5G 网络切片技术在工业互联网安全防护中的应用分析

李琴琴

新疆再生资源集团有限公司　新疆乌鲁木齐

【摘要】5G 网络切片技术作为 5G 核心能力之一，通过将物理网络划分为多个虚拟网络，实现资源的按需分配与隔离。工业互联网面临的安全威胁日益复杂，传统安全防护手段难以满足高效、灵活的安全需求。网络切片技术在工业互联网中不仅提升了网络资源利用率，还增强了不同应用场景的安全隔离能力，有效防范网络攻击与数据泄露。本文围绕 5G 网络切片在工业互联网安全防护中的应用，分析其关键技术及优势，探讨具体应用场景及存在的挑战，旨在为工业互联网安全防护提供创新思路和技术支持。

【关键词】5G 网络切片；工业互联网；安全防护；虚拟化；网络隔离

【收稿日期】2025 年 5 月 16 日　【出刊日期】2025 年 6 月 7 日　【DOI】10.12208/j.aics.20250019

Analysis of the application of 5g network slicing technology in industrial internet security protection

Qinqin Li

Xinjiang Renewable Resources Group Co., Ltd. Urumqi, Xinjiang

【**Abstract**】As one of the core capabilities of 5G, 5G network slicing technology enables on-demand resource allocation and isolation by dividing a physical network into multiple virtual networks. The industrial Internet is facing increasingly complex security threats, and traditional security protection methods struggle to meet the needs for efficient and flexible security. In the industrial Internet, network slicing technology not only improves the utilization of network resources but also enhances the security isolation capability for different application scenarios, effectively preventing network attacks and data leakage. Focusing on the application of 5G network slicing in industrial Internet security protection, this paper analyzes its key technologies and advantages, explores specific application scenarios and existing challenges, aiming to provide innovative ideas and technical support for industrial Internet security protection.

【**Keywords**】5G network slicing; Industrial Internet; Security protection; Virtualization; Network isolation

引言

工业互联网作为新一代信息技术与制造业深度融合的重要载体，促进了工业生产的智能化和数字化转型。但伴随大量设备接入与数据交互，工业网络面临越来越严峻的安全挑战，传统网络架构和安全策略难以应对复杂多变的攻击手段。5G 网络切片技术通过实现网络虚拟化和资源隔离，能够为不同工业应用提供定制化、安全可靠的网络环境，极大提升安全防护能力。本文将重点分析 5G 网络切片技术在工业互联网中的安全防护作用，深入探讨其技术优势及实际应用中的关键问题，助力推动工业互联网安全防护体系的创新发展。

1 工业互联网安全面临的挑战与需求

工业互联网的快速发展推动了制造业的数字化转型，但网络安全问题愈发严峻。工业互联网涉及大量工业终端、智能设备和数据中心，这些节点的互联互通导致攻击面急剧扩大。黑客攻击、恶意代码植入、拒绝服务攻击等威胁频繁出现，工业生产环境中传统 IT 安全防护体系在面对多样化、高复杂度攻击时显得力不从心。工业控制系统（ICS）与信息技术（IT）的深度融合，也导致网络边界日趋模糊，缺乏物理隔离手段，传统防火墙、入侵检测等机制难以对复杂的攻击路径和多样化威胁进行全面覆盖，暴露出巨大的安全隐患。

工业互联网对安全的需求具有显著的行业特征，要求通信网络具备高可靠性、低延迟和严格的隔离能力。在工厂自动化、远程监控、设备协作等场景下，安全事件可能直接影响生产连续性和工业过程安全，因此安全要求不仅仅局限于数据加密和身份认证，更包

括端到端的隔离、实时的异常检测、设备级安全策略下发等。不同工业业务对网络安全的要求差异较大，如工业机器人、智能物流、能源调度等业务的优先级和防护重点不同，需要定制化的安全防护方案，这对现有网络安全架构提出了新的挑战。

未来工业互联网的发展还将引入更多跨行业、跨区域的协作，安全管理的复杂性不断提升，单一的安全技术手段难以满足多层次需求。面对数字孪生、边缘计算等新兴技术的应用，工业网络的动态性和分布性进一步增强，要求安全防护机制能够灵活适配不同网络拓扑、终端设备和业务流程[1]。工业企业迫切需要一种能够同时兼顾网络性能、灵活部署和差异化安全防护能力的新型安全架构，以解决当前和未来的安全需求，这正是 5G 网络切片技术所能提供的关键价值。

2 5G 网络切片技术原理及安全特性

5G 网络切片是一种基于网络功能虚拟化（NFV）与软件定义网络（SDN）相结合的核心技术，通过逻辑上将一张物理网络划分为多个彼此独立的虚拟网络，各切片在资源、配置、功能和安全性上相互隔离。每一个切片可以根据不同工业应用的需求进行灵活配置，确保资源按需分配与最优使用。这种机制为工业互联网提供了高度定制化的网络支持，使得各类工业场景可以独立构建自己的安全策略与访问控制规则，从而减少传统共享网络架构中资源争用与潜在安全风险。

5G 网络切片在安全性方面具有天然优势。切片间的隔离性使得一个切片受到攻击时不会影响其他切片，从而在网络架构层面上提升整体安全性。通过细粒度的安全策略配置，可以对特定工业应用进行端到端加密、认证和完整性保护，实现业务与数据的隔离保护。切片的生命周期管理可动态调整，允许根据工业互联网应用需求的变化对切片的安全策略进行灵活更新，提升了应对新型安全威胁的能力。5G 网络切片支持边缘计算节点的安全功能下沉，能够在接近终端设备的边缘节点部署本地化安全策略，提升安全检测和响应的实时性。

在具体的工业互联网应用场景中，5G 网络切片技术结合人工智能（AI）手段，能够对网络流量和用户行为模式进行实时的深度分析，从而实现异常行为的快速识别和自动化响应。通过对不同工业业务切片的独立监控和管理，安全防护可以更加精准和有针对性。比如，对于关键的高价值资产监控业务，能够启用高级的入侵防御系统和异常检测机制，确保这些核心资产的安全和稳定运行；而对于一些普通的数据采集业务，则可以采用轻量化的安全策略，这样既节省了网络和计算资源，也降低了数据传输的时延[2-6]。这种灵活调配资源、差异化安全策略的能力，使得工业互联网能够在保证安全的前提下，兼顾性能和效率，打造一个可信赖、可控且持续发展的安全防护环境，为工业互联网的广泛应用和未来升级提供了坚实的技术支持。

3 5G 网络切片在工业互联网安全防护中的应用案例

在智能制造工厂中，生产车间对通信网络的要求极为严格，既需要保证超低延迟和高可靠性，又必须确保生产数据和控制指令的安全传输。5G 网络切片技术的引入，为工厂实现这一目标提供了有效手段。通过划分独立的网络切片，专门为生产控制业务量身定制专属的通信环境，在该切片中集成了访问控制、数据加密、入侵检测等多重安全防护机制，确保关键生产环节的实时响应和信息安全。企业办公网络和信息管理系统可以运行在另一个独立切片中，彼此之间实现物理和逻辑隔离。这样即使办公网络遭遇攻击，恶意行为也难以突破切片边界，横向渗透到关键的生产系统，从而有效防止安全事件对工厂整体运营的影响。通过这种多切片隔离和定制化安全策略，工厂能够在保障业务连续性的基础上，大幅提升网络安全防护的整体水平。

在能源互联网场景中，电网调度中心需要对分布广泛的智能终端和传感器进行远程监控与控制，这类业务对网络的安全性和可用性要求极高。通过 5G 网络切片技术，能源企业可以为调度业务建立高安全级别的切片，通过多因素认证、终端设备加固、链路加密等手段，保障电网关键数据与控制信令的安全传输。运维人员的管理系统可部署在不同的切片内，实现不同业务系统之间的访问隔离和安全防护，降低整体网络暴露面，提升能源基础设施的抗攻击能力与业务连续性。在远程工业运维与服务中，5G 网络切片可为企业提供高可用、低延迟的远程访问通道[7]。设备制造商为客户提供远程诊断和维护服务时，可通过独立切片对客户设备的运行状态进行监控与远程维护，切片中内嵌强身份认证、细粒度权限管理、日志审计等安全机制，确保仅授权人员能够访问目标设备，且所有操作均可追踪审计。这样不仅提升了运维效率，还降低了企业的安全风险，助力工业企业构建安全、可信的远程服务体系。

4 5G 网络切片技术应用中的安全问题及对策

5G 网络切片技术在工业互联网安全防护中展现出显著优势，但也带来了诸多新的安全隐患和挑战。切片的虚拟化特性使得网络资源在逻辑层面上被划分成

多个相互独立的虚拟网络，但物理资源仍然是共享的，这种架构虽然提升了灵活性和资源利用效率，却也无形中扩大了潜在的攻击面。攻击者可能通过入侵切片管理和编排系统，获得对多个切片的控制权限，进而非法访问、篡改甚至破坏不同切片中的配置和数据。尽管切片之间实现了逻辑隔离，但底层物理设备一旦被攻破，安全风险将迅速蔓延，波及整个网络环境。工业互联网环境中针对不同业务场景的切片高度定制化，导致安全策略复杂且多样，一旦配置不严谨或管理不到位，极易出现安全漏洞，成为黑客入侵的突破口。这些问题对切片安全管理提出了更高的要求，必须加强多层次防护和动态安全监控，确保工业互联网的稳定和安全运行。

应对这些安全问题，需要从体系架构和技术细节双重层面入手优化。切片编排与管理系统应采用零信任安全架构，确保所有访问请求均经过严格验证，减少来自内部和外部的恶意访问风险。在切片生命周期管理过程中引入安全自动化检测机制，定期对配置一致性、漏洞风险进行自动化扫描与修复。底层物理资源层应采用强加密与硬件安全模块（HSM）保护，确保共享资源在不同切片之间不发生数据泄露与非法访问，提升整个切片环境的安全防护水平。切片安全防护应结合人工智能与大数据分析手段，实时监控切片运行状态与流量特征，及时发现并应对异常行为。工业企业可通过安全编排与自动化响应（SOAR）平台，将多切片安全事件进行关联分析，形成统一的安全管理视图，提升跨切片的安全态势感知与处置效率[8]。切片安全策略需持续优化，确保覆盖从边缘终端到核心网的全链路防护，实现动态化、精细化和差异化的安全管理，真正发挥 5G 网络切片在工业互联网安全防护中的战略价值。

5 结语

5G 网络切片技术为工业互联网安全防护带来了全新的解决方案，通过实现网络资源的灵活划分与隔离，有效提升了不同业务场景的安全性和可靠性。尽管切片技术在提升网络性能和安全性方面优势明显，但其虚拟化架构带来的安全挑战也不容忽视。未来，结合先进的安全管理策略与智能化防护手段，持续优化切片的安全机制，将是保障工业互联网安全运行的关键。只有这样，才能充分发挥 5G 网络切片技术在工业互联网中的巨大潜力，助力工业数字化转型迈向更高水平。

参考文献

[1] 张纯洁.5G 移动通信技术和软交换技术在通信工程中的应用[C]//重庆市大数据和人工智能产业协会,西南大学,重庆工商大学,重庆建筑编辑部.人工智能与经济工程发展学术研讨会论文集.杭州纵横通信股份有限公司;,2025:851-854.

[2] 安再东,魏尚杰,韩立恒.5G 网络环境下面向工业互联网的低时延传输机制研究[J].中国宽带,2025,21(01):76-78.

[3] 唐开华.5G 网络切片技术在不同场景中的应用与优化[J].中国宽带,2024,20(05):10-12.

[4] 孟钰杰.5G 赋能工业互联网大数据处理优化策略研究[C]//中国电力设备管理协会.全国绿色数智电力设备技术创新成果展示会论文集（四）.浪潮工业互联网股份有限公司;,2024:207-209.

[5] 王苗苗.5G+MEC 使能工业互联网的探索与实践[J].电子元器件与信息技术,2024,8(04):156-159.

[6] 马景斌.基于 5G 的工业互联网通信网络优化及性能改进[J].中国宽带,2023,19(06):78-80.

[7] 任洁.网络切片的身份认证和资源分配技术研究[D].西安电子科技大学,2023.

[8] 谢婉芸.面向工业互联网的网络切片技术及其安全性研究[D].湖南大学,2023.