基于“云-边-端”的工业控制系统网络安全防御体系设计

Research on Design of Network Security Defense System of Industrial Control System Based on “Cloud-Edge-End”

李维汉[1]，戴晓婧[2]，周晓磊[2]，刘红再[2]，丁　攀[3]（1. 中国联合网络通信集团有限公司，北京 100033；2. 北京市产品质量监督检验研究院，北京 101300；3. 中国联通研究院，北京 100048）

Li Weihan[1]，Dai Xiaojing[2]，Zhou Xiaolei[2]，Liu Hongzai[2]，Ding Pan[3]（1. China United Network Communications Group Co.，Ltd.，Beijing 100033，China；2. Beijing Products Quality Supervision and Inspection Institute，Beijing 101300，China；3. China Unicom Research Institute，Beijing 100048，China）

摘　要：

在工业4.0的浪潮中，工业控制系统正面临着由数字化、互联网和智能化技术引领的深刻变革。现有的工业自动化架构存在限制，迫切需要向更灵活、更高效的“云-边-端”协同架构转变。以《工业控制系统网络安全防护指南》为指导，从技术、管理和运营等多个维度剖析“云-边-端”协同架构面临的安全风险并进行分析。聚焦防护指南的核心原则，并融入信息安全等级保护的评估实践，构建了一个全面而可靠的网络安全防御体系。

关键词：

“云-边-端”；工业控制系统；网络安全；风险评估

doi：10.12045/j.issn.1007-3043.2024.11.007

文章编号：1007-3043（2024）11-0037-06

中图分类号：TN915.1

文献标识码：A

开放科学（资源服务）标识码（OSID）：

Abstract：

In the wave of Industry 4.0，industrial control systems are facing profound changes led by digitalization，Internet and intelligent technologies. The existing industrial automation architecture has limitations，and there is an urgent need to shift to a more flexible and efficient “Cloud-Edge-End” collaborative architecture. Guided by the “Guide to Network Security Protection of Industrial Control Systems”，it analyzes the security risks faced by the “Cloud-Edge-End” collaborative architecture from multiple dimensions such as technology，management，and operation. Focusing on the core principles of the protection guidelines and integrating the assessment practices of classified information security protection，a comprehensive and reliable network security defense system is built.

Keywords：

Cloud-Edge-End；Industrial control system；Network security；Risk assessment

引用格式：李维汉，戴晓婧，周晓磊，等. 基于“云-边-端”的工业控制系统网络安全防御体系设计[J]. 邮电设计技术，2024（11）：37-42.

0 引言

在工业4.0的浪潮中，工业控制系统正面临着由数字化、互联网和智能化技术引领的深刻变革。这一变革的核心在于应用尖端信息技术来优化制造流程，增强生产效率和灵活性。通过融合创新技术，工业控制系统不仅提升了数据处理能力，还实现了更高级别的自动化和智能化。各类传统行业，如钢铁行业、装备制造行业、港口行业、电子行业等正不断探索数字化、智能化的发展道路，以期实现更高效、更智能的生产和管理[1]，原传统工业控制系统的架构正不断向云化方向发展。但在各行业利用云计算技术全面提升自动化生产力的同时，管理、技术、运营等多方面的网络安全风险不断暴露，多维度的网络安全问题不断升温，亟需建立新型网络安全防御体系。

本文针对基于“云-边-端”协同结构的工业控制系统提出新型网络安全防御体系，旨在全面提升云化工控领域的网络安全防御能力，为国家传统工控领域向更为智能高效的方向发展作出贡献！

1 基于“云-边-端”协同结构的工业控制系统

“云-边-端”协同架构实现的核心是要在金字塔

收稿日期：2024-10-15

内部体系实现解耦，并结合云计算技术实现云、边、端三方协同，这种新型架构包括如下3个层面[2-3]。

第一层面为云化控制系统管理平台，它可在集团企业的中心云平台部署，对分散在各工厂的云化控制系统进行管理，包括资源管理、组态管理、过程监控管理、算法与模型管理、接口管理、数据存储管理、安全管理等功能。

第二层面为边缘计算云平台，包含云化控制器、大数据分析、组态管理、过程监控模块。云化控制系统通过5G或有线网络实现对生产过程的控制和监视。

第三层面为工业网关，用于将现场设备接入云化控制系统，应具备接入管理、协议转换、数据处理、安全管理等功能。在协议转换方面，应支持不同厂家现场设备的统一接入。现场设备包括仪表、PLC、远程I/O设备、AGV、工业机器人等。

云端负责大规模数据处理、存储、智能分析和决策支持，而边缘端则更接近数据源，负责实时数据处理、预处理和快速响应，终端设备则负责数据采集、执行指令和现场控制。通过5G等高速通信技术，云、边、端之间可以实现快速、可靠的数据交换和协同工作[4]。“云-边-端”工业控制系统协同网络架构如图1所示。

2 网络安全风险及分析

由于将传统工业控制系统原有的全封闭架构进行解耦，将原来的软件及部分硬件产品实施云化控制和管理，“云-边-端”协同架构在工业控制系统中提供了强大的数据处理和存储能力，能够提升工业自动化和智能化水平[5-7]。在传统工业控制系统向云化控制和管理转型的过程中，同时也面临着一系列网络安全风险挑战，这些风险主要包括以下几个方面。

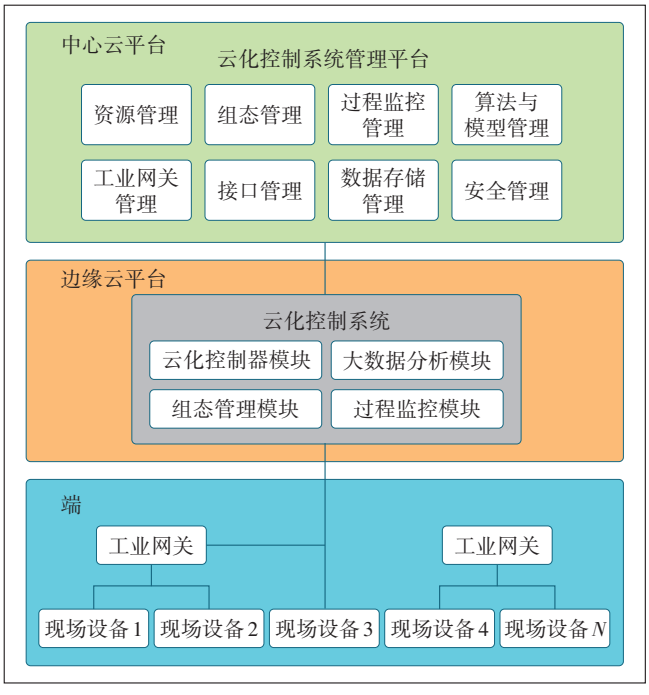

图1　“云-边-端”工业控制系统协同网络架构

a）安全管理方面风险。

（a）资产管理风险。由于资产识别不清、缺乏备份机制，可能导致数据丢失、法律问题、合规问题和潜在的财务损失[8]。

（b）配置管理风险。由于配置不当（如弱口令、权限设置不当等）及配置管理不完善，导致的未授权访问、敏感信息泄露风险。

（c）供应链安全风险。供应链中的任何环节都可能引入安全风险，特别是当使用第三方提供的硬件或软件时，攻击者可能通过供应链中的薄弱环节对工业控制系统进行攻击[9-10]。

（d）安全意识风险。由于人员安全意识不足导致的安全风险。

b）技术方面风险。

（a）主机与终端安全风险。由于防病毒措施缺失、非法安装恶意软件、设备身份鉴别策略不完善导致的数据泄露、非法入侵等安全风险。

（b）架构与边界安全风险。由于区域隔离不当、协议算法强度不足、标识不清导致的病毒传播、敏感信息截获、滥用等风险。

（c）上云安全风险。由于私有云安全整改不及时、云上虚拟化通信不受控、虚拟设备隔离措施不到位等导致的非法入侵、横向移动攻击、恶意流量攻击等风险[11]。

（d）应用安全风险。应用软件系统由于在运行使用过程中缺乏安全性测试以及快照完整性校验导致的恶意攻击、服务中断及数据丢失等风险[12]。

（e）系统数据安全风险。由于数据分类分级不明确、数据出境违规违法导致的数据可用性降低、数据完整性破坏以及法律法规风险。

c）安全运营风险。由于缺乏监测预警、应急处置措施，导致在发生安全事件时，缺乏快速响应机制，导致安全损失扩大，同时未定期进行系统安全评估和漏洞管理会导致机械故障、DDOS攻击等[13-15]。

依据国家《信息安全技术 信息安全风险评估方法》（GB/T 20984-2022）[6]及风险评估相关标准，风险

值计算的取值范围为1~25，按照5为一级的方法将风险等级划分为1~5共5个等级，风险等级越高对系统产生的危害就越大，风险越高（见表1）。

表1　风险对照表

风险值	1~5	6~10	11~15	16~20	21~25
风险等级	1	2	3	4	5
风险标识	很低	低	中等	高	很高

针对安全管理、技术、安全运营10类安全风险点，结合网络安全测评实践经验，使用定性和定量相结合的方式对以上风险点进行分析，得出每类风险的风险值和风险等级，最后得出风险等级很高的为3类，分别为应用安全、系统数据安全以及架构与边界安全，高风险问题为2类，分别为供应链安全以及上云安全。其余为中低风险问题。“云-边-端”工业控制系统风险值、风险等级分布及风险占比如图2和图3所示。

3 网络安全防御体系设计

云边端工控系统的网络安全架构是一个多层次、全方位的防御体系，它涵盖了从云端到边缘端再到终端设备的各个层面。针对不同级别的安全风险，从以下几个层面提出安全体系设计思路。

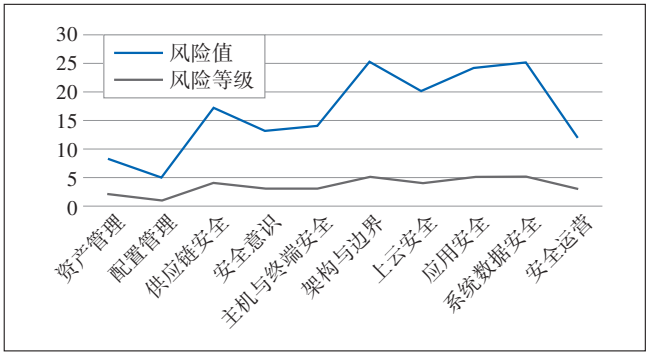

图2　“云-边-端”工业控制系统风险值及风险等级分布

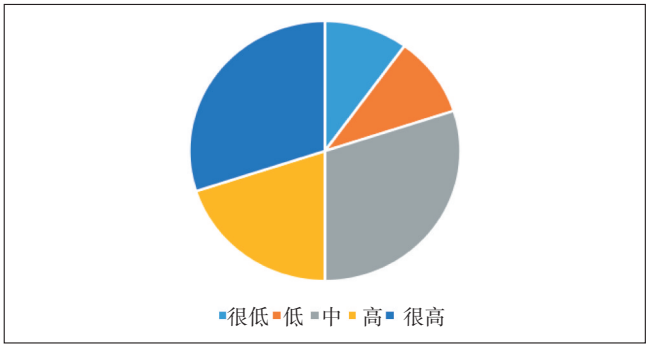

图3　“云-边-端”工业控制系统风险占比

3.1 管理层面设计

“技术是基础，管理是关键。”这一理念同样适用于工业控制系统的网络安全防护。为了确保这些系统的安全，关键在于建立一套高效的安全管理体系。这包括在资源配置、团队合作以及战略决策等方面采取有效措施，以确保网络安全措施能够充分发挥其应有的作用。管理层面安全设计包括如下几个方面。

a）梳理资产。为保护工业控制系统，需全面审查软硬件资产，建立更新的资产目录，并明确职责，定期审查。制定关键系统清单，加强保护，确保关键部件有备份。

b）强化配置。为降低工业控制系统受恶意攻击的风险，需强化网络安全管理，包括强化账户口令、制定安全配置清单，并定期审计调整策略。同时，应执行安全测试确保策略变更不影响功能安全，及时发现并解决安全问题。

c）注重评估。在加强工业控制系统网络安全时，企业需在技术和管理层面采取措施。技术方面，强化账户权限和口令管理，制定安全配置清单；管理方面，定期审查和更新安全策略。同时，进行安全测试以确保策略变更不影响系统功能和安全，及时发现并解决潜在问题。

d）明确责任。为了维护工业控制系统供应链的安全性，企业在与供应商签订合同时，应详细规定双方在安全管理体系、责任界定、访问授权、隐私维护、行为规范以及违约责任等方面的责任。这确保了所有合作伙伴都了解自己的安全职责，进而增强了合作期间的安全标准。

e）构建意识。工业企业应普及网络安全法规教育，提高员工安全意识，强化责任感。对运维人员进行专业培训和能力评估，构建全员参与的网络安全文化，保障工业控制系统安全。

3.2 技术层面设计

网络安全技术的应用以保障工业控制系统的功能安全为基础，已成为推动工业企业增长和创新的关键因素之一。它构成了强化工业控制系统网络安全防护的关键基础，通过提供有效的防御机制和保护措施，帮助企业应对针对这些系统不断演变的安全威胁和攻击。网络安全技术确保了工业控制系统的稳定运行，是提升其安全防护水平不可或缺的支撑。技术层面的安全设计包括如下几个方面。

3.2.1 主机和终端层面安全设计

主机和终端层面安全设计主要包括病毒防护和强化管控2个方面。

a）病毒防护。考虑到工业控制系统的特定需求，传统的桌面杀毒软件在工程师站、操作员站和数据库服务器等关键设备上的应用受到限制，可能不足以应对不断演变的安全威胁。因此，部署专门针对工业控制系统设计的防病毒软件对于维护系统安全至关重要，这些软件应专注于识别和阻止可能威胁工业控制系统的恶意代码和操作。在挑选工业主机的防病毒解决方案时，需要评估其适用性、操作便捷性、对系统性能的影响、技术支持的质量和更新服务的效率。同时，定期更新防病毒软件和评估安全措施的有效性，是保障工业控制系统主机安全的重要组成部分。

b）强化管控。利用工控安全卫士，可以为工业主机建立一个应用程序的白名单系统。这一系统通过制定一份包含合法应用程序、系统进程、对外开放的端口和程序以及允许访问的IP地址的白名单，实现对所有程序活动的严格监管。此外，实施双因素认证机制来控制访问和登录，以提高安全性。对于外部设备如光驱、USB接口、无线网卡和蓝牙等，进行细致的接口管理，并对U盘等移动存储设备的访问权限进行严格控制，提供多种访问控制策略选项。这些多元化的技术防护手段共同确保了只有合法的程序和用户才能执行相关操作，从而保护工控主机不受恶意软件和潜在的操作系统漏洞威胁。

3.2.2 架构与边界安全设计

架构与边界安全设计主要包括以下几个方面。

a）纵向边界防御。在企业管理网络与工业控制系统网络之间设置工业网闸，能够在物理和逻辑层面上实现两者的隔离，避免直接的网络连接。网闸的内外处理单元和安全数据交换机制，允许在内外网络主机间按照设定的时间间隔安全地传输数据。同时，在制造执行层、过程监控层和现场控制层部署工业防火墙，对工业通信协议进行深度分析，并利用通信白名单与智能学习技术，建立一个安全的工业控制网络通信架构，仅放行核准的协议，确保系统与外部网络的安全隔离。这些措施共同构成了一个多层次、全方位的工业控制系统网络安全防护体系。

b）横向边界防御。在工业控制系统架构中，过程监控层的工程师站和操作员站、实时数据库服务器，以及制造执行层的历史数据库服务器、先进过程控制（APC）服务器和生产计划服务器等组件，发挥着连接不同系统层级的核心作用。它们是数据收集和指令分发的枢纽，同时也负责不同通信协议间的转换任务。由于这些服务器所连接的设备和使用的通信协议通常是预先定义的，因此可以通过部署工业防火墙，实施基于数据包过滤和白名单机制的安全策略，以实现对这些服务器的横向逻辑隔离和访问权限控制。这样的措施确保了只有获得授权的设备才能够与服务器进行通信，从而保障了整个系统的安全性。

c）远程访问控制。在实现设备通过广域网公共通信链路接入以及进行远程访问和维护时，安全防护是至关重要的。通过部署边缘安全网关并启用其虚拟私人网络（VPN）功能，结合加密与认证技术，可以有效地保障远程访问的安全。利用国内商用密码算法对控制指令和重要数据在传输过程中进行加密保护，并在设备接入工业控制系统网络时进行身份验证，确保了数据传输和远程控制指令的安全性。这不仅保障了数据传输的机密性，也维护了数据的完整性，防止了在传输过程中的信息泄露或被篡改的风险。

3.2.3 上云安全设计

工业云平台网络安全的构建可通过整合虚拟化与硬件安全设备资源，创建一个统一的资源池，使得安全性能能够根据实际需求进行动态分配和扩展，从而更加精准地满足工业云平台的安全需求。同时，通过实施国产商用密码技术，建立数字证书和可信的认证机制，通过VPC、云防火墙或安全组设置访问控制规则，可以解决工业设备接入云平台时的安全问题，包括未经授权的访问、控制指令的篡改以及数据截取等风险。这些技术的应用确保了设备在连接到工业云平台时的身份验证过程的安全性。

3.2.4 应用安全设计

对于访问制造执行系统（MES）、组态软件及工业数据库等关键应用，应实施基于角色的身份认证，并为每个用户分配最小的访问权限。这有助于确保用户仅能访问其工作职责内的必要信息。同时，通过加强密码策略和账户验证，引入双因素认证，可以进一步提升安全性。此外，在应用程序中实施严格的输入验证和过滤，对于防止恶意输入和攻击者利用潜在的应用漏洞至关重要，有效防御跨站脚本攻击（XSS）和SQL注入等常见的网络攻击手段。通过校验技术或者密码技术对虚拟机镜像、快照完整性进行校验，发现镜像或快照变更时进行告警。

3.2.5 系统数据安全设计

在工业生产过程中，数据的生成遍布各个环节。为了确保数据在流转过程中的安全性，并充分发挥其潜在价值，对工业数据采取了包括分类、分级、标记用途、加密、访问控制和脱敏等一系列综合防护措施。这些措施覆盖了数据从采集、传输、存储到处理的整个生命周期，旨在实现数据安全的目标，即确保数据“拿不到”“看不懂”“改不了”以及“赖不掉”。通过这种全方位的数据保护策略，可以有效地保护工业数据的安全，同时确保数据价值的最大化。

a）收集安全。工业数据可分为生产、管理、研发和运维数据，按关键程度分为一般、重要和核心数据。这种分类和分级策略有助于系统化数据管理，优化存储、处理和分析流程，并提供精细化的数据安全保护。

b）存储安全。针对数据的分类和安全级别，实施一系列安全策略来保护数据存储的安全。这包括对数据进行加密处理，以防止未经授权的访问和解读；确保数据完整性，防止数据在存储或传输过程中被篡改；采取有效的数据防泄漏措施，以避免数据被非法复制或传输；通过精细的访问控制机制，确保只有授权用户才能访问敏感数据。这些综合性的安全措施共同构成了一个坚固的数据保护体系，以维护数据的保密性、完整性和可用性。

c）使用加工安全。工业数据的深度加工和应用是提升生产效率和质量的关键，需通过技术迭代优化流程。同时，保护高价值数据安全，实施防泄漏、访问控制等措施，确保数据安全和合法使用，以最大化数据价值。

d）传输安全。数据传输环节是数据安全的关键所在，因此采取密码技术、校验技术等方法来确保数据在传输过程中的保密性、完整性和可靠性是必不可少的。这些技术的应用可以有效防止数据在传输过程中遭受窃取或非法篡改，确保数据安全地从一个系统传输到另一个系统。这些措施构成了数据传输安全的基础，为数据的保密性和完整性提供了强有力的保障。

3.3 运营层面设计

随着针对工业控制系统的网络攻击手段层出不穷，仅靠安全设备的被动防御已不足以应对当前严峻的网络安全挑战。工业控制系统的网络安全运营是一个持续的、综合性的过程，它需要将人力资源、技术应用和操作流程有效结合，以保护系统免受网络攻击和威胁的侵害。网络安全运营必须考虑到工业企业生产环境的独特性、复杂性和多样性，依托安全运营中心，采用监测预警、应急处理、漏洞管理和安全评估等手段进行安全管理。这一过程强调安全资源的集中和高效利用，并以将安全措施与业务流程紧密结合为目标，建立一个能够适应工业生产业务流程的安全编排和自适应安全架构。通过引入自动化工具和技术，优化数据采集和分析流程，减少人为干预，同时提升数据的准确性和处理的及时性。

3.4 安全责任落实层面设计

工业企业承担本企业工控安全主体责任，建立工控安全管理制度，明确责任人和责任部门，按照“谁运营谁负责”“谁主管谁负责”的原则落实工控安全保护责任。强化企业资源保障力度，确保安全防护措施与工业控制系统同步规划、同步建设、同步使用。

综上所述，应构建安全管理、技术防护、安全运营三大层面网络安全防御体系，压紧压实网络安全责任，不断提升云化工控系统网络安全防御能力，“云-边-端”协同结构的工业控制系统安全防御体系架构如图4所示。

4 总结与展望

在“云-边-端”架构的支持下，工业控制系统构建了一套综合性的多层网络安全防御机制。这一机制通过云中心的集中管理、边缘计算的快速响应以及现场设备的直接控制，抵御各种安全威胁，确保工业生产的连续性和安全性。

面对新兴技术的快速发展，平衡创新与安全变得尤为重要。这需要政府、企业和社会各界的共同努力，不断提升安全防护措施，提高网络安全意识，共同应对日益复杂的安全挑战。推动工业控制系统向更智能、更高效、更安全的方向发展，以满足日益复杂的生产需求和安全挑战。

参考文献：

[1] 王健全，马彰超，孙雷，等. 工业网络体系架构的演进、关键技术及未来展望[J]. 工程科学学报，2023，45(8)：1376-1389.

[2] 马超伟. 边缘计算：一文理解云边端协同架构中的高性能云计算、边缘计算、云边协同[EB/OL]. [2024-08-14]. https://developer.aliyun.com/article/1143858.

[3] 边缘计算. “云管边端”协同的边缘计算安全防护解决方案[EB/OL]. [2024-08-14]. https://cloud.tencent.com/developer/article/1711148.

[4] 工业和信息化部. 工业和信息化部关于印发工业控制系统网络安

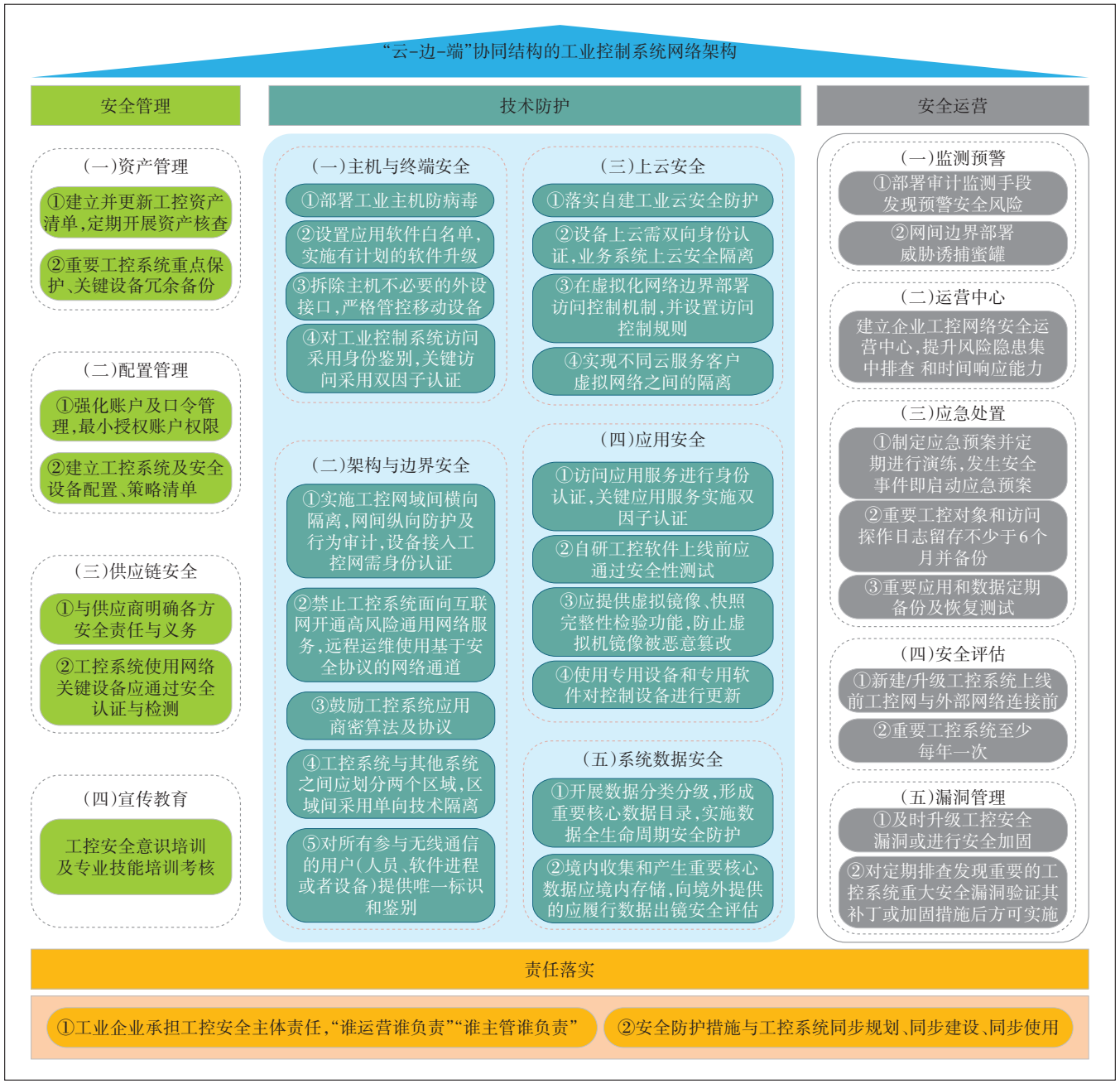

图4　“云-边-端”协同结构的工业控制系统安全防御体系架构

全防护指南的通知[EB/OL]. [2024-08-14]. http://www.cnpci.org.cn/uploads/soft/240202/1_1556528651.pdf.

[5] 国家市场监督管理总局，中国国家标准化管理委员会. 信息安全技术 网络安全等级保护基本要求：GB/T 22239-2019[S]. 北京：中国标准出版社，2019.

[6] 国家市场监督管理总局，中国国家标准化管理委员会. 信息安全技术 信息安全风险评估方法：GB/T 20984-2022[S]. 北京：中国标准出版社，2022.

[7] 邱云鹏，阎华，肖璐婷. 港口工控系统信息安全体系建设[J]. 港口科技，2024(2)：38-42.

[8] 陈飞，付德志，崔书方，等. 基于VMware虚拟化技术的企业数据中心网络安全架构研究[J]. 网络安全技术与应用，2024(4)：26-29.

[9] 张元龙，郭飞，陈雨，等. 基于安全域技术的网络安全架构优化初探——以辽宁省气象局为例[J]. 网络安全技术与应用，2024(6)：135-137.

作者简介：
李维汉，硕士，主要从事工业互联网解决方案研究工作；戴晓婧，硕士，主要从事网络安全技术研究工作；周晓磊，学士，主要从事商用密码应用安全性评估理论研究工作；刘红再，学士，主要从事网络安全等级保护测评理论研究工作；丁攀，硕士，主要从事网络与信息安全技术研究工作。