DOI 10.15302/J-SSCAE-2021.02.007

工业互联网安全产业发展态势及路径研究

王秋华[1]，吴国华[1]，魏东晓[2]，苗功勋[2]，徐艳飞[3]，任一支[1]

（1. 杭州电子科技大学网络空间安全学院，杭州 310018；2. 中孚信息股份有限公司，济南 250101；
3. 中国网络空间研究院，北京 100010）

摘要：工业互联网安全是实现我国工业互联网产业高质量发展的重要前提和保障，也是建设网络强国和制造强国战略的重要支撑。本文针对我国工业互联网安全产业发展面临的问题，分析了工业互联网安全在产业政策、标准体系、产业结构、产业规模等方面的发展现状，研判了工业互联网安全产业面临的历史机遇和发展趋势，提出了构建新一代工业互联网安全产业的发展路径。研究建议，加强顶层设计和政策引导，强化科技创新与转化，构建良好的产业发展生态，注重供应链安全与稳定，加强人才培养与队伍建设；立足全局、统筹联动，坚持“政产学研用”融合发展，探索出适合我国工业互联网安全产业的可持续发展路径。

关键词：工业互联网安全；产业生态体系；网络安全等级保护；自主可控

中图分类号：TP393　　**文献标识码：**A

Development Trend and Path of Industrial Internet Security Industry in China

Wang Qiuhua[1], Wu Guohua[1], Wei Dongxiao[2], Miao Gongxun[2], Xu Yanfei[3], Ren Yizhi[1]

(1. School of Cyberspace, Hangzhou Dianzi University, Hangzhou 310018, China; 2. Zhongfu Information Inc., Jinan 250101, China; 3. Chinese Academy of Cyberspace Studies, Beijing 100010, China)

Abstract: Industrial Internet security is a prerequisite and guarantee for the high-quality development of China’s industrial Internet industry; it is also important for enhancing China’s cyber and manufacturing industries. This study aims at the future development of the industrial Internet security industry in China. First, we analyze the development status of the industry in terms of industrial policies, standards system, industrial structure, and industrial scale. Subsequently, we elaborate on the opportunities and trends of the industry and propose the development path for the next-generation industrial Internet security industry in China. To explore a sustainable development path suitable for China’s industrial Internet security industry, top-level design and policy guidance should be enhanced; technological innovation and transformation should be reinforced; advantages of enterprises and organizations should be complemented to construct a healthy development ecosystem; the security and stability of the supply chain should be emphasized; and personnel training and team building should be promoted to support the research collaboration among government, industry, universities, research institutes, and application.

Keywords: industrial Internet security; industry ecosystem; classified protection of cybersecurity; independent and controllable

收稿日期：2021-01-20；**修回日期：**2021-02-22

通讯作者：任一支，杭州电子科技大学网络空间安全学院教授，研究方向为网络空间安全；E-mail: renyz@hdu.edu.cn

资助项目：中国工程院咨询项目“新一代工业互联网安全技术发展战略研究”(2020-XZ-02)

本刊网址：www.engineering.org.cn/ch/journal/sscae

一、前言

我国正处于新一轮工业革命的历史机遇期，工业互联网作为新型基础设施建设的重要组成部分，是推动数字经济与实体经济深度融合的关键路径。为此，国家高度重视，提出深入实施工业互联网创新发展战略的要求 [1]。自 2017 年国务院发布《关于深化“互联网 + 先进制造业”发展工业互联网的指导意见》以来，一系列配套政策相继出台，工业互联网创新发展战略逐步实施并取得显著进展。目前，我国工业互联网发展迅速，已广泛应用于能源、交通、制造、国防等行业领域，对经济社会发展的带动效应日益显著。工业互联网在构建全新生产制造和服务体系，为高质量发展和供给侧改革提供支撑的同时，也打破了传统工业环境相对封闭可信的状态，增加了遭受网络攻击的可能性 [2]。各国工业领域的安全事件频发，危害日益严重，网络攻击成为制约工业互联网发展的关键因素。工业互联网安全作为国家安全的重要组成部分，事关经济发展和社会稳定；消除工控安全威胁与隐患，建立科学、系统的安全防护体系成为必然 [3]。

从产品竞争格局来看，全球工业互联网产业可以分为硬件与网络、软件与平台、信息安全三大板块；2018 年硬件与网络产品占比为 49.8%，软件与平台产品占比为 48.3%，信息安全产品占比为 1.9%；2019 年全球工业互联网信息安全产业的市场规模为 156.6 亿美元，预计 2025 年为 222 亿美元 [4]。与发达国家相比，我国工业互联网安全产业中的软硬件产品自主研发能力有所不足，在核心技术、产业规模、推广应用等方面尚存差距；高端关键基础装备、控制系统、软件及平台市场长期被国外产品占据，如工业控制系统中的微控制单元（MCU）、数字信号处理器（DSP）、现场可编程门阵列（FPGA）等核心元器件技术与国外差距较大，数据采集与监视控制系统（SCADA）、可编程逻辑控制器（PLC）、分散控制系统（DCS）、过程控制系统（PCS）等较多依赖国外供应 [5]。为了加快构建工业互联网安全保障体系，提升工业互联网安全保障能力，我国需在推动工业互联网安全责任落实、构建互联网安全管理体系、提升企业互联网安全防护水平、强化互联网数据安全保护能力、完善国家工业互联网安全技术手段、加强工业互联网安全公共服务能力、推动工业互联网安全科技创新与产业发展 7 个方面持续发力。

二、我国工业互联网安全产业的发展现状

（一）工业互联网安全产业政策持续向好，不断细化深入

随着云计算、第五代移动通信（5G）、物联网等新一代信息技术与制造业的不断融合，工业领域的网络安全风险逐渐增大，工业互联网安全成为国家和企业高度关注的议题。我国从国家安全角度出发，对工业互联网安全体系进行了顶层设计和战略布局，坚持以安全保发展、以发展促安全、安全和发展并重的发展路径，确保安全保障与信息化建设同步规划、同步建设、同步运行 [6]，为工业互联网安全产业的健康发展奠定了良好基础。近年来，我国陆续出台了一系列政策、指南，从宏观、中观、微观层面不断细化完善工业互联网安全政策体系。2019 年 7 月，工业和信息化部等十部门联合印发了《关于加强工业互联网安全工作的指导意见》，体系化布局了工业互联网安全工作，为产业的健康发展指明了方向。可以预见，未来还将会有更多的产业政策出台，继续保持对工业互联网安全的扶持力度，引导其全面发展。

（二）工业互联网安全标准体系稳步推进，指导产业健康发展

工业互联网安全标准体系主要由基础共性类标准、安全防护类标准、安全服务类标准、垂直行业类标准组成 [7]（见表 1）。标准化对工业互联网安全保障体系建设至关重要。近年来，针对工业互联网标准的跨行业、跨专业、跨领域特点，我国加速开展相关标准的研制，陆续发布了《工业互联网安全防护总体要求》《工业互联网平台安全防护要求》等标准规范，印发了《工业互联网综合标准化体系建设指南》等，初步形成了涵盖设备安全、控制安全、网络安全、数据安全、应用安全、平台安全、安全管理的工业互联网安全标准体系（见图 1）。后续，工业互联网安全相关标准将会进一步完善，产业发展将更趋规范。

（三）工业互联网安全产业结构逐步调整并持续优化

工业互联网安全产业结构依据市场应用分为安全产品和安全服务两大类 [8]（见表 2）。目前，我国工业互联网安全产品类市场和服务类市场均在持续发展壮大，产品和服务体系正在加速构建，产业结构不断优化，呈现出以下特点。

在工业互联网安全产品方面，防护类产品中的边界、终端安全防护是当前的主要分布形态，发展相对成熟，市场占有率较大。随着网络安全等级保护 2.0 的正式实施，防护类产品将成为工业互联网安全整体解决方案中必备的基础安全措施，市场规模将继续稳定增长。此外，防护类产品中的网络检测、工业安全审计类产品的市场规模虽然较小，但发展速度较快。管理类产品中的态势感知、安全合规管理、安全运维等产品是安全厂商的重要布局方向。在国家和行业政策的双重推动下，我国工业企业用户对合规安全和内生安全的需求加快，未来该类产品的市场规模也将稳定增长。

表 1　工业互联网安全标准体系

标准类别	标准化方向
基础共性类标准	术语定义
	安全架构与模型
安全防护类标准	设备和控制安全
	边缘计算安全
	平台安全
	数据安全
	标识解析安全
	网络和通信安全
	应用安全
	安全管理
安全服务类标准	检查评估
	态势感知及预警
	应急服务
	运维服务
	检测认证
垂直行业类标准	面向汽车、钢铁、石油化工等重点行业领域，结合行业特色和需求，研制更具针对性、对行业更有指导作用的工业信息安全国家标准

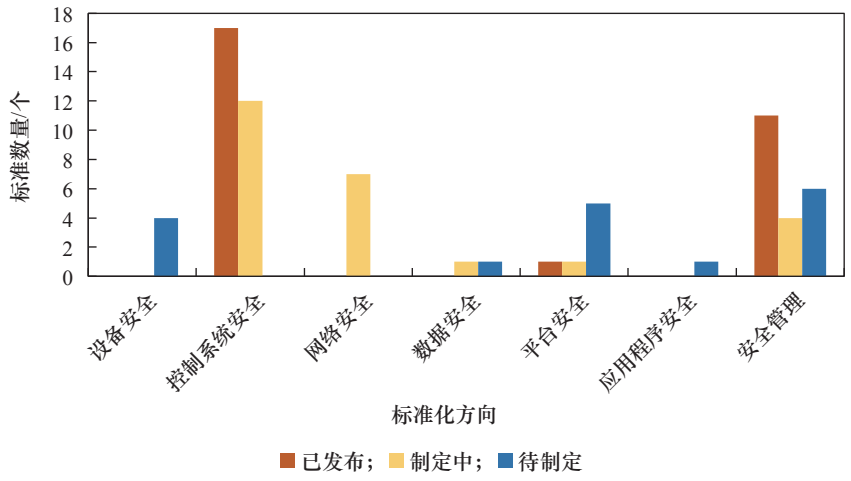

图 1　我国工业互联网安全标准的制定情况

在工业互联网安全服务方面，由于近年来工业网络威胁朝着多样化、复杂化方向演化，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；以风险评估、安全管理咨询、安全应急响应、安全托管服务等为主的安全服务获得更多关注，针对工业互联网安全评估和安全培训的需求日趋旺盛。此外，科研院所、高校对工业信息安全人才培养的重视程度显著提高，促进了安全培训服务市场快速增长，进一步优化了产业结构。

（四）工业互联网安全产业规模持续增长

有效的安全保障离不开坚实的产业支撑。随着我国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（见图 2）。2018 年我国工业互联网安全产业的市场规模为 94.6 亿元，预计 2022 年为 307.6 亿元，年均复合增长率约为 32.66% [9]。在政策环境与市场需求的共同作用下，加强安全保障将成为今后工作的重点，我国工业互联网安全产业进入快速发展的新阶段。

三、我国工业互联网安全产业的发展趋势

（一）产业政策利好进一步释放，产业基础更为坚实

工业互联网安全是我国实施制造强国和网络强国战略的重要保障，也是落实总体国家安全观的重要抓手。在 5G、工业互联网等新型基础设施建设加速发展的大背景下，统筹发展与安全将成为我国新时期制造业数字化转型的主旋律。随着工业互联网战略的深入推进，我国不断加强政策和财政支持力度，促进工业互联网安全产业的内需增长，引导企业加大安全技术投入，加快相关安全技术研发和产业化推进。随着国家相关法规政策的持续推进，

表 2　工业互联网安全产业结构

名称	一级分类	二级分类	典型产品或服务
工业互联网安全产业结构	安全产品	防护类产品	防火墙、网络隔离设备、防病毒软件、应用白名单、终端入侵检测、网络入侵检测、工业安全审计等
		管理类产品	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
	安全服务	咨询类服务	安全评估、安全咨询、安全审计等
		实施类服务	安全集成、安全加固等
		运营类服务	安全应急、安全培训、安全托管等

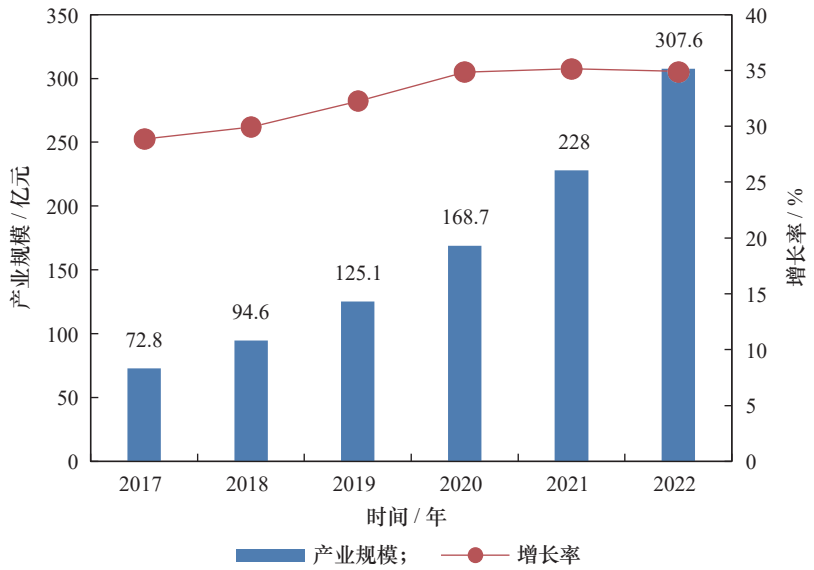

图 2　2017—2022 年我国工业互联网安全产业市场规模及预测

工业互联网产业环境将不断优化，产业基础更为坚实，产业聚集效应将逐渐形成。

（二）合规性需求是推动工业互联网安全产业发展的主要驱动力

网络安全等级保护 2.0 扩展了网络安全保护的范围，对工业控制系统提出了更高的安全扩展要求，以适用于工业控制的专有技术和应用场景特点。面对安全合规要求，工业企业须持续加强自身安全防护体系，进一步落实主体责任，加大安全投入，加强体系化的安全规划和布局。可以判断，工业互联网安全产业的内生需求将进一步扩大 [10]。

（三）工业互联网安全需求促使信息技术（IT）安全与运营技术（OT）安全不断深入融合

工业互联网安全是工业生产安全和网络空间安全相融合的领域，涵盖工业领域数字化、网络化、智能化过程中各个要素和各个环节的安全 [11]，需要专门的安全产品、技术和服务。当前，我国工业互联网企业多采用传统的网络信息安全防护技术，以工控系统的“外建”安全防护产品和解决方案为主，尚没有工业互联网 OT 方面的安全专用防护设备，整体安全解决方案还不成熟。

我国工业互联网安全技术体系可以分为外建安全（IT 安全）和内嵌安全（OT 安全）两大类。随着工业互联网的加速推进，来自工控系统、工业智能设备、工业平台、数据的安全问题不容忽视，对内嵌信息安全功能的产品和服务的市场需求激增。以 IT 安全为主的传统产品和服务已不能完全满足实际市场需求，应充分结合 OT 安全进行纵深发展。因此，未来工业互联网安全产业发展应统筹考虑 IT 安全和 OT 安全的市场需求，提升工业企业综合防护水平。在特殊性能需求方面，保障生产的连续性和可靠性是工业互联网的首要任务，网络时延或成本较高的 IT 安全方案将无法应用于 OT 网络，需要针对 OT 网络特点研究平衡安全风险和业务影响的技术方案 [9,12]。

（四）结合多领域、新技术的工业互联网安全解决方案不断涌现

随着大数据、云计算、人工智能（AI）、5G、边缘计算等新一代信息技术在工业互联网领域的快速应用，IT 和 OT 融合加速。与此同时，融合了新技术的工业互联网安全环境将变得更加复杂多样，安全风险呈现多元化特征；安全隐患发现难度更高，安全形势进一步加剧。这一系列技术和形势的变化，对安全理念和技术提出了新的要求，将促使安全态势感知、安全可视化、威胁情报、大数据处理等新技术在工业互联网安全领域不断取得应用突破 [10]；促使定制化安全产品加速出现，满足客户不同产品形态、性能的需求；安全服务将由现场服务为主、远程服务为辅转向远程化、云化、自动化、平台化发展。整体而言，围绕设备、控制、网络、应用、数据五大安全领域，结合多领域、新技术的工业互联网安全解决方案将不断出现，为工业企业部署安全防护措施提供可参考的模式。

（五）安全产品的国产化替代需求促进工业互联网安全产业快速发展

我国的重要工控系统较多采用国外技术和设备，存在核心技术受制于人的问题。大量工业企业的工控系统依赖国外厂商提供的运维服务，企业对系统运行的可控性较低；缺乏对国外产品和服务的必要监管机制和技术检测措施，存在一定的安全隐患 [10]。工业互联网安全事关经济发展和社会稳定，重要工业数据一旦被窃取、篡改或破坏，将对国家安全构成严重威胁。频繁爆发的窃密和攻击事件，使得各国在网络空间安全领域的对抗态势进一步加剧。需要高度关注信息安全产品的自主可控，将信息安全产品的国产化上升到国家安全的高度，依靠自主创新，积极发展具有自主知识产权的信息安全产品 [13]。近年来，在信息产品国产化政策的推动下，信息安全产品的国产化替代趋势趋于显现。

四、我国工业互联网安全产业发展面临的挑战

随着我国制造业向数字化、网络化、智能化转型升级，网络安全威胁日益向工业领域蔓延。我国工业互联网安全领域仍存在体制机制尚不健全、综合保障水平偏低、关键核心技术产品不成熟、高端技术人才匮乏等突出问题，工业领域面临的安全风险态势十分严峻 [10]。另外，随着新型基础设施建

设的推进，工业系统需要防护对象的数量大幅增加，工业系统的受攻击面不断扩大，防护要求和难度也不断提高；新技术与工业互联网的融合应用伴生了新兴安全问题，数据要素的共享流动则加剧了潜在安全风险。这些新挑战推动工业互联网安全技术产品加速变革，防护工作逐步向动态协同转变，促进安全生态体系创新 [14]。

（一）产业发展体制机制不健全，联动发展职责不明晰

我国出台了多项顶层政策文件以指导工业互联网安全发展，但工业企业在实际开展安全防护项目的设计、建设、实施、运维等过程中，仍存在缺乏具体政策文件统筹指导、安全主体责任不明等问题。工业互联网安全标准体系尚未完全建立，相关标准之间缺乏严格的逻辑关联，关键技术的管理标准缺失，无法为企业开展安全防护工作提供标准依据，难以满足产业发展的安全需求。工业互联网安全在保障目标对象、安全需求等方面具有特殊性，而工业属性伴生的保护场景多样性给其自身发展带来了挑战。因此，亟需建立针对性强、特色鲜明的工业互联网安全保障体系。

（二）防护建设运营机制不顺畅，综合保障能力难以提升

当前，我国工业互联网安全建设大多围绕工业企业的基本安全需求而开展，处于以设备采购为主的初级阶段。一方面，工业企业用户在完成工业互联网安全项目建设后，因缺少持续学习工业互联网安全配置、设备运维知识的相关渠道，无法发挥安全产品的最大效果；另一方面，企业用户普遍缺乏对安全措施有效性的量化考核和评估能力，存在安全制度形同虚设、安全设备较多闲置等问题。

（三）产品服务认证机制不完善，规模应用进展不平衡

虽已存在各类工业互联网安全产品和服务，但对应的市场准入和认证机制还不完善，缺乏检测认证标准规范和技术。这是因为工业互联网安全近年来才受到关注，相关标准仍在编制过程中，且标准制定存在一定的难度。工业互联网安全产业仍处于发展起步阶段，而制定的标准既要适应当前用户需求，又要具有一定的前瞻性，才能指导和引领该类产品的发展；不同行业和环境对工业互联网安全产品的需求差别较大，且工控协议种类繁多，也增加了标准的制定难度。现阶段对工业互联网安全产品和服务的检测多沿用传统 IT 安全检测认证标准和测评方法，这显然是不合适的。工业互联网安全产品和服务的统一标准、认证机制明显缺乏，使得相关认证难以面向市场快速推广，更难以进行规模化生产和产业化应用 [15,4]。

（四）产业创新聚集效应不明显，关键产品发展不成熟

在产业聚集方面，我国工业互联网安全产业起步晚、体量小，如外建安全产品和服务的市场规模占网络安全产业整体规模的比例不足 5%。我国从事工业互联网安全的企业约有 266 家，专注该领域的企业约有 47 家，企业规模普遍较小；传统信息安全企业、自动化背景企业、IT 系统集成企业进入工业互联网安全领域的时间普遍较短，存在技术创新能力不足、缺乏具有市场竞争力的核心产品等问题 [15]。目前，我国安全服务企业在外置防护产品技术方面成熟度相对较高，在内置信息安全工控产品技术方面的成熟度偏低；企业的安全服务能力难以满足现实需求，尚未形成引领产业发展的骨干龙头企业，产业创新集聚效应不明显，产业整体规模仍处于低位 [4,13]。在关键产品方面，我国工业互联网安全产业技术和产业化应用仍不成熟，工业软硬件产品对外依赖度较高，不可预知的安全隐患增多，安全风险加剧 [16]。

我国工业互联网安全技术体系的技术成熟度与应用情况如图 3 所示。①在外建安全防护方面，防护类技术的成熟度较高，市场应用水平也较高，如基于策略的访问控制、网络隔离和应用程序白名单等；但外建安全防护产品在工业场景兼容性、协议支持丰富度、智能化水平和可视化水平程度等方面与国外先进技术仍存在一定差距；在基于指纹匹配的资产识别、基于漏洞库的风险关联、威胁溯源等检测类和响应类技术方面尚存在不足，与国际工业互联网安全企业仍存在较大差距。②在内嵌安全防护方面，我国在通信访问控制、通信和数据加密、

身份识别等技术方面已取得一定突破，但与国际水平相比仍存在较大差距；由于工业系统整体兼容性不强、价格竞争优势不足等因素，市场应用水平整体偏低。

（五）安全人才结构布局不合理，人才核心竞争力不充分

网络安全实质上是攻击能力和防御能力的较量，归根结底是人才之间综合能力的比较。随着工业互联网安全风险日益突出，工业企业亟需持续提升安全能力，除了购买网络安全产品以获得安全能力外，还应通过培养网络安全人才、购买网络安全咨询服务来增强运维能力，弥补自身安全能力的不足。我国网络安全人才的缺口较大，亟需具备网络安全技能且适应复杂工业场景的安全防护复合型人才；人才供需失衡使企业间的人才竞争加剧，人才储备无法适应未来发展的挑战。

五、新一代工业互联网安全产业发展的路径建议

（一）加强政策引导与扶持，打造国内国际双循环相互促进的产业新发展格局

建议加强工业互联网管理体系建设，强化顶层设计，建立健全法律法规，实施政策引导和配套，持续完善产业发展的战略措施，形成持续发展的长效机制。强化“关口前移、防患于未然”的安全防护理念，及时制定工业大数据、工业云平台等新兴领域的安全管理政策体系和标准，规范和指导新安全技术与工业互联网领域的融合应用 [17]。注重政策落实效果，强化工业企业安全主体责任并提升防护意识，打造以国内大循环为主体，国内国际双循环相互促进的产业新发展格局。

（二）强化科技创新与转化，促使科技创新成为产业发展的内生动力

科技创新是“十四五”时期的首要任务，是新型基础设施建设的重要依托，也是网络安全的基础。建议工业互联网安全产业秉承创新发展理念，逐步建立基于自主知识产权的技术架构和标准，完成开放生态建设，打牢工业互联网安全产业健康发展的基础。

持续增强体系化技术创新能力，构建国家工业互联网安全保障体系，瞄准产业发展制高点，指导发布重点领域技术创新指南，在资产识别、风险管理、应急处置等技术领域梳理瓶颈短板清单，引导市场主体创新突破。不断探索工业互联网安全创新融合应用的解决方案，鼓励安全企业积极探索应用大数据、AI、5G、区块链等新兴技术解决工业互联网安全问题，形成典型解决方案，为工业企业部署

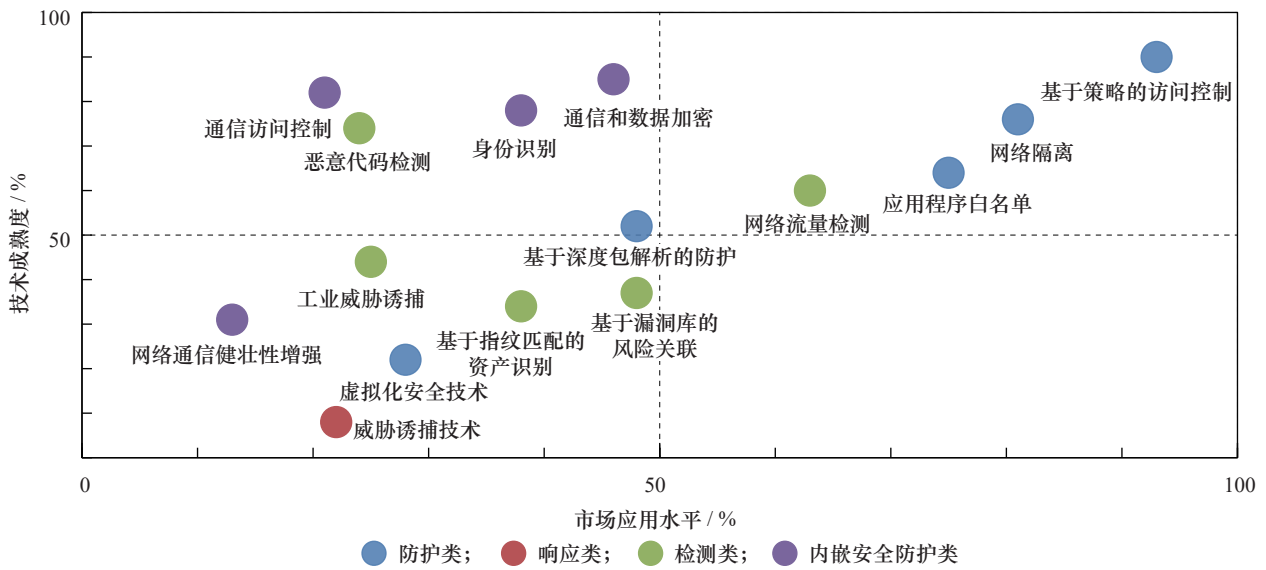

图 3　工业互联网安全技术成熟度与应用情况

安全防护措施提供可借鉴模式。

推动工业互联网安全技术产品的研发。建立以企业为主导的“产学研用”联合创新机制，瞄准工业互联网安全基础技术、共性关键技术、前沿技术以及重点工业领域的信息安全系统解决方案和核心环节，研究新兴工业互联网安全技术在工业领域的融合应用，尽快突破一批关键核心技术。加强协同攻关，以点带面、消除瓶颈，补齐短板、整体推进，重点发展一批高端产品，形成具有市场竞争力的产品体系。积极推动核心技术成果转化和交易，加强知识产权保护和管理，促进创新成果转化，不断提升创新链、产业链、价值链的整合能力。

（三）引导相关企业和机构优势互补，构建产业发展的良好生态

跨界合作是应对交叉领域安全问题的有效办法。随着越来越多的工业设备联网，仅靠企业自身力量很难对潜在的工业互联网安全风险进行全面防御，需要政府主管部门、科研机构、安全服务商、工业企业、工控设备提供商等进行优势互补，紧密配合，针对各工业行业的特点，协同构建多维度、多层次的防御机制，共同应对来自各领域的安全威胁与挑战，打造协同发展的良好产业生态体系[12,13]。

加强产业政策倾斜，鼓励工控系统制造企业、工业企业和网络安全企业深度合作。建议制定促进合作的相关政策，鼓励工业互联网各相关企业针对工业领域各行业的生产运营特征，聚焦行业痛点，将技术突破、模式创新与产业实际需求相结合，逐步形成政府引导、用户主导、厂商参与和资本推动的良性产业生态。

在能源、交通等重点产业进行集中攻关，整合“政产学研用”资源，发挥集中力量办大事的制度优势，形成关键核心技术攻坚体制，合作研发高精尖安全产品和解决方案，成立国家级的工业互联网安全企业。以问题为导向，加快建立关键共性技术体系，布局技术短板和下一代前沿技术，尽快突破关键核心技术瓶颈，确保自主可控。

重点培育龙头骨干企业，引导安全厂商不断革新商业模式，强化网络安全资源整合，聚焦产业多方协同，加快构建产业生态。基于用户需求重构产业链，工业互联网安全产业链上下游企业要共同发力，加快资本整合和战略合作步伐。集中力量构建开放的网络安全生态，将安全能力对外辐射给更多合作伙伴，践行合作共赢的发展理念。

优化产业生态环境，发挥政府管理部门、行业协会的引导与支持作用，拓宽企业在技术引进、投资融资、人才引进等方面的渠道。建议加快落实法律法规、政策标准等对工业企业信息安全的有关要求，挖掘企业安全需求，激发市场活力。统筹基础研究、技术创新与应用部署，增强上游技术研发与下游推广应用的协同互动效应，打造协同发展的产业生态系统。

（四）维护供应链安全与稳定，加强协调、联合评估、风险预警等机制建设

近年来，随着逆全球化思潮和经济民族主义的涌起以及新型冠状病毒肺炎疫情的暴发，全球供应链的不确定性进一步加剧。在大国博弈日益激烈、先进技术产业竞争态势加剧的背景下，加强供应链安全监管，建立全面的供应链安全管理体系已经迫在眉睫。

加强顶层设计，将供应链安全纳入国家安全整体框架，制定供应链安全管理的政策法规，加快出台工业互联网供应链安全领域的战略规划。加大落实力度，形成科学规范、运行有效的制度体系，推动供应链安全管理标准制定向专业化和精细化发展，为相关部门和机构在识别、评估、减轻供应链风险方面提供依据。

强化全球供应链系统风险识别与评估，建立全生命周期供应链风险管理制度，形成信息跟踪、风险识别、危机应对联动的管理体系，提升有关全球供应链风险的防控能力。

开展供应链安全评估与审查，梳理工业领域的关键薄弱环节，对重点领域的工业基础供应链进行风险预警和风险管控。创建供应链风险评估共享服务，强化审查监管，建立适应性强、可持续和安全的供应链。

（五）加强人才培养与队伍建设，建立跨界安全人才培训教育体系

鼓励政府、高等院校、科研院所、工业企业与

安全企业加强合作，联合开展工业互联网安全学科建设，培养专业人才，促进该领域产业链、岗位链、教学链有机结合。多方整合优势资源，共建专业实验室、特色课程体系、实习实训基地，保持理论学习与实践的有机结合，全面提升工业互联网安全学科水平，批量培养具有工业互联网安全领域应用能力的高水平人才。例如，安全企业和工业企业联合建立工控安全测试床和网络靶场，让学生开展虚拟化对抗，提高其实战性和实操性。支持从事工业互联网安全的企业设立相关教育培训机构。我国工业互联网安全人才缺口大，特别是防御型人才，通过社会力量开展大规模职业培训教育，是快速弥补人才短缺问题的有效途径。加强财政资助力度，设立专项人才培养基金，依托重点创新课题，积极开展高端人才的培育。

参考文献

[1] 中华人民共和国工业和信息化部.《工业和信息化部办公厅关于推动工业互联网加快发展的通知》政策解读 [EB/OL]. (2020-03-21) [2021-01-05]. http://www.gov.cn/zhengce/2020-03/21/content_5493935.htm.
Ministry of Industry and Information Technology of the People's Republic of China. Policy interpretation on *Notice of the General Office of the Ministry of Industry and Information Technology on accelerating the development of the industrial Internet* [EB/OL]. (2020-03-21) [2021-01-05]. http://www.gov.cn/zhengce/2020-03/21/content_5493935.htm.

[2] 本刊编辑部. 工业互联网安全的企业视角与实践 [J]. 中国信息安全, 2019 (6): 66–77.
Editor of China Information Security. An enterprise perspective and practice on industrial Internet industry security [J]. China Information Security, 2019 (6): 66–77.

[3] 工业互联网产业联盟. 工业互联网安全框架 [R]. 北京: 工业互联网产业联盟, 2018.
Alliance of Industrial Internet. Industrial Internet security framework [R]. Beijing: Alliance of Industrial Internet, 2018.

[4] 前瞻产业研究院. 2018年工业信息安全行业市场现状与发展趋势分析 技术提高是关键 [EB/OL]. (2019-04-23) [2021-01-08]. https://www.qianzhan.com/analyst/detail/ 220/190422-71978700.html.
Prospective Industry Research Institute. 2018 industrial information security industry market status and development trend analysis, technology improvement is the key [EB/OL]. (2019-04-23) [2021-01-08]. https://www.qianzhan.com/analyst/detail/220/190422-71978700.html.

[5] 姚羽. 工业互联网创新发展必须强化网络安全的"底座"作用 [EB/OL]. (2021-02-06) [2021-02-08]. https://www.china-aii.com/index.php?m=content&c=index&a=show&catid=29&id=41.
Yao Y. Industrial Internet innovation development needs to strength the cyber security [EB/OL]. (2021-02-06) [2021-02-08]. https://www.china-aii.com/index.php?m=content&c=index&a=-show&catid=29&id=41.

[6] 网络安全管理局.《加强工业互联网安全工作的指导意见》解读 [J]. 中国信息化, 2019 (9): 19–20.
Network Security Administration. Interpretation of *The guidance on strengthening industrial Internet security* [J]. China Informatization, 2019 (9): 19–20.

[7] 工业信息安全产业发展联盟. 工业信息安全标准化白皮书 (2019版) [R]. 北京: 工业信息安全产业发展联盟, 2019.
National Industrial Security Industry Alliance. White paper on industrial information security standardization (2019 edition) [R]. Beijing: National Industrial Security Industry Alliance, 2019.

[8] 工业信息安全产业发展联盟. 中国工业信息安全产业发展白皮书（2017版）[R]. 北京: 工业信息安全产业发展联盟, 2018.
National Industrial Security Industry Alliance. White paper on industrial information security standardization (2017 Edition) [R]. Beijing: National Industrial Security Industry Alliance, 2018.

[9] 工业互联网产业联盟. 中国工业互联网安全态势报告（2019）[R]. 北京: 工业互联网产业联盟, 2020.
Alliance of Industrial Internet. China industrial Internet security situation report (2019) [R]. Beijing: Alliance of Industrial Internet, 2020.

[10] 工业信息安全产业发展联盟. 工业信息安全态势白皮书（2017）[R]. 北京: 工业信息安全产业发展联盟, 2019.
National Industrial Security Industry Alliance. White paper on industrial information security situation (2017) [R]. Beijing: National Industrial Security Industry Alliance, 2019.

[11] 中国网络安全产业联盟. 中国网络安全产业分析报告（2020年）[R]. 北京: 中国网络安全产业联盟, 2020.
China Cybersecurity Industry Alliance. China network security industry analysis report (2020) [R]. Beijing: China Cybersecurity Industry Alliance, 2020.

[12] 康双勇, 胡万里. 工业互联网安全技术研究及我国工业互联网安全产业发展情况分析 [J]. 保密科学技术, 2020 (5): 27–31.
Kang S Y, Hu W L. Research on industrial Internet security technology and analysis of China's industrial internet security industry development [J]. Secret Science and Technology, 2020 (5): 27–31.

[13] 工业信息安全产业发展联盟. 中国工业信息安全产业发展白皮书（2019—2020）[R]. 北京: 工业信息安全产业发展联盟, 2020.
National Industrial Security Industry Alliance. White paper on industrial information security standardization (2019—2020) [R]. Beijing: National Industrial Security Industry Alliance, 2020.

[14] 中国信息通信研究院, 工业互联网产业联盟. 2020年上半年工业互联网安全态势综述 [R]. 北京: 中国信息通信研究院, 工业互联网产业联盟, 2020.
China Academy of Information and Communication Technology, Alliance of Industrial Internet. Overview of the industrial Internet security situation in the first half of 2020 [R]. Beijing: China Academy of Information and Communication Technology, Alliance of Industrial Internet, 2020.

[15] 工业信息安全产业发展联盟. 中国工业信息安全产业发展白皮书 (2018—2019) [R]. 北京: 工业信息安全产业发展联盟, 2019.

National Industrial Security Industry Alliance. White paper on industrial information security standardization (2018—2019) [R]. Beijing: National Industrial Security Industry Alliance, 2019.

[16] 国家工业信息安全发展研究中心信息政策所. 2018年度工业信息安全形势分析 [R]. 北京: 国家工业信息安全发展研究中心信息政策所, 2019.
Information Policy Institute of China Industrial Control Systems Cyber Emergency Response Team. Analysis of the industrial information security situation in 2018 [R]. Beijing: Information Policy Institute of China Industrial Control Systems Cyber Emergency Response Team, 2019.

[17] 汪礼俊. 加强工业信息安全建设, 为“一带一路”工作保驾护航 [J]. 中国信息化, 2019 (4): 8–10.
Wang L J. Strengthen the construction of industrial information security and escort the work of the Belt and Road [J]. China Informatization, 2019 (4): 8–10.