融合国密算法的工控协议动态自适应加固体系设计

王　蕊[1,2]，徐志浩[1,2]，董良遇[1,2]
（1. 国家工业信息安全发展研究中心，北京　100040；
2. 工业信息安全感知与评估技术工业和信息化部重点实验室，北京　100040）

摘　要：针对工业互联网融合背景下工控协议安全缺陷突出、防护能力不足的问题，开展工控协议安全分析与加固体系研究。通过剖析典型工控协议架构与通信机制，明确协议安全短板，揭示协议层攻击路径与危害机理。突破传统单点防御局限，提出融合国密算法、人机协同逆向与动态自适应加固的方案，构建覆盖协议解析、漏洞检测、主动防御的全生命周期防护体系。实验验证表明，该方案可显著提升攻击拦截与漏洞防御能力，兼顾实时性与兼容性。研究成果可为工控协议安全检测、漏洞挖掘及加固落地提供技术支撑，助力提升关键信息基础设施抗攻击能力。

关键词：工控协议；协议逆向分析；安全加固；国密 SM9；动态防御
中图分类号：TP309　　**文献标志码：**A　　**DOI：**10.19358/j.issn.2097-1788.2026.06.002

中文引用格式：王蕊，徐志浩，董良遇. 融合国密算法的工控协议动态自适应加固体系设计[J]. 网络安全与数据治理，2026，45(6)：9-16.
英文引用格式：Wang Rui，Xu Zhihao，Dong Liangyu. Design of dynamic adaptive reinforcement system for industrial control protocols integrated with national cryptographic algorithms[J]. Cyber Security and Data Governance，2026，45(6)：9-16.

Design of dynamic adaptive reinforcement system for industrial control protocols integrated with national cryptographic algorithms

Wang Rui[1,2]，Xu Zhihao[1,2]，Dong Liangyu[1,2]
（1. China Industrial Control Systems Cyber Emergency Response Team，Beijing 100040，China；
2. Key Laboratory of Industrial Information Security Perception and Evaluation Technology，
Ministry of Industry and Information Technology，Beijing 100040，China）

Abstract：Aiming at the prominent security defects and insufficient protection capability of industrial control protocols under the integration of the industrial internet，this paper conducts research on security analysis and reinforcement system of industrial control protocols. By analyzing the architecture and communication mechanisms of typical industrial control protocols，the security shortcomings are identified，and the attack paths and damage mechanisms at the protocol layer are revealed. Breaking through the limitations of traditional single-point defense，a scheme integrating national cryptographic algorithms，human-machine collaborative reverse engineering and dynamic adaptive reinforcement is proposed，constructing a full-life-cycle protection system covering protocol parsing，vulnerability detection and active defense. Experimental verification shows that the proposed scheme can significantly improve attack interception and vulnerability defense performance while ensuring real-time performance and compatibility. The research results can provide technical support for security detection，vulnerability mining and reinforcement implementation of industrial control protocols，and help enhance the attack resistance of critical infrastructure.

Key words：industrial control protocol；protocol reverse analysis；security hardening；national cryptography SM9；dynamic defense

0　引言

随着工业 4.0 与智能制造的快速推进，工业控制系统（Industrial Control System，ICS）正逐步打破封闭运行模式，实现 OT 网络与 IT 网络、互联网的深度融合。工控协议作为设备间指令交互、数据传输的核心载体，其安全边界不断模糊。不同于传统网络协议追求大带宽、广覆盖的特点，工控协议的设计初心更聚焦于高实时性、高可靠性与强抗干扰性，但却忽视了

安全防护机制的构建，导致传统工控协议，例如 Modbus、分布式网络协议 3（Distributed Network Protocol 3，DNP3）等存在先天安全缺陷[1]。同时，工业领域中大量私有工控协议因缺乏统一的设计规范与公开文档，其协议格式、字段语义的不透明性为漏洞挖掘与攻击实施提供了可乘之机[2]。

2025 年，美国网络安全和基础设施安全局（Cybersecurity and Infrastructure Security Agency，CISA）累计发布 ICS 相关网络安全官方通告超 340 份，其中高危/致命漏洞占比超 55%，大量漏洞可实现远程代码执行、系统接管、权限提升，覆盖施耐德、西门子、罗克韦尔等头部厂商核心产品，攻击者可通过协议漏洞实现远程代码执行、系统接管等恶意操作，波及能源、制造、水处理等关键信息基础设施领域[3]。这些事件充分暴露了工控协议安全防护的紧迫性，也凸显了对工控协议进行深度分析与创新加固的重要意义。现有工控协议研究主要分为协议逆向分析与安全加固两类。协议逆向分析以报文序列分析为主，对系统影响较小，但字段语义推断精度低、私有协议适配性不足[4]。安全加固多采用安全传输层协议（Transport Layer Security，TLS）加密、访问控制等被动防御手段，实时性适配差，难以抵御零日漏洞与未知攻击，且国密算法融合应用不足，无法满足关键信息基础设施安全合规要求。为此，亟需构建兼顾实时性、兼容性与安全性的工控协议动态防护体系。

1 工控协议体系结构与深度分析

1.1 工控协议的分类与核心特征

工控协议与传统网络协议存在本质差异，其设计围绕工业现场高实时性、高可靠性、强抗干扰性三大核心需求展开，根据传输介质、技术架构、应用层级与实时性，可分为五大核心类别，如表 1 所示。

工控协议的共性特征表现为：采用二进制编码，结构简洁、功能固定，部分协议仅通过 1~2 个比特表示核心功能，以满足底层设备有限的计算性能需求；采用主从架构或总线架构，通信模式固定，数据传输具有周期性。而在安全机制上，则普遍缺乏完善的身份认证、数据加密机制，设计上优先保障实时性，因而部分牺牲了安全性。

1.2 典型工控协议剖析

1.2.1 Modbus 协议解析

Modbus 协议是 1979 年推出的开放串行通信协议，基于主从架构，分为 Modbus RTU 与 Modbus ASCII 两种传输模式，其中 RTU 模式采用二进制编码，传输效率高，占工业现场应用的 90%以上。其协议帧结构包括地址域、功能码域、数据域与校验域，核心功能码定义了数据读写、设备控制等指令，如 01（读线圈状态）、03（读保持寄存器）等。

深度分析发现，Modbus 协议存在明显安全短板：缺乏身份认证机制，任意设备可发送指令并接收响应；数据传输未加密，指令与数据可被轻易监听、篡改——采用的 CRC 循环冗余校验机制简单，仅能检测传输错误，无法抵御恶意篡改与重放攻击。

1.2.2 DNP3 协议解析

DNP3 协议是输配电领域的核心通信协议，专为工业控制场景设计，支持多主站、多从站架构，具备较强的抗干扰能力与容错能力，其协议帧结构包括帧头、控制域、数据链路层地址、应用层数据与校验码，支持数据分片传输，适配长距离、大容量数据交互。

DNP3 协议的安全缺陷主要体现在：应用层缺乏统一的加密与身份认证机制，仅部分版本支持简单的密码认证；协议字段定义复杂，存在字段冗余与歧义，易被攻击者利用进行漏洞挖掘；对异常报文的检测能力薄弱，难以识别恶意篡改与伪造的控制指令。

1.3 协议逆向分析难点

工业领域中大量私有工控协议，如西门子 ProfiBus、施耐德专用协议等因缺乏公开的协议文档，其解析难度远高于标准协议[4]。相较于标准工控协议，厂商定制的私有协议逆向分析难度显著提升，其核心难点与标准协议的共性特征并无重叠，呈现出独特的技术挑战。

表 1　工控协议特征与应用场景

协议分类	典型协议	核心特征	典型应用场景	定位
基础串口通信协议	Modbus RTU/ASCII、RS232、RS485	低速、短距、二进制编码	现场仪表、PLC、传感器	工业设备的基础通信入口
现场总线协议	ProfiBus、CC-Link、DeviceNet	多设备联网、分布式控制	车间自动化、产线控制	工业自动化中期的核心协议
工业以太网协议	Profinet、EtherNet/IP、Modbus TCP	高速率、长距离、多层覆盖	控制层/监控层互联	当前工业通信的主流协议
工业无线通信协议	Wi-Fi HaLow、WirelessHART	移动适配、远程传输	移动设备、野外巡检	工业通信的补充与延伸
跨平台通用协议	MQTT、OPC UA	跨品牌、跨系统互通	工业互联网、云边协同	工业互联网与智能制造的核心支撑

（1）编码规则与字段语义极不透明。私有协议虽采用二进制编码，但摒弃标准规范，字段长度、划分及语义映射无公开标准，部分关键字段采用自定义压缩或混淆编码，字段语义还可能随设备状态动态变化，给帧结构拆分和指令推断带来基础障碍。

（2）加密机制封闭且多样。多数私有协议引入加密传输，但其算法、密钥生成方式均不公开，部分还采用“加密+混淆”双重防护，即便获取报文也难以解密还原，无法开展后续解析。

（3）状态机模型复杂且无公开文档。私有协议通信逻辑贴合专属设备运行流程，状态切换、交互时序等无公开说明，还可能存在动态主从切换等特殊逻辑，难以通过有限报文还原完整状态机。

（4）现有逆向方法适配性差。主流方法均针对标准协议设计，依赖固定帧结构等先验信息，而私有协议无任何先验规则，导致字段划分、语义推断精度极低，无法满足实际需求。

（5）协议迭代快且兼容性差。厂商频繁迭代协议版本，各版本在编码、加密等方面差异较大且无兼容规范，需针对每个版本单独逆向，大幅增加工作量。

2 工控协议安全漏洞挖掘与攻击机理分析

2.1 工控协议安全漏洞分类与特征

协议设计漏洞：由协议本身的设计缺陷导致，是最核心、最难修复的漏洞，如 Modbus 协议的无认证、无加密缺陷，DNP3 协议的字段歧义问题，此类漏洞具有普遍性，影响使用该协议的设备[1,4]。

实现漏洞：由协议在设备中的实现过程不规范导致，如字段处理不当、缓冲区溢出、权限控制不严等，CVE-2025-54923 漏洞即属于此类，可导致远程代码执行与系统接管。

配置漏洞：由用户配置不当导致，如默认密码未修改、非必要端口暴露、固件长期不更新等，此类漏洞易被攻击者利用，且发生率极高，2025 年西门子 SIMATIC ET 200AL 设备的未授权访问漏洞即源于配置缺陷。

高危害、广覆盖、易利用构成了工控协议漏洞的共性特征，攻击者可通过 Shodan、Censys 等网络扫描工具快速定位目标设备，无需复杂技术储备即可实施攻击。

2.2 典型攻击路径与机理分析

协议欺骗攻击：攻击者利用工控协议缺乏身份认证的缺陷，伪造合法设备身份，发送虚假控制指令或篡改传输数据，如伪造 Modbus 指令篡改储罐液位参数、粮仓温湿度设置，导致生产异常或设备故障。

漏洞利用攻击：针对协议实现漏洞，攻击者通过发送恶意报文触发漏洞，实现远程代码执行、权限提升或设备瘫痪，如利用 CODESYS Runtime 系列漏洞，对跨厂商设备实施批量攻击，导致多条生产线瘫痪。

中间人攻击：利用协议无加密传输的缺陷，拦截设备间的通信报文，窃取生产调度数据、设备配置等敏感信息，或篡改报文内容，实施重放攻击，如拦截水处理厂控制指令，篡改水压调节参数。

2.3 漏洞挖掘技术优化

针对现有漏洞挖掘技术对私有协议适配性差、零日漏洞检测能力不足的问题，本文提出一种融合协议逆向与模糊测试的漏洞挖掘优化方法，可为整体加固方案的协议解析层与漏洞预警层提供核心技术支撑。

（1）人机协同私有协议逆向解析

通过网络抓包工具采集私有协议原始通信报文数据集，完成报文预处理、去重与噪声过滤，剔除无效重传报文与异常干扰数据包；通过人工先验规则辅助自动聚类算法完成帧边界划分，逐层解析协议帧结构、字段类型、长度约束与语义映射关系，实现协议格式结构化还原。在此基础上依据报文交互时序逻辑，提取协议关键字段、指令映射规则，构建完整有限状态机模型，明确协议状态跳转条件、交互流程与指令约束关系。相较于传统纯自动逆向方法，该方法在协议字段解析准确率上显著提升，对未知语义字段识别覆盖度亦大幅提高，从而为后续模糊测试提供精准先验特征依据。

（2）面向工控特征的定制化模糊测试用例生成

结合工控协议固有的周期性传输、强实时性、设备资源受限等特点，针对已解析的协议字段权重划分危险等级，对控制指令、设备地址、数据载荷等核心敏感字段优先变异，对校验域、固定帧头等非关键字段弱化变异[5]。定义字段变异权重公式：

$$W_i=\alpha C_i+\beta S_i+\gamma F_i \tag{1}$$

式中，W_i 为第 i 个字段的变异权重，取值为 $[0,1]$，值越大优先级越高，在模拟协议欺骗攻击测试中，报文涉及控制功能字段的变异权重设置为 0.9；C_i 为字段关键性，控制指令字段取 1，普通数据字段取 0.5，校验字段取 0.1；S_i 为字段敏感性，地址/参数类字段取 1，一般数据字段取 0.3；F_i 为字段出现频率，归一化至 $[0,1]$；α、β、γ 为权重系数，分别取值为 0.5、0.3、0.2。

基于状态机跳转约束优化变异策略，限定报文变

异幅度与发送频率，按照工业设备正常通信周期自适应调节测试报文发送速率，严格控制单轮测试报文发送间隔，规避大量畸形报文冲击引发的设备宕机、生产线误动作、执行机构异常启停等风险，实现工控场景模糊测试。

（3）机器学习驱动异常检测与漏洞定位

引入轻量级机器学习分类模型构建异常行为判别体系，采集测试过程中设备响应报文、网络时延、数据返回码、设备运行状态等多维特征数据，完成正常通信特征库构建。在模糊测试过程中实时监测报文交互异常、数据返回异常、设备状态突变等行为，通过模型实时判别异常事件并回溯报文变异位置，精准定位漏洞触发字段、触发条件与载荷边界，有效挖掘未知零日漏洞，降低无效测试开销，提升漏洞挖掘命中率与检测效率。

3 工控协议安全加固方案设计

3.1 加固方案设计原则

结合工控系统的实时性、可靠性要求与协议安全痛点，确立三大设计原则。

（1）实时性优先：加固方案需最小化性能开销，确保协议通信时延不影响工业生产，如加密传输时延控制在 5 ms 以内，适配工控设备的实时控制需求。

（2）兼容性适配：支持标准工控协议与私有工控协议，适配老旧设备与新型设备，无需大规模改造现有系统，降低部署成本。

（3）主动防御：突破被动防御局限，实现漏洞预警、异常检测与动态加固的联动，提升对未知攻击与零日漏洞的防御能力。

3.2 主被动融合的工控协议分层自适应安全加固体系

本文构建主被动协同、分层联动、动态迭代的工控协议安全加固体系，如图 1 所示，整体架构划分为协议解析层、漏洞预警层、动态加固层、审计追溯层共计 4 层。协议解析层的输入为原始报文、设备信息及人工先验规则；输出为标准化帧结构、字段约束、协议状态机、解析规则库及协议特征向量。漏洞预警层的输入为协议特征、实时流量、漏洞库与历史基线；输出为异常判定结果、风险等级、加固策略、访问规则及预警日志。动态加固层的输入为风险等级、加固策略、设备 ID 与密钥；输出为加密报文、认证结果、拦截/放行动作及执行日志。审计追溯层的输入为规则更新记录、异常事件、加固日志及设备状态；输出为审计台账、误报漏报分析、迭代优化建议及合规报告。

3.2.1 协议解析层

协议解析层是整个安全加固体系的数据基础与协议认知核心，以人机协同逆向解析为技术主线，面向标准协议与私有协议提供无侵入式解析服务，支撑上层预警、加固与审计全流程。

面向 Modbus、DNP3 等标准工控协议，基于公开规范完成帧结构、字段语义、交互时序的标准化解析。面向私有工控协议，采用人机协同逆向机制：通过报文采集、预处理、聚类划分与人工先验辅助，还原协议格式、关键字段映射与状态机模型，生成可动态更新的解析规则。

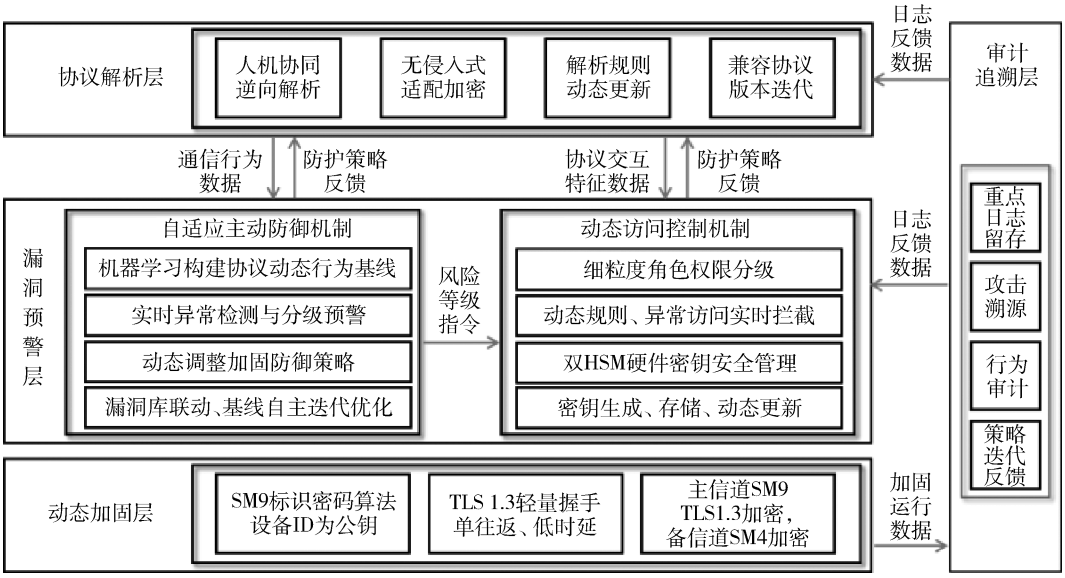

图 1 安全加固体系图

人机协同逆向解析模块：针对私有协议无公开文档、字段语义不透明等难点，采用人机协同逆向分析方法进行协议解析，具体流程如图 2。输入为 PCAP 格式原始报文，预处理阶段进行去重、噪声过滤和无效报文剔除；提取报文长度、字节熵值、固定位重复性等特征；采用加权欧式距离进行自动聚类，以轮廓系数≥0.7 为收敛指标，划分报文格式簇；字段边界依据熵值突变、长度一致性及语义关联进行识别，并判断识别结果是否存在歧义；若涉及歧义，人工介入聚类校验、边界修正、语义歧义判定及状态机补全，校正后生成结构化解析规则并形成解析规则库，支撑解析规则动态更新模块功能。

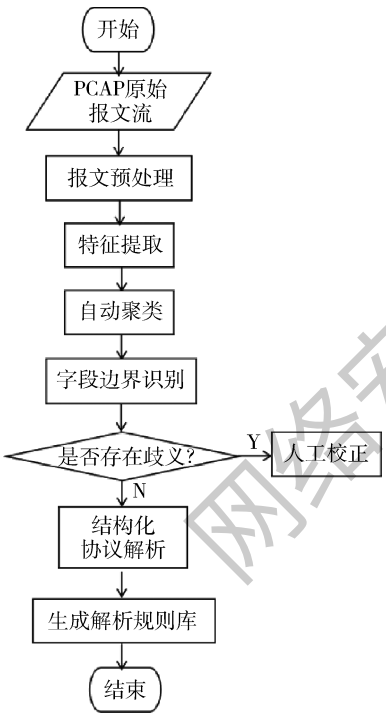

图 2　人机协同私有协议逆向解析流程图

无侵入式适配加密模块：无需修改协议底层实现与设备原有逻辑，以旁路解析方式完成协议识别与字段提取，实现无侵入式部署；并适配上层国密加密、访问控制等防护机制，降低对工控系统业务连续性的影响。

解析规则动态更新模块：基于逆向结果自动生成结构化解析规则，支持规则在线加载与热更新，无需重启服务即可完成规则升级，保障防护机制持续有效。

兼容协议版本迭代模块：面向厂商私有协议频繁迭代、多版本并存的特点，建立协议版本感知与兼容机制，适配不同版本协议的格式差异与交互逻辑，确保解析与防护能力随协议版本同步演进。

协议解析层最终输出标准化协议特征、字段约束、交互时序与状态跳转条件，为漏洞预警、动态加固提供精准先验依据，实现对标准协议、私有协议、新旧版本协议的全面覆盖与持续适配。

3.2.2　漏洞预警层

漏洞预警层融合多维度漏洞挖掘技术与网络报文实时监测能力，构建协议漏洞特征库与正常通信行为基线，依托机器学习与深度报文检测识别异常报文与攻击行为，对应基于行为基线的自适应主动防御机制与细粒度动态访问控制机制，实现安全风险全域感知、提前预警与快速响应。

（1）自适应主动防御机制

面向未知攻击、零日漏洞与协议层异常行为，构建以行为基线为核心的自适应主动防御体系，通过全链路流量感知与智能决策实现主动防护。

①机器学习构建协议动态行为基线。基于轻量级机器学习分类模型与时序特征分析，对正常通信周期、指令交互逻辑、字段取值范围、设备访问模式、报文交互时序[6] 等多维特征进行持续学习与建模，形成自学习、自校准的工控协议动态行为基线。

②实时异常检测与分级预警。采用深度报文检测（Deep Packet Inspection，DPI）与流量特征统计技术，实时监测协议通信状态，对偏离基线的异常流量、非法指令、畸形报文、非授权访问、越权操作等行为精准识别。为实现异常行为的量化评估与分级预警，构建风险评分函数，如式（2）所示。依据攻击类型、危害程度、影响范围实现分级预警。

$$R=w_1S+w_2P+w_3I \tag{2}$$

式中，R 为综合风险评分，取值范围为[0,10]，其中 $R\geq 7$ 为高危，$4\leq R<7$ 为中危，$R<4$ 为低危；S 为漏洞严重性，依据 CVSS 评分映射至[1,10]；P 为攻击可利用性，基于威胁情报评估，取值为[1,5]；I 为业务影响度，依据资产重要性分级，取值[1,5]；w_1、w_2、w_3 为归一化权重系数，分别取值为 0.4、0.3、0.3。

③动态调整加固防御策略。依据预警等级与威胁类型，自动调度并动态调整加固防御策略，包括加密强度适配、访问规则收敛、拦截阈值优化、通信链路限流、设备临时隔离、备用信道切换等多级响应手段。

④漏洞库联动和基线自主迭代优化。与工控漏洞库、威胁情报库实时联动，引入最新漏洞特征与攻击模式，自主迭代优化行为基线与异常检测规则，持续

提升对新型威胁、变种攻击的识别与防御能力。

（2）动态访问控制机制

针对工控协议身份认证缺失、权限管控薄弱等问题，构建身份可信、权限可控、密钥安全的动态访问控制机制，实现设备接入与指令操作的全流程管控。

①细粒度角色权限分级。基于设备唯一标识、通信角色、业务场景与操作风险等级，建立管理员、运维人员、监控设备、现场执行单元等多级权限边界，实现指令读写范围、控制操作类型、数据访问权限的细粒度划分。

②动态规则和异常访问实时拦截。依托动态访问控制规则库与状态机检测逻辑，对非法设备接入、未授权指令发送、异常指令序列、跨域访问等行为实时检测，实现异常访问即时阻断、告警上报与行为日志记录。

③双 HSM 硬件密钥安全管理。采用双硬件安全模块（HSM）冗余备份架构，为国密 SM9 标识密码、SM4 对称密码提供高安全等级密钥运行环境，支持密钥运算隔离、权限管控与抗物理破解。

④密钥生成存储和动态更新。覆盖密钥全生命周期安全管理，支持密钥安全生成、加密存储、权限隔离、在线动态更新与平滑切换，确保密钥更新过程无业务中断、无通信闪断，满足工控系统高可用要求。

3.2.3 动态加固层

动态加固层作为整个安全体系的核心执行中枢，聚焦解决工控协议明文传输、易被窃听篡改及身份假冒等核心风险，以国密算法为底层安全底座[7]，融合 SM9 标识密码体系与 TLS 1.3 轻量化传输协议，构建主备信道分级、动态策略调度的链路加固机制，实现工业控制通信的机密性、完整性与低时延需求。

（1）密码协议栈结构

为明确国密算法与传输协议的边界，构建四层安全协议栈，各组件分层如下。

应用层：承载工控业务协议，传输控制指令与传感器数据。

安全中间件层：部署 SM9 标识密码算法，负责身份认证、密钥交换与设备可信校验，独立于传输层，免证书部署。

传输层：部署 TLS 1.3 协议，集成国密密码套件 TLS_SM4_GCM_SM3，完成会话加密、完整性校验与 1-RTT 轻量化握手。

链路层：备信道独立部署 SM4 对称加密算法，用于高频传感器数据轻量化加密，不依赖 TLS 会话。

（2）SM9、SM4 与 TLS 1.3 的集成路径

主信道：传输控制指令，SM9 嵌入 TLS1.3 握手流程且 SM9 不独立运行于业务层。用设备唯一 ID 作为 SM9 公钥，替代传统数字证书，在 TLS 握手阶段完成 SM9 身份验签与会话密钥协商，协商结果直接作为 TLS 1.3 会话密钥，后续通信由 TLS 1.3 使用 SM4-GCM 加密传输。

备信道：传输传感器及其他工业数据，SM4 独立轻量化加密高频、大流量传感器数据，不经过 TLS 握手，直接在链路层采用 SM4 对称加密，密钥由 HSM 预分发或主信道动态下发，降低时延开销。

（3）主信道密钥协商与会话建立

主信道采用 SM9 嵌入 TLS 1.3 握手完成密钥协商。客户端发送设备 ID、国密套件与随机数；服务端返回选定套件、随机数及 SM9 签名；客户端验签完成身份认证。双方通过 SM9 算法生成预主密钥，结合随机数推导 TLS 1.3 会话密钥；最终建立基于 SM4-GCM 加密的安全会话，用于传输控制指令。

（4）备信道 SM4 轻量化加密流程

备信道采用 SM4 对称加密实现轻量化传输，传感器数据直接使用 HSM 分发的 SM4 密钥加密后发送。接收端解密恢复数据，无需 TLS 握手，兼顾低时延与数据机密性，适配高频传感数据传输场景。

3.2.4 审计追溯层

审计追溯层作为体系闭环迭代与合规审计的关键支撑，对协议通信报文、设备上下线、异常攻击事件、权限操作、加密链路调用及加固执行动作进行重点日志留存，确保数据不可篡改、可查可验。对设备访问、指令操作、密钥使用等行为开展全周期行为审计，及时发现违规操作与可疑风险。将审计结果、攻击特征、误报漏报信息与防御效果即时反馈至其他层，驱动解析规则、行为基线、访问策略与加密机制自主迭代优化。

4 实验验证与性能分析

4.1 实验环境搭建

为验证融合国密算法的工控协议动态自适应加固体系的有效性与工程适用性，搭建典型工控仿真测试环境。硬件平台包括西门子 S7-1200 PLC、远程终端单元 RTU、工业交换机、双 HSM 硬件安全模块及工控监测主机；软件平台部署协议逆向分析工具、定制化模糊测试平台[8]、加固原型系统与 Wireshark 报文监测工具；选取 Modbus RTU、DNP3 标准协议及某炼化企业私有协议作为测试对象，模拟协议欺骗、缓冲区溢出、

中间人攻击三类典型攻击场景[9]开展验证。

4.2 实验指标与测试方案

4.2.1 实验指标

围绕工控场景安全性、实时性、兼容性核心需求，设置三级量化评估指标，衡量加固体系性能。

安全性指标：包含攻击拦截率、协议漏洞防御率、数据篡改防护率，采用成功率分别进行计算，该类指标用于衡量对攻击行为的抵御与防护能力。

$$SR=\frac{P_{sucess}}{P_{test}}\times 100\% \tag{3}$$

式中，SR 为成功率；P_{sucess} 为被成功拦截的攻击报文数量/协议漏洞被有效抵御的报文数量/数据篡改行为被成功防范的报文数量；P_{test} 为测试报文总数量。

实时性指标：包含端到端通信时延、加密附加时延、异常检测时延[10]，用于验证加固对工业控制业务的时延影响。

兼容性指标：包含标准协议适配率、私有协议适配率、老旧设备适配率，采用适配率分别进行计算，该类指标用于衡量本方案在多类型协议、老旧异构设备场景下的实际部署与适配能力。

$$AR=\frac{N_{adapt}}{N_{test}}\times 100\% \tag{4}$$

式中，AR 为适配率；N_{adapt} 为可正常解析/加密/防护的协议/设备数量；N_{test} 为测试的协议/设备总数量。

4.2.2 测试方案

采用对照组对比测试法，分别对未加固系统、传统 TLS 加密系统、本文加固系统进行三组平行测试，确保实验结果可量化、可对比。

安全性测试：模拟协议欺骗、缓冲区溢出、中间人攻击三种典型攻击场景，分别测试未加固方案与本文加固方案的防御效果，统计攻击被成功拦截与漏洞被有效防御的比例，对比漏洞防御率与攻击拦截率。

实时性测试：分别测试标准协议与私有协议在加固前后的通信时延、加密附加时延，连续采集 1 000 组报文交互数据并取平均值，验证方案对工控系统实时性的影响。

兼容性测试：测试方案对标准协议、私有协议、老旧 PLC/RTU 等不同类型协议与不同型号设备的适配效果，统计可正常解析、加密、防护的比例，验证方案通用性与工程适配能力。

4.3 实验结果与分析

结合行业通用测试基准，未加固状态下设备对典型攻击的拦截率、漏洞防御率与防篡改率均处于较低基线水平，作为实验对照依据。实验结果如表 2 所示。

表 2　加固方案性能指标对比

测试维度	测试指标	未加固	传统 TLS	本文
安全性	典型攻击拦截率/%	≤65	≈75	98
	协议漏洞防御率/%	≤50	≈70	95
	数据篡改防护率/%	≤40	≈72	97
实时性	通信时延/ms	≤2	8~12	3
	加密附加时延/ms	—	≥1	0.4
兼容性	标准协议适配率/%	—	85	100
	私有协议适配率/%	—	50	90
	老旧设备适配率/%	—	60	85

安全性方面，本文方案典型攻击拦截率为 98%、协议漏洞防御率为 95%、数据篡改防护率为 97%，远高于未加固系统与传统 TLS 方案，可有效抵御协议欺骗、漏洞利用、中间人等主流工控协议层攻击，安全防护能力大幅提升。

实时性方面，加密附加时延低至 0.4 ms，整体通信时延小于 3 ms，满足工业控制系统毫秒级实时性约束。

兼容性方面，适配选取的两项标准协议，私有协议适配率为 90%，老旧设备适配率为 85%，支持老旧 PLC、RTU 无改造部署，有效解决传统方案对私有协议、老旧设备支持不足的问题，工程落地成本更低。

实验结果表明，本文所提加固方案在保障工控系统高实时性的前提下，实现了安全能力、兼容能力的同步提升，具备场景工程化部署价值。

5 结论

本文围绕工控协议与安全加固展开研究，通过对工控协议的体系结构、典型协议进行深度剖析，明确了协议的核心特征与安全短板，揭示了协议层攻击的路径与机理；提出了融合人机协同逆向分析、国密 SM9-TLS 1.3 加密、动态自适应防御的创新加固方案，构建了全生命周期安全防护体系。实验验证表明，该方案能够有效提升工控协议的抗攻击能力，兼顾安全性与实时性，适配标准协议与私有协议，可落地应用于关键信息基础设施的工控系统安全防护，解决了现有方案存在的防御能力弱、实时性差、私有协议适配性不足等问题。

本文研究仍存在一定不足：一是私有协议的语义推断精度仍有提升空间，对复杂私有协议的解析效率有待优化；二是动态行为基线的自适应调整速度可进一步提升，对极端攻击场景的防御能力需加

强；三是方案的大规模部署效果仍需在实际工业场景中验证。

未来可深化以下几方面研究：一是优化人机协同逆向分析算法，引入大语言模型提升私有协议的解析精度与效率；二是结合工业互联网平台，实现加固方案的规模化部署与集中管理，构建跨领域、跨行业的工控协议安全防护体系；三是深入研究供应链安全风险传导机制，将协议加固与供应链安全防护相结合，提升工控系统的整体安全水平。

参考文献

[1] 方栋梁,刘圃卓,秦川,等. 工业控制系统协议安全综述[J]. 计算机研究与发展,2022,59(5):978-993.

[2] 王朝斌. 面向私有工控协议的协议逆向分析技术研究[D]. 广州:广州大学,2021.

[3] 张昊. 关键信息基础设施领域工控主机安全防护技术研究与实践[J]. 中国信息安全,2023(9):67-68.

[4] 边祥迪. 未知工控协议逆向分析关键技术研究[D]. 长沙:湖南大学,2021.

[5] 尚文利,李文轩,陈春雨,等. 基于特征矩阵的工控协议模糊测试方法[J]. 信息与控制,2020,49(4):436-443,454.

[6] Oliveira P,Santin A,Horchulhack P, et al. Defense-in-depth and machine learning-based intrusion detection for industrial control systems[J]. Journal of Network and Systems Management,2025,34(1):9.

[7] 苏彬庭,陈明志,许力,等. 国密算法在工业互联网安全中的应用研究[J]. 信息技术与网络安全,2021,40(3):28-31.

[8] 杨鸿森. 基于生成对抗网络的工控协议模糊测试方法研究及应用[D]. 洛阳:河南科技大学,2024.

[9] 刘化冰. 基于协议逆向与模糊测试的工控系统漏洞挖掘技术研究[D]. 南京:东南大学,2023.

[10] Birihanu E,Lendák I. Explainable correlation-based anomaly detection for industrial control systems[J]. Frontiers in Artificial Intelligence,2025. DOI:10. 3389/frai. 2024. 1508821.

（收稿日期：2026-04-28）

作者简介：

王蕊（1995-），女，硕士，工程师，主要研究方向：网络安全、工业控制系统、代数与密码学。

徐志浩（2001-）男，本科，助理工程师，主要研究方向：网络安全、工业控制系统、工业互联网。

董良遇（1989-），通信作者，女，硕士，高级工程师，主要研究方向：网络安全、工业控制系统、工业互联网。E-mail:dongliangyu78@ 163. com。

版权声明

凡《网络安全与数据治理》录用的文章，如作者没有关于汇编权、翻译权、印刷权及电子版的复制权、信息网络传播权与发行权等版权的特殊声明，即视该文章署名作者同意将该文章的汇编权、翻译权、印刷权及电子版的复制权、信息网络传播权与发行权授予本刊，本刊有权授权本刊合作数据库、合作媒体等合作伙伴使用。同时，本刊支付稿酬已包含上述使用的费用，特此声明。

《网络安全与数据治理》编辑部