工业互联网信息安全防护技术研究

刘军涛　王　冰
河南省信息咨询设计研究有限公司　河南　郑州　450008

摘　要：工业互联网信息安全防护技术研究旨在应对日益复杂的网络安全威胁，确保工业系统的稳定运行和数据安全。通过探讨工业互联网信息安全防护策略和技术，包括数据加密、访问控制、自适应防护架构等，构建全面的安全防护体系，致力提升工业互联网的整体安全水平，保障工业生产的安全性和连续性，推动工业领域的数字化转型和智能化升级。

关键词：工业；互联网；信息安全；防护技术

引言：工业互联网信息安全防护技术研究在数字化转型背景下显得尤为重要。随着工业互联网的广泛应用，其面临的网络攻击和数据泄露风险也日益增加。为确保工业生产的安全稳定，保护关键数据不受侵害，需深入研究并应用先进的信息安全防护技术。本文旨在探讨工业互联网信息安全防护的关键技术，为构建安全可靠的工业互联网环境提供理论支持和实践指导。

1 工业互联网概述

工业互联网是全球工业系统与高级计算、分析、感应技术以及互联网连接深度融合的产物，它通过智能机器间的连接，最终实现人机连接，结合软件和大数据分析，重构全球工业，激发生产力，使世界更加美好、快速、安全、清洁和经济。工业互联网的核心在于其平台，该平台能够将设备、生产线、工厂、供应商、产品和客户紧密地连接融合起来，形成一个开放、全球化的网络。它支持大规模设备的连接和管理，实现数据的实时采集、传输和分析，为企业提供实时的生产运营信息和决策支持[1]。同时，工业互联网还引入了人工智能、机器学习等先进技术，实现设备和系统的智能化管理，包括设备故障预测、优化生产计划、自动化决策等功能。另外，工业互联网的应用领域广泛而深入，几乎涵盖了所有工业制造领域。在智能制造方面，它帮助企业实现生产线的自动化、信息化和智能化，提高生产效率、降低生产成本，并实现个性化的定制生产。在智能供应链管理方面，工业互联网能够实现供应链各环节的数据共享和协同，优化资源配置，提高物流效率，降低库存成本。

2 工业互联网信息安全防护关键技术

2.1 固件安全增强

固件是嵌入在硬件设备中的软件，负责控制设备的基本功能和行为。在工业互联网环境中，固件的安全直接关系到整个系统的稳定性和数据的安全性。固件安全增强的深度实现，需要从多个方面入手。（1）工业互联网设备供应商需从操作系统内核、协议栈等核心层面进行安全加固，通过优化代码结构、增强访问控制、实施加密措施等手段，防止恶意代码的传播与运行。这要求供应商具备深厚的底层技术能力和丰富的安全开发经验。（2）固件安全增强还需关注固件的自主可控性。供应商应努力实现固件代码的自主可控，避免使用第三方库或组件可能带来的安全漏洞。通过自主研发和测试，确保固件在设计和实现过程中不存在已知的安全隐患。（3）固件安全增强还需要与硬件安全相结合。例如，为接入工业互联网的现场设备提供基于硬件特征的唯一标识符，为上层应用提供基于硬件标识的身份鉴别能力。同时，将安全芯片或安全固件作为系统信任根，为设备的安全启动以及数据传输的机密性和完整性提供硬件级别的保护。

2.2 漏洞修复加固

随着工业互联网的快速发展，设备和系统日益复杂，漏洞的存在成为威胁系统安全的重要因素。首先，漏洞修复加固的核心在于及时发现并修复系统中的安全漏洞。这要求工业互联网企业建立全面的漏洞管理机制，包括漏洞扫描、漏洞评估、漏洞修复和漏洞验证等环节。通过定期或不定期的漏洞扫描，企业可以及时发现系统中存在的安全漏洞，并评估其危害程度。随后，根据漏洞的严重性和影响范围，制定详细的修复计划，并尽快实施修复措施。在漏洞修复加固过程中，企业还需要注重以下几个方面的深度实施：及时性：漏洞的修复必须迅速及时，以避免漏洞被恶意利用造成损失。企业应建立快速响应机制，确保在发现漏洞后能够迅速启动修复流程。全面性：漏洞修复应覆盖系统中的所有设备和组件，不留死角。有效性：修复措施必须有效，能够彻底消除漏洞带来的安全威胁。在修复完成后，企业

应进行漏洞验证测试，确保漏洞已被成功修复且未引入新的安全问题。持续性：漏洞修复加固是一项长期的工作，企业需要持续关注系统和设备的安全状况，定期进行漏洞扫描和修复加固工作。

2.3 补丁升级管理

补丁升级管理的深度实施，要求企业建立科学、高效的补丁管理机制，确保补丁的及时获取、测试、部署和监控。工业互联网企业应密切关注各类安全漏洞的发布情况，及时从权威机构（如CVE、中国国家信息安全漏洞库等）获取最新的漏洞信息和补丁更新。这要求企业具备高度的安全意识和敏锐的市场洞察力，能够迅速响应安全威胁。另外，在获取补丁后，企业需要进行严格的测试验证，确保补丁的兼容性和稳定性。测试过程中，应模拟生产环境，对补丁进行全面的功能测试和性能测试，以避免补丁部署后引发的新的安全问题。随后，企业应制定详细的补丁部署计划，明确部署的时间、范围、步骤和责任人。在部署过程中，需要确保补丁的完整性和准确性，避免出现补丁损坏或安装错误的情况。同时，还需要对补丁的部署过程进行严格的监控和记录，以便后续的安全审计和追溯。最后，补丁升级管理还需要注重后续的监控和维护工作。企业应建立补丁管理的长效机制，定期对已部署的补丁进行复查和更新，确保系统的安全性和稳定性。

2.4 硬件安全增强

硬件安全增强主要涉及多个方面，首先是硬件设计的加固。这包括采用防篡改设计原则，确保硬件系统的安全性和完整性，防止任何未经授权的修改或破坏。例如，通过高强度的物理防护措施，如加密芯片、防拆卸设计等，可以有效防止硬件被物理破坏或篡改。除此之外，硬件安全模块（HSM）的集成也是硬件安全增强的重要手段。HSM是一种用于保护密钥和加密操作的独立硬件单元，通过提供安全的密钥存储和加密操作环境，可以显著提高系统的抗攻击能力。这种模块通常具有防篡改、防物理攻击等特性，能够确保密钥和敏感数据的安全。在工业互联网环境中，硬件安全增强还需要考虑与软件安全、网络通信安全等其他安全技术的协同作用[2]。例如，通过硬件级别的身份认证和访问控制机制，可以确保只有合法用户和设备才能访问系统资源，从而有效防止非法入侵和数据泄露。同时，硬件安全增强还需要与软件安全加固、网络通信加密等技术相结合，形成多层次的防护体系，以应对日益复杂的网络安全威胁。

2.5 运维管理

工业互联网信息安全防护的运维管理技术是一项复杂而关键的任务，它要求企业在日常运营中持续监控、维护和优化整个系统的安全状态。（1）工业互联网企业应建立全面的运维管理体系，明确各级运维人员的职责和权限，确保运维工作的有序进行。这一体系应涵盖从设备巡检、故障排查到应急响应等各个环节，确保在出现安全事件时能够迅速响应并有效处置。（2）运维管理需要借助先进的技术手段，如自动化运维工具、智能监控系统和大数据分析平台等，实现对工业互联网系统的实时监控和预警。通过这些技术手段，运维人员可以及时发现潜在的安全威胁和异常行为，并采取相应的措施进行处置，从而有效降低安全风险。（3）运维管理还需要注重流程优化和持续改进。企业应定期对运维流程进行评估和审查，发现存在的问题和不足，并制定相应的改进措施。通过不断优化运维流程，提高运维效率和安全性，确保工业互联网系统的稳定运行。

3 工业互联网信息安全防护措施

3.1 提升人员招聘标准

在工业互联网信息安全防护领域，提升人员招聘标准是确保整个安全防护体系有效性的关键一步。企业应明确安全岗位的职责和要求，确保招聘标准与岗位需求紧密匹配。这包括但不限于对候选人的专业技能、工作经验、教育背景等方面的具体要求。例如，在招聘网络安全工程师时，企业可以设定诸如“熟悉常见安全漏洞的原理、危害及解决方案”、“具备扎实的网络安全理论基础和实战经验”等具体标准。接着，企业应注重考察候选人的综合素质和潜力。除了专业技能外，良好的学习能力、沟通能力、团队协作能力以及创新思维等也是安全人员不可或缺的品质。这些素质将直接影响到候选人在未来工作中的表现和发展潜力。为了提升招聘标准的深度和广度，企业可以采取多种措施。例如，建立科学的招聘流程，包括简历筛选、笔试、面试、背景调查等环节，确保每个环节都能全面、深入地评估候选人的能力和素质。同时，企业还可以利用专业的招聘工具和技术手段，如在线测评系统、人工智能筛选等，提高招聘效率和准确性。

3.2 制定并实施统一的安全策略

工业互联网信息安全防护措施中，制定并实施统一的安全策略确保了所有设备和系统都能遵循一致的安全标准，从而有效降低安全风险。（1）明确安全目标。企业需要明确工业互联网信息安全防护的总体目标，如保护关键基础设施、防止数据泄露、确保业务连续性等。这些目标将作为制定安全策略的基础和导向。（2）风险评估与策略制定。企业应对工业互联网系统进行全面的

风险评估，识别潜在的安全威胁和漏洞。这包括对网络架构、设备配置、应用软件、数据存储与传输等方面进行深入分析。基于风险评估结果，制定针对性的安全策略。策略应涵盖身份认证、访问控制、数据加密、漏洞管理、应急响应等多个方面，确保每个关键环节都有相应的安全措施。（3）策略实施与监督。将制定好的安全策略落实到具体工作中，包括配置安全设备、部署安全软件、培训员工等。实施过程中应确保所有设备和系统都能按照安全策略的要求进行配置和管理。建立监督机制，定期对安全策略的实施情况进行检查和审计。通过监控日志、安全事件报告等手段，及时发现并纠正不符合安全策略的行为。

3.3 建立安全数据仓库

安全数据仓库的首要任务是集成来自工业互联网各个环节的数据，包括设备数据、网络数据、应用数据等。这些数据往往来源于不同的系统和平台，格式多样、质量参差不齐。因此，在集成过程中，需要进行数据清洗和转换，确保数据的准确性和一致性。另外，安全数据仓库需要支持大规模数据的存储和处理，因此应选择高性能、可扩展的数据存储技术，如分布式文件系统或列式存储。为确保数据的安全性，应对存储的数据进行加密处理，防止数据泄露和非法访问[3]。制定完善的数据备份和恢复策略，确保在数据丢失或损坏时能够迅速恢复。安全数据仓库不仅用于存储数据，更重要的是对数据进行深度分析和挖掘，以发现潜在的安全威胁和异常行为。通过运用大数据分析、机器学习等技术手段，可以实现对海量数据的快速处理和智能分析，为安全防护提供有力支持。基于安全数据仓库的分析结果，企业可以不断优化和调整安全策略。例如，根据威胁情报和攻击趋势，调整防火墙规则、加强访问控制等，以提升整体安全防护水平。

3.4 建立自适应防护架构

工业互联网信息安全防护措施中，建立自适应防护架构是应对复杂多变安全威胁的重要手段。这一架构通过动态分析安全环境、自动调整防护策略，确保工业互联网系统能够持续、有效地抵御各类攻击。

3.4.1 核心要素

自适应防护架构包含多个核心要素，如感知层、分析层、决策层和执行层。感知层负责收集来自工业互联网系统的各类安全数据；分析层则运用大数据分析、机器学习等技术对数据进行深度挖掘，识别潜在的安全威胁；决策层基于分析结果制定防护策略；执行层则负责将策略转化为实际行动，如阻断攻击、隔离受感染设备等。

3.4.2 动态调整

自适应防护架构的核心在于其动态调整能力。随着安全威胁的不断演变和变化，传统的静态防护策略往往难以应对。而自适应防护架构则能够根据安全环境的变化，自动调整防护策略，确保防护措施的针对性和有效性。这种动态调整能力有助于企业及时应对新型攻击手段，降低安全风险。

3.4.3 协同防御

在工业互联网系统中，各个设备和系统之间往往存在复杂的交互关系。因此，自适应防护架构还需要具备协同防御的能力。通过实现各节点之间的信息共享和联动响应，自适应防护架构能够构建一个多层次、全方位的防护体系，提升整体安全防护水平。

3.4.4 持续监控与优化

为了确保自适应防护架构的有效性，企业还需要建立持续监控与优化的机制。通过对系统运行的实时监控和定期评估，企业可以及时发现并修复潜在的安全漏洞和弱点，优化防护策略和措施，确保工业互联网系统的长期稳定运行。

结语

总之，工业互联网信息安全防护技术的研究对于保障工业生产的顺利进行和数据资产的安全至关重要。随着技术的不断进步和威胁的日益复杂，我们需持续关注并探索更加高效、智能的安全防护策略。未来，通过加强技术创新、完善防护体系、提升应急响应能力，我们有信心构建出更加坚固的工业互联网信息安全防线，为工业数字化转型和智能化发展保驾护航。

参考文献

[1]杨帆,闫育芸,魏玉峰,杭肖.基于工业互联网平台数据安全评估的设计[J].工业控制计算机,2021,34(5):1-2.

[2]姚卓.基于实战化的集团企业网络安全主动防御技术研究与实践[J].信息技术与网络安全,2022,41(5):25-31.

[3]重视智能网联汽车产业发展与安全共振[J].自动化博览,2020(11):56-59.