ICS 35.240.50
UNSPSC 43.22.26
CCS R 80

团 体 标 准

T/UNP 332—2024

工业智能网关通讯系统技术要求

Technical requirement for industrial intelligent gateway communication system

2024－11－28 发布 2024－11－28 实施

中国联合国采购促进会 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。

本文件由武汉登辰科技有限公司提出

本文件由中国联合国采购促进协会归口。

本文件起草单位：武汉登辰科技有限公司、武汉力控控制科技有限公司、杭州乐芯科技有限公司、武汉楚林数字科技有限公司、武汉湘君机电制造有限公司。

本文件主要起草人：仪忠江、袁涛、黄滔、王志勇、雷鸣。

引　言

为助力中国企业参与国际贸易，推动企业高质量发展，中国联合国采购促进会依托联合国采购体系，制定服务于国际贸易的系列标准，这些标准在国际贸易过程中发挥了越来越重要的作用，对促进贸易效率提升，减少交易成本和不确定性，确保产品质量与安全，增强消费者信心具有重要的意义。

联合国标准产品与服务分类代码（UNSPSC，United Nations Standard Products and Services Code）是联合国制定的标准，用于高效、准确地对产品和服务进行分类。在全球国际化采购中发挥着至关重要的作用，它为采购商和供应商提供了一个共同的语言和平台，促进了全球贸易的高效、有序发展。

围绕UNSPSC进行相关产品、技术和服务团体标准的制定，对助力企业融入国际采购，提升国际竞争力具有十分重要的作用和意义。

本文件采用UNSPSC分类代码由6位组成，对应原分类中的大类、中类和小类并用小数点分割。

本文件UNSPSC代码为“43.22.26”，由3段组成。其中：第1段为大类，“43”表示“信息技术广播和电信”，第2段为中类，“22”表示“数据、语音或多媒体网络设备或平台及配件”，第3段为小类，“26”表示“网络服务设备”。

工业智能网关通讯系统技术要求

1 范围

本文件规定了工业智能网关通讯系统的系统架构、功能要求、性能要求、数据要求、安全要求、接口要求、运维要求和评价与改进。

本文件适用于工业智能网关通讯系统的设计、开发、应用及维护。

2 规范性引用文件

本文件没有规范性引用文件。

3 术语、定义和缩略语

3.1 术语和定义

下列术语和定义适用于本文件。

3.1.1

底层工业现场 lower-level industrial field

实际的工业生产环境中最基础的操作层面。

3.1.2

采集接口 acquisition interface

工业智能网关通讯系统用于底层工业现场设备收集数据的通道。

3.1.3

上层业务应用 upper-level business applications

基于工业生产数据进行业务处理和功能实现的各类应用程序或系统。

3.1.4

南向接口 southbound interface

工业智能网关通讯系统提供给底层工业现场设备的接口（通常指采集接口）。

[来源：GB/T 30269.901—2016，3.3，有修改]

3.1.5

北向接口 northbound interface

工业智能网关通讯系统提供给上层业务应用和资源管理系统的接口（通常指转发接口）。

[来源：GB/T 30269.901—2016，3.2，有修改]

3.2 缩略语

下列缩略语适用于本文件。

MTBF：平均无故障工作时间（Mean Time Between Failures）

MAC：媒体接入控制（Media Access Control）

QoS：服务质量（Quality of Service）

WSN：无线传感器网络（Wireless Sensor Network）

4 系统架构

工业智能网关通讯系统架构包括应用层、支撑层、网络层、硬件层、运维层、接口层和安全层，其中应用层包括实时数据监控、设备接入、协议转换、数据传输、远程访问、系统设备信息管理、云组态、系统配置、报警记录、断电自恢复等功能，系统框架图见图1。

图 1　工业智能网关通讯系统架构图

各功能模块功能如下：

a) 应用层：包括实时数据监控、设备接入、协议转换、数据传输、远程访问、系统设备信息管理、云组态、系统配置、报警记录、断电自恢复；
b) 运维层：负责系统的日常管理、应急响应、监控等运维工作；
c) 支撑层：提供操作系统、数据库、中间层等支撑，保障系统正常运行；
d) 网络层：实现底层工业现场设备和上层业务应用系统之间的通信连接，支持数据传输；
e) 硬件层：为工业智能网关通讯系统提供物理基础，包括各类硬件设备；
f) 接口层：包括南向接口、北向接口和其他接口，用于与底层工业现场设备、上层业务应用系统及外接设备进行连接和交互；
g) 安全层：保障工业智能网关通讯系统的接入安全、访问控制、攻击防护、安全审计等安全需求。

5　功能要求

5.1　实时数据监控

实时数据监控要求如下：

a) 监控点可移动到不同分组中；
b) 数据可实时监控并修改，监控实时数据点为 20 个～300 个。

5.2　设备接入

工业智能网关通讯系统应支持多种接口、多种采集协议与工业现场设备互联，传送设备命令、获取设备状态和设备数据。工业智能网关通讯系统数据采集应根据有线方式和无线方式等进行设计。

5.3　协议转换

协议转换要求如下：

a) 应具备将来自不同感知控制设备的不同接入协议转换至同一种约定协议的功能，通过北向接口完成数据的上报；

b） 应具备将来自北向接口的协议转换成不同类型协议的功能，通过南向接口连接至相应的感知控制设备完成设备的控制。

5.4 数据传输

工业智能网关通讯系统应支持底层工业现场设备和上层业务应用系统之间的通信连接，并支持传输数据。

5.5 远程访问

工业智能网关通讯系统应支持APP远程访问。

5.6 系统设备信息管理

应支持对自身的本地信息进行管理，工业智能网关通讯系统设备自身信息包括但不限于：

a） 登录信息；
b） 操作记录；
c） 外部攻击记录；
d） 电源管理；
e） 软件升级。

5.7 云组态

云组态功能如下：

a） 集中监控：可进行新增分组、编辑分组、新建工程、编辑工程等操作；
b） 权限管理：可进行分配工程以及设置组态权限等操作。

5.8 系统配置

工业智能网关通讯系统配置要求如下：

a） 工业智能网关通讯系统应支持远程配置管理；
b） 应对工业智能网关通讯系统的 WSN 网络侧接口进行配置，包括物理层参数、MAC 层参数、业务调度与 QoS 参数、宽带等；
c） 当网络结构发生改变时，工业智能网关通讯系统应自动更新；
d） 工业智能网关通讯系统具备 VLAN、帧过滤等以太功能时，应对其进行配置；
e） 工业智能网关通讯系统具备加密功能时，应对密码协议和参数进行设置；
f） 工业智能网关通讯系统宜具备对已配置的信息进行数据预览功能，及对配置的采集、计算、转发等运行情况及主要资源使用和占用情况进行查看的功能。

5.9 报警记录

报警记录要求如下：

a） 支持查看当前报警记录及历史报警记录，报警消息通知可通过短信、邮件、APP 推送等方式收取到信息；
b） 监控报警数据点为 20 个～300 个；
c） 工业智能网关通讯系统设备发生故障时，系统应立即报警。

5.10 断电自恢复

工业智能网关通讯系统应在断电恢复后5 s内恢复原设置并正常使用。

6 性能要求

6.1 可靠性

无故障工作时间（MTBF）应至少达到500000 h。

6.2 系统报警响应时间

从案发到主站接收报警信息所需要的时间不应大于30 s。

7 数据要求

7.1 通用数据配置

工业智能网关通讯系统通用数据配置满足要求如表1所示。

表 1 工业智能网关通讯系统通用数据配置要求

序号	数据名称	配置要求	说明
1	网关基本信息	必配，且只出现一次	包括网关配置数据结构的版本号、网关标识、网关描述、网关厂家、网关型号、网关软硬件版本号等
2	物理端口参数	必配，可出现多次	包括接口标识、接口类型和共享标志等
3	数据解析协议参数	必配，可出现多次	包括协议标识、版本号、描述信息、设备连接参数等。不同数据解析协议包括不同数据项寻址信息、数据项格式信息等
4	协议解析器参数	必配，可出现多次	包括标识、版本号、描述信息、参数表、适用的接口类型列表和支持的数据解析协议列表等
5	设备参数	必配，可出现多次	包含设备的名称、类型、型号、生产厂家、设备编号等

7.2 数据采集

7.2.1 工业智能网关通讯系统的数据采集速率、采集转发周期、并发接入、数据融合、协议数量、缓存容量、点容量应满足实际应用场景需求，支持数据稳定的采集、处理、转发，支撑上层业务应用系统的正常运行。

7.2.2 工业智能网关通讯系统的点容量分级如表 2 所示，宜达到 C2 级别。

表 2 点容量性能分级

数据采集性能等级	点容量（NC）
C1	0＜NC≤100
C2	100＜NC≤1000
C3	1000＜NC≤5000
C4	5000＜NC≤10000
C5	NC＞10000

7.3 加密传输机制

工业智能网关通讯系统加密传输机制要求如下：

a) 支持 DES、3DES 等多种加密方式；
b) 具备 MAC 地址过滤功能；
c) 支持 WPA 加密规则。

7.4 历史数据

历史数据要求如下：

a) 在历史数据中，支持根据需求选用列表或曲线形式查看详细信息；
b) 监控历史数据点数为 20 个～100 个；
c) 历史数据保存天数为 60 天/100 万条或 90 天/100 万条或 180 天/100 万条。

8 安全要求

8.1 接入安全

工业智能网关通讯系统应对接入的底层工业设备进行认证，保证接入设备标识的唯一性，并能通过网络标识、MAC地址或口令等手段对接入设备进行身份鉴别。

8.2 访问控制

访问控制要求如下：

a) 工业智能网关通讯系统应对用户访问进行控制，能控制系统和数据的本地或远程 APP 访问，对支持远程配置的工业智能网关通讯系统应提供控制访问权限、增加现场确认、增设物理开关等安全措施；

b) 工业智能网关通讯系统的用户应有唯一标识，支持通过用户名和密码进行身份鉴别。采用用户名和密码认证的密码的长度应不少于 8 个 ASCII 字符，并由数字、字符和特殊符号组成。

8.3 攻击防护

工业智能网关通讯系统受到攻击时，宜能自动记录攻击的发起地址、攻击时间及攻击类型等关键信息，生成报警信息，工业智能网关通讯系统宜支持口令破解、恶意扫描探测等攻击防护功能。

8.4 安全审计

生成审计记录（记录应包含事件发生的时间、事件类型和主体身份），对审计数据按权限进行分级访问控制。

8.5 数据处理

工业智能网关通讯系统宜提供感知控制设备接入数据的预处理、边缘处理和储存的功能（细化）。

9 接口要求

9.1 南向接口

工业智能网关通讯系统应具备提供给底层工业现场设备的南向接口，如I/O端口、RS232/485/422串口、网口、无线接口、CAN等。

9.2 北向接口

工业智能网关通讯系统应具备提供给上层业务应用系统的北向接口，如以太网口、无线接口（包括2G/3G/4G/5G、Wi-Fi）等。

9.3 其他接口

工业智能网关通讯系统应具备用于连接外接设备所需的相关接口，如USB端口、TF口、供电口或冗余电口、调试口等。

10 运维要求

10.1 日常管理

日常管理要求如下：

a) 应制定工业智能网关通讯系统更新计划和策略，定期更新系统软件版本；

b) 在制定系统更新策略时，考虑用户（包括工业现场操作人员、系统维护人员等）的使用习惯和业务需求，减少更新对用户操作流程和业务连续性的影响。更新前，要进行测试和验证，确保新功能在工业网络环境下的稳定性和与现有设备、系统的兼容性，避免因更新导致通信中断或数据错误等问题；

c) 设立专门的用户培训部门，为用户提供培训和支持服务。制作并提供在线帮助文档和视频教程，培训内容涵盖系统的基本操作方法（如网关的配置、参数调整等）、功能介绍（各种通信协议转换、数据采集与传输功能等）、常见问题解决（如连接故障、数据丢失问题的处理）等方面，帮助用户熟练掌握系统的使用和维护；

d) 建立版本管理制度，管理系统各个版本，确保不同版本在工业现场的部署和使用过程中的版本控制和一致性，避免因版本混乱导致的通信异常或安全隐患。

10.2 应急响应

应急响应要求如下：

a) 制定应急响应计划，包括安全事件（如网络攻击、设备故障影响通信等）的报告、响应和恢复流程，划分在紧急情况下各部门和人员的职责与操作步骤，确保应急处理有序进行；
b) 制定安全事件处理方法，涉及事件的调查、分析、处理和恢复等环节。在处理安全事件时，遵循“先恢复业务，后查找原因”的原则；
c) 定期进行安全演练和应急演练，提高系统管理人员和操作人员的应急响应能力；
d) 安全演练和应急演练应具有针对性和实战性，根据工业智能网关通讯系统的实际运行情况和可能遇到的安全风险（如工业环境中的电磁干扰、网络攻击类型等）进行设计，使演练场景贴近真实情况；
e) 对安全演练和应急演练进行总结和评估，及时发现演练过程中暴露出的问题（如应急流程不畅、人员操作不熟练等）并进行改进，不断完善应急响应机制。

10.3 监控要求

10.3.1 服务器监控

10.3.1.1 系统应能自动监控服务器的最大连接数和连接时间，及时发现服务器的负载情况和潜在问题。
10.3.1.2 监控系统应能实时显示服务器的连接数、连接时间、CPU 使用率、内存使用率等关键指标，便于系统管理人员及时采取措施进行调整和优化。
10.3.1.3 具备切断无效连接的功能，当服务器连接数达到一定阈值或连接时间过长时，系统应能自动切断无效连接，释放服务器资源，确保系统的稳定性和性能。
10.3.1.4 应根据实际情况调整和优化切断无效连接的策略，避免对正常用户的使用造成影响。

10.3.2 性能监控

10.3.2.1 对系统的性能指标进行实时监控和分析。
10.3.2.2 性能监控应具有预警功能，系统性能指标超过预设的阈值时，应及时发出预警信息，通知系统管理人员进行处理，预警信息应包括问题的具体描述、影响范围以及建议的处理方法等方面，便于系统管理人员快速做出响应。

10.3.3 日志监控

10.3.3.1 系统的日志应进行实时监控和分析，生成日志报表。
10.3.3.2 日志监控应包括系统日志、应用日志等方面。
10.3.3.3 日志监控应具有搜索和过滤功能，便于系统管理人员能快速查找特定的日志信息。

11 评价与改进

依据第5章～第10章的要求确定系统的评价内容，定期开展系统功能、性能、数据、安全、接口、运维方面的评价，审查不合格项，并有针对地采取纠偏措施。

参 考 文 献

[1] GB/T 22239—2019 信息安全技术网络安全等级保护基本要求
[2] GB/T 28827.1—2022 信息技术服务运行维护 第1部分：通用要求
[3] GB/T 30269.901—2016 信息技术 传感器网络 第901部分：网关：通用技术要求
[4] GB/T 35273—2020 信息安全技术个人信息安全规范