工业互联网背景下的网络安全风险评估与应对策略

赵宝春
中国电力科学研究院有限公司 北京 100192

摘　要：本文在工业互联网快速发展的背景下，深入研究了网络安全风险评估与应对策略。通过对工业互联网架构及其安全挑战的分析，系统评估了网络安全风险，识别了感知层、网络层、平台层和应用层的关键风险点。采用定性、定量和综合评估方法，构建了适用于工业互联网的网络安全风险评估框架。以智能工厂为案例，详细分析了其面临的网络安全风险，并提出了包括技术防护、管理制度和教育培训在内的综合性应对策略。研究表明，综合应用这些策略能够有效提升工业互联网的整体安全防护水平，保障企业的正常运营和社会稳定。最后，对研究的不足之处进行了反思，并展望了未来工业互联网网络安全的发展趋势和研究方向。

关键词：工业互联网；网络安全；风险评估；应对策略；智能工厂

引言

工业互联网是新一代信息技术与工业系统深度融合的产物，因全球工业转型升级需求而生，通过集成物联网等技术实现生产智能化，应用于多领域且意义重大。

但其快速发展伴随突出的网络安全问题：敏感数据泄露风险高，网络攻击或致生产中断、设备损坏，且其复杂性使传统防护难应对新型威胁。

本文旨在研究工业互联网环境下的网络安全风险评估与应对策略，通过系统评估识别关键风险点并提出针对性措施，以提升整体安全防护水平，这对保障企业运营及维护社会、国家安全意义重大。

1 工业互联网概述及其安全挑战

工业互联网是指将互联网技术、物联网技术、大数据分析、云计算等新一代信息技术与工业系统深度融合的新型基础设施。其核心要素包括智能设备、网络连接、平台服务和数据分析。智能设备是工业互联网的基础，负责数据的采集和执行指令；网络连接确保数据在不同设备、平台之间的传输；平台服务提供数据存储、处理和应用开发环境；数据分析则是通过对海量数据的挖掘，实现智能决策和优化。

然而，工业互联网的发展也面临着严峻的安全挑战。首先，数据泄露是其中一个重要问题。工业互联网涉及大量敏感数据，如生产数据、用户信息等，一旦泄露，将造成严重损失。其次，网络攻击威胁日益加剧。黑客可能通过攻击工业控制系统，导致生产中断甚至设备损坏。此外，工业互联网的复杂性和多样性也增加了安全管理的难度，传统的安全防护手段难以应对新型攻击手段。

工业互联网的安全问题不仅影响企业的正常运营，还可能对社会稳定和国家安全造成威胁。因此，必须采取有效的应对策略，如加强数据加密、提升网络防护能力、建立多层次的安全防护体系等。同时，还需加强安全技术研发和人才培养，构建全面的工业互联网安全防护体系。

2 网络安全风险评估方法

在工业互联网背景下，网络安全风险评估是确保系统安全的重要环节。常见的网络安全风险评估方法包括定性分析、定量分析和综合评估等。

定性分析方法主要通过专家经验和主观判断来评估风险，具有操作简便、成本低的优点。其核心在于对风险因素进行分类和等级划分，适用于缺乏历史数据或技术细节的场景。然而，定性分析的局限性在于主观性强，评估结果可能因专家意见不同而存在较大差异。

定量分析方法则依赖于数据和数学模型，通过量化风险发生的概率和潜在损失，提供更为精确的评估结果。该方法的优势在于客观性强，能够直观反映风险程度。但其局限性在于对数据质量要求高，且在数据缺乏的情况下难以应用。

综合评估方法结合了定性和定量的优点，通过多层次、多维度的分析，全面评估网络安全风险。该方法能够弥补单一方法的不足，提供更为全面的风险评估结果。但其复杂性和实施成本较高，需要跨学科的专业知识和资源支持。

针对工业互联网的特点，构建适用的网络安全风险评估框架至关重要。该框架应涵盖风险识别、风险分析、风险评价和风险应对等环节。首先，风险识别应全面考虑工业互联网的各个层级，包括感知层、网络层、平台层和应用层。其次，风险分析需结合定性和定量方法，评估风险发生的可能性和影响程度。再次，风险评价应根据评估结果对风险进行排序，确定优先处理的风险。最后，风险应对应制定针对性的安全策略，包括技术防护、管理措施和应急响应等。

为更清晰地展示风险评估流程，图 2 提供了网络安全风险评估流程图。如图所示，整个流程从风险识别开始，经过风险分析、风险评价，最终到达风险应对环节，形成一个闭环管理过程。

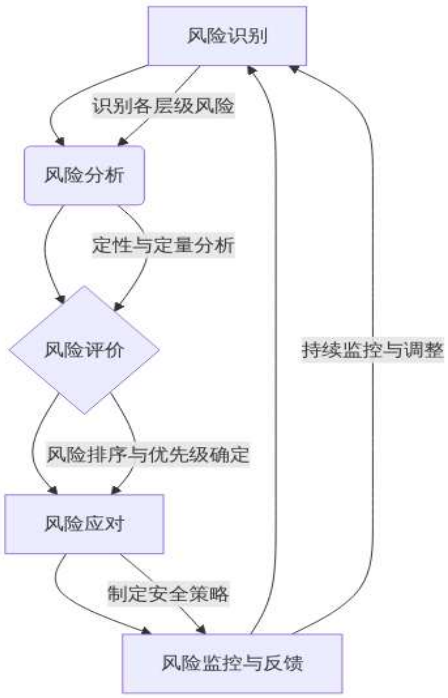

图 1 网络安全风险评估流程图

通过该框架，工业互联网企业可以系统地评估网络安全风险，制定有效的应对策略，提升整体安全防护水平。

3 工业互联网网络安全风险评估案例分析

在工业互联网背景下，选取智能工厂作为具体的应用场景进行网络安全风险评估。智能工厂集成了物联网、大数据、云计算等先进技术，实现了生产过程的自动化和智能化。然而，其复杂的技术架构也带来了诸多安全风险。

首先，进行风险识别。智能工厂的网络安全风险主要分布在感知层、网络层、平台层和应用层。感知层涉及大量传感器和执行设备，易受物理破坏和信号干扰；网络层是数据传输的通道，面临数据泄露和网络攻击的风险；平台层负责数据存储和处理，存在数据篡改和系统漏洞的风险；应用层直接面向用户，易受到恶意软件和钓鱼攻击。

接下来，采用综合评估方法进行风险分析。结合定性和定量分析，评估各项风险发生的可能性和影响程度。定性分析通过专家打分法，对各项风险进行等级划分；定量分析则通过历史数据和数学模型，计算风险发生的概率和潜在损失。

根据评估结果，编制风险评估结果表（见表 1）。表中列出了各项风险的等级和具体描述。

表 1 风险评估结果表

风险类别	风险等级	风险描述
感知层物理破坏	高	传感器和执行设备易受物理破坏，导致数据采集失效
网络层数据泄露	高	数据在传输过程中易被窃取，造成敏感信息泄露
平台层数据篡改	中	数据存储和处理过程中存在被篡改的风险，影响生产决策
应用层恶意软件	中	用户端易受到恶意软件攻击，导致系统瘫痪或数据丢失
网络层网络攻击	高	面临 DDoS 攻击、钓鱼攻击等，可能导致系统瘫痪或数据泄露

通过表 1 可以看出，智能工厂的主要安全风险集中在网络层和感知层。网络层的数据泄露和网络攻击风险等级均为高，表明数据传输过程的安全性亟待加强。感知层的物理破坏风险同样等级较高，说明设备的物理防护措施需进一步完善。

进一步分析发现，平台层和应用层虽风险等级相对较低，但也不容忽视。平台层数据篡改风险可能影响生产决策的准确性，应用层恶意软件攻击则直接威胁用户端的系统安全。

综上所述，智能工厂在工业互联网背景下面临多层次的网络安全风险。高风险区域主要集中在网络层和感知层，需重点加强数据传输的加密保护和设备的物理防护。同时，平台层和应用层的安全措施也应同步提升，确保整体系统的安全稳定运行。

4 网络安全应对策略

在工业互联网背景下，针对智能工厂所面临的网络安全风险，提出综合性应对策略至关重要。首先，技术防护是基础且关键的一环。具体实施方法包括：在感知层，采用物理隔离和加固技术，确保传感器和执行设备免受物理破坏；在网络层，部署高级加密标准（AES）和虚拟专用网络（VPN），防止数据在传输过程中被窃取或篡改；在平台层，引入多层

次的身份验证和访问控制机制，防止未授权访问和数据篡改；在应用层，使用防病毒软件和入侵检测系统（IDS），及时识别和阻断恶意软件和钓鱼攻击。预期效果是显著提升各层级的防护能力，降低安全事件的发生概率。

其次，管理制度的建设和完善是保障网络安全的重要手段。具体措施包括：制定详细的网络安全政策和管理流程，明确各级人员的职责和操作规范；建立风险评估和应急响应机制，定期进行风险评估，制定应急预案并进行演练；实施日志管理和审计制度，记录和分析系统活动，及时发现异常行为。预期效果是通过规范化管理，提升整体安全意识和应急处理能力。

综上所述，综合性应对策略的实施能够从技术、管理和人员等多维度提升工业互联网的网络安全防护水平。技术防护提供了基础保障，管理制度确保了规范运行，教育培训则增强了人员素质，三者相辅相成，共同构建起坚实的网络安全防线。通过这种综合性的应对策略，可以有效降低网络安全风险，保障工业互联网的稳定运行。

5 结论与展望

本文深入探讨了工业互联网背景下的网络安全风险评估与应对策略，系统评估了网络安全风险，识别了关键风险点，并提出了针对性的应对措施。研究表明，智能工厂等应用场景面临多层次的网络安全风险，尤其是网络层和感知层的高风险区域需重点防护。技术防护、管理制度和教育培训的综合应用，可有效提升工业互联网的安全防护水平。

展望未来，工业互联网网络安全的发展趋势和研究方向主要包括：一是加强跨学科融合，推动风险评估方法的创新；二是提升应对策略的智能化和自适应能力，实现动态防护；三是构建多方协同的安全生态，形成全社会共同参与的防护体系。通过持续研究和实践，有望进一步夯实工业互联网的安全基础，保障其健康可持续发展。

参考文献：

[1] 肖玉梅 , 黄渝铭 , 李丹 , 等 . 面向 5G 网络的工业互联网安全技术分析 [N]. 河北经济日报 ,2025–01–24(011).

[2] 王宝岩 , 周宁 . 面向工业互联网的网络安全防护技术研究 [J]. 家电维修 ,2025,(01):71–73.

[3] 罗进 . 工业互联网环境下电力设备网络安全风险评估 [J]. 邮电设计技术 ,2024,(11):75–81.

[4] 张宇 . 工业互联网网络数据安全分析与研究 [J]. 中国信息界 ,2024,(07):57–58.

[5] 吕金虎 , 任磊 , 谭少林 , 等 . 工业互联网层级架构与安全 : 复杂网络新视角 [J/OL]. 中国科学 : 技术科学 ,1–11[2025–07–10].http://kns.cnki.net/kcms/detail/11.5844.TH.20241017.2108.004.html.

作者简介：赵宝春（1993—），男，汉，河北保定，中国电力科学研究院有限公司，大学本科，无，网络安全。