面向5G网络的工业互联网安全技术分析

Analysis of Industrial Internet Security Technology and Development for 5G Network

陈焱/CHEN Yan[1]，陈丹/CHEN Dan[1]，袁琦/YUAN Qi[2]，刘小丽/LIU Xiaoli[2]，徐晓娜/XU Xiaona[2]
（1. 深圳中广核工程设计有限公司，中国 深圳 518100；
2. 中国信息通信研究院，中国 北京 100083）
(1. China Nuclear Power Design Co., Ltd. (Shenzhen), Shenzhen 518100, China;
2. China Academy of Information and Communication Technology, Beijing 100083, China)

DOI：10.12142/ZTETJ.202502010
网络出版地址：http://kns.cnki.net/kcms/detail/34.1228.TN.20240926.1153.004.html
网络出版日期：2024-09-27
收稿日期：2024-07-15

摘要：5G与工业互联网的融合面临接入安全、网络安全、数据安全等诸多安全问题，亟需新的安全技术来应对。总结了面向5G网络的工业互联网安全政策、标准和产业发展情况，研究了面向5G网络的工业互联网在终端、网络、云平台和数据安全方面面临的安全威胁，分析了面向5G网络的工业互联网在终端、网络、云平台和数据方面的安全技术。面向5G的工业互联网安全技术方案，需要立足工业互联网实际应用场景，从终端、网络、云平台和数据安全多个维度引入防护技术，构建全面防护体系，预防安全威胁，提升安全防护水平。

关键词：5G网络安全；工业互联网安全；云平台安全

Abstract: The integration of 5G and the industrial Internet faces numerous security issues such as access security, network security, and data security, so there is an urgent need for new security technologies to address these issues. This paper summarizes the security policies, standards and industrial development of the 5G-oriented industrial Internet, also studies the security threats faced by the 5G-oriented industrial Internet in terms of terminal, network, cloud platform and data security, and finally analyzes the security technologies of the 5G-oriented Industrial Internet in terms of terminal, network, cloud platform and data security. The security technology solution for the 5G-oriented industrial Internet needs to be grounded in the actual application scenarios of the industrial Internet, introduce protection technologies from multiple dimensions including terminals, networks, cloud platforms, and data security, construct a comprehensive protection system, prevent security threats, and enhance the level of security protection.

Keywords: 5G network security; industrial Internet security; cloud platform security

引用格式：陈焱，陈丹，袁琦，等. 面向5G网络的工业互联网安全技术分析[J]. 中兴通讯技术，2025，31(2)：72-76. DOI：10.12142/ZTETJ.202502010
Citation：CHEN Y, CHEN D, YUAN Q, et al. Analysis of industrial internet security technology and development for 5G network [J]. ZTE technology journal, 2025, 31(2): 72-76. DOI: 10.12142/ZTETJ.202502010

随着中国5G商用的推进，5G网络建设稳步发展。5G作为新一代移动通信系统，以高带宽、低时延、海量连接等为特性，提升工业互联网的信息化水平，筑牢工业生产的网络基石，为工业的数字化转型注入强劲动力。5G网络的三大场景能够支撑工业互联网的不同功能应用需求，提升网络连接能力和稳定性，推动人、机、物的全面互联，实现工业互联网向智能化、服务化、高端化转型。

5G与工业互联网融合叠加，促进了工业企业数字化、网络化和智能化升级，给工业互联网带来前所未有的发展机遇[1]。但5G与工业互联网的融合也将大量的信息通信技术（ICT）系统威胁和挑战带入工业运营技术（OT）网络中。网络系统的硬件、软件乃至整个系统受到病毒、木马、高级持续性攻击等安全风险的威胁日益加剧，使得面向5G网络的工业互联网在接入安全、网络安全、数据安全和应用安全等方面面临安全威胁。因此，需要提出新的安全技术来应对这些威胁，提升工业互联网的安全保障能力。

目前，面向5G网络的工业互联网安全是业界研究的热点问题。本文将对面向5G网络的工业互联网安全发展情况、

面临的安全威胁以及现行的安全技术进行研究和分析。

1 面向5G网络的工业互联网安全发展现状

1.1 政策发展现状

国际上，美国与欧盟相继出台了5G和工业互联网相关政策。2016年9月，美国工业互联网联盟（IIC）发布《工业互联网安全框架》，定义了工业互联网的五大安全特性，为工业互联网安全体系建设和部署实施提供最佳实践指南。2019年5月，美国在布拉格5G安全大会上通过了《布拉格5G提案》。2020年1月，美国出台《保障5G安全及其他法案》，同月欧盟发布《5G网络安全欧盟工具箱》。2020年3月，美国发布《美国5G安全国家战略》，该文件正式制定了美国保护5G基础设施的框架，将5G安全进一步提升到更高的战略地位。

中国对面向5G网络的工业互联网安全发展也非常重视，近年来国务院、工业和信息化部等相继出台了各项指导意见和指南等政策，规范并推动5G+工业互联网安全发展。2019年7月，工业和信息化部等十部委联合发布《加强工业互联网安全工作的指导意见》，意见制定了工业物联网安全管理体系，为开展工业互联网安全工作提供了切实可行的指引。工业和信息化部在2019年发布《工业互联网企业网络安全分类分级指南（试行）》，并在2021年1月发布《开展工业互联网企业网络安全分类分级管理试点工作的通知》，以加快构建分类分级管理制度，形成可复制可推广的工业互联网网络安全分类分级管理模式；随后在2021年12月印发《工业和信息化部办公厅关于组织开展工业领域数据安全管理试点工作的通知》（工信厅网安函〔2021〕295号），要求企业构建数据安全管理体系，有效保障工业企业数据安全。2022年5月，工业和信息化部又印发了《工业和信息化部办公厅关于开展工业互联网安全深度行活动的通知》（工信厅网安函〔2022〕97号），以健全自主定级、定级核查、安全防护、风险评估等工作机制，提升工业互联网安全保障能力。

1.2 标准发展现状

在行业标准方面，2018年5月中国通信标准化协会（CCSA）TC13 WG5开始研制工业互联网安全标准。2021年工业和信息化部发布了数据安全方面的行业标准，并完成了工业互联网平台安全、网络安全等相关标准，目前正在进行数据采集终端设备安全、设备安全防护等标准研制工作。另外TC13 WG5正在进行家电制造行业、钢铁生产、船舶、航天装备制造和矿山等行业安全应用的标准研制。

在国家标准方面，全国网络安全标准化技术委员会（简称“TC260”）在2018年发布了工业控制系统安全管理、信息安全分级、风险评估等标准，在2019年发布了工业控制系统安全检查指南、工业控制系统漏洞检测等标准，并在2022年发布了工业控制系统信息安全防护能力成熟度模型方面的标准。

随着工业互联网进入规模发展的新阶段，中国需要不断完善工业互联网安全标准，加强面向5G网络的工业互联网安全标准研制工作，提升工业互联网安全防护能力。

1.3 产业发展现状

面向5G网络的工业互联网以信息化为基础，以网络化和智能化为核心，成为传统工业企业升级智慧化工厂的核心发展路径。网络安全等级保护2.0进一步扩展了网络安全保护范围，对工业互联网提出了更高的安全扩展要求，有力推动了工业互联网安全产业发展。

面向5G网络的工业互联网安全产业分为安全产品和安全服务两大类：

1）工业互联网安全产品分为防护类和管理类产品。防护类产品主要有防火墙、防病毒软件、网络隔离设备、终端/网络入侵检测、工业安全审计等。管理类产品主要有资产管理、补丁管理、身份认证管理、安全运维管理、安全合规管理等产品。防护类和管理类产品成为工业互联网安全整体解决方案的重要组成部分，其市场规模也在持续稳定增长。

2）工业互联网安全服务分为咨询类、实施类和运营类服务。咨询类主要包括安全评估、安全咨询和安全审计等。实施类主要包括安全集成和安全加固等。运营类主要包括安全应急、安全培训和安全托管等。由于近年来工业网络威胁朝着多样化、复杂化的方向演化，传统的单一安全产品模式已难以满足用户的安全防护需求。在工业互联网安全设计、实施和运维阶段采用全面的工业互联网安全服务，可有力保障工业互联网安全产业发展。

随着中国5G+工业互联网战略的全面实施，政府及企业不断加大安全投入，工业互联网安全产业迎来快速增长期。在政策环境与市场需求的共同作用下，中国工业互联网安全产业进入快速发展的新阶段。

2 面向5G网络的工业互联网安全威胁

5G网络在工业互联网的应用，打破了传统工控系统独立、封闭的天然屏障，使得大量工业互联网设备暴露在公共

网络中。虽然很多工业企业对传统网络采取了一定的防护措施，但与系统稳定性、实时性和鲁棒性相比，对网络信息安全性的考虑仍显不足。工业互联网中仍存在大量漏洞和安全威胁[2-3]，包括终端安全威胁、网络安全威胁、云平台安全威胁和数据安全威胁，如图1所示。一旦出现安全问题，工业互联网将受到严重影响。

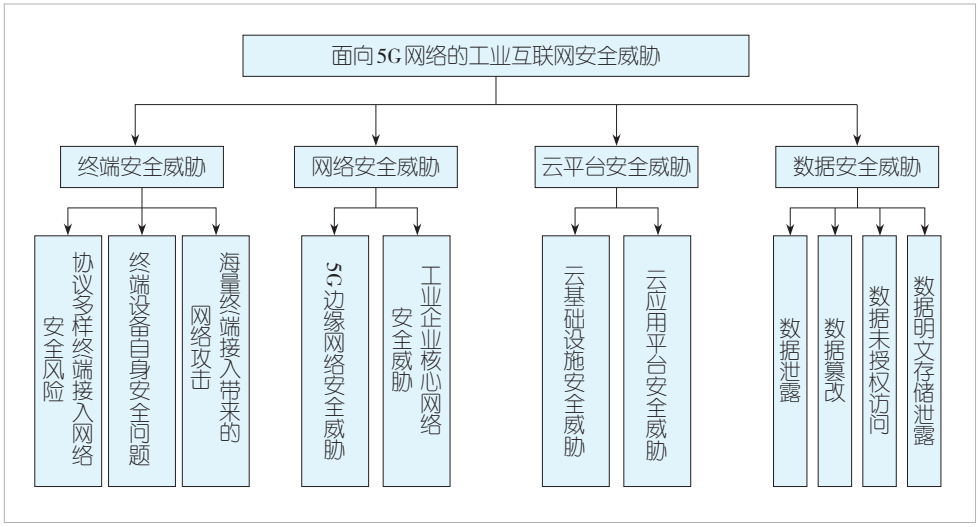

图1 面向5G网络的工业互联网安全威胁

2.1 终端安全威胁

5G与工业互联网的融合使得海量工业终端接入成为可能，但同时也给工业互联网带来了更多的攻击风险点。面向5G工业互联网的终端协议种类多样化，能够提供信息量巨大的数据。这些数据分类众多，应用场景多元，但尚无统一的安全标识和认证管理机制，极大增加了接入网络的安全风险。终端设备所用的芯片、操作系统、编码规范、第三方应用软件等，通常存在漏洞、缺陷、后门以及权限滥用等安全问题。海量终端接入面向5G的工业互联网后，一旦被入侵利用，这些终端就有可能形成规模化的设备僵尸网络，成为新的分布式拒绝服务（DDoS）攻击源，进而对工业互联网平台系统和应用等发起DDoS网络攻击。

2.2 网络安全威胁

工业互联网网络安全包括5G边缘网络安全和工业企业核心网络安全等。5G网络在边缘计算、能力开放等方面存在安全风险，导致面向5G网络的工业互联网存在网络安全边界不清晰等威胁，给传统基于物理实体隔离的安全防护模式带来极大压力。通过攻击工业互联网的入口，工业互联网中的生产设备在连接到企业核心网络后，非常容易遭受黑客、病毒、高级持续性威胁（APT）、DDoS等攻击。这可能会导致整个网络安全防线失守，进而危害工业生产的稳定运行。

2.3 云平台安全威胁

面向5G的工业互联网平台安全主要包括云基础设施安全和云应用平台安全。针对这两个方面的安全威胁主要包括：1）云基础设施有很多虚拟机/宿主机，这些虚拟机/宿主机容易被少数别有用心的云租户侵入，通过虚拟机的约束来破坏其他虚拟机或者宿主机；2）不同的云应用设置在不同的服务器上，使得安全边界变得模糊，安全域的划分比较困难，这就可能导致网络和数据安全风险问题；3）云应用平台存在安全漏洞，会使得云服务的安全性得不到有效保障。

2.4 数据安全威胁

面向5G网络的工业互联网数据量巨大，且形态多样。在数据采集、传输、存储、处理等各个环节中，存在数据泄露、篡改、未授权访问、明文存储等安全风险。如果无法有效应对这些风险，国家核心行业就会面临安全威胁。这不仅会严重破坏生产的稳定运行，阻碍相关产业发展，还可能对国家网络安全造成冲击，危及国家安全。

3 面向5G网络的工业互联网安全技术

5G网络通过提供通信安全、边缘计算安全以及能力开放安全保障，赋能工业互联网安全发展。面向5G网络的工业互联网安全架构，按照信息安全等级保护第三级技术要求进行建设和部署，如图2所示，需要从终端安全、网络安全、云平台安全和数据安全方面来保障自身的安全[4-5]，以满足工业企业不同场景的安全需求。

3.1 终端安全技术

在终端可信接入安全方面，5G网络对终端接入进行双向认证，在接入网络切片时进行二次认证。在此基础上，还需要建设终端管理系统，使用统一身份认证、国际移动设备识别码（IMEI）绑定、网络准入等复合认证手段，加强接入管控。当发现存在终端设备有风险时，应执行阻断接入操作，将设备下线。

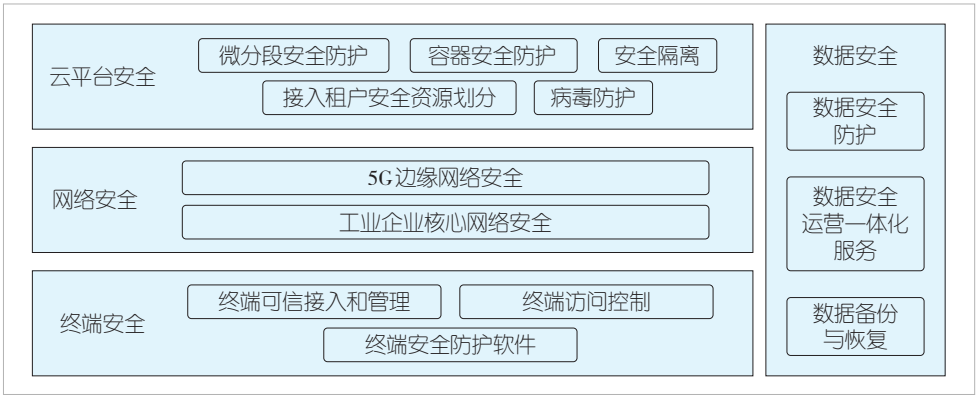

图2 面向5G网络的工业互联网安全架构

通过接入网关加强终端接入控制，并制定网络安全策略（如设置黑白名单的访问控制列表，只允许白名单终端访问），以此实现对接入工业互联网中终端的访问控制。

另外，还需要在终端安装安全防护软件，比如安全防火墙、防病毒软件等，以便及时发现病毒和漏洞，确保接入的终端安全。

3.2 网络安全技术

3.2.1 5G边缘网络安全

在面向5G网络的工业互联网中，企业将部署5G边缘计算系统，实现工业互联网业务和应用。具体而言，把原本部署于运营商核心网侧的用户平面功能（UPF），下沉至企业园区内或园区附近，以保障企业业务数据本地存储，提高数据安全性，保证互联网业务和应用的实时性。

在企业园区的UPF侧设置防火墙，可实现UPF侧边界的防护，同时部署入侵防御系统（IPS），可使系统具备入侵防护能力。为了防止边缘计算系统受到DDoS攻击，可以部署全流量检测系统，进行DDoS攻击检测，发现并清洗恶意流量攻击。另外，为了达到安全等级保护三级的要求，还可以部署防病毒网关、堡垒机、主机防护系统等，以增强安全服务能力。

5G边缘计算系统应支持安全通信功能，尽量不使用明文通信。例如：支持互联网协议安全（IPSec）协议，在核心网网元以及边缘计算应用之间建立安全通道，对传输的数据进行机密性和完整性保护，保护传输的数据安全。

5G边缘计算系统应支持网络隔离和访问控制，边缘计算网元的管理、控制、用户平面应分配独立的物理网口，保证多接入边缘计算（MEC）的业务管理、编排控制与用户数据3个平面之间彼此隔离。

5G边缘计算系统可使用OAuth 2.0认证机制对各种访问进行认证和授权，并同时开启自主访问控制和强制访问控制，遵循最小权限原则，配置合理的访问控制策略，防止非授权访问、篡改等。

3.2.2 工业企业核心网络安全技术

为了满足信息安全等级保护第三级的要求，在工业企业网络的核心层旁路部署安全系统，例如防火墙、入侵检测系统、数据库审计系统、堡垒机、漏洞扫描系统等，可满足边界防护、流量分析、日志审计、恶意代码防范等安全保障要求。

此外，工业企业网络还需要部署高级威胁检测系统。该系统通过对网络行为进行智能分析，实现对网络攻击尤其是新型网络攻击行为的分析，识别其中的已知威胁、未知威胁和异常行为，还原攻击链并进行取证溯源。

针对工业企业网络的业务系统主机和服务器，部署防病毒软件（白名单防护软件）、采用白名单技术，不仅能使主机免受病毒等各种非法攻击，还能有效管控主机的通用串行总线（USB）外部端口。针对Windows系统主机，防病毒软件可以提供适用于工控行业的安全防护，保障关键业务运行，建立稳定运行环境，有效遏制病毒及其变种的运行，满足信息安全等级保护三级的恶意代码防范、安全管理的要求。

3.3 云平台安全技术

工业互联网云平台是指基于硬件和软件等资源，为使用者提供网络、存储及计算的服务平台。云平台安全通过微分段安全防护、容器安全防护、安全隔离、接入租户安全资源划分和病毒防护实现云平台的安全防护。

1）微分段安全防护。建立虚拟化环境下的微分段网络安全保护能力，实现虚拟化环境主机层部署微分段安全防护、东西向虚拟下一代防火墙（vNGFW）和虚拟入侵检测与防御（vIDP），以及虚拟机之间的安全保护。

2）容器安全防护。在运行环境加固方面，利用安全基线对容器主机和容器编排工具进行安全加固，保证容器运行环境安全。在容器网络安全方面，通过部署一定的访问控制安全策略，采用白名单策略实现网络访问控制，实现容器之间、容器与宿主机平台之间、容器与外部网络之间的安全访问控制。

3）安全隔离。需要在虚拟机之间、虚拟机与宿主机之间进行隔离，也需要对安全边界进行详细的责任划分，对安全域进行进一步细化，对不同的安全域和不同安全级别的安

全域进行不同的访问控制设计。

4）接入租户安全资源划分。对接入租户进行划分，利用虚拟专用网络（VPN）、VRF和虚拟可扩展局域网（Vx-LAN）等技术，通过在物理网络上构建虚拟的网络层，为租户提供安全服务。同时为了实现云平台的安全控制与权限隔离，可通过新一代防火墙、入侵防御系统（IPS）和负载均衡产品技术，为每个租户分配独立非共享的安全防护资源。

5）病毒防护。通过在虚拟机中部署防病毒软件，系统可识别并处置针对虚拟机的恶意攻击行为；同时部署防病毒引擎（AVE）网关，提供病毒查杀功能，抵御木马、蠕虫、恶意软件的攻击。

3.4 数据安全技术

由于面向5G网络的工业互联网场景中会使用海量智能节点、物联网终端设备，设备和业务应用中包含很多重要数据。因此，需要针对数据的采集、传输、存储和处理等全生命周期，采取数据标记、明示用途、数据加密、数据备份、访问控制和安全审计等多种安全防护技术，建设数据安全运营一体化服务能力，包括数据资产识别、数据分类分级管理、数据脱敏和加密、数据防泄漏、数据流动监测管理等，满足复杂化、多样化业务场景下的数据安全治理要求。

与此同时，在工业企业网络部署数据备份与恢复系统，不仅能实现实时数据自动备份、异地容灾、热备等功能，为数据提供可靠性保护，还能够定期进行备份数据恢复测试，确保实际备份数据的异机可恢复性，并进行记录及分析。当业务系统出现故障或数据损坏时，上述措施能快速恢复数据，确保重要数据不丢失。

4 结束语

面向5G的工业互联网安全技术方案结合工业互联网实际的应用场景，通过在终端、网络、云平台和数据安全方面引入安全防护技术，构建全面的安全防护能力，能够有效预防工业互联网的安全威胁，提升工业互联网的安全防护水平，为面向5G网络的工业互联网领域安全发展提供有效的参考。

参考文献

[1] 杨波, 宋翼. 5G在工业互联网中的安全应用研究 [J]. 通信技术, 2020, 53(11): 2867-2871
[2] 岳守振, 张琦, 吕金华, 等. 5G+工业互联网网络安全威胁及应对浅析 [J]. 网络安全技术与应用, 2022(10): 100-102
[3] 张子扬, 韦素萍. 5G网络中工业互联网安全问题研究 [J]. 中国新通信, 2019, 21(7): 136-137. DOI: 10.3969/j. issn. 1673-4866.2019.07.116
[4] 尹曾, 王雪源, 吴婷婷. 5G+工业互联网安全防护设计与实践 [J]. 工业信息安全, 2022(10): 76-84
[5] 范勇杰, 赵磊, 蒋小燕. 5G+工业互联网一体化安全防护体系分析与研究 [J]. 工业信息安全, 2022(10): 85-91

作 者 简 介

陈焱，深圳中广核工程设计有限公司工程师；主要从事核电、电力工程领域的通信网络业务及信息化、数字化、智能化业务的研究、规划及设计工作。

陈丹，深圳中广核工程设计有限公司通信主管设计师；主要从事核电厂无线通信系统和电磁兼容方面的研究工作。

袁琦，中国信息通信研究院部门主任，正高级工程师；主要从事移动互联网、物联网和安全技术领域科研专项、标准等方面的研究工作；主持或参与国家级或省部级科研专项20余项，主持或参与制定国家或通信行业标准100余项，牵头完成重要研究报告80余项，获省部级奖励9项，发表论文40余篇，获授权专利7项，出版专著3部。

刘小丽，中国信息通信研究院工程师；主要从事工业互联网和5G安全技术领域标准、软科学、测试等研究工作。

徐晓娜，中国信息通信研究院工程师；主要从事终端安全技术领域标准、软科学、测试等研究工作。