工业互联网供应链安全治理研究*

李正文[1,2]，董良遇[1,2]
（1. 国家工业信息安全发展研究中心，北京 100040；
2. 工业信息安全感知与评估技术工业和信息化部重点实验室，北京 100040）

摘 要：针对工业互联网供应链面临的新型安全威胁与治理困境，系统分析了供应链攻击面的结构性特征、典型攻击类型及其演进趋势，识别出供应链透明度不足、工业环境固有约束、跨组织信任缺失及检测能力局限等核心技术挑战。在此基础上，构建供应链安全风险量化评估模型，并设计涵盖技术防护、供应商管控与监管合规的三层治理框架，以评估模型输出结果驱动供应商分级管控决策。该框架以零信任架构向供应链延伸及安全左移为设计原则，从完整性保障、身份访问控制、威胁检测响应、供应商分级准入、合同标准化、第四方风险穿透管理及法规协同等方面构建纵深防御体系。研究成果可为工业互联网平台运营方、设备制造商及行业监管机构提供系统化的安全治理参考路径。

关键词：工业互联网；供应链安全；安全治理
中图分类号：TP393. 08　　**文献标志码**：A　　**DOI**：10. 19358/j. issn. 2097-1788. 2026. 06. 004

中文引用格式：李正文，董良遇. 工业互联网供应链安全治理研究[J]. 网络安全与数据治理，2026，45(6)：24-30.
英文引用格式：Li Zhengwen，Dong Liangyu. Research on supply chain security governance of industrial internet[J]. Cyber Security and Data Governance，2026，45(6)：24-30.

Research on supply chain security governance of industrial internet

Li Zhengwen[1,2]，Dong Liangyu[1,2]
（1. China Industrial Control Systems Cyber Emergency Response Team，Beijing 100040，China；
2. Key Laboratory of Industrial Information Security Perception and Evaluation Technology，
Ministry of Industry and Information Technology，Beijing 100040，China）

Abstract：Addressing the emerging security threats and governance challenges faced by the industrial internet supply chains，this paper systematically analyzes the structural characteristics of supply chain attack surfaces，typical attack patterns，and their evolutionary trends，identifying four core technical challenges：insufficient supply chain transparency，inherent constraints of industrial environments，absence of cross-organizational trust mechanisms，and limited threat detection capabilities. Building on this analysis，a quantitative supply chain security risk assessment model is constructed，and a three-layer governance framework encompassing technical protection，supplier management，and regulatory compliance is proposed，with model-derived risk indices driving tiered supplier control decisions. The framework adopts the extension of zero-trust architecture to supply chains and security-by-design as its core principles，establishing a defense-in-depth system that spans integrity assurance，identity and access control，threat detection and response，tiered supplier admission，contract standardization，fourth-party risk penetration management，and regulatory coordination. The findings provide a systematic security governance reference for industrial internet platform operators，equipment manufacturers，and industry regulators.

Key words：industrial internet；supply chain security；security governance

0 引言

在“工业 4. 0”与“中国制造 2025”战略的双重驱动下，工业互联网作为新一代信息通信技术与工业经济深度融合形成的新型基础设施、应用模式和工业生态[1]，既是承载新质生产力实践价值的关键领域，也是推动新质生产力培育成型的核心支撑，对推进经

* 基金项目：国家重点研发计划（2023YFB3107700）

济高质量发展具有重要意义。随着工业互联网发展加速向纵深拓展，其供应链日益呈现出数字化、全球化发展趋势[2]，从原材料采购到硬件制造，从固件分发到软件集成，再到云端服务与数据流转，每一环节都涉及数量庞大、来源多元的供应主体，导致供应链潜在攻击面持续扩大，硬件篡改、软件后门注入、开源组件投毒等新型供应链安全威胁频发，亟须构建覆盖设计、开发、集成、运维全生命周期，由技术防护、安全管控、监管合规共同构成的韧性安全治理框架。

1 工业互联网供应链安全威胁态势

1.1 供应链攻击面的结构性分析

工业互联网供应链并非单一线性链条，而是一个沿原材料、硬件、固件、软件、服务、数据纵向延伸的复杂网络，每个层级包含设计、加工、组装、制造等不同关键环节，涉及实体包括生产商、批发商、配送商、服务商等多种类型，如图 1 所示。在原材料与硬件层，稀土、芯片、传感器、PLC 模块等关键元器件往往经由设计、晶圆制造、封测、分销等多个环节流转，产地与供应渠道透明度极低；在固件与软件层，嵌入式实时操作系统、工业协议栈、组态软件及工业 APP 依赖大量第三方开源与商业组件，形成深度嵌套的依赖图谱；在服务与数据层，云平台托管、设备远程运维通道、工业互联网平台及其上运行的第三方应用，进一步将外部信任依赖引入原本相对封闭的工业控制网络。每一层次均构成独立的攻击面，层与层之间的接口则形成额外的风险传导路径。

与传统 IT 供应链相比，工业互联网供应链呈现出四点差异，深刻影响着安全威胁的形态与响应难度。一是实时性要求高，工业控制系统对控制指令的响应时延要求往往在毫秒级，任何影响系统可用性的安全措施均面临来自生产运营侧的强烈阻力。二是设备生命周期长，工业控制设备平均使用寿命可达 15～20 年，远超 IT 设备的 3～5 年换代周期，这意味着大量设备在设计之初从未预设现代安全机制。三是补丁部署周期慢，工业互联网场景中，工控系统计划外停机的经济成本极高，企业往往将安全补丁的部署拖延至定期停产维护窗口，部分高危漏洞的暴露窗口期长达数年。四是 OT 环境封闭性强，传统工业网络依赖物理隔离作为主要防护手段，既缺乏完善的流量监控基础设施，也缺少适配工业协议的安全分析能力，导致威胁感知能力先天不足。这四项特征共同决定了工业互联网供应链一旦被渗透，攻击者将获得远比 IT 环境更长的驻留窗口，产生的破坏力度也更大。

1.2 典型供应链攻击类型

依据攻击发生的供应链环节，可将工业互联网供应链攻击归纳为五类，如表 1 所示。

（1）硬件植入与供应篡改。攻击者在元器件生产或物流运输环节对目标设备实施物理篡改，植入硬件木马电路或以假冒器件替换正品。此类攻击隐蔽性极强，无法通过软件层面的安全检测发现，可在目标系统中蛰伏数年，待特定触发条件（特定时间、特定指令序列或物理信号）激活后实施定向破坏。

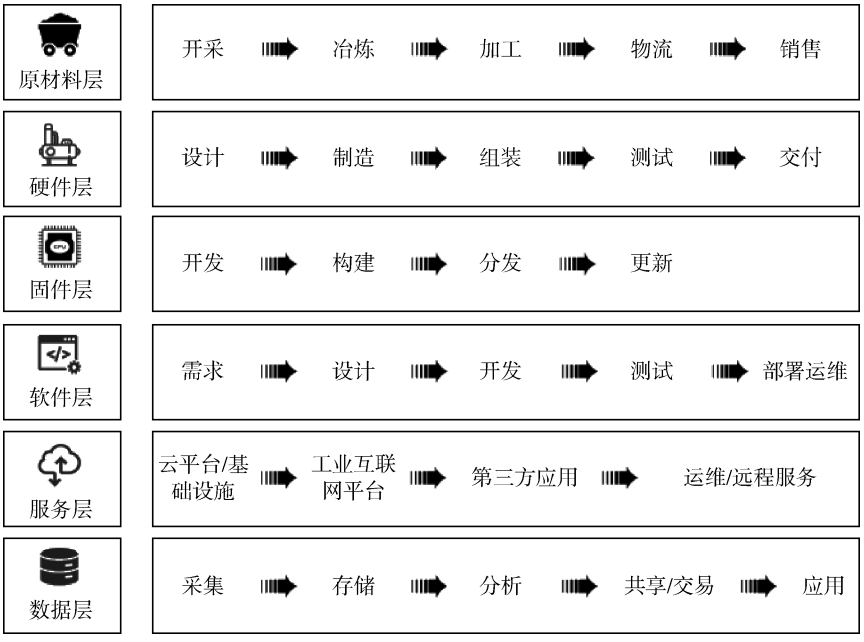

图 1　工业互联网供应链组成以及各层级主要环节

表 1　工业互联网供应链攻击类型与典型案例

攻击类型	主要侵入环节	攻击路径摘要	典型案例
硬件植入与供应篡改	生产/运输	物理植入木马电路或假冒元器件替换	黎巴嫩通信设备爆炸事件（2024）
固件/软件后门注入	开发/集成	渗透构建服务器，后门随签名更新包推送	SolarWinds 攻击事件（2020）
开源组件投毒	开发/集成	长期潜伏取得维护权后植入后门代码	XZ Utils 攻击事件（2024）
第三方运维通道劫持	运维/维护	利用 MSP 平台漏洞向下游客户推送恶意载荷	Kaseya VSA 攻击事件（2021）
工业协议漏洞利用	部署/运行	利用工业协议缺陷篡改控制逻辑或致 SIS 失效	震网病毒攻击事件（2010）

（2）固件/软件后门注入。SolarWinds 事件是该类攻击的标志性案例[3]。攻击者渗透 Orion 软件的构建服务器，将恶意代码注入编译过程，使后门伴随官方签名更新包分发。由于整个分发路径均经过官方渠道，传统基于签名验证的安全检测完全失效，用户本身难以发现和防范。

（3）开源组件投毒。XZ Utils 事件是典型的开源组件投毒攻击案例，攻击者历时两年持续向 XZ Utils 开源项目提交高质量补丁、建立社区信誉，取得核心维护者权限后在正式系统版本中植入后门代码，一旦扩散将对全球数百万台 Linux 服务器构成直接威胁。

（4）第三方运维通道劫持。2021 年的 Kaseya VSA 事件中，攻击者利用托管服务提供商远程管理平台中的零日漏洞，绕过认证机制直接向平台管控的约 1 500 家下游企业推送 REvil 勒索软件。运维通道因其高权限、广覆盖的特性，已成为工业供应链攻击中价值最高的中间跳板。

（5）工业协议漏洞利用。2010 年曝光的震网病毒攻击事件开创了通过供应链渗透实施物理破坏的先例[4]，其针对西门子工控系统的定向攻击首次将网络行动的后果从数据窃取延伸至工业设施的实体损毁，最终造成伊朗纳坦兹核设施约 1 000 台离心机损毁。

1.3　威胁态势趋势研判

工业供应链攻击的规模与烈度均呈现加速上升态势，从趋势特征来看，供应链攻击具有以下三个主要特点。一是攻击主体高级化，攻击者正从黑客组织、网络犯罪团伙向国家级高级长期威胁（Advanced Persistent Threat，APT）组织演进，对我国关键信息基础设施、重要信息系统、关键人员等进行攻击渗透。据统计，仅 2024 年境外国家级 APT 组织对我国重要单位的网络攻击事件就超过 600 起，其中国防军工领域是受攻击的首要目标[5]。二是攻击手法隐蔽化，暴力渗透与大规模漏洞扫描逐渐让位于长潜伏期隐蔽植入策略。2022 年公开披露的美国对我国的攻击案例中，均是潜伏多年的 APT 组织，如 APT-C-40 针对行业龙头企业开展长达十余年时间的攻击就是典型例证[6]。三是工业目标战略化，工业基础设施作为国家经济命脉与社会运转基础，其战略价值在大国博弈背景下日益凸显，针对关键基础设施的供应链攻击正从纯粹的经济犯罪动机向地缘政治博弈工具演变，这一趋势深刻改变了工业安全威胁的性质与应对逻辑。

2　工业互联网供应链安全技术挑战

2.1　供应链透明度严重不足

透明度缺失是工业互联网供应链安全的根本性困境，其成因根植于供应链的结构性特征。处于供应链末端的工业企业通常仅与一级供应商存在直接合同关系，对二级以下供应商的身份、资质与安全实践几乎一无所知。这种“可见性断崖”导致一旦供应链上游发生安全事件，下游用户往往无法及时判断自身是否受到波及，更无法快速定位受影响资产的范围。软件物料清单（Software Bill of Materials，SBOM）作为解决软件层透明度问题的核心工具，在工业场景中的落地面临多重现实阻力。在硬件溯源层面，物理不可克隆函数与防伪标签技术虽已在学界获得广泛验证，却在规模化工业部署中遭遇实用化瓶颈。

2.2　工业环境固有约束

工业设备的计算资源局限是制约安全能力部署的先天障碍。以 PLC 与 RTU 为代表的现场控制设备，其处理器主频往往在数十至数百 MHz 量级，可用内存通常不超过数 MB，这使得即便经过专门优化的轻量级密码算法在部分设备上也难以实现流畅运行，TLS 1.3 等现代安全通信协议的完整握手过程更是遥不可及。在此限制下，大量工业通信仍以明文形式传输，缺乏基本的身份认证与完整性保护。主机安全防护软件在工控设备上几乎无法部署，安全运营团队的检测能力只能依赖网络侧的被动旁路监听，而无法借助终端侧的深度感知手段。同时，受制于高昂的停产替换成本与复杂的工艺兼容性验证要求，“带病运行”成为许多工业企业不得不接受的现实[7]。

2.3 跨组织信任体系缺失

工业互联网场景中，设备制造商、系统集成商、工业互联网平台运营方、云服务提供商与第三方运维商等多类主体共同构成深度交织的信任网络，但各方之间的安全责任边界在合同层面普遍缺乏精确界定。当安全事件发生时，“谁的组件出了问题、谁负责应急响应、谁承担损失赔偿”的追责链条往往陷入多方推诿的僵局，根本原因在于责任划分条款从未在采购合同中被具体化。

2.4 威胁检测能力的先天局限

供应链攻击固有的长潜伏期与低噪声特征，从根本上瓦解了传统检测方法的有效性。基于已知攻击签名的规则引擎依赖对历史威胁模式的提前感知，而供应链攻击者刻意使用合法工具与合规操作掩护恶意行为，使得规则匹配几乎无从触发，比如以正常固件更新通道推送恶意载荷、以合法运维账号执行横向移动。基于统计基线的异常检测方法同样面临困境，工业控制过程本身具有高度的周期性与确定性，攻击者完全可以通过缓慢渐进的方式将恶意行为“融入”正常生产节律，规避阈值告警。

3 工业互联网供应链安全治理框架

3.1 框架设计原则

为应对工业互联网供应链日益严峻的安全威胁，需要突破以往补丁式安全措施的局限，建立图 2 所示的系统性、前瞻性安全治理框架。本文提出的框架以三项核心原则为基础，贯穿框架各层设计逻辑。

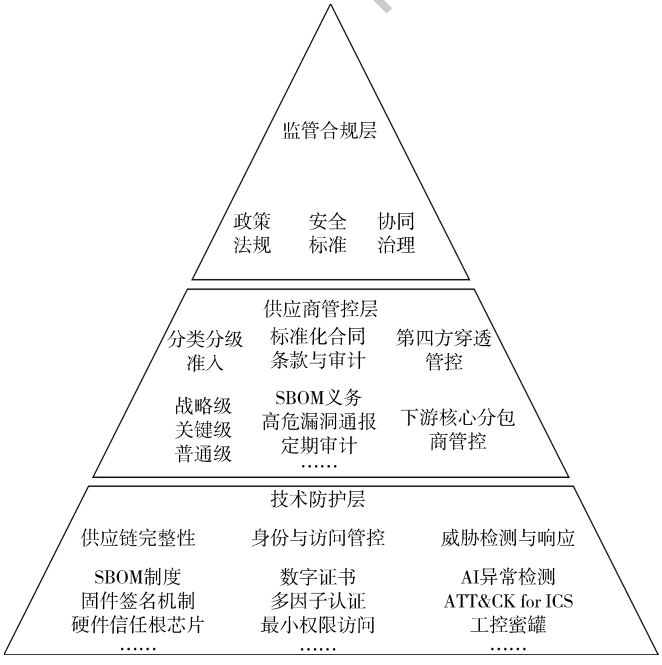

图 2　工业互联网供应链安全治理框架

一是零信任架构向供应链场景延伸。传统安全体系将通过外部审核的供应商视为可信主体，在网络接入、数据访问与操作权限方面给予隐式信任授权，这一假设在供应链攻击日趋复杂的背景下已根本失效。零信任架构的核心主张“绝不信任，始终验证”[8] 应扩展适用于每一次供应商交互，无论供应商的历史信用记录如何，每次远程访问、每批软件更新、每个第三方组件的引入，都须在当时的完整上下文条件下重新进行身份核验与权限评估，不得将过去可信等同于此刻授权。

二是安全左移覆盖全生命周期。将安全评估与管控前移至研发、采购、部署、运维、退役各阶段，分别通过威胁建模、供应商评估、完整性验证、持续监测与安全擦除等手段介入，从源头降低供应链引入风险，而非在系统运行后补救。

三是纵深防御各层独立设防。在软件、固件、硬件、网络、管理五个层面分别构筑独立的安全防线，各层防线相互独立、不共享失效路径。单一层面的安全突破不应自动导致全局失守，攻击者需突破多道独立防线方能实现攻击目的，以此大幅提升攻击成本与复杂度。

为使上述原则在供应商管控环节得到量化落地，本文在框架各层实施之前，先行构建供应链安全风险量化评估模型（见 3.2 节），以模型输出的综合风险指数作为供应商分级准入的客观依据，确保后续各层治理措施的差异化部署具有可计算的决策基础。

3.2 供应链安全风险量化评估模型

3.2.1 模型构建思路

供应商分级管控的有效性依赖于对供应商安全风险的客观量化。本文在三层治理框架基础上，构建了一套两级评估架构的供应链安全风险量化模型：第一级在各评估维度内部，依据细化子指标对维度得分进行加权求和；第二级基于各维度得分，通过加权聚合计算供应商综合风险指数（Supply Chain Security Risk Index，SCSRI），并依据阈值区间映射至分级管控级别。

模型选取威胁暴露度 P、脆弱性水平 V、资产重要性 C、管控成熟度 M 四个维度作为一级指标，在各维度下进一步设置 3~4 个可量化二级子指标，共计 14 项，以提升评估的精度与可重复性。四个维度从攻击侧（P、V）与防守侧（C、M）两个视角刻画供应商风险全貌：P、V 决定原始威胁量级，C 决定风险业务影响权重，M 作为管控折减项部分抵消前三者的

综合风险。

3.2.2 评估指标体系构建

各维度子指标设计遵循可量化、可重复采集、独立性强三项原则，具体如表 2 所示。所有子指标原始数据均须经归一化处理后再参与计算，确保不同量纲指标具有可比性。

表 2 供应链安全风险评估指标体系

维度	代码	子指标名称	量化依据	组内权重
威胁暴露度 P	$P1$	行业 APT 活跃指数	威胁情报平台近 2 年活跃度数据，归一化至［0，1］	0.5
	$P2$	历史安全事件频率	近 3 年安全事件数量/同类供应商均值，归一化	0.3
	$P3$	地缘政治风险因子	供应商注册地国家/地区安全风险评级映射	0.2
脆弱性水平 V	$V1$	高危 CVE 未修复率	当前未修复高危 CVE 数/历史披露高危 CVE 总数	0.35
	$V2$	开源组件依赖深度	直接+间接依赖层数归一化，层数越深得分越高	0.3
	$V3$	第三方接入通道数	具有访问权限的外部接口数量，归一化	0.2
	$V4$	代码审计覆盖率（反向）	1~近 12 月代码审计覆盖率，覆盖率越低得分越高	0.15
资产重要性 C	$C1$	业务关键性	停用对核心业务影响等级，专家 5 分制打分后归一化	0.5
	$C2$	单一来源依赖度	可替代供应商数量反向归一化，唯一来源得分最高	0.3
	$C3$	数据敏感等级	供应组件涉及数据的敏感性分级（公开/内部/机密）评分	0.2
管控成熟度 M	$M1$	安全认证等级	持有认证级别（ISO 27001/CMMC 等）映射评分，归一化	0.35
	$M2$	SBOM 提供完整度	SBOM 覆盖率及 CycloneDX/SPDX 规范符合度评分	0.3
	$M3$	安全响应时效	历次高危漏洞修复平均响应时间，反向归一化	0.2
	$M4$	历史审计得分	近 3 年安全审计平均得分归一化	0.15

3.2.3 指标权重确定

采用 1-9 标度法[9]，邀请行业专家、供应链专家、安全专家等成立专家组，对各层级指标进行两两比较，构造判断矩阵。为验证判断矩阵合理性，需进行一致性检验，计算一致性指标 $CI=(\lambda_{max}-n)/(n-1)$，其中 n 为矩阵阶数。查表得平均随机一致性指标 RI，计算一致性比率 $CR=CI/RI$。当 $CR<0.1$ 时，认为判断矩阵具有满意的一致性；否则需调整判断矩阵。最后，计算权重采用层次分析法中广泛应用的特征根方法，对于判断矩阵 $\boldsymbol{A}$，计算最大特征根 λ_{max} 的特征向量 $\boldsymbol{w}$，经归一化处理后可以得到各维度的相对权重。

下面是权重计算过程示例，假设经专家打分汇总后构造判断矩阵如表 3 所示。

表 3 一级维度判断矩阵

	威胁暴露度 P	脆弱性水平 V	资产重要性 C
威胁暴露度 P	1	1/2	1/4
脆弱性水平 V	2	1	1/2
资产重要性 C	4	2	1

计算最大特征根 $\lambda_{max}=3$，$CI=0$，$CR=0<0.1$，说明判断矩阵符合一致性验证要求。λ_{max} 对应的特征向量 $\boldsymbol{w}=(1,2,4)^{T}$，求和归一化得到 P、V、C 的权重分别为 $\boldsymbol{w}_P=1/7$，$\boldsymbol{w}_V=2/7$，$\boldsymbol{w}_C=4/7$。

3.2.4 综合风险指数计算

基于各维度得分，采用加权线性组合与管控折减相结合的方式计算 SCSRI，理论取值范围为[0,1]，具体计算步骤如下：

（1）维度得分计算。对第 k 个维度（$k\in\{P,V,C,M\}$），其得分 D_k 由该维度下 n_k 个子指标加权合成：

$$D_k=\sum_{j=1}^{n_k} w_{kj}\cdot x_{kj} \tag{1}$$

其中，w_{kj} 为第 k 维度下第 j 个子指标的组内权重（满足 $\sum w_{kj}=1$），$x_{kj}\in[0,1]$ 为该子指标归一化得分，n_k 为第 k 维度的子指标数目（$n_P=3$，$n_V=4$，$n_C=3$，$n_M=4$）。子指标的组内权重在各维度内部由专家打分法独立确定，各维度组内权重之和均为 1，具体取值见表 2。

（2）SCSRI 计算。将威胁暴露度、脆弱性水平与资产重要性三个维度得分按一级权重加权聚合，再通过管控成熟度维度引入折减项，得到综合风险指数：

$$SCSRI=(\boldsymbol{w}_P\cdot D_P+\boldsymbol{w}_V\cdot D_V+\boldsymbol{w}_C\cdot D_C)\cdot(1-\beta\cdot D_M) \tag{2}$$

其中 $\boldsymbol{w}_P=1/7$、$\boldsymbol{w}_V=2/7$、$\boldsymbol{w}_C=4/7$ 为三个风险维度的一级权重（由层次分析法确定，满足 $\boldsymbol{w}_P+\boldsymbol{w}_V+\boldsymbol{w}_C=1$），$\beta$ 为管控折减弹性系数（取值范围为［0.6，0.8］，默认取 0.7），D_M 为管控成熟度维度得分。

3.3 技术防护层

技术防护层是本文框架的执行基础，包括供应链完整性保障、身份与访问管控、威胁检测与响应三个部分。

（1）供应链完整性保障。软件层面，推行工业软件 SBOM 制度，要求设备制造商与平台服务商提供涵盖所有直接与间接依赖组件的可机器读取清单，并与 CVE 漏洞数据库实现自动关联，实现组件级的漏洞可见性。固件层面，推行固件代码签名机制与启动可信技术链，确保固件分发与安装的完整性可验证，阻断固件层面的持久化植入。硬件层面，在关键控制设备中嵌入硬件信任根芯片，为密钥存储与完整性度量提供不可绕过的可信执行环境。

（2）身份与访问管控。采用短期数字证书与多因子认证相结合的身份验证机制，按实际维护任务动态授予最小权限集合，禁止跨工艺段横向访问，对所有远程操作行为进行全程录制与实时审计。建立工业设备数字证书统一管理平台，覆盖证书签发、续期与吊销全流程。在 OT 网络内部通过微隔离划定安全域边界，防止攻击者在工控网络内部横向移动。

（3）威胁检测与响应。基于适配工业控制场景的 AI 异常检测模型[10]，利用工业控制过程固有的周期性与确定性特征构建精细化行为基线，识别掺杂在正常生产节律中的低噪声异常控制指令与通信模式。建立基于 MITRE ATT&CK for ICS 框架[11] 的知识图谱，将供应链攻击的已知攻击链与 MITRE 战术分类进行结构化映射，支持安全事件的关联分析与溯源推演。在工控网络中布设高仿真度工控蜜罐，诱捕并记录攻击者在侦察与横向移动阶段的行为轨迹，为威胁情报积累和攻击归因分析提供数据来源。

3.4 供应商安全管控层

供应商安全管控层聚焦于外部信任关系的规范化治理，通过准入分级、合同约束与穿透管控三个机制共同构筑供应商侧的安全屏障。

（1）供应商分级分类准入评估。将供应商从高到低划分为战略级、关键级与普通级三档。战略级需接受年度现场安全审计与持续监控，关键级需提供经认可机构颁发的第三方安全认证及年度安全评估报告，普通级适用标准化安全问卷评估与合同约束机制。供应商分级采用“硬性约束优先、SCSRI 兜底”的双层判定逻辑，以克服单一量化指数在极端情形下的局限性。第一层为硬性约束条件，凡触发以下任一条件，无论 SCSRI 得分如何，均直接锁定或上调分级：①单一来源依赖度为 1（当前无可替代供应商）的直接列为战略级；②近两年内发生过数据泄露、勒索软件攻击等重大安全事件的，在 SCSRI 计算结果基础上自动上调一级；③供应商注册地或主要运营地属于高地缘政治风险地区的，须启动人工复核并由安全委员会确认最终分级。第二层为 SCSRI 量化分级，在不触发任何硬性约束的情形下，依据 3.2 节模型输出的 SCSRI 综合风险指数按表 4 阈值划定档位。两层判定结合，既保留了量化模型的客观性与可重复性，又通过硬性规则覆盖了纯指数评估难以捕捉的战略风险与极端情形。分级结果与供应商采购优先级、合同续签决策直接挂钩，形成安全表现影响商业关系的正向激励机制。

表 4　SCSRI 风险阈值与供应商分级对应关系

SCSRI 区间	供应商分级	对应管控要求
（0.7，1]	战略级	年度现场审计与持续监控
（0.4，0.7]	关键级	第三方安全认证及年度评估报告
[0，0.4]	普通级	标准化安全问卷评估及合同约束

（2）供应链安全合同条款标准化。将供应链安全要求系统性纳入采购合同标准条款体系，核心条款涵盖 SBOM 完整提供义务及格式规范、高危漏洞分级通报时限、安全事件应急响应机制、定期安全审计义务、供应商合同变更触发条款等内容。合同中须明确约定安全责任的违约赔偿标准，避免安全责任在追责阶段陷入多方推诿。

（3）第四方风险穿透式管控。在合同层面要求一级供应商对其下游核心分包商适用等同的安全管控要求，并赋予甲方对穿透审计权利。建立第四方风险动态台账，定期识别高风险第四方并要求一级供应商提供替代方案或风险缓释措施，防止单点第四方风险通过供应链传导引发系统性危机。

3.5 监管合规层

监管合规层为整体治理框架提供外部约束力，从政策法规、标准体系与协同治理机制三个方面形成从底线要求到最佳实践的完整规范链条，为框架提供外部约束力。

政策法规方面，国内层面，2026 年出台的《国务院关于产业链供应链安全的规定》为供应链安全治理提供立法保障；网络安全等级保护 2.0 标准对工业控制系统提出了专项安全扩展要求，覆盖工控网络安全防护、工业主机加固与安全审计等方面；工业和信息化部发布的《工业互联网安全分类分级管理办法》依据平台规模、行业重要性与用户规模，将企业划分为三级，分级明确供应链安全主体责任。国际层面，NIST SP 800-

161r1[12]专门针对 ICT 供应链风险管理提出了覆盖识别、评估、响应与监控的全生命周期管控框架，是目前最系统的供应链安全管理指南；IEC 62443 系列标准从产品、系统与运营三个维度构建了工业自动化控制系统的安全生命周期框架，已成为国际通行标准。

标准体系方面，我国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[13]，其中 GB/T 44462. 2—2024《工业互联网企业网络安全 第 2 部分：平台企业防护要求》、GB/T 44462. 4—2026《工业互联网企业网络安全 第 4 部分：数据防护要求》等标准对供应链安全管理有部分要求。目前，我国正在构建涵盖 ICT 供应链安全、供应链安全管理体系、关键信息基础设施安全保护、软件供应链安全等多层次的标准框架，逐步向数字化、网络化、智能化延伸，旨在应对国际经贸环境不确定性，提升供应链韧性与安全水平。

协同治理方面，构建政府、行业、企业三级联动机制。政府以法规与强制标准划定安全底线并建立跨部门联动响应机制；行业依托联盟组织，以龙头企业为牵引推广安全评估最佳实践与威胁情报共享；企业将供应链安全纳入网络安全战略与采购决策核心流程，推动安全能力向供应商侧延伸，形成覆盖整体供应生态的安全共同体。

4 结论

本文围绕工业互联网供应链安全这一核心议题，从威胁态势、技术挑战、风险评估与治理框架四个维度展开系统性研究。所构建的供应链安全风险量化评估模型（SCSRI）为供应商分级管控提供了可计算的决策依据，在此基础上提出的“技术防护—供应商管控—监管合规”三位一体框架，以零信任架构延伸和安全左移理念为核心设计原则，在供应链全生命周期各环节分别构筑独立防线。安全治理框架的主要价值在于将分散的安全措施纳入统一的体系化逻辑，为工业互联网平台运营主体、设备制造商及行业监管机构提供可落地的参考路径。

参考文献

[1] 中国工业互联网研究院. 工业互联网基础[M]. 北京：人民邮电出版社，2025.

[2] 樊佩茹，李俊，王冲华，等. 工业互联网供应链安全发展路径研究[J]. 中国工程科学，2021，23(2)：56-64.

[3] 张晓玉，陈河. 从 SolarWinds 事件看软件供应链攻击的特点及影响[J]. 网信军民融合，2021(4)：37-40.

[4] 李东. 震网病毒事件浅析及工控安全防护能力提升启示[J]. 网络安全技术与应用，2019(1)：9-10，24.

[5] 国家互联网应急中心. 美情报机构频繁对我国防军工领域实施网络攻击窃密[EB/OL]. (2025-08-01) [2026-04-15]. https://www. cert. org. cn/publish/main/8/2025/20250801150853298552601/20250801150853298552601_. html.

[6] 桂畅旋. 全球高级持续性威胁总体态势、典型手法及趋势研判[J]. 中国信息安全，2023(6)：85-90.

[7] 张晓菲，卢春景，于盟. 工业互联网供应链安全风险研究[J]. 网络空间安全，2020，11(7)：23-27.

[8] 王航宇，吕飞，程裕亮，等. 工业物联网零信任安全研究综述[J]. 计算机研究与发展，2025，62(11)：2784-2805.

[9] 刘清华. 基于层次分析法的制造业企业财务风险评价研究[J]. 现代商业，2026(4)：173-176.

[10] 张婷. 基于人工智能的物联网边缘设备异常检测方法研究[J]. 网络安全和信息化，2025(11)：55-57.

[11] MITRE. ATT&CK matrix for ICS[EB/OL]. (2022-05-05) [2026-04-15]. https://attack. mitre. org/matrices/ics/.

[12] National Institute of Standards and Technology. Cybersecurity supply chain risk management practices for systems and organizations [EB/OL]. (2022-05-05) [2026-04-15]. https://csrc. nist. gov/pubs/sp/800/161/r1/final.

[13] 王秋华，吴国华，魏东晓，等. 工业互联网安全产业发展态势及路径研究[J]. 中国工程科学，2021，23(2)：46-55.

（收稿日期：2026-05-06）

作者简介：

李正文（1988-），男，博士，工程师，主要研究方向：工业互联网、工控安全、云安全。

董良遇（1989-），通信作者，女，硕士，高级工程师，主要研究方向：网络安全、工控安全、工业互联网安全。E-mail：dongliangyu78@ 163. com。

版权声明

凡《网络安全与数据治理》录用的文章，如作者没有关于汇编权、翻译权、印刷权及电子版的复制权、信息网络传播权与发行权等版权的特殊声明，即视该文章署名作者同意将该文章的汇编权、翻译权、印刷权及电子版的复制权、信息网络传播权与发行权授予本刊，本刊有权授权本刊合作数据库、合作媒体等合作伙伴使用。同时，本刊支付稿酬已包含上述使用的费用，特此声明。

《网络安全与数据治理》编辑部