交叉科学学报
Acta Interdisciplinary Science
2025 年第 02 卷第 02 期
Vol. 02, No. 02, 2025

SCIENCE FOOTPRINT PRESS

研究性论文
http://www.scifootprint.com/AIS/index.html

# 我国关键软件产业链供应链安全问题与对策研究

李丹丹[1,*]，李　敏[2]

（1. 中国电子科技集团有限公司电子科学研究院，北京 100041；
2. 国家工业信息安全发展研究中心，北京 100040）

**摘要**：当前，全球格局正经历快速的演变过程，经济全球化的趋势遭遇了逆向发展，单边主义和保护主义抬头，地缘冲突加剧，全球产业链供应链加速重塑。以美国为代表的美西方国家，将软件产业链供应链安全上升为国家战略，出台系列政策加强关键软件供应链安全。对比欧美发达国家，产业基础能力薄弱和产业链水平不高的问题，已成为影响我国制造业高质量发展乃至国家经济安全的“阿喀琉斯之踵”。因此，提升我国关键软件产业链供应链安全水平对培育新质生产力、推进新型工业化、落实总体国家安全观具有重要意义。文章从安全视角，梳理我国关键软件产业链供应链发展现状与成效，深入解构技术自主、生态构建、风险防控等方面存在的潜在风险与薄弱环节，并从战略布局、技术突破、体系建设、产业集群等维度提出建议，为构建我国关键软件产业链供应链安全治理体系提供支撑。

**关键词**：关键软件；产业链供应链安全；经济安全
**DOI**：10.48014/ais.20250420003
**引用格式**：李丹丹，李敏．我国关键软件产业链供应链安全问题与对策研究[J]．交叉科学学报，2025，2(2)：78-85.

## 引言

产业链供应链安全是新发展格局构建的核心支撑要素，既是推动产业高质量发展、保障实体经济稳健运行的战略基石，也是国家经济安全体系的关键构成。美西方国家迅速把握这一趋势，率先将核心产业链供应链安全纳入国家战略布局，将其视作维系经济优势、筑牢安全防线的重要举措。以美国为例，政府通过《建立供应链韧性、振兴美国制造、促进广泛增长》等系列政策工具，系统性推进半导体、医药等战略产业的本土化重构，着力构建风险可控的产业生态体系。我国在构建新发展格局进程中，始终将产业链现代化作为战略支点。习近平总书记强调“产业链、供应链在关键时刻不能掉链子，这是大国经济必须具备的重要特征”，并提出“要重点提升产业链体系的抗风险能力和国际竞争力，加快构建自主可控、安全高效的现代化供应链体系”等重要指示。2024 年出台的深化改革开放纲领性文件，特别强调要建立基础软件、工业软件等重点产业安全评估与动态监测体系，完善从基础研发到产业应用的制度保障，为培育具有国际竞争力的现代产业链提供了系统性解决方案。

## 1　我国软件产业链供应链韧性稳步提升

“十四五”时期，我国着力提升软件产业链供应链安全水平，在国家相关部委指导下，行业企业加快技术创新，不断增强关键软件供给能力，我国软件产业的产业韧性与增长潜力显著释放，业务收入始终保持两位数增速，产业规模持续扩大，以自主可控为核心的技术创新生态系统持续优化，产业供

* 通讯作者　Corresponding author：李丹丹，youyoudandan1992@163.com
收稿日期：2025-04-20；　录用日期：2025-05-21；　发表日期：2025-06-28

给侧结构性改革成效显著,软件产品与服务质量实现系统性跃升,软件产业迎来提质升级的高质量发展新阶段。

### 1.1 产业链现代化稳步推进

产品供给水平加速提升。基础软件方面,国产操作系统、数据库产品兼容适配性能稳步提升,与国际主流产品差距逐渐缩小,截至2024年底,鸿蒙操作系统装机量超过10亿台,欧拉操作系统累计装机量超过1000万套,达梦、人大金仓数据库特定场景性能赶超国际巨头甲骨文[1]。工业软件方面,广州建成"设计仿真工业软件适配验证中心",武汉成立国家数字化设计与制造创新中心,研发工业软件一体化平台,推出"天工"工业软件生态。中望、华天、同元软控等自主研发的计算机辅助设计、仿真、计算等软件在几何建模引擎、仿真求解器、科学计算等核心技术取得突破,并已在航空航天、船舶等重点行业实现应用验证。新兴平台软件方面,基于云计算、大数据、人工智能、区块链等技术的新兴平台软件在重点行业典型场景深化应用,阿里云推出基于"自研飞天+CIPU"的新一代云计算架构,百度昆仑芯实现大规模商业化落地,深度求索DeepSeek、百度文心一言、阿里云通义千问、科大讯飞星火大模型等人工智能语言大模型产品纷纷涌现,推动着人工智能技术在娱乐、教育、医疗、工业等领域的应用边界不断拓展。产业基础能力持续强化。底层技术方面,操作系统内核等基础软件组件实现新突破。重点专业船舶CAE(Computer-Aided Engineering,计算机辅助工程)软件加速迭代升级,结构专业仿真软件已具备对国外同类产品的替代能力,流体专业预报精度已追平国际主流商用软件,电磁专业仿真精度接近国外同类软件水平。标准体系方面,软件和系统工程标准体系逐步建成,生存周期管理、方法与工具、软件价值等重点领域国家标准陆续研制和发布。价值保障方面,国内累计超过30个省市出台了首版次软件应用补偿政策,山东、安徽、四川等地已落地实施,共推动近1000款产品通过首版次软件认定[2]。

### 1.2 产业创新能力持续增强

我国软件产业已从"跟随式创新"转向"引领式突破",通过技术自主化、生态全球化、应用场景化,成为全球数字经济的核心驱动力。研发投入方面,根据工业和信息化部数据,2023年我国软件与信息技术服务业研发投入总额突破1.5万亿元人民币,同比增长约15%,占全行业营收的12%[3]。中国软件研发投入规模位居全球第二,仅次于美国(2023年约3800亿美元),占全球软件研发总支出的25%[4]。根据中国版权保护中心计算机软件著作权登记信息统计,2023年全国共完成计算机软件著作权登记2495213件,同比增长35.95%,登记数量和增速均创5年来新高[5]。科创板60家软件行业上市公司在2024年前三季度的研发投入总计达97.64亿元,平均研发强度近37%,超过科创板平均水平[6]。产学研用协同创新方面,从单点技术突破转向"硬件+软件+服务"全链条安全加固。例如在信创领域,龙芯、飞腾等CPU企业联合统信、麒麟操作系统厂商,通过"1+N"适配模式(1个芯片架构+N个行业解决方案),累计完成200万+软硬件适配认证[7-9]。产教合作方面,教育部2024年统计显示,全国已建成207个软件领域现代产业学院,校企联合开发教材5800余部,实习实训覆盖90%以上的关键软件企业,人才供需错配率下降至15%[10]。模式与机制创新方面,工业和信息化部联合财政部、国家金融监督管理总局开展首版次软件保险补偿机制试点工作,制定相关认定管理办法,完善国产软件应用保障机制,鼓励各地政府出台相关政策措施为首版次软件健康发展保驾护航。"软件定义"方面,国内重点科技企业研制面向电子消费、高端装备、智能网联汽车、智慧城市等典型行业领域的"软件定义"解决方案得到市场高度认可,例如,华为推出软件定义汽车的全栈式智能汽车解决方案,引领我国智能网联新能源汽车创新发展新风潮。

### 1.3 自主软件应用生态不断优化

国产软件攻关和推广应用有序推进。截至2024年12月,重点工业企业数字化研发设计工具普及率达82%,具备行业、区域影响力的工业互联网平台超340个,连接工业设备超9600万台(套),工业互联网实现工业大类全覆盖[11]。制造业数字化转型升级成效显著。2024年我国工业软件产品

2940 亿元，同比增长 7.4%[12]，软件应用已覆盖研发设计、生产制造、运维服务、企业管理等制造业各关键环节。重点领域数字化发展提速。农业数字化加快向全产业链延伸，农业生产信息化率超过 25%[13]。浙江中控、艾普工华等制造业数字化重点企业研发出的生产管控软件在石油化工、汽车与装备制造等重点行业已具备较强竞争力，创新应用成效显著。企业主体地位凸显。截至 2023 年底，全国注册的软件和信息技术服务业企业数量已突破 4.5 万家，国家级专精特新“小巨人”软件企业约 2000 家，A 股上市软件企业超 500 家，总市值占比超 10%[14]。全球独角兽榜单中，中国软件企业占约 25%，涵盖人工智能、企业服务、网络安全等细分领域[15,16]。开源生态初步建成。开放原子开源基金会累计推动至少 32 项开源项目进入孵化期[17]。截至 2024 年 10 月，欧拉社区全球开发者数量超过 2 万人，生态伙伴超 1800 家[18]；截至 2024 年 12 月 31 日，开放原子开源鸿蒙社区累计超过 8200 名贡献者，共 63 家成员单位，社区生态初具规模[19]。产业高效集聚发展。国家发布《中国软件名城（园）管理办法》，推动各地启动中国软件名园创建筹备工作。2023 年，14 家中国软件名城软件业务收入突破 9.7 万亿元，同比增长 13%，占全国比重接近 80%，名城名园名企联动机制初步形成[3]。

## 2 当前我国关键软件产业链供应链安全面临的问题

### 2.1 新代差风险增加，关键基础软件自主创新不足

基础软件开发难度大、壁垒高、周期长、盈利难，需要长期的技术积累和资源投入。我国基础软件发展起步晚，对外技术依赖度高，源头技术和底层关键技术自主化程度低，国内市场长期被美西方垄断，受外部制约风险高。在通用操作系统和数据库领域，国产产品正处于急需加快迭代优化和扩大应用规模的关键期，但“不愿用、不敢用、不真用”问题依然突出，严重制约产品成熟度提升和发展生态建设。在嵌入式操作系统领域，美国风河公司 VxWorks 系列产品占据国内 50%以上市场[20]，国产产品主要通过购买国外产品源码或利用国外开源软件进行二次开发，尚未全面掌握关键核心技术，仅处于“可用”水平，应用场景严重不足，安全风险巨大。在编程语言及编译器领域，国内研发企业极少，国产产品仅实现了从无到有，但产品成熟度严重不足，应用仍处于起步阶段。在软件建模工具、软件开发和测试工具领域，我国市场仍被国外产品垄断，国产产品技术水平低，企业小、散、弱。在应用和数据迁移工具领域，国产产品通用性弱，兼容适配基础软件数量少，迁移效率低。在开源社区关键平台软件领域，相比国际主流产品，国产平台的项目储备量和社区活跃度存在数量级差距，开源软件供应链管理能力弱。

伴随社会进入“人机物”融合时代，以区块链和人工智能等技术为核心，实现数据可控，支撑建立数据确权、流通和分配机制的消费端新型操作系统，以及基于新型计算模式、连接万亿规模各类物联终端，实现制造模块个性化定制、智能化匹配和轻量化应用的新型工业操作系统呼之欲出。当前，美西方加快发展第三代互联网（Web3.0）、ChatGPT、元宇宙等颠覆性技术和产品，抢抓新兴领域发展先机，而国内目前处于起步阶段，新的发展代差正在形成，面临的安全风险和挑战加大。

### 2.2 市场壁垒高筑，工业软件创新发展遇困境

工业操作系统作为工业控制的“中枢”，是支撑工业高质量发展的关键环节，主要包括嵌入式软件、工业协议及控制单元三部分。当前，美西方国家构筑了工业操作系统全产业链“护城河”，占据市场主导地位。嵌入式软件方面，美国 Vxworks、RT-Linux 以及加拿大 QNX 等产品占据全球 90%以上的市场。工业协议方面，全球由美国、德国、日本主导的协议（含相关衍生协议）合计占比超 90%[21]。工业控制单元方面，美、德、法等国在大型可编程逻辑控制器（Programmable Logic Controller，PLC）、安全仪表系统（Safety Instrumented System，SIS）等领域具有较大优势。芯片方面，美国在微控制单元、数字信号处理等方面处于全球领先地位。

作为工业软件“卡脖子”环节，国产三维计算机辅助设计（Computer Aided Design，CAD）、计算机辅助工程（Computer Aided Engineering，CAE）等

高端设计仿真软件及中大型 PLC 软件供给能力严重不足,核心引擎、求解器等关键技术存在卡点,难以满足专业性要求高的复杂场景应用需求。我国90%以上研发设计类软件、50%以上的生产控制类软件、70%以上的运维服务类软件依赖进口,经营管理类软件中国产软件虽占有 70%的国内市场份额,高端市场领域仍以 SAP、Oracle 等国外企业为主[22]。电子设计自动化(Electronic design automation,EDA)软件几乎被新思科技(Synopsys)、铿腾电子(Cadence)、明导国际(Mentor Graphics)三家垄断。以 MATLAB 为代表的科学和工程计算软件被广泛应用于航空航天、汽车等重大装备领域。达索公司、参数技术公司、西门子公司等在仿真设计领域占据主导地位,国产软件多基于国外二次开发。我国企业积累形成的数据库、模型库、工艺库等关键数据资源大多被国外工业软件企业所掌控。一旦断供停服,将导致我国面临核心数据被封锁、数字化转型受阻,甚至军工装备研制瘫痪的严重风险。

## 2.3 生态基础薄弱,开源软件供应链风险已成为重大威胁

开源软件(Open Source Software,以下简称 OSS)是指遵循特定许可协议的软件,该协议确保用户能够自由地访问、利用、修改以及传播其源代码。以 Linux 操作系统、Apache 服务器、TensorFlow 机器学习框架为代表的典型项目,已成为全球数字基础设施的重要支撑,尤其在云计算、人工智能等领域的技术演进中发挥着关键作用。在我国产业数字化进程中,OSS 呈现出深度渗透特征:通信网络领域应用覆盖率突破 80%,金融科技、智慧医疗等民生领域部署比例超 65%[23]。这种技术生态的构建不仅加速了行业创新进程,更推动了国产软件产业从"跟随式"向"引领式"发展的战略转型。值得关注的是,OSS 的规模化应用与安全防护能力失衡现象日益凸显。开源组件的依赖嵌套导致漏洞传导风险倍增,恶意攻击者通过污染上游代码库、植入隐蔽后门等手段实施供应链攻击的案例年均增长率达 37%[24]。建立覆盖代码引入、漏洞修复、许可证审查的全生命周期治理体系,已成为保障数字供应链安全的关键举措。

全球开源技术供应链呈现"中心-边缘"治理格局,以硅谷科技巨头、标准制定机构及代码托管平台形成的技术联盟掌握着核心技术治理权。数据显示,全球排名前 50 的开源基金会中 82%注册于美国,其技术路线决策直接受到《出口管理条例》(Export Administration Regulations,EAR)等法规制约,形成隐形的技术主权壁垒[25]。我国虽在应用层实现快速渗透,但在基础架构层仍面临三重依赖困境:其一,Apache、CNCF 等主流基金会均受属地法律约束,重要代码仓如 GitHub 需遵循出口管制合规框架;其二,RISC-V 等开放标准的技术演进方向受制于美国产业政策;其三,开发工具链关键环节存在单点故障风险,2020 年 DockerHub 对中国实体实施访问限制即为典型案例[26],充分暴露数字主权冲突下我国产业链供应链的脆弱性,一旦供应链"命门"被别人掌握,随时可被断供制裁,造成重大安全风险。

## 2.4 同质化竞争激烈,国内产业分布制约产业链供应链稳定

一方面,全国各地区软件产业分布不合理。目前基础软件、工业软件等关键软件领域发展成效突出的区域集中在北上广深等发达地区,武汉、成都等产业基础雄厚的中西部城市发展势头迅猛,其余地区仍停滞于满足基本需求的应用软件领域。业务模式上,以传统的系统集成业务为主,针对底层技术和基础研究的软件开发业务相对欠缺。同时,从全国产业链分布来看,目前尚未形成区域一体化联动发展模式,各省市关键软件技术产品点状突破、各自为战,"生态烟囱"极大地制约了全国软件产业链供应链安全稳定。

另一方面,产业集聚发展特色化不足。作为软件产业集聚发展的核心载体,软件园区成为维护产业链供应链安全的主力军。目前国内软件园区普遍存在"重应用,轻基础"的问题。目前近 350 家软件园区中,有近六成的园区以应用软件为主导方向,园区之间同质化竞争严重,对优秀企业、重大项目和高端人才的争夺趋于白热化。而对于面临"卡脖子"风险的基础软件、工业软件等领域,园区普遍缺少系统谋划布局,资源投入少,产业链培育迟缓。一旦遇到极端情况,我国软件园为代表的产业集群

将受到极大的安全风险挑战。

## 3 保障关键软件产业链供应链安全的应对策略思考

### 3.1 落实国家战略部署要求,打好关键软件攻坚战

一是聚力攻坚基础软件,加强操作系统内核、编程语言及工具链等源头和底层关键技术攻关研究,联合开放原子开源基金会等社会团体组织积极培育基础软件根技术自主生态。加强自主路线探索,深化开源鸿蒙(OpenHarmony)微内核架构研发,扩大重点行业适配应用范围。建立操作系统性能基准测试平台,制定中国版 SPEC CPU 标准,量化评估国产系统与国外产品的代际差距,在不断对比中优化国产系统性能指标,追赶国际主流操作系统。二是重点突破高端工业软件,大力发展关键工业控制软件,提升标准研制、测试验证、集成适配、联调联试等公共服务能力,推动研发设计类工业软件在重点行业的集成应用。打造高水平工业互联网平台,构建“边缘层—平台层—应用层”全栈技术体系,突破边缘计算节点轻量化部署、工业大数据建模分析、数字孪生引擎等关键技术。三是前瞻布局船舶、汽车、石化等重点行业新兴工业操作系统,以设备更新和技术改造为契机,建设工业操作系统创新中心,联合产业链上下游生态伙伴加强供需结对攻关,开展关键核心技术攻关研发、行业标准制定、场景验证与产业生态培育,打造集“研发-测试-应用-孵化”于一体的创新枢纽,构建我国工业软件自主创新生态。四是建立关键共性技术联合攻关机制,为产业发展提供综合保障环境,完善包括协同开发与集成验证环境、应用推广平台、公共开放计算平台以及知识库、组件库、数据库等基础资源平台。

### 3.2 围绕国家重大工程,加快关键软件自主创新

一是充分借鉴信息技术应用创新经验,加快基础软件、工业软件自主发展,按照分级分类分批的方式推动重点行业关键环节软件迭代升级,加快工业操作系统、设计仿真软件、生产制造软件等应用推广。加强产业链上下游企业的合作,包括芯片、操作系统、数据库、中间件、应用软件等企业,实现协同创新,共同解决关键软件的兼容性、性能等问题。二是顺应开源共享、开放的趋势,推行“开源+闭源”双模开发:基础算法层开源(如有限元求解器),行业应用层闭源,推广“开放核心(Open Core)”模式,实行基础功能开源+高级功能商业化。三是围绕金融、电信、能源、石化、船舶等行业典型应用场景需求,搭建供需对接桥梁,加快协同攻关与体验推广中心建设,组建“芯片-操作系统-中间件-应用”四级适配矩阵,形成自动化测试流水线,构建全栈式适配验证体系,提升技术攻关与测试验证等公共服务能力。四是构建国内基础软件、工业软件应用容错机制,推动建立软件首版次应用保险补偿机制,探索建立多元化的风险分担机制,通过保险补偿方式降低企业和用户的风险,促进首版次软件的市场推广。加强对首版次软件的知识产权保护,切实维护软件企业的合法权益,为软件企业创新提供良好的法律环境。

### 3.3 加强开源软件安全管理体系建设

一是持续完善我国开源软件基础设施,建立国产软件开源组件库,鼓励国内软件企业、科研机构和开发者将自主研发的优质组件贡献到开源组件库中。支持建设优质代码托管平台,存储和管理组件的源代码。二是提升开源治理支撑及安全保障能力,建立开源风险评估与治理公共服务平台,基于平台能力逐步面向重点地区、重点行业、开源社区、重要用户单位等,提供开源软件安全合规检测、漏洞发布和修复建议等服务。构建评估模型,从安全漏洞、许可证合规性、社区活跃度、代码质量等多维度评估开源项目的风险,提出开源合规使用的最优化解决方案。三是健全开源安全漏洞应急响应机制,推动建设软件物料清单(SBOM)管理平台,通过漏洞扫描、许可证合规检查,提前发现供应链安全隐患。选择重点行业、重点业务系统(如核心交易系统、门户网站)进行 SBOM 管理试点,验证平台功能与业务流程适配性。对接国家网络安全公共服务平台,共享 SBOM 数据与威胁情报,提升全国软件供应链安全态势感知能力。四是建立完善开源代码检测、知识产权分析、供应链安全防护等技

术支撑手段,提供代码安全测试、代码质量评估、开源许可证检测等公共服务,建立开源软件检测认证体系,围绕开源软件及发行版的质量和安全形成“白名单”,为地方数字产业、电子信息、汽车、高端装备等重点行业领域应用提供支撑服务,提升开源软件安全合规保障水平。

### 3.4 有效发挥产业园作用,提升产业链供应链布局水平

一是围绕京津冀、粤港澳大湾区、长三角一体化、中部地区崛起等国家区域战略布局,推动产业链上下游企业开展协同配套、联合攻关。以长三角地区为例,加强上海、江苏、浙江、安徽“三省一市”在软件产业的协同创新,建立统一的创新资源共享平台,促进科技成果转化、知识产权保护等方面的合作。推动长三角软件园发展集聚区建设,共同打造有影响力的长三角软件产业集群,联合开展软件技术难题攻关,鼓励企业之间进行技术合作和产品配套,提高区域软件产业的整体竞争力。二是以国家级特色软件园区建设为契机,引导各地因地制宜打造软件园“名牌”,鼓励各方加大资源投入,优化产业布局,出台支持技术攻关、企业引培、人才培养等政策,完善公共服务体系,完善区域产业创新发展环境。三是加强构建央地联动、部省共建机制,探索在地方开展关键工业软件园区共建机制,围绕集成电路、新能源汽车、机器人、大飞机等场景,引入工业软件开发商、系统集成商、应用企业等,促进企业之间的协同创新和合作发展,构建“技术研发-成果转化-产业孵化-生态协同”的全链条创新体系,打造具有国际竞争力的工业软件产业集群。

**利益冲突**:作者声明无利益冲突。

## 参考文献(References)

[1] 财联社. 开源欧拉操作系统累计装机量超过 1000 万套[EB/OL]. (2024-11-15)[2025-01-20]. http://m.toutiao.com/group/7437330868512834086/? upstream_biz=doubao.

[2] 人民网. 全国超 30 省市出台首版次软件支持政策 助力国产软件“破茧”[N/OL]. (2023-12-05)[2025-03-20]. http://it.people.com.cn.

[3] 工业和信息化部. 2023 年软件和信息技术服务业年度统计数据[R/OL]. (2024-10-25)[2025-01-07]. https://www.miit.gov.cn/rjnj2023/rj_index.html.

[4] Statista. Global Technology Research and Development Report 2023[R/OL]. (2023-01-01)[2025-03-20]. https://www.statista.com/reports/global-tech-rd-2023.

[5] 国家版权局. 关于 2023 年全国著作权登记情况的通报(国版发函〔2024〕5 号)[EB/OL]. (2024-02-07)[2025-03-02]. https://www.gov.cn/zhengce/zhengceku/202402/content_6933554.htm.

[6] 何昕怡. 科创板软件企业构筑数字基座 助力科技自立与产业升级[EB/OL]. 上海证券报·中国证券网,(2025-03-12)[2025-03-22]. http://www.zqrb.cn/stock/gupiaoyaowen/2025-03-12/A1741785457484.html.

[7] 龙芯中科技术股份有限公司. 龙芯中科技术股份有限公司官方网站[EB/OL]. (2025-02-26)[2025-03-14]. http://www.loongson.cn.

[8] 飞腾信息技术有限公司. 飞腾信息技术有限公司官方网站[EB/OL]. (2025-03-10)[2025-03-12]. http://www.phytium.com.cn.

[9] 统信软件技术有限公司. 统信软件技术有限公司官方网站[EB/OL]. (2024-12-10)[2025-03-14]. http://www.uniontech.com.

[10] 教育部. 中国教育年鉴(2024)[M]. 北京:人民教育出版社,2024.

[11] 王政,刘温馨. 近万家中小企业数字化改造 工业互联网实现工业大类全覆盖[N/OL]. 人民日报. (2025-01-07)[2025-01-24]. 中国政府网. https://www.gov.cn/yaowen/liebiao/202501/content_6996621.html.

[12] 工业和信息化部. 2024 年软件业运行良好[EB/OL]. (2025-01-26)[2025-03-13]. http://www.miit.gov.cn/gxsj/tjfx/rjy/art/2025/art_7565395dd0be48c6962639256f23e5f9.html.

[13] 农业农村部信息中心. 中国数字乡村发展报告(2022 年)[R/OL]. (2023-03-01)[2025-01-03]. https://www.gov.cn/xinwen/2023-03/01/content_5743969.html.

[14] 中国软件行业协会. 2023 年中国软件与信息技术服务业发展蓝皮书[R]. 北京:中国软件行业协会,2024.

[15] 胡润研究院. 2023 全球独角兽榜[R/OL]. (2023-12-01)[2024-07-20]. https://www.hurun.net.

[16] CB Insights. 2023 Global Unicorn Report[R/OL]. New York: CB Insights, (2024-02-01)[2025-03-20]. https://www.cbinsights.com/research/report/2023-global-unicorn-report.

[17] 开放原子开源基金会. 开放原子开源基金会官方网站[EB/OL]. (2025-03-14)[2025-03-14]. https://www.openatom.cn/

[18] 刘晶. 五年累计装机 1000 万套 欧拉实现规模商用[N/OL]. 中国信息化周报. (2024-11-27)[2024-12-20]. https://baijiahao.baidu.com/s?id=1816842682789841798&wfr=spider&for=pc.

[19] 开放原子开源基金会. 开源鸿蒙 OpenHarmony 社区运营报告[R/OL]. (2025-01-27)[2025-02-13]. https://www.elecfans.com/d/6452276.html.

[20] 李佳. 市占率超对手两倍,风河领先全球嵌入式市场[EB/OL]. 21ic 中国电子网. (2015-02-02)[2025-01-13]. http://www.21ic.com/embed/hardware/drivers/201502/34212.html.

[21] HMS Networks. Industrial Network Market Shares 2023:The Global Market for Industrial Networks [R/OL]. (2023-05-16)[2025-02-22]. https://www.hms-networks.com.

[22] 王海成. 从国家战略高度重视国产工业软件产业高质量发展[EB/OL]. (2021-08-27)(2025-01-03]. https://baijiahao.baidu.com/s?id=1709249090963233854&wfr=spider&for=pc.

[23] 袁豪杰,赵冉,唐刚. 面向开源软件的安全风险分析与防范[J/OL]. 信息安全与通信保密. 2023(10):125-134[2025-01-03]. https://www.zhangqiaokeyan.com/academic-journal-cn_information-security-communications-privacy_thesis/02012101444598.html.

[24] 代韫. 开发者使用开源软件如何有效避免许可证传染?[EB/OL]. (2023-03-30)[2025-03-28]. https://zhuanlan.zhihu.com/p/618144762.

[25] 云计算标准和开源推进委员会. 全球开源生态洞察报告(2024 年)[R/OL]. (2024-07-25)[2025-03-01]. http://221.179.172.81/images/20240705/27981720160008486.pdf.

[26] 佚名. Docker 禁令生效,开始限制所有被美国列入实体清单的公司和个人使用 Docker [EB/OL]. (2020-08-19)[2025-01-03]. https://blog.csdn.net/z136370204/article/details/108107957.

# Research on Security Issues and Countermeasures of Key Software Industry Chain and Supply Chain in China

LI Dandan[1,*], LI Min[2]

(1. China Electronics Technology Group Corporation Electronic Science Research Institute, Beijing 100041, China; 2. National Industrial Information Security Development Research Center, Beijing 100040, China)

**Abstract**: Currently, the global landscape is undergoing rapid transformation. The trend of economic globalization is experiencing a reversal, unilateralism and protectionism are on the rise, geopolitical conflicts are intensifying, and global industrial and supply chains are undergoing accelerated restructuring. Represented by the United States, Western countries have elevated software supply chain security to a national strategy and introduced a series of policies to strengthen critical software supply chain security. Compared with developed countries in Europe and America, the weak industrial foundation and low level of industrial chain have become the "Achilles heel" that affects the high-quality development of China's manufacturing industry and even national economic security. Therefore, improving the security level of China's key software industry chain and supply chain is of great significance for cultivating new quality productivity, promoting new industrialization, and implementing the overall national security concept. From a security perspective, this article combs through the development status and achievements of China's critical software industry chain and supply chain, deeply deconstructs the potential risks and weak links in such aspects as technological autonomy, ecological construction, and risk prevention and control, and puts forward suggestions from the dimensions of strategic layout, technological breakthrough, system construction, industrial cluster, etc., so as to provide support for building a security governance system for China's critical software industry chain and supply chain.

**Keywords**: Key software; the security of the industry chain and supply chain; economic security

**DOI**: 10.48014/ais.20250420003

**Citation**: LI Dandan, LI Min. Research on security issues and countermeasures of key software industry chain and supply chain in China[J]. Acta Interdisciplinary Science, 2025, 2(2): 78-85.

Copyright © 2025 by author(s) and Science Footprint Press Co., Limited. This article is open accessed under the CC-BY License (http://creativecommons.org/licenses/by/4.0/).