ICS 35.200
CCS L 78

T/HEBQIA

团　　体　　标　　准

T/HEBQIA XXXX—2026

智能电子仪器仪表通信接口技术规范

（征求意见稿）

2026－XX－XX 发布　　2026－XX－XX 实施

河北省质量信息协会　　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。

本文件由纵揽建设发展有限公司提出。

本文件由河北省质量信息协会归口。

本文件起草单位：纵揽建设发展有限公司、耐力股份有限公司、张家口九茂建筑工程有限公司、张家口市人力资源服务行业协会、中创鼎华建设有限公司、河北磐程工程项目管理有限公司、众赢国际咨询有限责任公司、河北东方华宸建筑工程有限公司、河北嘉盛计量检测服务有限公司、张家口市韶光建设工程质量检测有限责任公司、XXXXX。

本文件主要起草人：石乐乐、王子旋、邢福海、朱长斌、任英坤、孙晓哲、李会龙、于彩连、米志刚、韩丽、高洁、张建江、李锋、张东青、李晓琦、谢军、邢翰飞、于曙光、郝翠、XXXXX。

智能电子仪器仪表通信接口技术规范

1 范围

本文件规定了智能电子仪器仪表通信接口的总体架构、接口类型、通信协议、数据传输格式规范、配置与管理、测试与验证方法和安全要求。

本文件适用于智能电子仪器仪表的设计、生产、测试及应用。

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。

GM/T 0028 密码模块安全技术要求

3 术语和定义

本文件没有需要界定的术语和定义。

4 总体架构

4.1 系统架构及功能

4.1.1 智能电子仪器仪表通信接口应包括物理层、数据链路层、网络层、传输层和应用层。

4.1.2 物理层负责定义接口的电气特性、机械特性以及数据传输的基本单元。

4.1.3 数据链路层负责帧的封装与解封装、错误检测与纠正等功能的实现。

4.1.4 网络层负责处理数据包的路由与转发，确保数据能够在复杂的网络环境中准确到达目标节点。

4.1.5 传输层负责提供端到端的可靠数据传输服务，如流量控制和拥塞避免机制。

4.1.6 应用层负责面向用户需求，定义了各种通信协议和服务，如 Modbus 和 DLT645 等专用协议。

4.2 支持的通信类型

智能电子仪器仪表通信接口应支持有线通信和无线通信两大类通信类型，有线通信主要包括RS-232、USB和以太网接口，无线通信主要包括Wi-Fi、蓝牙和ZigBee。

5 接口类型

5.1 有线通信接口应支持 RS-232 接口、USB 接口和以太网接口，RS-232 接口应采用 DB9 或 DB25 连接器，USB 接口的物理连接器应采用 Type-A、Type-B 和 Type-C 连接器，以太网接口物理连接方式应采用 RJ45 接口。

5.2 无线通信接口应支持 Wi-Fi 接口和蓝牙接口。

6 通信协议

6.1 通用通信协议应包括 Modbus 协议和 DLT645 协议
6.2 特定行业专用协议应针对特定领域的需求进行设计，应考虑环境适应性、系统复杂性和安全性要求。
6.3 自定义通信协议的设计应遵循简洁性、可扩展性和兼容性的原则。

7 数据传输格式规范

7.1 基本数据类型传输格式应包括数值型数据传输格式和字符型数据传输格式
7.2 5.2 复杂数据结构传输格式应包括数组与结构体传输格式和数据压缩与加密传输格式
7.3 数据加密应符合 GM/T 0028 的要求，采用经认证的加密算法和安全协议。
7.4 宜使用 AES-128 或 AES-256 对称加密算法对序列化后的数据包进行加密，加密密钥应通过安全密钥分发机制（如基于 PKI 体系的数字证书）进行管理，并定期轮换，避免长期使用单一密钥带来的风险。
7.5 为确保数据完整性，应在压缩与加密流程中引入哈希校验机制。宜使用 SHA-256 算法生成数据摘要，并随数据包一同传输。
7.6 通信接口应具备根据网络负载、设备算力和数据重要性动态选择压缩与加密模式的能力。
7.7 复杂数据结构传输格式应符合表 1 的要求。

表 1 复杂数据结构传输格式

应用场景	序列化格式	压缩算法	加密算法	安全协议
实时传感器数据上传	JSON	LZ4	AES-128	TLS 1.3
设备配置信息同步	XML	gzip	AES-256	TLS 1.2
固件远程升级	JSON（二进制封装）	ZIP	SM4	TLS 1.3+数字签名
医疗仪器数据传输	JSON	Snappy	AES-256	TLS 1.3+HMAC

8 配置与管理

8.1 配置方式

智能仪表应支持以下至少两种配置方式：
a) 本地配置：通过按键、LCD 菜单或 USB 工具；
b) 远程配置：通过 Web 页面、上位机软件或 API；
c) 自动配置：通过 DHCP Option、Zeroconf 或云平台下发。

8.2 参数管理

关键参数应包括：
a) 通信地址/ID ；
b) 波特率、数据位、校验位；
c) IP 地址、子网掩码、网关；
d) 服务器地址（MQTT Broker、OPC UA Server）；
e) 采样周期、上报间隔；
f) 报警阈值。
所有参数应支持保存至非易失存储器（EEPROM/Flash）。

8.3 日志与诊断

8.3.1 应记录通信错误、认证失败、配置变更等事件。
8.3.2 日志容量应≥100 条，支持循环覆盖。
8.3.3 应支持通过接口导出日志（CSV/JSON 格式）。

9 测试与验证方法

9.1 测试环境搭建

9.1.1 硬件测试环境

测试硬件环境应包含以下基本组件：

a) 测试主机：配备标准通信接口（USB、以太网、RS-232/485 等）；
b) 被测设备：智能电子仪器仪表原型或成品；
c) 接口转换器：用于不同物理层接口的转换；
d) 信号发生器：用于模拟各种输入信号；
e) 负载设备：用于模拟实际工作环境。

9.1.2 软件测试环境

9.1.2.1 测试管理软件应支持自动化测试用例执行。
9.1.2.2 协议分析工具应用于捕获和分析通信数据包。
9.1.2.3 性能监控工具应实时监测系统资源使用情况。
9.1.2.4 日志分析系统应收集和分析测试过程日志。

9.2 功能测试

9.2.1 基础通信功能测试

9.2.1.1 测试项目应包括：
a) 接口初始化和配置测试；
b) 数据发送和接收功能验证；
c) 连接建立和断开测试；
d) 多设备并发通信测试。
9.2.1.2 测试方法：通过测试主机向被测设备发送标准测试数据包，验证设备是否能够正确接收、处理并返回预期响应。测试应覆盖正常数据、边界数据和异常数据三种情况。

9.2.2 数据格式验证测试

9.2.2.1 测试内容应包括：
a) 基本数据类型传输正确性；
b) 复杂数据结构序列化/反序列化；
c) 数据压缩与解压缩功能；
d) 加密与解密功能验证。
9.2.2.2 验证方法：使用预定义的测试数据集，通过对比发送前和接收后的数据内容，验证数据在传输过程中的完整性和正确性。

9.3 性能测试

9.3.1 传输性能测试

9.3.1.1 测试指标应包括：

a) 吞吐量：单位时间内可传输的数据量（Mbps）；
b) 延迟：数据从发送到接收的时间延迟（ms）；
c) 丢包率：在特定负载下的数据包丢失比例；
d) 重传率：需要重传的数据包比例。

9.3.1.2 测试场景应包括：

a) 低负载场景（＜30%带宽利用率）；
b) 中等负载场景（50%～70%带宽利用率）；
c) 高负载场景（＞90%带宽利用率）。

9.3.2 资源占用测试

9.3.2.1 资源占用测试应包括：

a) CPU 占用率：通信处理过程中的 CPU 使用情况；
b) 内存占用：通信缓冲区和协议栈的内存使用；
c) 功耗测试：不同通信模式下的设备功耗。

9.4 兼容性测试

9.4.1 跨平台兼容性

测试设备应在不同操作系统平台（Windows、Linux、macOS）和不同硬件平台下的通信兼容性。

9.4.2 协议版本兼容性

应验证设备对不同版本通信协议的向下兼容能力，确保新旧设备之间的互操作性。

9.5 可靠性测试

9.5.1 长时间运行测试

应测试连续运行72小时以上的稳定性，监测系统在长时间运行过程中的性能衰减和故障发生情况。

9.5.2 异常恢复测试

应模拟各种异常情况（网络中断、电源波动、信号干扰等），测试系统的故障检测和自动恢复能力。

9.5.3 安全性测试

安全性测试应包括：数据加密强度验证、密钥管理安全性、防重放攻击能力和权限控制机制。

9.6 测试用例设计

9.6.1 正向测试用例

应验证系统在正常工作条件下的功能正确性，包括标准数据传输、正常连接建立等场景。

9.6.2 反向测试用例

应测试系统在异常条件下的处理能力，包括：非法数据格式输入、超时重传机制、错误校验码处理和非法指令响应。

9.7 测试结果评估

9.7.1 通过标准

通过测试的标准为：

a) 所有正向测试用例 100%通过；
b) 反向测试用例按预期处理异常；
c) 性能指标达到设计要求；
d) 无严重级别以上的缺陷。

9.7.2 缺陷管理

应建立缺陷跟踪系统，记录缺陷的发现时间、严重程度、修复状态和验证结果。

10 安全要求

10.1 通信安全

通信安全要求如下：

a) 无线通信应启用加密（WPA2/WPA3、TLS、DTLS）；
b) 有线通信在敏感场景下应支持 TLS（如 Modbus TCP over TLS）；
c) 不应使用明文传输密码或密钥。

10.2 身份认证

身份认证要求如下：

a) 应支持用户名/密码认证（密码应哈希存储）；
b) 应支持数字证书认证（X.509）；
c) 默认出厂密码不应为弱口令（如 123456、admin），且首次登录强制修改。

10.3 访问控制

应实现基于角色的访问控制（RBAC）：

a) 观察者（只读）；
b) 操作员（读写参数）；
c) 管理员（配置网络、固件升级）。

应支持 IP 白名单限制。

10.4 固件安全

固件安全要求如下：

a) 固件升级包应数字签名；
b) 应支持安全启动（Secure Boot）机制（鼓励）；
c) 升级过程应支持断点续传与回滚。