DOI 10.15302/J-SSCAE-2021.02.008

工业互联网供应链安全发展路径研究

樊佩茹，李俊，王冲华，张雪莹，郝志强

（国家工业信息安全发展研究中心，北京 100040）

摘要：工业互联网供应链在促进企业生产效率提升、降低企业经营成本的同时，扩大了工业控制系统、生产设备等的受攻击面，引入了新的安全风险。针对工业互联网供应链安全发展问题，本文描述了工业互联网供应链发展形势，梳理了工业互联网供应链存在的典型安全问题，分析了我国工业互联网供应链面临的安全挑战。研究提出了我国工业互联网供应链安全的创新发展路径：发挥制造产业种类齐全的良好优势，加强工业互联网安全知识产权布局，加速实现信息创新产业体系建设，提升工业互联网供应链技术安全保障能力，重视工业互联网供应链渠道安全，鼓励上下游企业良性协同发展，优化工业互联网供应链安全发展环境。

关键词：工业互联网；供应链；网络安全；发展路径

中图分类号：TP393　　**文献标识码：**A

Security Development Path for Industrial Internet Supply Chain

Fan Peiru, Li Jun, Wang Chonghua, Zhang Xueying, Hao Zhiqiang

(China Industrial Control Systems Cyber Emergency Response Team, Beijing 100040, China)

Abstract: While an effective industrial Internet supply chain improves production efficiency and reduces operating costs of enterprises, it broadens the attack surface of industrial control systems and production equipment, introducing new security risks. This study focuses on the security development path of the industrial Internet supply chain. First, the current status of the industrial Internet supply chain is introduced. Subsequently, typical security problems are summarized and challenges faced by China are analyzed. Furthermore, an innovative security development path is proposed for the industrial Internet supply chain. Considering the full range of manufacturing, China should further enhance the layout of intellectual property for industrial Internet and construct an industrial system for information innovation. Moreover, its capabilities for technically guaranteeing the security of the industrial Internet supply chain should be promoted, with a focus on channel security. Furthermore, coordinated development between upstream and downstream enterprises should be encouraged, and a secure development environment should be optimized for the industrial Internet supply chain.

Keywords: industrial Internet; supply chain; network security; development path

收稿日期：2021-01-16；**修回日期：**2021-02-23

通讯作者：王冲华，国家工业信息安全发展研究中心高级工程师，研究方向为工业互联网安全、网络与系统安全、网络攻防；E-mail: chonghuaw@live.com

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

工业互联网作为新一代信息技术与制造业深度融合的产物，日益成为新工业革命的关键支撑、深化“互联网 + 先进制造业”的重要基石。供应链作为工业领域不可缺少的组织形态，以客户需求为导向，以提高质量和效率为目标，以整合资源为手段，实现产品设计、采购、生产、销售、服务等全过程的高效协同，成为工业制造业的重要组成部分。工业互联网新技术体系及其能力对行业转型的牵引力不断增强，工业领域出现了丰富的新模式新业态 [1]。随着工业互联网与实体经济的不断融合，工业领域供应链逐步开展数字化转型，形成工业互联网供应链。

本文将工业互联网供应链定义为：在工业互联网架构下，由工业设计、研发、原材料采购、加工、组装、制造、运输、销售等环节中一组过程和资源构成的网络；既包括生产商、批发商、物流商、配送商和其他工业制造过程中所涉及的企业，又包括企业间数据汇聚、分析、管理过程中所涉及的信息通信产品及服务。工业互联网供应链能够满足企业数据及时汇聚、分析、再利用的需求，促进提升生产效率、降低经营成本，但同时扩大了工业控制系统、生产设备的受攻击面，将引入新的安全风险。

当前，全球范围内工业互联网供应链安全事件频发 [2~4]，断供、网络攻击等威胁加剧。一方面，带来众多的重大生产事故和重要经济损失，甚至危害到社会稳定和国家安全；另一方面，对工业企业的信息化建设构成重大隐患，严重制约工业互联网的健康安全发展。在此背景下，工业领域关键技术产品供应中的安全问题成为社会各界关注的焦点，已有学者对当前芯片、基础软件、工业互联网平台、工业应用等的发展及安全问题进行了分析，提出若干解决对策和建议 [5~8]。然而，当前在工业互联网供应链安全问题及发展路径研究方面尚存缺失。

针对于此，2020 年中国工程院启动了“新一代工业互联网安全技术发展战略研究”咨询项目，旨在分析国际工业互联网安全领域技术趋势和发展态势，创新探索我国工业互联网安全技术发展路径。本文作为“工业互联网供应链安全”方向研究成果的学术性展示，总结工业互联网供应链发展情况，梳理工业互联网供应链安全问题，针对我国工业互联网供应链面临的现实挑战，提出工业互联网供应链安全创新发展路径，以期为新一代工业互联网安全发展提供参考。

二、工业互联网供应链发展形势

在工业互联网与制造业深化融合应用背景下，数字化和全球化是工业互联网供应链发展的必然趋势。

（一）数字化转型

随着“互联网 +”行动计划的日益深入，商业新模式新业态不断涌现，工业按需定制、弹性供给、高效配置的需求不断增长，生产制造技术体系和供给能力不断成熟，工业领域供应链的数字化需求和意愿加快释放，全面数字化转型已经成为共识。

工业互联网供应链通过对上下游工业企业的信息化管理和信息的数字化连接，借助信息通信产品与服务，实现从工业产品需求分析到原材料采购、智能制造、仓储、再到风险控制各环节的数字化。现如今，工业企业之间的竞争已经演变为工业互联网供应链之间的竞争。工业互联网供应链以企业内外部各种信息系统的对接为基础，通过采购、仓储、生产等各业务流程数据的实时获取和共享，配合外部供应商的协作，提高产品技术交互准确率、采购计划准确率、物资供应与财务结算效率，降低库存堆积，实现工业企业降本增效的目的。工业互联网供应链打破了传统信息的阻隔，打通了从工业生产需求、物资供应、物流运输到销售售后的各个环节，达成了全方位信息覆盖式的资源统筹调配共享和高效率协同作业。

（二）全球化发展

改革开放以来，越来越多的工业企业将产品研发、物料采购、生产制造、物流配送、销售及服务进行全球化布局，形成具有全球化特征的供应链体系。随着全球互联网化和产业链的变化，一个核心部件可能包含多种关键技术与产品，由多个核心企业生产供应；同时这些核心企业可能分布在多个国家，并在全球范围内采购原材料。

工业互联网供应链将不同产业的多个参与主体串联起来，通过人工智能、大数据、物联网等新

技术实现不同角色的高效协作和信息传递的无缝衔接，使传统制造业供应链由单一链条上企业的单线链接转向网络化、多层次的全方位链接，助力企业缩短供应链环节，降低供应链成本。南京大学长江产业经济研究院发布的《2019 中国进口发展报告》显示，自 2009 年起，我国稳居世界第二大进口国，进口来源涵盖全球 230 多个国家和地区。中国海关总署进出口商品统计数据显示，2019 年工业制品进口总额为 9.26 万亿元，占商品进口总量的 64.69%，相比 2018 年部分类别商品的进口数额仍在增长；如动力机械及设备类增加 3.8%，通用工业机械设备及零件类增加 1.5%，电力机械、器具及电气零件类增加 0.8%。2019 年美国联合包裹运送服务公司（UPS）发布《工业采购趋势洞察》亚太地区研究报告，调研中国、日本、泰国等国企业的工业采购者后发现，当今工业呈现采购来源日益国际化的趋势，亚洲地区约有 33% 的企业采购来自区域外的供应商。

三、工业互联网供应链典型安全问题分析

工业互联网供应链涉及的系统、实体、活动多样及结构复杂等特性扩大了其受攻击面。国内外已经发生了多起工业互联网供应链安全事件，本文将主要风险分为供应链的断供和网络攻击两类。

（一）供应链断供

中国和美国在科技、制造领域存在结构性、长期性的竞争关系，而我国工业互联网供应链在部分核心关键技术产品方面对美国等发达国家的依赖程度较高。国际形势瞬息万变，工业互联网供应链一旦断裂，我国的工业生态稳定性将受到严重威胁。

随着中美经贸摩擦的不断演进，美国不断出台限制措施以阻断我国重点领域供应链。1990 年，美国将中国升级为“重点观察国家”；1991 年对我国发起“特别 301”调查，此后公布的《特别 301 报告》都将中国列入“黑名单”重点调查，2017 年根据调查结果对我国实施单边制裁。笔者根据美国联邦公报（Federal Register）的公开数据进行统计，截至 2021 年 1 月，美国将 484 个中国实体列入“实体清单”，针对关键新兴技术、基础技术和相关产品进行出口管制；仅在 2020 年，新增列入“实体清单”的中国实体数量多达 145 家。芯片断供、内存禁售、呼吸机关键元器件缺货等事件表明，我国科技制造业发展仍受制于工业互联网供应链的短板弱项。

新型冠状病毒肺炎疫情来临之后，全球经济动荡，各国间的不信任度增加，单边主义和贸易保护主义盛行，严重冲击了全球既有的供应链；各国着手构建更独立、完整、安全的工业互联网供应链将是新的趋势。2020 年 4 月，美国和日本公开鼓励本国企业撤出中国，欧洲通过《自贸协议》引导“4 换 1”计划（用日本、韩国、越南、印度来整体替换中国的世界工厂）。随着劳动力成本升高、贸易摩擦加剧等因素影响，我国制造业可能失去原有的国际竞争力，我们要警惕全球供应链和产业链的去中国化并针对性做好长期准备。

（二）供应链网络攻击

在工业互联网供应链全球化态势下，能接触到工业企业核心技术产品、核心部件、敏感数据的供应商和服务商数量大大增加，工业企业的受攻击面大幅延展。针对企业外部合作伙伴、供应商或第三方服务商的供应链攻击已经成为一种新型威胁。近年来，工业互联网关键技术产品在开发、交付、使用等不同环节遭受了多起实际攻击，利用企业外部合作伙伴的安全疏忽与缺陷造成的关键基础设施破坏、敏感数据泄露、信息系统入侵等网络安全事件层出不穷。

一是工业生产厂商预留后门。厂商在开发过程中忘记删除测试版本中的调试后门、方便售后管理或出于其他目的预留的超级后门，都可能被攻击者发现并直接登录，获得工业产品的控制权。2013 年 6 月，“棱镜门”事件披露了美国在全球范围内开展的绝密电子监听计划，以思科公司、国际商业机器公司（IBM）、谷歌公司、苹果公司等为代表的科技巨头利用其在全球软硬件供应链中广泛渗透的优势在科技产品中隐藏“后门”，协助美国政府对世界各国实施大规模信息监控。2017 年 8 月，知名电信设备制造商 Arris 生产的调制解调器存在 3 个硬编码后门账号漏洞，可被攻击者利用获取设备控制器、安装恶意固件、架设僵尸网络等。

二是基础软件被污染。开发工具、协议栈等基础软件被植入恶意代码、后门并编译到其他应用程序中进行分发时，将造成威胁扩散，且难以在

事中、事后由一般用户发现和根除。2015 年 9 月，“XcodeGhost”事件引发关注，攻击者在 Mac 操作系统上的集成开发工具 Xcode 中加入恶意模块并进行传播，开发者使用被污染的软件版本编译应用程序时会植入恶意逻辑，可能导致弹窗攻击和被远程控制，仅我国感染该恶意程序的用户当月就达到 2.14×10^7 个。2018 年，安全公司 ESET 发布的 OpenSSH 跟踪报告指出，被植入后门代码并经过编译的 OpenSSH 能被攻击者用于窃取合法登录账户和密码。

三是工业产品存在漏洞。攻击者通过利用工业产品漏洞来实现远程设备控制、拒绝服务攻击等。2018 年 3 月，思科公司发布了智能安装客户端远程代码执行漏洞（CVE-2018-0171）预警，随后该漏洞被用于攻击我国多个互联网数据中心及组织机构，导致交换机因配置信息被清空而瘫痪，造成业务网络不可用等问题。2019 年 2 月，苏格兰远程监控系统制造商开发的制冷控制系统被发现存在重大安全缺陷，攻击者利用默认账户和密码登录系统后台，可修改制冷系统的温度、报警阈值等参数，进而影响设备正常运行。

四是工业产品供应渠道劫持。工业产品在采购、销售、物流等供应渠道中被劫持和篡改，攻击者在产品中构建后门或漏洞以实现入侵。2009 年，伊朗核设施的数据工控系统供应商、离心机制造商、零部件供应商已陆续被国家力量攻破并植入“震网”病毒，病毒被成功引入伊朗核设施并造成破坏，导致伊朗核计划推迟数年之久。2015 年，卡巴斯基安全实验室披露“方程式”组织拥有的超级信息武器库，包括能对数十种常见品牌硬件固件重编程的恶意模块；该攻击可以通过在特定目标采购、返修主机或硬盘过程中修改硬盘固件程序实现，受攻击目标包括中国、俄罗斯、印度等国家。2017 年，维基解密曝光了美国中央情报局的 Vault7 武器库，可以推测其通过物流渠道劫持，在全新的 iPhone 手机中刷入固件达到入侵目的。

五是工业软件升级劫持。软件产品在整个生命周期中要进行功能升级、补丁修复等更新，攻击者通过劫持软件升级过程中的更新模块或下载链接，在工业软件中植入恶意代码。2017 年，乌克兰专用会计软件 me-doc 的升级程序被劫持，用户更新软件时会感染 Petya 勒索病毒变种 NotPetya，导致乌克兰、俄罗斯、印度、法国、英国等多个国家的政府、银行、电力系统、通信系统等受到不同程度的影响。

近年来，一些国家对我国通信行业领头企业实施了各种维度的供应链封锁，硬件断供会导致企业停产，软件断供将扼杀企业硬件设计和实验试制能力。全球典型网络安全事件表明，针对工业互联网供应链的攻击在数量上尚不及传统网络安全事件，但攻击一旦成功可能影响上亿个用户，造成巨大的经济损失，严重时甚至威胁国家安全。部分工业领域依靠进口外国信息技术产品缓解关键零部件的供应需求，短时间内可以取得高速发展，但实则将为我国工业互联网安全埋下隐患。我们需重视工业互联网供应链安全风险，针对当前的安全问题，探寻针对性发展路径。

四、工业互联网供应链安全挑战

工业互联网供应链存在的断供、网络攻击等安全风险，归因于现阶段我国工业互联网供应链安全面临的两大现实挑战：部分关键技术产品受制于人，网络安全防护水平不足。

（一）部分关键技术产品受制于人

一是基础工业技术历史欠账较多。我国虽然建立了大而全的工业体系，在高速铁路、运载火箭等重大装备领域达到世界领先水平，但基础零部件、基础材料、基础工艺等基础工业仍欠账较多。低端产品大量出口，高端产品依赖进口，部分高端领域与发达国家差距较大，关键核心技术被垄断。基础工业技术复杂度高，需要长周期的研发投入，国外企业在领域内已深耕多年，形成了较高的技术壁垒。相比之下，我国基础工业产业起步较晚，核心技术落后较多，如在工业软件开发过程中，存在顶层系统架构搭建难度大、设计开发程序使用门槛高、硬件环境构建开销大、知识产权受限、后期维护繁琐等问题。多数企业或者基于国外技术开展本地化的二次开发，或者在国外软件的基础上集成其他功能应用；但“二次开发”“代理集成”的核心技术产权依然属于国外企业，国产基础工业技术“空心化”

严重，无法控制知识产权，难以突破国外限制。

二是部分关键产品高度依赖国外企业。在工业软件方面，我国飞机、船舶、冶金、化工、生物医药、电子信息制造等重点制造领域长期以来习惯使用国外工业软件，对于背后的设计原理了解不够，缺乏基础工艺研发数据的长期积累，导致基础技术积累存在明显差距。工业控制系统及软件高度依赖国外技术产品，工业基础软件、研发设计软件、生产控制软件、信息管理软件、工业嵌入软件等基本依靠进口；工业操作系统、工业软件开发平台、工业数据实时数据库等重要基础软件全产业链缺失，导致工业控制应用软件几乎空白；工业软件必须由工业实时数据库提供后台支撑，但我国尚缺乏国产工业实时数据库产品。在计算机辅助设计、辅助分析、辅助制造、辅助工艺规划等工具软件方面，以达索公司、西门子股份公司为代表的国外厂商仍占有绝对优势；在制造执行系统、工业自动化系统等生产控制关键领域，通用电气公司（GE）、ABB 集团等公司保持了行业龙头地位；在供应链管理、定制化应用集成平台系统、协同办公系统等信息管理软件领域，SAP、甲骨文股份有限公司等仍占据相当的份额。在工业硬件方面，对于工控微控制单元（MCU）、数字信号处理（DSP）、现场可编程逻辑门阵列（FPGA）等核心元器件和数据采集与监视控制系统（SCADA）、可编辑逻辑控制器（PLC）、分散控制系统（DCS）等系统，国外产品占领大部分国内市场；超高精度机床、高端工业机器人技术和产品基本掌握在国外厂商手中。

三是工业协议标准由国外标准化组织和厂商主导。工业互联网基础设施所应用的关键核心协议大都由国际标准化组织（ISO）、国际电工委员会（IEC）、OPC 基金会等国际组织联合主要工业厂商制定，各种现场总线通信协议标准、OPC 协议标准等一直由国外机构控制。全球各类自动化厂商、研究机构、标准化组织围绕设备联网推出了数百种现场总线协议、工业以太网协议和无线协议，协议标准众多且相对封闭；西门子股份公司、施耐德电气有限公司、罗克韦尔自动化有限公司等企业通过将私有协议、工业控制设备与制造设备捆绑销售，已经形成了事实上的标准垄断。在现场总线方面，罗斯蒙特公司、霍尼韦尔国际公司、ABB 集团、GE、西门子股份公司等长期控制着国际标准的制定。在工业以太网方面，国内厂商主要选择适用于专有工控产品的工业以太网协议，如西门子 Profinet、施耐德 Modbus TCP/IP、罗克韦尔 Ethernet/IP 等。

（二）网络安全防护水平不足

一是网络攻击手段多变导致风险加剧。工业互联网供应链网络攻击风险主要源于企业外部合作伙伴存在的安全疏忽与缺陷，被攻击者用于破坏企业数据及入侵企业系统。工业互联网供应链网络攻击涉及工业产品开发、交付、使用等不同环节，包括污染软件开发、测试、部署、维护环境或工具，在设备上预装恶意软件，感染合法应用以分发恶意软件，盗用合法证书签名恶意软件 4 种典型手段。面对日益普遍且影响复杂的工业互联网供应链攻击活动，原材料采购、加工、包装、运输、配额、售后等诸多环节都可能遭到攻击，网络安全隐患较为突出。工业互联网供应链一旦遭受攻击，几乎很难发现，但破坏力巨大、覆盖面积广，通过召回或升级产品阻止攻击的成本高、周期长，应对较为困难。

二是工业互联网安全技术产品尚处于攻关阶段。工业互联网供应链包含工业产品或服务从开发到交付过程中涉及的通信网络、软硬件设备等信息系统，安全防护对象扩大、连接范围更广。传统网络安全技术的防护对象和方法与工业互联网供应链并不完全一致，不考虑区别直接套用必然导致防护效果不佳、存在安全风险。我国安全厂商目前大多以网络安全业务为主，在工业信息安全、工业互联网安全等领域的产品积累和服务经验不足，仍处于攻关阶段；已有安全能力重点关注提升工业设备、工控系统、工业企业单点的安全防御能力，难以保障工业互联网供应链各环节的安全。为了抵御日益增多的有组织、针对性、不计成本的网络攻击，需要重新评估和审视工业互联网供应链安全防护架构与边界，构建覆盖监测感知、协同防御、响应恢复的安全技术体系。

三是工业互联网供应链安全管理能力不足。工业互联网供应链涉及制造商、供应商、系统集成商、服务提供商等多个实体以及技术、法律、政策等软环境。当前我国多数企业存在应对网络

攻击的意识不强、安全管理制度不完善、安全检测评估机制不健全、对工业企业网络安全的引导不够等问题。工业互联网供应链的安全取决于链上所有合作伙伴之间的配合，安全协同发展仍面临巨大挑战。

五、工业互联网供应链安全创新发展路径

我国高度重视工业互联网供应链安全问题，自2016 年起相继发布《国家网络空间安全战略》《网络空间国际合作战略》《关于积极推进供应链创新与应用的指导意见》《关于进一步做好供应链创新与应用试点工作的通知》《网络安全审查办法》《中共中央关于制定国民经济和社会发展第十四个五年规划和二〇三五年远景目标的建议》等多项政策文件。

针对我国工业互联网供应链安全面临的现实挑战，依据国家相关政策要求，本文提出工业互联网供应链安全创新发展路径（见图 1）。立足我国制造产业种类齐全的良好优势，首先从知识产权布局、信创产业建设、技术安全保障 3 个方面给出建议，通过技术手段应对工业互联网供应链断供和网络攻击问题；其次从重视渠道安全、上下游企业协同、优化发展环境 3 个方面给出解决思路，通过供应途径、企业协同、总体环境 3 个角度的安全管理，保障工业互联网供应链安全技术的有效落实。

（一）发挥制造产业种类齐全的良好优势

改革开放以来，我国制造业持续快速发展，建成了门类齐全、规模最大的工业体系，有机地嵌入全球供应链之中，形成显著的产业优势，为我国工业互联网供应链安全发展提供了新机遇。一是基于我国超大规模、多层次、多元化的内需市场，发挥我国工业门类齐全、生产能力强大、配套能力齐全、适应能力灵活的优势，扩大消费水平，提升传统制造业水平。二是在各行业中下游产业形成合力，着力补短板、强弱项，扫除工业互联网供应链中的瘀点和堵点，促进国内各个环节、各个产业、各个区域之间的畅通。三是促进国内与国外的经济联通，构建国内国际相互促进的新发展格局，提高供给侧制造体系与需求侧的适配性，带动高价值、高水平、系统性的供需循环，构建完整、安全、可靠的工业互联网供应链体系。

（二）加强工业互联网安全知识产权布局

立足我国产业规模优势、配套优势、部分领域先发优势，针对工业互联网供应链安全领域的短板弱项，运用新思想、新理论、新方法、新模型、新发现，完善工业互联网安全知识产权布局，从“基础”“源头”锻造长板优势，缓解“断供”威胁。一是加强基础理论和前沿技术研究，注重原创导向，充分发挥基础研究对工业互联网供应链安全的源头供给和引领作用。二是加强标准研制，围绕工业互

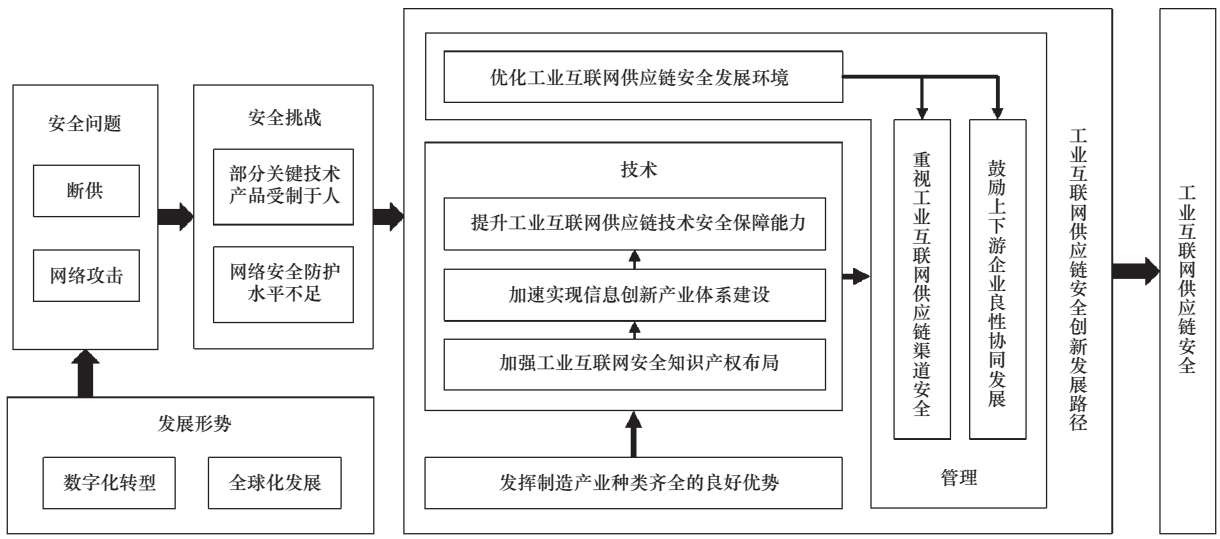

图 1　工业互联网供应链安全创新发展路径

联网供应链数字化、全球化带来的安全发展要求，促进工业互联网供应链安全标准的同步规划、同步制定，从适用性、先进性、规范性方面提高标准质量，加强标准信息服务能力和符合性测试能力，提升参与和塑造国际标准的能力和水平。三是健全知识产权风险评估体系，加强工业互联网供应链全环节、全领域安全的专利布局，探索建立知识产权风险评估制度，充分发挥知识产权的应有作用，在工业互联网供应链安全专利许可、技术转让、开源软件风险测评、工业数据信息、商业秘密保护等方面加强预警，切实提升风险应对能力。

（三）加速实现信息创新产业体系建设

着力产业体系建设要求实现从 IT 底层基础软硬件到上层应用软件全产业链的信息技术应用创新发展。基于我国工业制造业种类齐全、信息化基础良好的优势，加速实现信息创新产业体系建设，规避直接使用国外技术产品可能存在的工业生产厂商预留后门或开发工具被“污染”问题。一是制定信息技术应用创新产业发展规划，从技术体系引进、产业基础强化两个方面推动工业互联网供应链安全关键技术产品的创新发展，重点突破高端制造与高科技技术产品，将智能制造作为产业端升级的新方向。二是推动信息技术应用创新产业关键技术和产品的规模化部署，开展试点应用，分行业、分场景形成可推广、可复制、可移植的解决方案和试点示范。三是构建信息技术应用创新产业链，构建区域级产业聚集集群，打造覆盖芯片、服务器、存储、交换机、操作系统、数据库、中间件、工业操作系统、政务软件、办公软件等完整的工业互联网供应链体系，保障工业设计、生产、加工、销售过程中工业智能芯片、工业控制系统等工业设备产品的安全。

（四）提升工业互联网供应链技术安全保障能力

工业互联网供应链涉及的实体和环节多样，直接套用传统网络安全技术会导致防护效果不佳，需针对工业互联网供应链安全防护对象开展核心技术攻关，抵御日益复杂的网络攻击。一是分析工业互联网供应链安全防护对象的新特征和新需求，从传统网络安全技术中借鉴思路和方法，发展可统筹兼顾工业互联网供应链全环节安全的技术体系。二是研究工业产品安全检测技术，加大在开源代码安全检测、漏洞挖掘与分析、恶意软件识别及清除、网络劫持检测、智能情报、动态预警等方面的资源投入，充分发挥技术创新在工业产品安全保障中的作用。三是研究工业产品安全防御技术，利用工业产品的安全标识、安全审查、产品溯源、假冒产品排查、威胁监测、态势感知、攻防演练等手段，提升对工业产品的安全控制能力。四是融合应用新技术保障工业互联网供应链安全，研究人工智能、区块链、可信计算、威胁情报、知识图谱、基础安全资源库等在安全技术中的应用，促进构建工业互联网供应链安全技术体系。五是推进企业侧工业软硬件安全防护措施部署，对企业信息资产进行跟踪，加强工业生产、主机、智能终端等设备安全接入和防护，强化网络协议、装置设备、工业软件等安全保障，强化工业互联网平台、工业应用程序安全，强化应用过程中关键信息和数据的安全保护，落实相关网络安全标准要求，提升企业内外网安全防护能力。

（五）重视工业互联网供应链渠道安全

工业互联网供应链的产品、零部件、软件由上游向下游的转移过程依赖互联网，任一环节遭到攻击，都可能在最终工业产品中引入软件缺陷或漏洞，埋下安全隐患。需重视工业互联网供应链的渠道安全，应对工业产品供应渠道和软件升级劫持攻击。一是针对工业互联网供应链上的各类渠道，设计针对性的安全防护措施，重点保障负责软件、产品交付的集中式分发渠道安全，支持软件供应商和用户及时识别恶意渠道。二是在正规渠道发布技术或产品，向用户提供可验证正确性的校验数据；在安装或升级软件时，校验相应安装包或升级模块的签名，防止软件升级劫持等风险。三是从正规渠道购买、下载软硬件，采用可信的第三方开源、商业库、算法，采购安全可信的软件外包服务等；关注所用组件的安全信息，针对已被披露的严重安全问题，通过配置或加入其他安全措施进行控制，及时升级相关组件，缓解安全影响。四是加强对合作第三方的安全管理，在合同或协议中明确双方的安全责任，要求合作第三方定期进行自

评估并及时反馈评估结果。五是积极引入专业安全人才，设立专职的网络安全技术岗位、安全运营服务岗位；建立安全操作及运维管理制度，加强企业员工网络安全培训及审计，提升企业内部人员安全意识，避免由人员引入的工业互联网供应链渠道劫持风险。

（六）鼓励上下游企业良性协同发展

工业互联网供应链涉及的实体和环节多样，受攻击面广；基于某些环节必然被突破的假设，需推动上下游企业联动协调、相融共生、协同发展，共同抵御层出不穷的网络攻击活动。一是深入调查研究工业互联网重点技术及核心企业上下游供应链关系，整合和优化供应商、制造商、经销商以及自主知识产权等各种资源信息。二是针对供应链薄弱环节和供需短板，围绕企业解决用工、原材料供应、物流、融资等需求，全面梳理并摸清堵点、难点，针对性施策，打通上下游关联环节，畅通供应链大循环。三是加强工业互联网上下游企业的产销对接，鼓励链上合作伙伴建立良性互动关系，链上企业坚持保障本环节的安全，形成企业间利益共享、风险共担、共同成长的生态群落，促进工业互联网供应链协同安全发展。四是在工业生产的各个环节建立检查点，将安全性评估列为必要评审项，严格遵守安全规范，防止因配置错误导致后门、漏洞等安全威胁；自主研发或采购的软硬件在投入使用前应经由独立的内部或外部测评组织进行安全性评估，及时解决所发现的问题。

（七）优化工业互联网供应链安全发展环境

我国已出台相应的法规制度，发布了相关安全标准，以保障工业互联网供应链安全；但相比于工业强国，尚缺乏有效的网络安全风险审查评估机制和手段，在专项政策法规和配套措施、组织实施等方面亟需提升。一是建立针对性的工业互联网供应链安全管理框架，明确各方在供应链攻击防护中需要承担的责任和义务，在国家层面保障工业互联网供应链安全发展。二是建立健全工业互联网供应链安全监管制度，制定相关审查评估规范，对关键工业软硬件产品进行检测，评估其安全性和合规性，形成负责任的供应商清单，并对供应商进行分级管理。三是制定适合国情的工业互联网供应链网络安全评价标准，重点针对新技术新应用带来的安全风险，加强调查研究，在开源软件风险测评、工业数据安全防护等方面加强预警，提升风险应对能力。四是推动工业企业和配套企业建立完善的工业互联网供应链安全管理制度，引导企业建立供应商审核制度，从行业资质、管理体系、技术能力、产品质量、网络安全防护能力等多个角度对供应商进行安全评估，并采取针对性的管控措施，及时淘汰不符合要求的供应商。五是加强国际产业安全合作，开展技术、标准、检测检验、认证等方面的国际交流，建立多渠道、多层次供应链安全体系，增强产业链供应链韧性，形成具有更强创新力、更高附加值、更安全的工业互联网供应链。

六、结语

当前国际环境日趋复杂，世界经贸格局的不确定性明显增加，我国工业互联网供应链安全正在遭遇严峻考验。作为制造业大国，我国拥有全球最全的工业门类，最多的工业设备，丰富的工业互联网生态以及大量的工业和信息化人才。我国应充分利用这一优势条件，加强知识产权布局，加速开展信息技术应用创新产业体系建设，提升技术安全保障能力，重视渠道安全，鼓励上下游企业良性协同发展，优化安全发展环境；以技术和管理相结合的思路创新我国工业互联网供应链安全发展路径，保障工业互联网产业安全健康发展。

参考文献

[1] 何伟, 张伟东, 王超贤. 面向数字化转型的“互联网+”战略升级研究 [J]. 中国工程科学, 2020, 22(4): 10–17.
He W, Zhang W D, Wang C X. Strategic updating of Internet plus considering digital transformation [J]. Strategic Study of CAE, 2020, 22(4): 10–17.

[2] 何熙巽, 张玉清, 刘奇旭. 软件供应链安全综述 [J]. 信息安全学报, 2020, 5(1): 57–73.
HE X X, Zhang Y Q, Liu Q X. Survey of software supply chain security [J]. Journal of Cyber Security, 2020, 5(1): 57–73.

[3] 祝国邦, 陈洁. 软件供应链安全现状与对策建议 [J]. 中国信息安全, 2018 (11): 44–47.
Zhu G B, Chen J. The status and countermeasure suggestion of software supply chain security [J]. China Information Security, 2018 (11): 44–47.

[4] Luszcz J. How maverick developers can create risk in the software and IoT supply chain [J]. Network Security, 2017, 2017(8): 5–7.

[5] 高青松, 刘惠玲. 全球供应链深度互嵌下芯片产业关键节点的产业链安全研究 [J]. 经济论坛, 2020 (3): 11–21.
Gao Q S, Liu H L. Research on industrial chain security of key nodes in the chip industry with deeply interconnected global supply chain [J]. Economic Tribune, 2020 (3): 11–21.

[6] 谢劲松, 符兴斌, 赵文辉. 面向信息产业发展的基础软硬件生态研究 [J]. 信息技术与网络安全, 2020 (9): 1–5.
Xie J S, Fu X B, Zhao W H. Research on the basic software and hardware ecology for development of information industry [J]. Information Technology and Network Security, 2020 (9): 1–5.

[7] 王晨, 宋亮, 李少昆. 工业互联网平台: 发展趋势与挑战 [J]. 中国工程科学, 2018, 20(2): 15–19.
Wang C, Song L, Li S K. The industrial Internet platform: Trend and challenges [J]. Strategic Study of CAE, 2018, 20(2): 15–19.

[8] 宁振波. 力筑工业之基 重铸智造灵魂 [J]. 软件导刊, 2021, 20(1):1–5.
Ning Z B. Build the foundation of industry, recast the soul of intelligent manufacturing [J]. Software Guide, 2021, 20(1): 1–5.