基于多策略协同的加注控制系统网络安全防护研究

张　超[1]，陈　佳[2]，秦志伟[1]，李　闯[1]，李　静[1]
（1. 中电智能科技有限公司，北京　102209；2. 中国电子信息产业集团有限公司第六研究所，北京　102209）

摘　要：针对加注控制系统所遭遇的非法访问、数据篡改及外部恶意攻击等安全威胁，以提升系统安全防护能力为目标，开展了网络安全防护研究。针对控制系统四大核心层级的安全需求，提出多策略协同与分层架构相结合的安全防护方案，可融合多种安全防护技术与策略，构建立体化防护架构，并分析了安全防护强度与系统实时性的平衡问题。研究成果形成了适用于加注控制系统的系统性安全防护方案，可有效提升系统防御内外部安全威胁的能力，为工业加注系统安全稳定运行提供技术保障。

关键词：加注控制系统；网络安全防护；网络安全策略；安全防护技术
中图分类号：TP393.08　　**文献标志码：**A　　**DOI：**10.19358/j.issn.2097-1788.2026.06.003

中文引用格式：张超，陈佳，秦志伟，等. 基于多策略协同的加注控制系统网络安全防护研究[J]. 网络安全与数据治理，2026，45(6)：17-23.
英文引用格式：Zhang Chao，Chen Jia，Qin Zhiwei，et al. Research on network security protection for refueling control system based on multi-strategy collaboration[J]. Cyber Security and Data Governance，2026，45(6)：17-23.

Research on network security protection for refueling control system based on multi-strategy collaboration

Zhang Chao[1]，Chen Jia[2]，Qin Zhiwei[1]，Li Chuang[1]，Li Jing[1]
（1. Intelligence Technology of CEC Co.，Ltd.，Beijing 102209，China；
2. The 6th Research Institute of China Electronics Corporation，Beijing 102209，China）

Abstract：In response to the security threats faced by the refueling control system，such as illegal access，data tampering，and external malicious attacks，with the goal of enhancing the system′s security protection capabilities，the paper conducts research on network security protection. Addressing the security requirements of the four core levels of the control system，this paper proposes a security protection scheme combining multi-strategy coordination and a hierarchical architecture. It integrates various security protection technologies and strategies to establish a three-dimensional protection architecture，and analyzes the balance between security protection strength and system real-time performance. The research results have developed a systematic security protection scheme applicable to the refueling control system，effectively enhancing the system′s ability to defend against internal and external security threats，and providing technical support for the safe and stable operation of industrial refueling systems.

Key words：refueling control system；network security protection；network security strategy；security protection technology

0　引言

在石油化工、航空航天等关键领域，加注控制系统承担着精准地加注燃料、原油等物料的重要职责[1]。以航天发射为例，加注系统通过精确控制加注量和加注流程保障产品的质量，其“多贮箱并行加注、分阶段精准控制”的独特工艺特性，使其在实时性、可靠性需求上有更高的要求：加注各阶段需实时匹配贮箱状态，全系统精准同步，发射全流程需零中断运行，具备硬件—软件—网络—数据各方面冗余容错能力和抗干扰能力。随着工业互联网的兴起，加注控制系统接入网络，实现了智能化管理与远程操作，但也因此暴露出恶意攻击、数据泄露、系统被篡改等网络安全问题，给系统正常运行和行业生产安全带来严重威胁。

黑客入侵数据采集与监视控制（SCADA）系统，通过发送大量虚假请求致其瘫痪，进而引发供水系统中断[2]；虚假数据注入攻击非法获取或修改数据库信

息，造成传感器采集量不准影响产品质量[3]；恶意软件入侵可能窃取关键数据或控制加注设备，引发安全事故[4]；内部人员违规操作也会破坏系统稳定性和数据保密性。这些威胁不仅影响正常生产，严重时还会因加注失控导致爆炸、泄漏等重大灾难。比如某石化企业曾因系统漏洞遭受注入攻击，加注参数被修改使原料加注过多，引发局部装置异常，造成重大经济损失和环境污染。

目前，现有的安全防护方案普遍存在防护维度单一、协同性不足、动态适配能力欠缺等局限，有些方案侧重单一防护策略，难以抵御复合型网络攻击[5]，有些仅对控制系统单层分析，无法实现各层协同防护，部分方案采用静态防护架构，难以适配加注控制系统在不同运行阶段的动态安全需求[6]。本文结合加注控制系统的层级结构与安全需求，采用系统设计方法，设计了一套全面的立体化安全防护方案，明确各层级、各策略的功能定位，形成覆盖加注控制系统设备层、控制层、监控层和平台层的全生命周期防护，抵御各类网络攻击，保障系统安全稳定可靠运行。

1 网络安全策略设计

1.1 身份认证

身份认证技术作为加注控制系统安全防护的安全闸口，通过“身份验证—权限设定”机制精细管理人员设备。采用静态密码、密钥、生物特征识别等多维认证方式验证用户身份真实性，按权限最小化原则并结合岗位职能、职责边界和工作场景给用户分配操作权限，精确确定权限层级和系统访问范围，如一线加注操作员只能调阅加注参数、启停流程，技术维护员额外能校准参数、诊断设备状态，管理员则可调阅全流程数据、调整权限规则。

1.2 网络防火墙

网络防火墙作为加注控制系统安全防护的核心边界屏障，通过“边界过滤—流量控制”机制严格管控内外网交互与数据传输。依托访问控制列表（Access Control List，ACL）技术对进出加注控制系统的数据包进行精准筛选，根据功能区域划分和用户角色动态配置访问规则，通过比对数据包的源 IP、目的 IP、端口号及协议类型等关键信息判定数据包的合法性——仅当数据包来源合法、目标匹配系统允许范围、端口对应开放服务且协议类型符合规范时方可放行，否则立即拦截，形成动态安全防护体系[7]。

1.3 数据加密

数据加密技术作为加注控制系统安全防护的数据安全保护舱，通过“传输加密—存储加密”机制管控数据隐私。依托对称和非对称加密技术保证加注全流程数据在传输和存储时的隐私，防止敏感信息被非法获取或破解。在传输环节，为保证低延迟与流畅性，对加注终端与中控服务器间的实时数据（如加注压力、流量、加注量等参数），采用 AES-256 对称加密算法，通信两端共享唯一密钥，加密数据需密钥解密才能读取，避免传输中被拦截破解。在存储环节，为兼顾安全性与可读性，对数据库中的历史加注记录、用户权限配置等重要数据使用 RSA-2048 非对称加密算法。该方案通过公钥加密、私钥解密，私钥由专人离线保管，即便数据库被入侵，若无私钥也无法解读加密数据。同时，该机制还能支撑数据权限分级管理，加密解密权限和用户角色绑定，确保各岗位人员只能访问权限内的加密数据。

1.4 完整性校验

完整性校验技术作为加注控制系统安全防护的数据质检员，通过“即时校验—存储验证”机制管控数据完整性。采用哈希算法、循环冗余校验（Cyclic Redundancy Check，CRC）等手段保障加注数据在产生、传送、保存各环节不被篡改破坏以维护数据真实性与可靠性。数据产生时针对每次加注操作生成的实时参数（如加注量），即时生成唯一标识值（如 SHA-256 值）并与数据绑定。数据传送时接收端重新计算哈希值并与发送端附带的标识值比对，不一致即判定数据被篡改并立即停止接收。数据保存时通过 CRC32 算法对数据库历史数据进行周期性批量校验，检测因存储介质故障或恶意修改导致的数据损坏，确保长期存储的数据完整性。同时，该技术能通过多维度校验增强数据可信度，确保数据真实可靠，为加注流程追溯及故障分析提供精准数据支撑。

1.5 漏洞扫描

漏洞扫描技术作为加注控制系统安全防护的主动排查者，通过“主动排查—提前修复”机制严格管控系统软硬件缺陷和配置漏洞。运用端口扫描、漏洞匹配、配置核查技术全面检测交换机、服务器、计算机、PLC 等网络设备以精准定位潜在安全风险，相比被动防御能提前发现隐患，防止因漏洞利用引发生产事故。端口扫描逐一探测设备开放端口，识别未授权高危端口及对应服务已知漏洞；漏洞匹配通过内置库比对软件版本与组件型号，快速识别已知风险；配置检查针对账户密码强度、防火墙规则、数据库权限等配置项进行合规检测以发现弱口令、防火墙规则宽松、数据

库权限过度开放等配置漏洞，从根源排查攻击者可利用的安全隐患。

2 网络安全防护整体架构设计

加注控制系统按照功能和层级可分为平台层、监控层、控制层和设备层四大核心层级[8]，系统架构如图 1 所示。

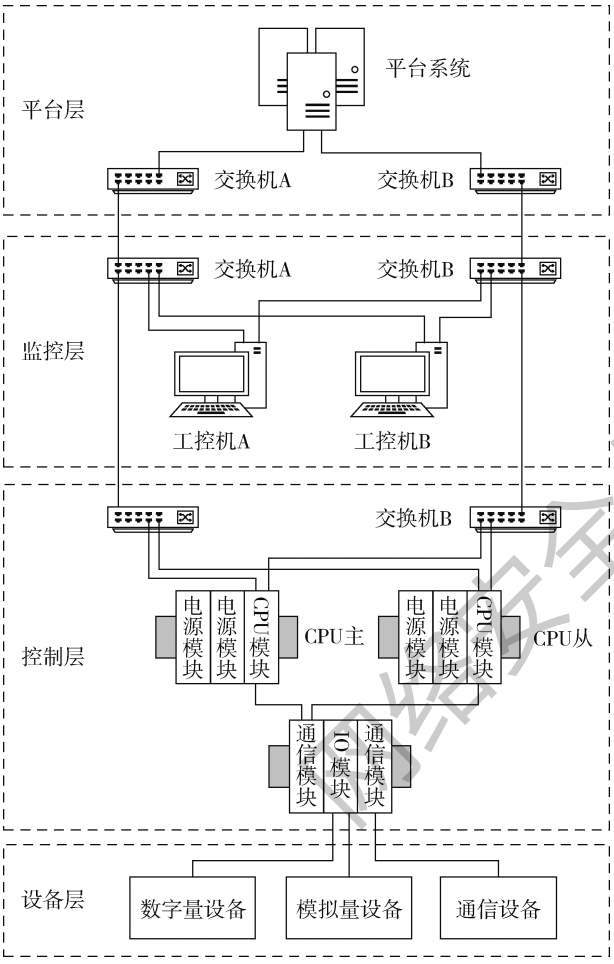

图 1　加注控制系统架构图

2.1 设备层

设备层是加注控制系统执行与感知的关键部分，包含数字量、模拟量及通信三类设备。数字量设备主要包括：气动阀门，用于控制管路通断和流量；点式液位计，用于判断加注液位到位情况。模拟量设备包含：压力传感器，检测管路内压力；温度传感器，检测贮罐内温度；液位传感器，检测储罐内介质液位；流量传感器，实时检测介质的瞬时流量和累计流量；电动调节阀，采集调节阀开度反馈并输出控制阀门开度调节管路流量。通信设备通过变频器连接屏蔽泵，采用 ModbusRTU 或者 CAN 通信方式采集屏蔽泵运行状态、电压、电流等信息并控制启停及调节频率。设备层采集设备将数据传输给控制层，为控制层的调节和决策提供依据，控制层的调节和决策又及时作用到设备层的控制设备上。

设备层中的通信设备通过 485、ModbusTCP 等通信协议传输，通信数据错误可能引起设备控制错误继而引发控制失效和系统故障，可以在通信设备与工业控制系统之间部署传感器数据校验网关，对传感器上传的原始数据进行加密校验，确保数据未被篡改或替换，实现数据完整性校验。设备层网络安全设计如图 2 所示。

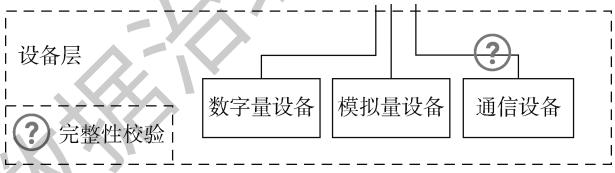

图 2　设备层网络安全设计图

2.2 控制层

控制层是加注过程的逻辑控制中心。可编程逻辑控制器（PLC）是其核心设备，能执行复杂逻辑运算、定时和计数等控制指令，该层级按照监控层下达的操作指令执行预设工艺程序，精准控制设备层执行机构的动作如控制阀门开关和泵启停顺序。控制层通过接收传感器反馈信号并与设定值对比自动调节执行机构，确保加注参数的稳定，并经工业交换机与监控层实时交互上传设备状态。

工业环境中长期运行的工业交换机、PLC 可能存在固件漏洞、端口配置不当、协议兼容性缺陷等问题[9]。漏洞扫描可识别开放的危险端口、检测弱口令配置，从而封堵数据传输链路安全缺口，保障工业网络通信的稳定性。同时工业环境中设备类型复杂、协议多样，工业交换机易成为流量攻击目标，防火墙可实时监测异常流量并对违规数据进行过滤，避免关键操作因流量拥堵延迟。部署网络防火墙能有效阻断非授权访问，防止外部恶意终端或非法数据包通过交换机渗透至核心控制层，避免因设备被篡改、数据泄露引发生产故障。控制层网络安全设计如图 3 所示。

2.3 监控层

监控层是连接平台层和控制层的重要纽带，其核心设备为运行上位机软件的监控工作站，实时显示加注过程各类数据如流量、压力、加注量等，清晰展示加注流程画面如传感器、阀门、泵等设备及加注流程

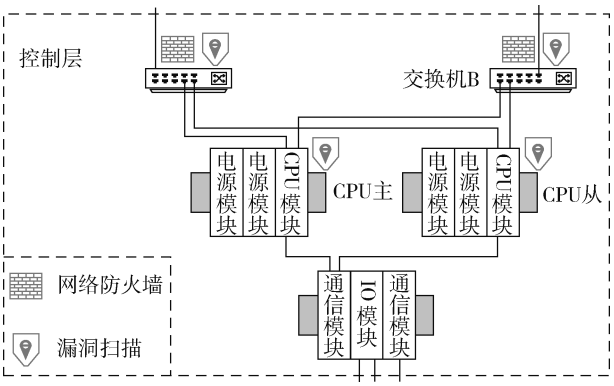

图 3　控制层网络安全设计图

的实时状态，同时还提供直观的操作界面，方便现场人员进行参数设置和操作，实现设备参数统一配置维护，生成各类业务报表实现加注全流程追溯。当系统出现异常时上位机报警提醒操作人员干预，并同步上传部分数据至平台层，同时在本地进行短期存储以保证数据连续性。

当前工控环境中存在身份冒用、密码泄露等风险，可能导致非授权人员非法登录工控机篡改控制参数、窃取敏感数据，采用多因素认证方式，结合密码、密钥、生物特征等，确保操作者身份唯一性与真实性，避免单一认证方式的漏洞。同时基于角色划分权限范围，如操作人员仅能执行预设控制指令，维护人员可进行参数配置，管理员拥有全局管理权限，避免权限过度集中引发风险。

监控层的工业交换机和工控机可借鉴设备层和控制层的安全策略，部署网络防火墙、完整性校验和漏洞扫描技术。监控层网络安全设计如图 4 所示。

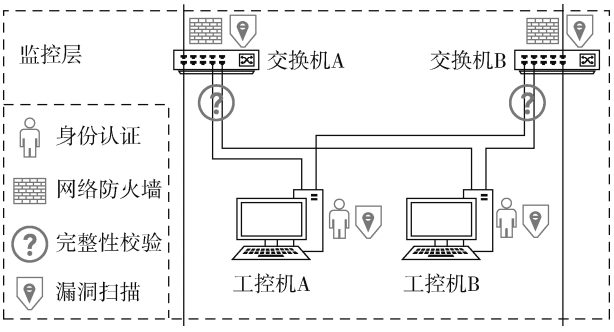

图 4　监控层网络安全设计图

2.4　平台层

平台层作为加注控制系统的管理决策核心，配备了数据库服务器、应用服务器等关键设备，用以存储全系统各类数据（包括历史加注记录、设备运行参数等），通过收集监控层上传的大量数据进行深入分析和趋势预测，为管理层决策提供依据。客户端终端如管理工作站和大屏显示器为管理人员提供了便捷的人机交互界面。

在工业控制系统环境中面临的静态数据泄露、动态数据篡改及隐私信息窃取等威胁[10]，可能引发加注参数的非法修改、关键工艺数据的外露，从而对加注流程的稳定性和安全性构成威胁。为了加强数据安全防护，实施多层次加密策略，运用 AES-256 对称加密技术确保实时传输的压力、流量、加注量等动态信息的安全性和高效性，同时通过 RSA-2048 非对称加密方法保护历史加注记录及用户权限配置等重要数据，实现密钥分发，从而保障加注控制系统的整体数据安全性。

平台层的工业交换机和平台系统可借鉴监控层的安全策略，部署身份认证、网络防火墙、完整性校验和漏洞扫描技术。平台层网络安全设计如图 5 所示。

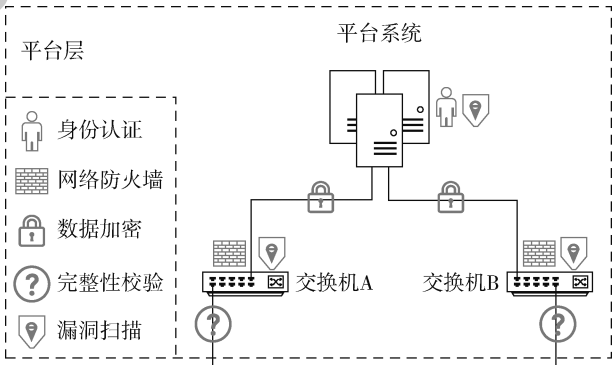

图 5　平台层网络安全设计图

2.5　网络安全策略协同工作

协同机制以纵向层级联动、横向策略互通为核心运行机制，实现四层架构、五类安全策略的动态协同。整体网络安全设计如图 6 所示。

纵向联动表征设备层、控制层、监控层、平台层自下而上状态上报、自上而下管控加固的层级递进，实现“底层拦截—中层检测—上层管控”的纵向协同。定义四层防护层级集合 $S=\{S_1,S_2,S_3,S_4\}$，其中 S_1 为设备层，S_2 为控制层，S_3 为监控层，S_4 为平台层；定义安全防护策略基础集 $\Omega=\{A_1$ 身份认证，A_2 网络防火墙，A_3 数据加密，A_4 完整性校验，A_5 漏洞扫描$\}$，根据各层级防护功能定位，分配策略子集，满足子集约束关系，P_1、P_2、P_3、P_4 分别对应设备层、控制层、监控层、平台层的策略集合。

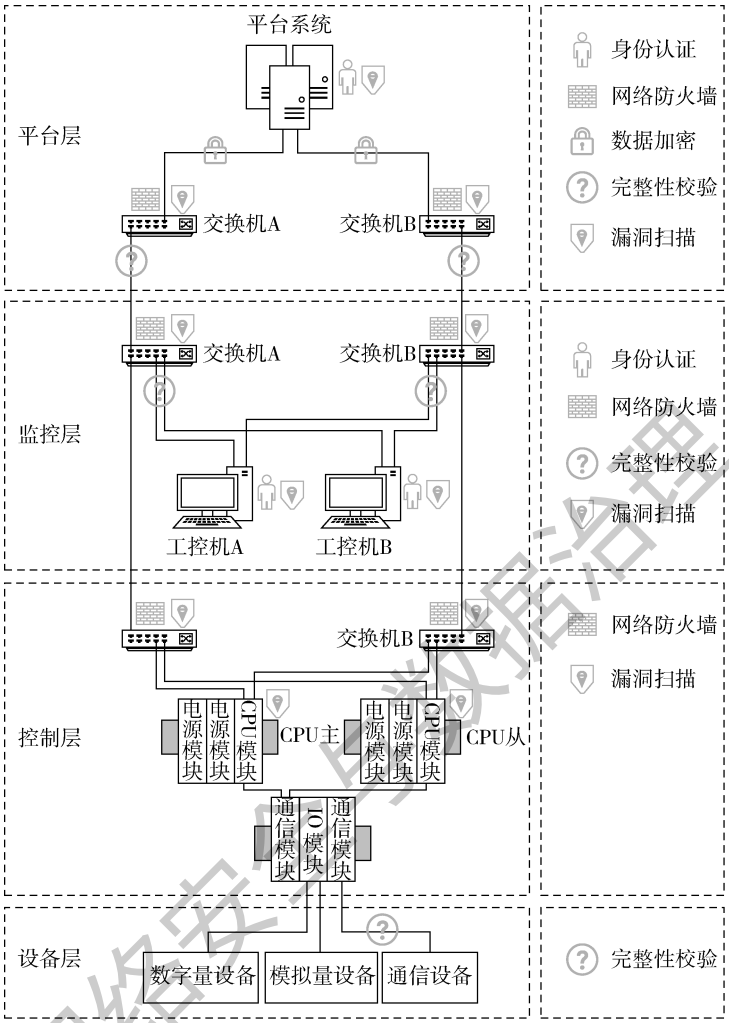

图 6　整体网络安全设计图

$$P_1 \subset \Omega, P_1 = \{A_4\} \tag{1}$$

$$P_2 \subset \Omega, P_2 = \{A_2, A_5\} \tag{2}$$

$$P_3 \subset \Omega, P_3 = \{A_1, A_2, A_4, A_5\} \tag{3}$$

$$P_4 \subset \Omega, P_4 = \{A_1, A_2, A_3, A_4, A_5\} \tag{4}$$

定义纵向层级安全状态函数 $f(S_i, P_i)$，用于表征第 i 层级在对应策略集 P_i 防护下的实时安全状态，包含风险状态、运行状态与告警状态。纵向多级状态转移链路可表示为：

$$f(S_1, P_1) \xrightarrow{\text{状态上报}} f(S_2, P_2) \tag{5}$$

$$f(S_2, P_2) \xrightarrow{\text{风险推送}} f(S_3, P_3) \tag{6}$$

$$f(S_3, P_3) \xrightarrow{\text{预警归集}} f(S_4, P_4) \tag{7}$$

$$f(S_4, P_4) \xrightarrow{\text{管控下发}} (f(S_1, P_1), f(S_2, P_2), f(S_3, P_3)) \tag{8}$$

为量化纵向整体防护协同效能，引入层级权重系数，构建纵向协同效能加权模型：

$$E_{\text{long}} = \sum_{i=1}^{4} \omega_i \cdot f(S_i, P_i) \tag{9}$$

$$\sum_{i=1}^{4} \omega_i = 1, \omega_i \in (0, 1) \tag{10}$$

式中，ω_i 为各层级安全防护权重，可根据系统防护优先级动态赋值。

横向互通包含同一层级内不同策略相互支撑和不同层级间通过信息同步实现协同。定义跨层级信息交互算子 $T_{i,j}$，实现不同层级安全状态的双向同步：

$$T_{i,j}: (f(S_i, P_i), \Theta_i) \leftrightarrow (f(S_j, P_j), \Theta_j), i \neq j \tag{11}$$

式中，Θ_i、Θ_j 为对应层级的安全数据集，包含攻击特征、漏洞信息、校验日志与异常记录。

基于全量跨层交互关系，构建横向协同平均效能模型：

$$E_{\text{cross}} = \frac{1}{C_4^2} \sum_{1 \le i < j \le 4} T_{i,j}(f(S_i, P_i), f(S_j, P_j)) \tag{12}$$

式中，C_4^2 为四层架构的跨层组合数，用于归一化全域横

向协同收益，客观表征系统横向信息互通的整体效果。

系统整体防护协同效能由纵向联动效能与横向互通效能耦合构成，构建综合协同评价模型：

$$E_{\text{total}}=\alpha E_{\text{long}}+\beta E_{\text{cross}} \tag{13}$$

式中，α、β 分别为纵向、横向协同影响系数，$\alpha+\beta=1$，$\alpha>0$，$\beta>0$。α、β 可根据场景需求动态配置，实现立体化防护体系的全局最优协同效果。

层级协同结构流程如图 7 所示。

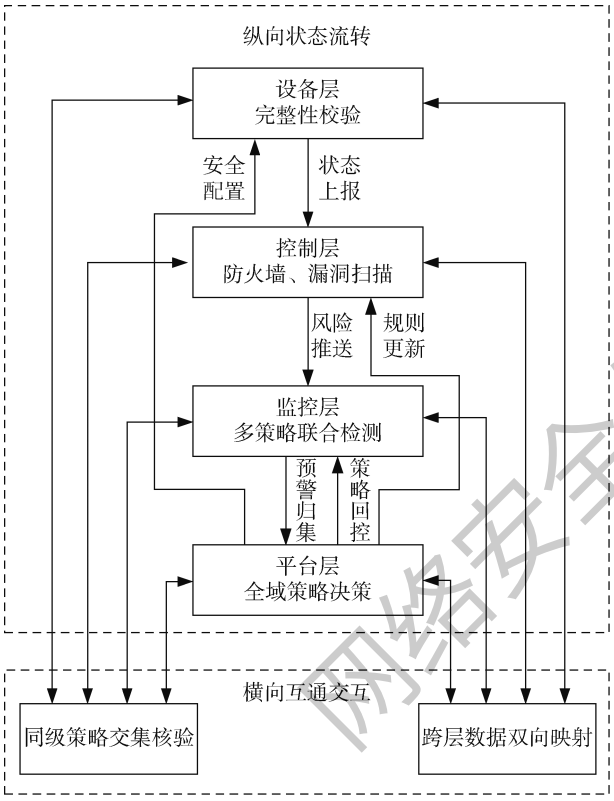

图 7　层级协同结构流程图

3　网络安全策略实施的挑战

多策略协同网络安全防护是保障系统安全的重要手段，但在实际应用中防护手段冗余或策略配置不当会影响系统实时性。比如操作人员在进行加注参数设置和启动加注流程时需多层验证身份权限，每次验证都须比对校验数据，这会延长操作响应周期，而加注控制系统对实时性要求高，即使短暂延迟都可能影响加注精度和节奏。同时频繁漏洞扫描虽能及时发现系统安全隐患却会占用大量网络系统资源，因其要全面检测模块、端口、数据链路等，消耗大量系统处理能力。若在加注操作时扫描还会导致指令传输延迟、数据处理降速，从而影响整体效率。

因此，如何平衡安全防护强度与系统实时性，实现安全不拖慢效率、高效不牺牲安全，是网络安全策略实施的关键挑战。结合加注控制系统的运行特性，实时采集加注阶段（加注准备、加注执行、加注结束、系统维护）、报警等级（无报警、一级预警、二级预警、紧急报警）、安全风险等级（低、中、高）三大核心维度数据，构建基于运行状态综合评估的自适应安全策略调整模型，基于综合评估结果，设计差异化自适应安全策略，动态调整安全防护的强度与方式实现风险与防护匹配、场景与策略适配。如在高需求场景优先保障系统实时性，自动精简身份验证层级，暂停漏洞扫描等非紧急安全操作；在中需求场景，保留核心安全验证环节，启动轻量化漏洞扫描（仅针对关键模块端口）；在低需求场景，逐步提升防护强度，启动全面漏洞扫描。在系统维护期，启动最高等级安全防护，开展全模块、全链路安全检测，完成权限排查、加密模块升级、漏洞修复等工作。同时通过实时采集系统运行数据、安全事件反馈信息，定期对安全策略的参数优化调整，完善模型动态迭代机制，提升策略适配性。

4　结论

本文针对加注控制系统面临的安全痛点，解决了单一防护策略防御能力不足、安全与实时性难以平衡、全流程防护存在短板等关键问题，提出了多策略协同与分层架构相结合的网络安全防护方案。该方案的核心特征是构建“预防—检测—响应—恢复”闭环协同机制，以身份精准核验为前提、边界严格管控为屏障、数据加密校验为核心、漏洞动态排查为保障，实现从操作人员身份管控到数据保护、从网络边界防御到系统内部管控的全方位、多层次防护，既有效降低了各类安全风险，又兼顾了加注系统的操作精准性与运行实时性。

本研究成果不仅为加注控制系统提供了可落地、可复制的系统性安全防护解决方案，更对石油化工、航空航天、能源等相关工业领域的传统控制系统，具有重要的实践指导意义和广泛的推广潜力。在实践层面，该方案可直接应用于各类工业加注场景，规避网络攻击引发的加注失控风险，预防重大事故，减少系统故障导致的生产中断和经济损失；在行业层面，该方案所构建的协同防护架构与技术体系，可为同类工业控制系统的网络安全防护提供参考，提升全行业网络安全防护水平，为产业高质量、可持续发展筑牢安全屏障。

未来，控制系统网络安全防护将深度融合新兴技术，呈现出智能化、自适应化、去中心化趋势。与人

工智能技术的深度融合，让安全策略具备自主学习能力，动态优化检测模型，精准识别新型未知威胁；大数据技术的应用实现全网安全态势实时感知，通过多设备日志关联分析预判潜在风险点，推动安全防护模式从“被动防御”向“主动预警”转变。

参考文献

[1] 邵业涛,周宏,晏政,等. 液体运载火箭液氧煤油并行加注适应性研究[J]. 宇航总体技术,2022,6(3):32-39.
[2] 李佳玮,郝悍勇,李宁辉. 工业控制系统信息安全防护[J]. 中国电力,2015,48(10):139-143.
[3] 孙彦斌,汪弘毅,田志宏,等. 工业控制系统安全防护技术发展研究[J]. 中国工程科学,2023,25(6):126-136.
[4] 李靖. 浅析工业生产过程控制系统网络安全[J]. 软件,2025,46(8):184-186.
[5] 张鑫. 基于国密算法的工业控制系统安全防护策略研究[J]. 电脑知识与技术,2025,21(22):90-92.
[6] 刘小君. 核电厂工业控制系统网络安全防护体系研究[J]. 工业信息安全,2025(5):77-83.
[7] 彭勇,江常青,谢丰,等. 工业控制系统信息安全研究进展[J]. 清华大学学报(自然科学版),2012,52(10):1396-1408.
[8] 丁长富. 工业控制系统全生命周期网络安全防护研究[J]. 机电信息,2024(9):17-20.
[9] 向登宁,马增良. 工业控制系统安全分析及解决方案[J]. 信息安全与技术,2013,4(11):28-30.
[10] 鲍金鹏,梁光明,刘伟. 一种工业控制系统应用层数据安全防护方法[J]. 现代电子技术,2016,39(8):14-17,20.

（收稿日期：2026-01-27）

作者简介：

张超（1992-），男，硕士，高级工程师，主要研究方向：工业自动化、工业控制。

陈佳（1993-），女，硕士，工程师，主要研究方向：计算机技术、网络安全。

秦志伟（1989-），男，本科，工程师，主要研究方向：运动控制、流程自动化。

“密码前沿技术与应用”主题专栏征稿启事

随着量子计算技术的快速发展、人工智能与大模型应用的广泛渗透，以及数据要素市场化对隐私保护的迫切需求，密码学作为网络空间安全的核心支撑，正迎来前所未有的机遇与挑战。一方面，能够抵抗量子计算攻击的后量子密码算法正加速从理论走向标准化与工程化部署，另一方面，数字经济的深化催生了隐私计算技术的爆发，全同态加密、安全多方计算等展现出巨大应用潜力，与此同时，人工智能与大模型的崛起，既为密码分析提供了新的范式，也对密码技术保护 AI 安全提出了新的需求。为了集中展示我国在密码前沿领域的创新成果，促进学术交流与产学研深度融合，《网络安全与数据治理》拟在 2026 年第 8 期推出“密码前沿技术与应用”主题专栏。现诚邀相关领域的专家学者、科研人员踊跃投稿。

一、征文主题：密码前沿技术与应用

包括但不限于以下学术方向：

1. 抗量子计算密码：后量子密码算法的设计、分析、侧信道防护及标准化迁移应用。

2. AI 与密码学融合：利用 AI 进行密码算法辅助设计/自动化分析；密码技术在 AI 模型安全中的应用。

3. 前沿隐私计算技术：全同态加密、安全多方计算、零知识证明、差分隐私等。

4. 轻量级密码与物联网安全：面向资源受限设备的密码算法及物联网安全协议。

5. 数字身份与零信任安全：抗量子身份认证、分布式数字身份、零信任架构。

6. 可信数据空间密码技术：面向可信数据空间的密码技术与应用。

7. 新型密码分析与评估：量子环境下的密码分析、自动化安全评估平台。

二、投稿要求

1. 稿件请用 word 格式录入，并套用本刊模板（http://files. chinaaet. com/files/Periodical/pcachina_ Templates. doc）。

2. 投稿文章不存在一稿多投现象。

3. 无抄袭、剽窃、侵权、虚假引用等不良学术行为，且不违反相关法律法规，不涉及国家、企业秘密，稿件文责自负。

4. 论文要求观点鲜明、逻辑严谨、论据充分、方法合理，字数在 5000~8000 字。

5. 请在官方投稿网站（http：//www. pcachina. com）注册、投稿。投稿请选“主题专栏”栏目，“稿件标题”填写“密码技术+文章题目”。稿件经评审合格录用后，在《网络安全与数据治理》2026 年第 8 期（正刊）以主题专栏形式发表。

三、时间安排

截稿日期：2026 年 7 月 15 日

出版日期：2026 年 8 月 15 日

《网络安全与数据治理》编辑部

2026 年 3 月

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