《基于人工智能的工业协议解析技术应用指南》

团体标准编制说明

一、任务来源

《国务院关于深入实施“人工智能+”行动的意见》（国发〔2025〕11 号）、《“人工智能+制造”专项行动实施意见》（工信部联科〔2025〕279 号）等国家政策文件，明确提出深化人工智能与制造业深度融合、健全工业领域安全标准体系、鼓励依托产学研用力量制定团体标准的工作要求，为工业人工智能应用及工业网络安全标准化建设划定发展方向。

当前，人工智能等技术快速迭代，为工业协议智能解析提供了坚实技术支撑，但行业仍缺乏统一的技术规范、应用流程与实施准则，亟需建立标准化指导文件规范技术落地与工程应用。为响应国家政策部署，夯实人工智能+工业领域安全保障底座，落实标准化引领产业高质量发展的工作目标，由北京信联数安科技有限公司牵头，联合北京邮电大学、信联科技（南京）有限公司、北京明博信安信息技术有限公司、华夏宏源（北京）科技有限公司、工信君阳（北京）科技有限公司等产学研用相关单位，共同提出并组织编制团体标准《基于人工智能的工业协议解析技术应用指南》，为人工智能技术在工业协议解析领域应用提供标准化指导。

二、制定规范的必要性和意义

制定《基于人工智能的工业协议解析技术应用指南》（以下简称本标准）对于推动人工智能与工业安全领域的深度融合、提升工业安全防护水平具有重要意义，具体表现如下：

1. 在技术层面，它将促进人工智能应用于工业协议解析技术的标准化与成熟化，降低对私有、非标准工业协议的信息获取门槛，提升工业控制系统漏洞发现与防御的主动能力。

2. 在行业层面，标准有助于统一工业协议解析标准，推动设备厂商、安全企业和研究机构协作，形成开放共享的工业协议安全生态。

3. 在安全实践层面，指南可为关键基础设施运营方提供可操作的技术参考，

助力构建基于协议深度感知的防护体系，从而有效应对日益复杂的工业网络攻击，保障生产运行的连续性与稳定性，助力国家工业信息安全保障体系的完善。

制定和推行本标准的主要目的是指导基于人工智能的工业协议解析框架建设以及多种协议解析机制的应用，包括：

1.构建基于人工智能的工业协议解析技术应用框架

确立“多种工业协议载体输入→协议载体智能解析→工业协议特征输出”的技术应用框架，实现面向协议规范、流量数据、固件的智能解析。

2.多种协议载体的智能解析方法

描述面向协议规范的智能解析方法（第 7 部分）、面向网络流量的智能解析方法（第 8 部分）以及面向二进制程序的智能解析方法（第 9 部分），为相关系统或模块的设计、开发、测试提供指导。

三、主要编制过程

1.第一阶段，成立规范研制起草工作组（以下简称工作组）编制项目立项材料和标准草案。工作组由 15 名相关专家和专业人员组成，来自北京信联数安科技有限公司、联合北京邮电大学、信联科技（南京）有限公司、北京明博信安信息技术有限公司、华夏宏源（北京）科技有限公司、工信君阳（北京）科技有限公司等单位。工作组通过查阅文献，形成理论框架和工作方法，并对已有相关内容基础进行了梳理，多轮研讨沟通，形成立项申请材料和标准草案。工作组内部多次召开立项准备沟通会，为项目立项制定完整方案。

2.第二阶段，项目立项评审。工作组于 2026 年 3 月 18 日在中关村知识产权大厦 A 座，北京软件和信息服务业协会 210 会议室召开了项目立项专家评审会。评审专家包括：中国电子工业标准化技术协会高级工程师陈庆帅、中国矿业联合会智能矿山专委会副主任委员种国双、中国信通院人工智能研究所高级工程师李荪、北京航空航天大学软件学院教授王宝会、中国仿真学会工业互联网与智能系统专业委员会委员战天明。标准立项通过专家评审后，信息在全国团体标准信息平台和协会官方网站和北京软协官网发布。

3.第三阶段，编写规范征求意见稿。围绕标准草案及各方意见，工作组开展了进一步调查研究，通过多轮内部研讨和标准内容文件修订，形成征求意见稿，并提交北京软协开始征求意见。

四、制定规范的原则和依据，与现行法律、法规、标准的关系

本标准的制定是促进人工智能与工业融合、推动工业私有协议智能解析能力、提升工业网络安全防护的关键举措。其制定工作并非从零开始，而是在国家现有的法律法规、政策指导和标准体系的坚实基础上进行深化与细化。

（一）标准制定应遵循的核心原则

制定该标准时，应首先确立其核心指导原则，确保标准兼具开放性、前瞻性、实用性与合规性。

1.统筹规划与业务驱动原则

立足人工智能与工业融合发展总体布局，紧扣工业控制系统安全、工业互联网互联互通、私有协议解析等实际业务需求，以解决工业现场协议不透明、解析效率低等痛点为导向，统筹技术路径、应用场景与实施流程，确保标准内容贴合政策要求、产业实际，支撑工程落地。

2.合规性优先原则

严格遵守国家网络安全、数据安全、个人信息保护、人工智能监管、工业控制系统安全等相关法律法规，全面对标国家与行业标准，坚守安全底线；在协议数据采集、处理、存储、应用全流程落实安全与隐私保护要求，确保标准应用合法合规。

3. 技术先进性与实用性兼顾原则

充分吸纳人工智能大模型、机器学习、流量分析、二进制解析等前沿技术成果，保持标准前瞻性与技术引领性；同时立足工业现场可靠性、稳定性要求，简化实施门槛、明确可操作步骤，兼顾技术先进性与工程实用性，便于企业理解、实施与验收。

4.可持续发展与迭代优化原则

充分考虑人工智能技术快速迭代、工业协议持续更新的特点，采用模块化、可扩展架构设计，预留技术升级与场景扩展空间；建立标准实施反馈与动态修订机制，适配新技术、新场景、新需求，实现标准可持续演进。

（二）标准制定的主要依据

1.国家政策依据

《国务院关于深入实施“人工智能+”行动的意见》：提出要深入实施“人

工智能+”行动，推动人工智能与经济社会各行业各领域广泛深度融合，重点推进工业全要素智能化发展。

《“人工智能+制造”专项行动实施意见》：提出要强化标准引领，攻关智能终端安全测评等关键技术，筑牢应用赋能安全保障。

《工业控制系统网络安全防护指南》：提出应对重要工业控制系统定期开展漏洞排查并及时发现和预警系统漏洞。

《关键信息基础设施安全保护条例》：提出应对关键基础设施开展网络安全监测、检测和风险评估等。

2.国家与行业标准依据

1.GB/T 36323-2018《信息安全技术 工业控制系统安全管理基本要求》对工业协议测评进行了多项要求，如信息系统、系统组件及系统服务的开发者应制定并实施安全评估计划，针对相关的功能属性、外部可见接口、顶层设计、底层设计、系统硬件、源代码等进行安全测评；应在 ICS 系统上线前、系统维修期间或非业务高峰期对指定系统及相关应用程序进行脆弱性扫描分析，标识并报告可影响该系统或应用的新漏洞。这些要求也为本标准提供了应用需求。

（三）与现行法律、法规、标准的关系

本标准的定位是应用指南标准，其与现行体系的关系可概括为“遵循、细化、互补”。

1. 对上层法律与法规的遵循与细化

本标准是法律法规在工业防护领域的具体化。法律法规定义了“什么不能做”和“必须遵守的原则”，而本标准则详细规定了“应该如何做”才能符合这些原则。

2. 对现有标准的遵循与补充

本标准在遵循现有标准的基础上，重点解决人工智能+工业协议解析方向面临的新兴挑战和空白领域，充分发挥补充和创新作用。

五、主要条款的说明，主要技术指标、参数、试验验证的论述

本文件给出了基于人工智能的工业协议解析技术的总体原则、应用框架以及面向协议规范、网络流量、二进制程序进行协议解析的应用指南。本文件适用于指导工业协议智能分析相关系统或功能模块的设计、开发与测试。

主要技术内容包括：

第 1 部分：总体原则。明确了工业协议解析的核心底线，要求在保证通用协议与私有协议格式、字段、交互流程准确解析的基础上，严格满足工业场景误检率、漏检率要求，同时对工业敏感数据实施全流程安全保护，确保数据不泄露、不篡改、不丢失。

第 2 部分：应用框架。构建了输入层、解析层、输出层三位一体的技术体系，输入层覆盖协议规范文档、工业流量、二进制文件三类数据源，解析层依托人工智能算法与大模型实现三种协议载体的智能解析，输出层统一形成协议消息格式、字段定义、交互流程等结构化结果，为全场景解析提供统一技术架构。

第 3 部分：协议规范解析。针对非结构化协议文档，依次规范文本清洗、结构化分块、数据标注、协议规约提取、结果验证五大环节，实现从协议手册中自动提取结构化规约信息，并通过人工与自动化双重验证保障解析结果准确可信。

第 4 部分：网络流量解析。面向无文档私有协议流量，明确流量去噪过滤、报文聚类、协议规约提取、结果验证流程，通过特征聚类、字段边界分析、时序与状态机建模实现盲流量逆向解析，满足工业现场未知协议识别需求。

第 5 部分：二进制程序解析。针对无文档、无流量的黑箱程序，通过汇编还原、通信函数定位、协议规约提取、结果验证，从固件与程序中逆向还原协议格式与交互逻辑，覆盖工业协议解析复杂的应用场景。

六、重大意见分歧的处理依据和结果的说明

本规范研究制定过程中未出现重大分歧。

七、采用国际标准或国外先进标准程度的说明，以及国内、外同类产品或标准的对比情况

（一）采用国际标准或国外先进标准程度的说明

不涉及

（二）国内外同类标准和技术状况

1. 国内外同类标准状况

目前国内外结合人工智能实现工控协议解析及应用尚无明确标准。相关标准如 GB/T 19582-2008《基于 Modbus 协议的工业自动化网络规范》、GB/T 37399-2019《工业自动化系统与集成 OPC 统一架构 第 1 部分：概览和原则》、

IEC TR 62541-1:2020 OPC Unified Architecture - Part 1: Overview and concepts、GB/T 38775.10-2025《电动汽车无线充电系统 第 10 部分：通信协议一致性测试》、GB/T 28847.6-2023《建筑自动化和控制系统 第 6 部分：数据通信协议一致性测试》、GB/T 26796.2-2011《用于工业测量与控制系统的 EPA 规范 第 2 部分：协议一致性测试规范》，主要聚焦工控协议编码规范及协议一致性测试方法，在协议规范、对比验证等方面可以为本标准提供技术指导。

2. 国内外技术状况

当前，国内外在工业协议解析与应用领域的技术发展呈现出需求迫切但发展不均衡的态势。在协议解析方面，部分研究机构与安全企业已开始探索将机器学习、深度学习等人工智能技术应用于网络流量序列分析、协议字段自动聚类与语义标注，并在特定私有协议的逆向工程中取得初步成果；然而，整体上仍严重依赖专家经验与手工分析，自动化、智能化的通用解析工具平台尚不成熟，且对二进制程序进行深度协议提取的技术能力较为薄弱。总体而言，当前技术实践呈现点状突破，亟需通过标准引导整合技术资源，推动形成协同发展的产业生态。

八、实施标准的措施建议

标准正在征求意见阶段，鼓励相关企业积极参与本标准的意见反馈工作。

九、其他说明

无。

附件：标准立项意见汇总处理表

《基于人工智能的工业协议解析技术应用指南》标准工作组

2026 年 5 月 7 日

标准立项意见汇总处理表

标准项目名称：《人工智能 工业协议解析及应用指南》
标准项目负责起草单位：北京信联数安科技有限公司

2026 年 3 月 19 日填写

序号	标准章条编号	意 见 内 容	提出单位（或个人）	处理意见	备注
1	标题	建议修改标准名称，应聚焦协议解析而非人工智能	中国信通院李荪、中国电子工业标准化技术协会陈庆帅、北航王宝会	采纳	修改为《基于人工智能的工业协议解析技术应用指南》
2	1 范围	范围需要明确，不用写成技术规范书的样式	中国信通院李荪	采纳	
3	2 规范性引用文件	应按实际引用情况进行补充	中国矿业联合会智能矿山专委会种国双	采纳	
4		需考虑解析过程中的数据安全	中国矿业联合会智能矿山专委会种国双	采纳	
5		应明确 AI 技术的实时性、兼容性对工业控制系统的要求及影响	北航王宝会	采纳	
6		应用图的形式对应用框架进行描述	北航王宝会、中国信通院李荪、中国电子工业标准化技术协会陈庆帅	采纳	
7	第 6 部分	应明确私有协议的范围，避免出现技术壁垒	中国仿真学会工业互联网与智能系统专业委员会占天明	采纳	
8	第 6 部分	应调整反编译的说法，规避法律风险	北航王宝会、中国仿真学会工业互联网与智能系统专业委员会占天明	采纳	

本征求意见中共 8 条，其中采纳的是 8 条，不采纳的是 0 条，部分采纳是 0 条。