 外设与接口规范

5.2.1 设备配置的各类对外接口，物理形态、引脚定义、电气参数宜采用行业通用规格，保证不同厂商设备间基础对接能力。
5.2.2 数字接口、模拟接口、网络接口及调试接口等，应具备防误插、防短路设计，接口防护与机械耐久性能应符合 GB/T 34989 相关规定。
5.2.3 外设驱动电路应与外接部件电气特性相匹配，接口驱动能力、信号电平保持稳定，外接负载变化时不应造成端口损坏或信号异常。
5.2.4 调试、运维专用接口宜设置权限管控或物理防护，避免非授权人员随意接入，降低误操作带来的运行风险。

### 5.3 电气安全要求

5.3.1 设备供电回路设计应合理，适配工业现场常用供电制式，电压波动范围内设备应正常工作，过压、欠压工况下宜具备保护功能。
5.3.2 整机电气安全应符合 GB/T 5226.1，设备外壳、可触及部件不应存在漏电风险。
5.3.3 设备应设置过流、过温、浪涌保护电路，应对上电冲击、线路异常、瞬时浪涌等工况，防止硬件烧毁或功能失效，浪涌防护设计可参照 GB/T 17626.5。
5.3.4 接地设计应规范，保护接地、功能接地分区清晰，接地线路连接牢固、接触可靠，有效规避静电、漏电带来的安全隐患。

### 5.4 结构与防护要求

5.4.1 设备整体结构布局应合理，内部器件排布规整，走线、固定方式兼顾散热、抗震与检修便利性，机械结构设计应满足现场安装、拆卸的使用需求。
5.4.2 外壳及内部支撑结构应具备足够机械强度，正常搬运、安装及使用过程中，不应出现变形、开裂、部件脱落等问题。
5.4.3 设备外壳防护性能应满足本文件 4.3.4 要求，防尘、防水结构设计与装配工艺，应符合 GB/T 4208.1 的判定条件。
5.4.4 设备散热结构应适配整机功耗与现场环境温度，自然散热或辅助散热结构应保证内部元器件工作温度处于额定区间，避免积温过高影响硬件寿命与运行性能。
5.4.5 针对电子制造车间粉尘、油污、腐蚀性气体等环境，结构缝隙、开孔位置宜做密封处理，减缓有害物质侵入对内部硬件的损害。

## 6 嵌入式系统要求

### 6.1 嵌入式固件基本要求

6.1.1 设备搭载的嵌入式固件应适配电子制造工业运行场景，固件程序应经过编译优化与稳定性测试，运行过程中不应出现程序崩溃、死循环、异常退出等问题。
6.1.2 固件应具备轻量化特性，适配嵌入式设备有限的硬件资源，无冗余无效程序代码，程序运行效率应满足设备实时数据采集、协议解析与业务处理需求。
6.1.3 固件开发与编译应遵循安全规范，预留的程序接口、后台服务应最小化配置，杜绝非法后门、冗余端口。
6.1.4 固件版本应唯一可追溯，支持版本标识、版本查询功能，便于设备全生命周期的运维与版本管理。

### 6.2 系统资源管控要求

6.2.1 嵌入式系统应对 CPU、内存、存储空间等核心硬件资源进行动态管控，合理分配系统进程与业务进程资源，避免资源占用过载导致设备卡顿、死机。
6.2.2 系统应具备资源监测能力，可实时采集硬件资源占用数据，当资源占用达到阈值时，宜主动进行资源清理、进程优化，保障设备持续稳定运行。
6.2.3 系统日志、运行缓存、临时数据等内容应具备自动清理机制，避免长期堆积占用存储资源，影响设备使用寿命与运行性能。

6.2.4 嵌入式系统资源调度策略应适配工业实时性需求，关键业务进程优先级应高于普通辅助进程，保障生产数据采集、设备控制等核心业务不被中断。

### 6.3 升级与容错机制要求

设备嵌入式系统应具备完善的远程升级与运行容错机制，具体要求如下：

——系统应支持远程在线升级与本地离线升级两种模式，升级数据包应支持校验验证，杜绝破损、篡改固件包写入设备；

——升级过程应具备断点续传、异常保护功能，断电、断网等突发工况下，不应造成固件损坏、设备变砖等不可逆故障；

——系统升级后应自动完成兼容性自检，自检不通过时应自动触发版本回滚机制，恢复至上一稳定运行版本；

——系统运行过程中出现程序异常、数据报错、进程卡死等故障时，应具备自动容错、异常重启恢复能力，保障核心业务连续性；

——系统应留存升级日志与故障容错记录，完整记录升级时间、版本信息、故障类型及处理结果，日志数据可长期留存、可查询追溯。

## 7 通信与接入技术要求

### 7.1 通用通信协议适配要求

#### 7.1.1 基础协议适配

7.1.1.1 电子制造嵌入式物联网设备应适配工业现场主流通信协议，至少支持 MQTT、Modbus TCP、OPC UA 三种基础协议，满足生产数据采集与设备交互需求。

7.1.1.2 所有协议帧结构、校验规则、交互时序应完全符合协议官方规范，不得存在自定义私有字段导致的兼容性异常。

7.1.1.3 协议参数应支持本地及远程可视化配置，可按需调整心跳周期、上报频率、超时阈值，适配不同产线工况。

#### 7.1.2 协议传输稳定性

7.1.2.1 设备通信链路应具备超时重传机制，网络瞬时抖动情况下，应保证关键生产数据不丢失、不重复上报。

7.1.2.2 长连接通信应支持心跳保活，可自动识别断链状态并主动重连，重连成功率应满足工业连续运行要求。

7.1.2.3 批量数据传输场景下，设备应支持流量控制，避免高频报文挤占带宽导致通信拥堵。

7.1.2.4 协议通信稳定性要求可参照 GB/T 38637.1 执行。

#### 7.1.3 轻量化协议优化

7.1.3.1 针对嵌入式设备资源受限特性，设备宜启用协议轻量化配置，精简冗余报文，降低 CPU 与内存占用。

7.1.3.2 低频次监测场景可采用休眠上报机制，在保证业务不中断的前提下降低通信功耗。

### 7.2 设备入网接入规范

#### 7.2.1 有线入网要求

7.2.1.1 设备以太网接口应支持 10M/100M 自适应速率，通信链路稳定可靠，适配车间固定组网场景。

7.2.1.2 有线通信端口应具备电气隔离与抗浪涌能力，可耐受工业现场电磁干扰，避免端口击穿、通信中断。

7.2.1.3 设备有线接入应支持链路状态实时检测，异常断连时应主动生成日志并上报平台。

7.2.1.4 有线网络接入基础要求应符合 GB 50311 中有线网络布线的物理层设计与施工要求。

#### 7.2.2 无线入网要求

7.2.2.1 设备无线通信模块应适配工业车间复杂电磁环境，具备信道抗干扰、自动择优切换能力。
7.2.2.2 无线入网应采用加密认证方式，禁止裸链路明文传输，防止数据窃听与非法劫持。

#### 7.2.3 入网认证与安全管控

7.2.3.1 设备入网前应完成身份合法性认证，支持设备唯一标识码校验、密钥校验等准入机制，杜绝非法设备混入组网。
7.2.3.2 入网配置参数应加密存储，禁止明文留存，防止参数被恶意篡改。
7.2.3.3 设备入网、退网、重连全过程应留存操作日志，支持溯源审计。

### 7.3 互联互通兼容性要求

#### 7.3.1 设备互操作性要求

7.3.1.1 设备对外交互的数据字段、报文格式应标准化，可与主流工业物联网平台、边缘网关正常解析对接。
7.3.1.2 跨厂家同类设备之间宜实现参数互通、状态同步，满足产线设备统一管控需求。

#### 7.3.2 平台系统兼容要求

7.3.2.1 设备应支持标准化南向接入协议，可无缝对接工业互联网平台、MES、SCADA 等上位系统。
7.3.2.2 设备接口应具备向下兼容特性，固件迭代升级后，不应影响原有平台接入方式。
7.3.2.3 异构系统对接出现字段差异时，设备宜支持本地适配转换，保证数据正常上报。

#### 7.3.3 组网兼容适配要求

7.3.3.1 设备应支持多类型网络拓扑适配，可适配星型、链型、边缘分布式组网结构。
7.3.3.2 在多设备密集组网场景下，设备通信频点、报文时序应相互兼容，无信号冲突、报文干扰问题。
7.3.3.3 互联互通总体要求应参照 GB/T 41782.1 中的具体内容。

## 8 数据采集与交互要求

### 8.1 数据采集规范

#### 8.1.1 采集对象与范围要求

设备数据采集范围与采集对象应符合以下要求：
——设备应针对电子制造生产场景，采集设备运行状态、工艺参数、现场工况、故障告警等核心业务数据，覆盖设备监测与生产管控所需的全部关键点位；
——数据采集应聚焦生产业务需求，不应采集无关冗余数据，避免无效采集占用设备资源与通信带宽；
——设备采集点位、采集数据类型宜支持本地或远程配置调整，可适配不同生产线、不同工艺场景的差异化采集需求。

#### 8.1.2 采集精度与实时性要求

8.1.2.1 设备数据采集精度应匹配电子制造工艺管控标准，模拟量数据采集误差应控制在设备标称精度范围内，保证生产数据真实有效。
8.1.2.2 常规状态数据采集周期宜可配置，关键工艺数据、异常告警数据应支持毫秒级高频采集，满足工业生产实时管控需求。
8.1.2.3 数据采集过程中的数据源要求和交互动态操作可参照 GB/T 38619 相关规定执行。

#### 8.1.3 采集有效性控制要求

8.1.3.1 设备应具备数据采集滤波去噪能力，可自动过滤车间电磁干扰、设备抖动产生的无效杂波数据，避免异常数据上传。

8.1.3.2 采集异常、传感器故障、信号中断时，设备应主动识别采集失效状态，标记无效数据并生成异常日志，禁止上传错误数据。

## 8.2 数据传输与编码要求

### 8.2.1 传输基础要求

8.2.1.1 设备采集的业务数据应支持定时上报、事件触发上报、主动问询上报三种传输模式，适配不同生产监测场景。
8.2.1.2 数据传输过程中应保持完整性、有序性，无丢包、错包、乱序等问题，关键生产数据传输成功率应不低于 99.99％。
8.2.1.3 网络链路不稳定时，设备应暂缓非关键数据传输，优先保障告警、故障、核心工艺数据优先传输。

### 8.2.2 数据编码规范

8.2.2.1 设备交互数据应采用标准化编码格式，宜支持 JSON、Protobuf 等通用工业数据格式，编码规则应统一、规范，便于平台及上位系统解析。
8.2.2.2 数据字段命名、数据类型、单位定义应遵循行业通用规范，禁止自定义私有歧义字段，保障异构系统数据互通。

### 8.2.3 传输容错与重传机制

8.2.3.1 设备应具备数据传输校验机制，通过校验码比对判定数据完整性，对传输失败的数据应自动触发重传机制。
8.2.3.2 短时断网工况下，设备应缓存待传数据，网络恢复后自动补传未上报数据，保证数据连续性。

## 8.3 数据存储与缓存要求

### 8.3.1 本地数据存储要求

8.3.1.1 设备应配置本地存储区域，用于存储设备参数、运行日志、历史采集数据、故障记录等关键信息。
8.3.1.2 存储容量应满足设备全周期数据留存需求。
8.3.1.3 本地存储的数据应具备防篡改、防丢失保护能力，断电重启后数据不应丢失、错乱。
8.3.1.4 物联网终端数据存储基础应符合 GB/T 40684 中的要求，保证数据完整性和安全性。

### 8.3.2 临时缓存管控要求

8.3.2.1 设备运行过程中的临时采集数据、待传输报文应设置独立缓存区域，缓存空间应设置阈值上限，避免缓存溢出导致系统异常。
8.3.2.2 缓存数据应具备生命周期管理能力，已成功上传的缓存数据应自动清理，释放硬件资源。
8.3.2.3 缓存队列应具备优先级排序功能，优先留存、上传高优先级生产业务数据。

### 8.3.3 数据留存与清理要求

8.3.3.1 设备关键生产数据、故障日志、升级记录应长期留存，普通监测数据可根据配置周期自动清理。
8.3.3.2 数据手动或自动清理前，应对重要数据进行备份，防止误删除导致数据缺失。

# 9 信息安全技术要求

## 9.1 设备身份认证要求

9.1.1 设备接入网络、平台交互及对外服务过程中，应建立唯一、可信的身份认证机制。
9.1.2 身份认证总体要求应符合 GB/T 35273，具体要求如下：

——设备应具备唯一固化设备身份标识，标识信息不可篡改、不可复制，作为设备入网、交互、溯源的唯一凭证；

——设备入网对接物联网平台、网关设备时，应采用双向身份认证机制，禁止无认证直接接入，防范伪造设备非法入网；
——设备宜支持密钥认证、证书认证等多种认证方式，可根据现场安全等级需求灵活切换适配；
——身份认证失败时，设备应主动拒绝接入请求并记录异常日志，留存非法接入溯源信息。

## 9.2 访问控制安全要求

### 9.2.1 权限分级管控

9.2.1.1 设备应建立分级权限管理体系，区分管理员、运维、普通访问等不同权限角色，不同角色对应差异化操作权限，严格遵循最小权限管控原则，杜绝超权限操作风险。
9.2.1.2 非授权用户及外部终端，不应访问设备核心配置、固件参数、私密生产数据等关键内容，禁止私自修改设备运行参数与组网配置。
9.2.1.3 设备权限账号应支持定期更换、密码复杂度校验，默认初始账号密码应支持强制修改，规避弱口令带来的安全隐患。

### 9.2.2 接口访问防护

9.2.2.1 设备调试接口、运维接口、数据交互接口应设置访问限制，仅授权终端、授权 IP 可接入访问，杜绝任意终端随意接入。
9.2.2.2 长期闲置的对外接口宜支持手动或自动禁用，减少设备攻击面，降低被恶意利用的安全风险。
9.2.2.3 所有对外开放接口应做访问频次限制，针对高频重复访问、异常试探访问行为，设备应自动拦截并告警记录。
9.2.2.4 设备本地调试接口仅允许现场物理授权使用，远程运维接口宜搭配身份认证后方可开放使用。

### 9.2.3 访问日志审计

9.2.3.1 设备应完整记录所有外部访问、参数修改、设备配置操作日志，日志内容应包含操作时间、操作主体、操作内容、操作结果等关键信息。
9.2.3.2 访问审计要求应符合 DB33/T 2579 相关审计规范，日志数据应支持本地留存与远程上报，且不可随意篡改删除。

## 9.3 数据安全与加密要求

### 9.3.1 数据传输加密

9.3.1.1 设备与平台、网关之间传输的生产数据、设备参数、身份密钥等敏感数据，应采用加密传输方式，全程禁止明文传输。
9.3.1.2 设备通信链路宜采用 TLS 加密协议进行链路防护，有效规避数据窃听、劫持、篡改等各类传输安全风险。
9.3.1.3 设备断点续传、补发历史数据过程中，应保持加密传输机制不失效，保障补传数据的传输安全。

### 9.3.2 数据存储安全

9.3.2.1 设备本地存储的密钥、账号、核心工艺参数等敏感数据，应进行加密存储处理，全程禁止明文留存。
9.3.2.2 设备废弃、格式化前，应支持敏感数据彻底清除或粉碎处理，防止数据泄露，数据存储安全要求参照 GB/T 35273 及物联网终端数据安全通用要求执行。
9.3.2.3 设备加密存储的密钥文件、配置文件应定期自动备份，避免硬件故障导致核心安全数据丢失。
9.3.2.4 临时缓存的敏感数据在使用完毕后，应即时自动清除，避免长期留存产生安全隐患。

### 9.3.3 数据完整性保护

9.3.3.1 设备采集、传输、存储的业务数据，应通过校验算法保障数据完整性，可有效识别数据篡改、缺失、错乱等异常情况。
9.3.3.2 检测到数据异常时，设备应主动标记异常数据、终止异常数据交互并上报故障信息。

### 9.4 设备安全防护与漏洞防护

设备应具备终端主动安全防护与漏洞闭环处置能力，抵御工业场景常见网络攻击与固件漏洞风险，具体要求如下：

——设备应具备基础网络攻击防护能力，可抵御端口扫描、恶意报文攻击、高频非法请求等常见网络威胁，异常攻击行为应及时拦截并记录日志；

——设备固件应定期完成漏洞排查，针对已知安全漏洞，应支持固件迭代修复，实现漏洞闭环整改；

——设备应禁止预留非法后门、隐蔽端口及未授权服务，所有运行服务、开放端口应可查询、可管控、可关闭；

——设备遭遇恶意攻击、漏洞利用导致功能异常时，应具备自我保护机制，可自动阻断异常连接、重启恢复核心业务，避免设备失控、数据泄露；

——设备应建立常态化安全自查机制，定期巡检设备运行服务、开放端口及固件运行状态，及时排查并处置潜在安全隐患，实现设备安全常态化防护。

## 10 设备管控要求

### 10.1 设备状态监测要求

#### 10.1.1 运行状态监测

10.1.1.1 设备应具备全维度运行状态自主监测能力，可实时采集并统计设备在线状态、运行时长、工作模式、任务执行进度等基础运行信息。

10.1.1.2 设备应对嵌入式系统资源进行实时监测，包括 CPU 占用率、内存使用率、存储空间占用情况，资源超限应触发状态预警。

10.1.1.3 设备运行状态监测数据应实时同步至本地日志及上层管理平台，保障管理人员可实时掌握设备运行工况。

#### 10.1.2 硬件工况监测

10.1.2.1 设备应支持核心硬件工况监测，涵盖主控模块、通信模组、存储单元、传感采集模块的工作状态及温度、电压等关键参数。

10.1.2.2 当硬件工作参数超出额定阈值时，设备应主动标记异常状态，区分轻微偏差、临界异常、严重故障不同工况等级。

10.1.2.3 硬件监测精度应匹配工业设备管控需求，杜绝误监测、漏监测问题，保障硬件运行状态可查、可追溯。

10.1.2.4 硬件状态监测机制设计可参照 GB/T 34071 相关要求执行。

#### 10.1.3 通信状态监测

10.1.3.1 设备应实时监测通信链路状态，包含网络连接状态、信号强度、数据丢包率、通信时延、心跳连接状态等关键通信指标。

10.1.3.2 针对通信波动、链路抖动、短时断连等异常工况，设备应精准识别并记录异常时段、异常类型，为故障排查提供数据支撑。

### 10.2 故障诊断与处置要求

设备应具备自主故障诊断、分级告警、闭环处置能力，可适配电子制造场景连续运行管控需求，具体要求如下：

——设备应搭载内置故障诊断逻辑，可自主识别硬件故障、通信故障、数据异常、系统运行异常、参数配置异常等各类常见故障；

——设备应建立故障分级机制，按照故障影响范围、危害程度划分为一般故障、重要故障、严重故障，实施差异化处置策略；

——针对一般性瞬时故障，设备应具备自主自愈能力，可通过重连链路、重启进程、重置临时参数等方式自动恢复正常运行；
——针对无法自主修复的重要及严重故障，设备应立即终止高危运行动作，主动上报告警信息，留存完整故障快照与日志，等待人工运维处置；
——设备故障诊断与处置逻辑应具备可迭代性，可通过固件更新优化故障识别精度、新增故障处置策略，适配产线工艺迭代需求。

### 10.3 设备生命周期管理要求

#### 10.3.1 入网与部署管理

10.3.1.1 新设备接入生产网络前，应完成身份认证、参数初始化、功能校验等入网流程，校验合格后方可正式投入生产运行。
10.3.1.2 设备部署信息、入网时间、初始配置参数应全程留存归档，作为设备全生命周期溯源的基础数据。

#### 10.3.2 运行与运维管理

10.3.2.1 设备运行阶段应全程留存运行日志、操作日志、故障日志、升级日志，实现运行过程全记录、全溯源。
10.3.2.2 设备支持远程运维、现场运维两种模式，运维操作应全程留痕，禁止无记录私自修改设备配置与运行参数。
10.3.2.3 设备运维管理要求可参照 GB/T 36468 中设备运维管控相关规范。

#### 10.3.3 迭代与报废管理

10.3.3.1 设备在服役周期内，应支持固件迭代、功能优化、参数升级，持续适配生产工艺更新与安全管控升级需求。
10.3.3.2 设备达到服役年限、出现不可逆硬件故障或不满足生产工艺要求时，应执行报废下线流程，及时退出生产组网。
10.3.3.3 设备报废前，应完成敏感数据清除、设备解绑、权限注销等操作，杜绝报废设备造成数据泄露、非法入网等安全隐患。

## 11 检验、测试与验收要求

### 11.1 通用测试条件

11.1.1 设备各项性能测试、功能测试及安全测试，均应在常规标准大气环境下开展，保证环境温湿度稳定适宜，满足设备正常试验工况。
11.1.2 开展高低温、湿热、振动、防尘防水等环境适应性试验时，应按照梯度化工况参数开展测试，全面覆盖电子制造常规生产环境与严苛极限环境。
11.1.3 全程测试过程中，应规避突发环境波动、外力触碰、电磁干扰等外部因素。
11.1.4 测试前设备应完成整机装配、线路检查、参数初始化及上电预热，保持正常待机或额定工作状态，整机无硬件故障、程序报错、参数异常等问题。
11.1.5 所有测试项目均应在设备常规运行模式下开展，不得刻意关闭防护功能、修改运行参数、屏蔽异常机制以优化测试结果。
11.1.6 多批次、多台设备对比测试时，应保持所有设备运行状态、配置参数一致，保障测试条件统一。
11.1.7 测试所用仪器、仪表及试验设备应状态完好、精度达标，可精准匹配各类测试项目的检测需求。
11.1.8 测试前期应完成仪器调试、线路对接、参数校准，规范操作流程，最大限度降低人为操作误差。
11.1.9 测试设备应具备全程数据记录功能，完整留存试验过程数据、工况参数及测试结果，满足可追溯要求。
11.1.10 重复性测试、对比测试应固定配套测试设备与试验场景，杜绝测试条件偏差影响试验判定。

### 11.2 性能测试项目

11.2.1 设备应开展长时间连续运行稳定性测试，模拟工业现场 7×24 h 不间断运行工况，全程监测设备是否出现死机、无故重启、程序卡顿、进程退出等异常故障。
11.2.2 应测试设备高负载运行状态下的资源调度能力，核查 CPU、内存、存储空间的分配与调度合理性，不应出现资源溢出、进程抢占紊乱、系统卡死等问题。
11.2.3 对设备数据采集功能进行全项测试，核验数据采集精度、采集周期、响应时延、滤波去噪效果，各项性能指标应满足设备实际生产使用需求。
11.2.4 模拟正常、弱网、网络抖动等不同网络工况，应测试设备数据传输稳定性，核查数据丢包、错包、乱序等问题，保障传输质量稳定可靠。
11.2.5 针对性测试设备缓存存储、断点续传、断网补传功能，设备在网络中断、上电重启后，应保证历史数据无缺失、无重复、无错乱。
11.2.6 应测试设备数据清理、缓存迭代机制，验证临时数据自动清理、过期数据迭代更新功能正常，无资源堆积问题。
11.2.7 对设备支持的各类工业通信协议应开展一致性测试，核验协议报文格式、交互时序、校验机制、参数适配的规范性与准确性。
11.2.8 测试多协议并行运行、协议切换、跨设备跨平台对接的兼容能力，在复杂组网环境下，设备通信交互应顺畅稳定、无冲突异常。

### 11.3 安全测试项目

11.3.1 开展设备绝缘性能、接地性能、漏电防护测试，设备可触及金属部位及外壳不应存在漏电隐患，整体电气防护安全可靠。
11.3.2 模拟过压、欠压、过流、瞬时浪涌等异常电气工况，测试设备防护电路的响应能力，设备应有效自我保护，无硬件烧毁、电路击穿、功能失效等问题。
11.3.3 测试设备入网认证、身份校验、权限管控功能，非法设备接入、越权操作、匿名访问等行为应被有效拦截。
11.3.4 核查设备数据传输及本地存储的加密效果，敏感运行参数、生产数据、密钥信息不应出现明文存储、明文传输的情况。
11.3.5 模拟端口扫描、恶意报文攻击、高频非法访问等场景，测试设备抗干扰、抗攻击能力，设备应可识别并拦截异常攻击行为，留存安全日志。
11.3.6 测试设备漏洞自愈、异常恢复能力，出现轻微程序异常、链路劫持风险时，设备可自主阻断风险、恢复安全运行状态。
11.3.7 应开展防尘防水、机械振动、机械冲击测试，验证设备外壳结构、内部器件固定的可靠性，试验后无结构变形、部件松动、功能失效问题。
11.3.8 开展高低温循环、恒定湿热等环境试验，设备在极限环境工况下，核心功能应保持完整，性能无明显衰减，可正常完成数据采集与通信交互工作。

### 11.4 验收判定准则

设备出厂检验、成品验收及现场部署验收，应结合设备性能测试、安全测试、环境适应性测试的全部结果综合判定，整体验收遵循以下准则：

——设备所有安全类指标、强制性技术指标应全部合格，不允许存在不合格项，安全指标不合格直接判定验收不通过；
——设备核心运行性能、数据采集交互、通信适配对接等关键功能指标，应完全符合本文件技术要求，无功能缺失、性能不达标的问题；
——经过环境试验、稳定性试验后，设备无硬件损坏、结构失效、数据错乱、频繁异常重启等问题，可满足工业长期连续运行要求；
——设备固件功能、容错机制、安全防护、全生命周期管控功能完整可用，可正常适配电子制造生产线组网、运行与运维管理场景；
——对于不影响设备安全、核心性能及正常生产运行的轻微一般性缺陷，完成整改复检合格后，可判定设备验收通过。