国外数字化工厂网络安全保障机制研究*

——以洛克希德·马丁公司为例

杜洪涛，李云志
（国家工业信息安全发展研究中心，北京　100040）

摘　要：数字化工厂是融合新一代信息技术和先进制造技术的关键工业设施，也是推进我国制造业数字化转型、增强国家科技和经济竞争力的重要载体。由于数字化工厂的网络化、智能化和开放性等特点，传统的网络集成式安全架构难以适应更复杂的业务流、供应链和不断变化的业态模式，成为制造业数字化转型的重大挑战。如何保障其安全稳定运行，成为各国政府和工业界关注的焦点。以洛克希德·马丁公司数字化工厂建设为例，研究该企业数字化转型战略、工厂数字化架构，并分析其工业物联网设备的连接通信框架（智能工厂框架），以及在云平台、无线物联网、网络安全治理、研发运营等多方面的安全措施。在此基础上，对我国如何强化重点行业数字化工厂网络安全保障机制建设，提出多角度的综合性建议。

关键词：数字化工厂；网络安全架构；智能工厂框架；数字化转型；安全治理
中图分类号：TP393；C931　　**文献标识码：**A　　**DOI：**10.19358/j.issn.2097-1788.2024.05.002

引用格式：杜洪涛，李云志. 国外数字化工厂网络安全保障机制研究[J]. 网络安全与数据治理，2024，43(5)：11-17.

Research on the cyber security protection mechanism of digital factories abroad

——taking Lockheed Martin as an example

Du Hongtao, Li Yunzhi
(China Industrial Control Systems Cyber Emergency Response Team, Beijing 100040, China)

Abstract: A digital factory is a key industrial facility that integrates new generation information technology and advanced manufacturing technology. It is also an important carrier for promoting the digital transformation of China's manufacturing industry and enhancing the country's technological and economic competitiveness. At the same time, due to the characteristics of networking, intelligence, and openness of digital factories, traditional network integrated security architecture is difficult to adapt to more complex business flows, supply chains, and constantly changing business models, becoming a major challenge for the digital transformation of the manufacturing industry. How to ensure its secure and stable operation has become a focus of concern for governments and industries around the world. Takes the construction of Lockheed Martin digital factory as an example to study its digital transformation strategy, factory digital architecture, and analyze its industrial Internet of Things equipment connection communication framework (intelligent factory framework), as well as security measures in cloud platforms, wireless Internet of Things, network security governance, research and development operations, and other aspects. On this basis, comprehensive suggestions from multiple perspectives are proposed on how to strengthen the construction of network security protection mechanisms for digital factories in key industries in China.

Key words: digital factory; cyber security architecture; intelligent factory framework; digital transformation; security governance

*基金项目：国家自然科学基金专项项目（T2241023）；教育部哲学社会科学研究重大课题攻关项目（23JZD016）

0 引言

数字化工厂是将物联网、大数据、人工智能、5G 通信等信息技术，深度融合先进制造、精益制造和先进管理技术的新型关键工业设施，也是世界各国推进制造业数字化转型、增强制造业实力和科技竞争力的重要举措。由于数字化工厂具有高度数字化、网络化、智能化等特点[1]，其面临的网络安全数据安全风险大幅增加，特别在航空、航天、船舶、电子、能源等重点领域，更容易成为有组织网络攻击的对象。近些年安全事件频发，如德国钢铁生产商 ThyssenKrupp 遭黑客攻击（2016 年）、挪威铝业公司遭勒索软件攻击（2019 年）、日本丰田汽车供应商遭网络攻击（2022 年）等事件，导致企业核心技术数据被窃、生产线大面积停工等严重后果。同时，在涉密等级较高的重点领域数字化工厂建设过程中，还面临着信息化开放性和安全防护的结构性矛盾问题[2-3]，传统的网络集成式安全架构难以适应更复杂的业务流、供应链和不断变化的业态模式，成为制造业数字化转型的重大挑战。

数字化转型为制造业高质量发展注入了新动能，但随着数字化工厂建设的不断深入，面临的网络安全风险问题日益突出。主要包括以下几个方面：生产过程直接遭受网络攻击破坏；企业工业软件系统部署于云平台导致攻击面扩大问题；供应链的全球化延伸带来供应链安全问题；数据分析与“脏数据”注入导致更多数据安全问题；人工智能存在误导决策风险等。因此，如何保障数字化工厂等工业设施安全稳定运行，成为各国政府和工业界普遍关注的焦点。

我国制造业门类齐全，为经济社会发展提供了有力支撑，但创新能力与部分发达国家相比仍有差距，保证高端装备制造领域的网络安全显得尤为重要。本研究以洛克希德·马丁公司（Lockheed Martin Space Systems Company，以下称 LMT 公司）为例，梳理美国企业数字化转型战略下的数字化工厂建设现状和成效，以及数字化工厂架构和工业连接框架，分析其数字化工厂网络在相关安全域的保障措施，并结合我国实际和制造业数字化转型战略需求，致力于建立健全我国数字化工厂的网络安全保障机制。

1 数字化转型战略牵引的数字化工厂建设

1.1 数字化转型战略实施

作为国际知名的科技型防务装备企业集团，LMT 公司在数字化转型方面同样走在行业前列。近年来，基于自身在先进设计与制造领域的雄厚实力，其与 Microsoft、Amazon、NVIDIA、SAP、Siemens 等信息技术服务商合作，在数字工程、先进生产、下一代软件、数字化赋能、数据作为战略资产五个方面进行业务数字化转型，重点推进任务驱动的数字化转型战略。该企业先后提出“打造闭环的数字线索”“数字织锦”“产品数字集”等概念，构建从产品设计到生产及维护的全生命周期数字线索，实施虚拟化制造、组装、检查和测试，以满足客户服务所需的反应速度、敏捷性和洞察力，在外部环境变化的情况下保持领先地位。同时，企业将数据视为重要资产，以数据驱动人工智能在产品研发和企业经营的赋能作用。数据安全也成为其数据治理项目中的核心任务，现阶段正在构建全球基础设施，以实时、安全地共享数据。

目前，该企业数字化技术应用已在新一代战机、Raider-X 直升机等先进防务装备项目中发挥重要作用，甚至将先进计算、数字孪生和人工智能技术成功用于森林防火等民用领域，并已在多个业务板块应用了人工智能驱动的预测分析。

1.2 数字化工厂建设

建设数字化工厂是 LMT 公司战略转型的重要体现，在 2021 至 2022 两年间投资建成了四座数字化“未来工厂”[4]，具体如下：

（1）佛罗里达州 STAR 中心。作为 NASA“猎户座”飞船的尖端生产中心，其融合的智能制造技术包括基于智能工厂框架的连接、自动化 Web 应用、数字化车间管理、集成协作、远程支持、沉浸式技术等。

（2）加州棕榈谷“臭鼬工厂”智能车间（代号 648 号建筑）。该车间可以同时批量生产航空及防御等多个产品项目，其融合的智能制造技术包括基于智能工厂框架的连接、柔性工厂空间和工具、敏捷和移动机器人、集成数字化计量等。

（3）阿拉巴马州联合空对地防区外导弹（JASSM）工厂。该工厂融合的智能制造技术包括基于智能工厂框架的连接、工厂仿真、增强现实、先进机器人、集成数字计量、机器人喷涂等。

（4）阿拉巴马州高超声速导弹工厂。该工厂融合的智能制造技术包括机器人涂层、增强现实、柔性工厂空间、电子模板、智能扭矩工具等。

除了上述工厂，LMT 公司的其他工厂也在逐步进行数字化转型，比如得克萨斯州沃斯堡的 F-35“闪电”II 工厂、康涅狄格州的先进复合材料中心。基于工业物联网（Industrial IOT）技术，LMT 公司推出自己的智能工厂框架（Intelligent Factory Framework，IFF），目前这些工厂均已将设备接入 IFF。

1.3 工厂的数字化架构

LMT 公司将数字化融入产品设计到物流保障各个环节，搭建云计算平台、物联网、边缘计算立体信息化设

施，集成 ERP、MES、MRO、PDM、PLM 等各类业务系统，在 DevOps 敏捷开发模式基础上推动实施 DevSecOps 安全敏捷开发模式，将安全无缝集成到开发周期中，总体的工厂数字化架构如图 1 所示。

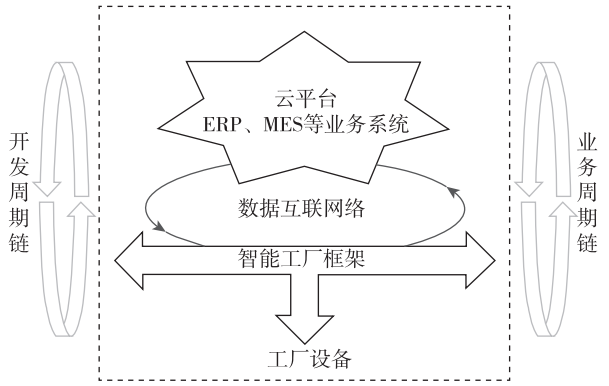

图 1　工厂数字化基本架构示意图

如图 1 所示，高安全等级的云平台主要用于部署各类业务软件系统和协同开发系统等，智能工厂网络用于安全连接工厂内各类设备数据，二者通过 PLM 等数据互联工具实现数据资源协同共享。该数字化架构可支撑基于 DevSecOps 模式的各开发环节，以及产品从设计、生产到物流、售后的全生命周期。此外，该分层集成方式的架构与 ANSI/ISA-95 及 IEC/ISO 62264[5] 等国际标准相一致，实现了从生产现场设备、生产线数据采集与控制、生产（车间）管理到企业管理的纵向贯通。

总体看，LMT 公司通过数字化工厂的建设或改造，实施智能工厂框架、技术驱动的先进制造环境、灵活的工厂架构，以加快对尖端产品的开发和交付，并且已经开始获得经济效益。ARC Advisory Group 在 2022 年发布的《工业数字化转型 25 强》报告中公布了实施数字化转型的全球领先企业，LMT 公司位列其中[6]。

2　基于工业物联网连接的智能工厂框架

智能工厂框架（IFF）是 LMT 公司最新提出的概念，是以数字优先为原则的基于工业物联网的解决方案，以数字方式连接生产设施，通过更贴近现场的边缘计算系统[7] 来进行高效的数据分析，实现对工况、状态和优化情况的深刻洞察及实时的响应能力。LMT 公司智能工厂策略要求厂内机器设备接入到该架构，目前已超过 7 个工厂部署了 IFF，并正在向全公司扩展。

（1）IFF 是全新的、安全的和基于标准的边缘计算网络平台。该平台基于应用程序编程接口（API）、机器学习和软件定义网络等技术，接入框架中的机器会自动实时报告其性能数据和状态，可以自动预测维护需求、分析生产性能和监控质量。

（2）IFF 的核心是安全性和标准化。安全性方面，IFF 符合美国国防部《网络安全成熟度模型认证（CMMC）》2.0 版的网络安全要求，等同采用美国国家标准与技术研究院（NIST）特别出版物（SP）800－171 和 800－172 安全条款为主。其中，NIST SP 800－171《保护非联邦系统和机构的受控非密信息》针对关键过程或高价值资产提出了系统和通信保护、系统和信息完整性、风险评估、人员安全、意识和培训、事件响应能力六个安全控制类别的增强要求[8]，以重点保护“受控非密信息（以高价值的企业业务信息为主）”的保密性、完整性、可用性。

标准化方面，IFF 采用通用数据标准，数据格式无需进行转换即可共享和分析，实现了高度自动化。比如，工厂的电子产品生产设备是通过国际电子工业联接协会 IPC－2591 Connected Factory Exchange（CFX）工业数据交换标准，连接到公司的 Factory Logix 制造执行系统平台，交换标准主要包括传输通道、编码、定义、关键参数、消息封装、操作信息和端点配置[9]，并采用 IPC－2581《印制板组装产品制造描述数据和传输方法的通用要求》标准作为数据设计参考，消除了对其他格式数据的需要，避免了与第三方中间件相关的风险和成本，实现数据驱动的智能制造目标。其中，CFX 架构是开放的数据互联总线架构（如图 2 所示），可以实现机器与机器之间（M2M）、机器到 IT/OT 网络的数据交换。

3　数字化工厂的网络安全措施

在规划和建设数字化工厂网络安全保障体系时，LMT 公司遵循物理空间和治理空间相结合、技术和管理深度融合的原则，实施全方位的综合性网络安全保障措施。其中，物理空间包括富集业务功能的云平台安全措施和无线物联网通信安全措施，治理空间包括网络安全治理体制机制和面向研发及运营服务等业务层面的内嵌式安全措施。

3.1　云平台安全方面

LMT 公司使用 Amazon Web Services（AWS）、Microsoft Azure 的特别云托管服务，逐步将业务系统迁移至云平台。将最新的 SAP S/4HANA ERP 系统迁移到 AWS Gov Cloud（这是一个隔离的 AWS 区域，用于托管敏感数据和受监管工作负载），基于内存服务器对数据库工作负载进行了优化，配置 SAP 沙盒环境，实现开发敏捷性，并确保数据安全，满足《国际防务装备贸易条例（ITAR）》等安全监管要求。

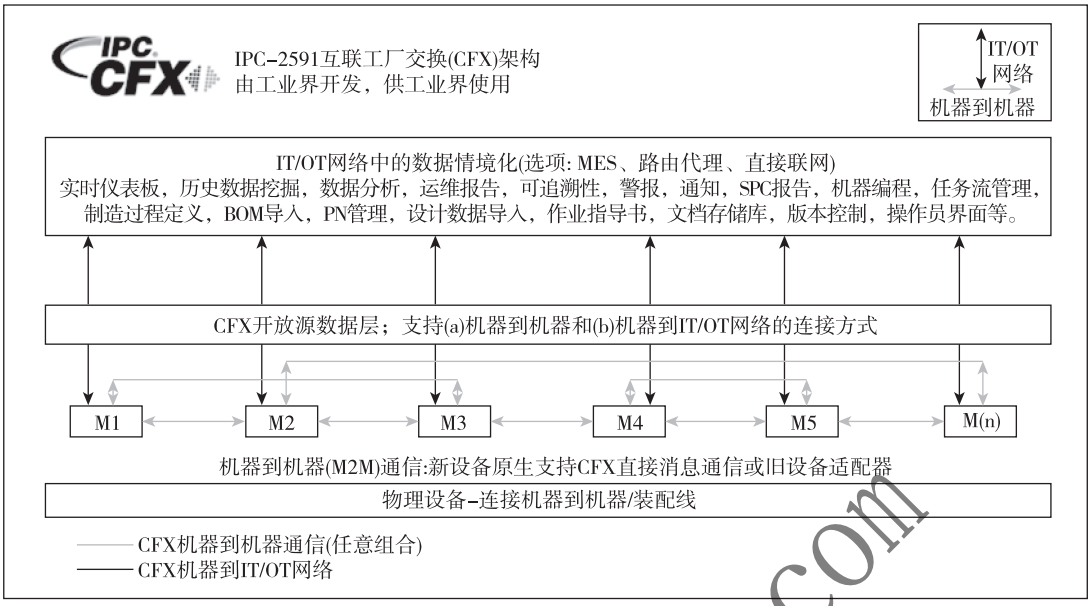

图 2　IPC 2591 互联工厂交换（CFX）架构

［资料来源：IPC-2591-Version 1. 2 Connected Factory Exchange（CFX）］

2022 年，该公司成为 Microsoft 机密云（Microsoft Azure Government Secret）中独立运营的非政府实体，实现将机密数据安全地进入云端，并将公司先进的 5G. MIL® 技术、关键数据处理和分析以及沉浸式体验带到边缘，以支持随时随地作出决策。需要说明的是，Microsoft 提供的大规模多租户云平台，根据用户和区域不同，所提供的服务安全等级也不同，以 Office 365 环境为例，可提供商业公共云服务、一般政府社区云（GCC）服务、符合国防部安全要求准则级别 4 控件进行设计的 GCC High 云服务、符合国防部安全要求准则级别 5 控件并专门服务于国防部的 DoD 云服务。

采用平台化、集散式服务的系统架构，除了有助于业务打通和灵活服务，还有助于达到稳定、有层次的安全防护效果。目前，基于 LMT 公司数字化转型部门开发的 LMX ERP A2R（Acquire to Retire Value Stream）架构、1LMX ECT 弹性云技术，集成 ERP、MES、PLM、MRO 等业务系统，实现全寿命周期的流程、架构、数据模型融合应用。同时，集成网络安全和云安全技术，可以为机密的业务线提供自动化、可持续和一致的网络产品和服务，比如 ADP（高级开发计划），网络安全人员与运营机密网络安全组织和行业机密信息技术组织合作，识别、构建、保护和实施云基础设施和安全工具，实现基础设施即代码（IaC）的治理和风险管理。

3.2　无线物联网通信安全方面

物联网设备是数字化工厂建设首要考虑的安全要点，许多设备存在严重的信息安全隐患[10]。IFF 依据 NIST SP 800 – 171 和美国国防部 CMMC2. 0 的要求，定义安全流程、管理和工具，保障物联网和通信数据安全。CMMC2. 0 包括 14 个关键安全域和 110 个控制项目，其中关键安全域包括：访问控制（AC）、意识与培训（AT）、审计与责任（AU）、配置管理（CM）、识别和认证（IA）、事件响应（IR）、维护保养（MA）、媒体保护（MP）、人员安全（PS）、物理保护（PE）、风险评估（RA）、安全评估（CA）、系统和通信保护（SC）、系统和信息完整性（SI）[11]。

此外，IFF 采用的 IPC CFX 标准的独特性质，单一的制造数据协议，机器内置的通用语言，具有“即插即用”能力。IPC-2591 CFX 通信组件采用合格产品清单（QPL）制度，只有通过独立第三方认证的设备，才能列入 IPC-CFX-2591 合格产品清单，在使用 IPC CFX 时获得信任。IPC 也在不断地更新和升级 IPC-CFX 标准，定期发布 IPC – CFX SDK 新版本以支持行业发展，确保标准保持适用和更加通用，从而有效避免与第三方中间件相关的风险和成本。

在涉密项目数量占比高达 95% 的“臭鼬工厂”中，其数字化智能工厂设施内依然开通了 Wi-Fi 协议无线通信，以便数据可以更容易、更灵活地发送到车间和工厂内的其他地方，而不需要物理线缆连接。比如，移动机器人可快速地在整个工厂内从一个项目无缝移动到另一个项目，工厂设施可通过无线不断重新配置。

3.3 网络安全治理方面

首先，执行联邦政府、客户和贸易组织的法规或指令，确保业务和信息系统的合规性。法规与指令主要包括国防部信息系统局安全技术实施指南（DISA STIG）、联合特殊访问计划实施指南（JSIG）、国家工业安全计划操作手册（NISPOM，也称为 DoD 5220.22-M）、DoD 8570 系列信息保障指令，中央情报局关于保护信息系统中敏感分区信息的局长指令（DCID 6/3）、美国国家标准与技术研究所的风险管理框架（RMF）、NIST SP 800 信息安全系列标准等，增强实时安全风险防范和网络漏洞修补功能。

在安全治理团队方面，企业内部设置网络安全经理、信息系统安全官（ISSO）、信息系统安全经理（ISSM）、风险管理框架分析师、信息保障工程师等多层级安全保障岗位，依据 DoD 8570 指令（国防部信息安全保障人力资源提高计划），必须获得相应的信息安全专业资格认证，包括信息保障技术员（IAT）、信息保障管理员（IAM）、信息保障系统架构师（IASAE）和计算机网络防护员（CND-SP）[12]。

关键技术、运维和管理岗位人员，需获得政府安全许可才能上岗工作。数字化生产设备和物联网设备的使用维护人员上岗前需要得到政府机密级安全许可，比如 PLC（可编程逻辑控制器）、NC（数控）、CNC（计算机数控）、DNC（直接/数字数控）机器、机器人或其他设备的维护人员。

3.4 研发及运营服务方面

基于业务云平台，采用 DevSecOps 模式，将专用工具、第三方工具、开源工具和人工测试等信息安全措施集成到产品全生命周期中。强调从软件构建伊始就注重安全性，并将安全检查部署至 CI/CD（持续集成/持续交付）流水线的每个自动化测试步骤中。以 N-MRO 服务方案为例，从功能上集成了 COTS 物流软件、信息系统和三维数字孪生模型平台、具有 AI/ML 功能的预测性维护功能的嵌入式数据分析，使用 DevSecOps 部署的数据交换服务，支持软件部署和自动安全扫描，以获得持续的 ATO/网络安全认证。

LMT 公司的软件工厂普遍使用典型的 DevSecOps 模式，在软件开发的每一个步骤中嵌入 DevSecOps，以确保在开发的每一步都考虑到最佳的网络安全实践，可以根据快速变化的任务需求，为客户提供定制软件解决方案，并经常更新这些解决方案[13]，如图 3 所示。

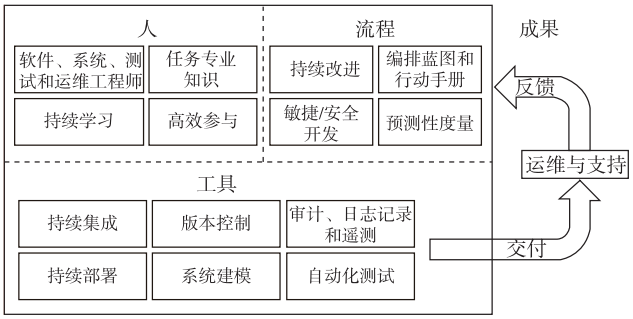

图 3 LMT 软件工厂 DevSecOps 模式

（资料来源：LMT 公司网站）

4 对我国的启示与建议

4.1 数字化转型是制造业的重要发展趋势

LMT 公司作为世界著名的高科技工业巨头，其业务信息保密要求极为苛刻，同时面对不断变化的国际形势和市场需求，实施任务驱动战略，全方位地加快数字化转型，以实现业务数字化、智能化，覆盖产品服务的全生命周期，以及工厂的各个业务部门。成立了专门的 RMS 数字化转型部门，组建了人工智能、数据科学、软件工程等专业团队，与国内外诸多 ICT 服务商合作，提升了智能制造、网络、创新等多方面能力。

我国亟需加快制造业数字化转型步伐，在保守国家秘密和企业秘密同时，积极挖掘数据要素驱动能力，探索信息共享办法，借助新一代信息技术，提升在产品研发、流程优化、生产运行、供应链保障等方面的能力，夯实重点领域的网络安全态势。

4.2 重视数字化转型带来的新型网络安全风险

在“数据－信息－知识－智能”的智能制造赋能层级递进模式下，也可能带来从产品设计到交付全周期的网络安全风险[14]。基于人工智能的深度合成技术可能生成和传播虚假信息，被违法犯罪活动利用，甚至危及国家安全和社会稳定[15]。数字化转型需要基于合规性约束、功能可用性、业务效率、业务质量等多重目标建立价值准则，在此基础上形成动态、持续的风险识别机制。目前，国际上比较主流的 NIST 网络安全体系框架（NIST CSF 模型）在 2024 年初最新发布的升级版本中，特别强调通过治理形成识别与应对当前和未来风险的文化[16]。治理是安全体系的核心，包括组织、制度、规划、决策和资源配置等，可以将网络安全融入更全面的企业风险管理中，以此为基础形成风险识别、安全保护、审计检测、事件响应、状态恢复等一系列持续改进的安全管理能力。

我国正在推进新型工业化、打造新质生产力，数字化工厂系统架构将逐步由传统封闭集成模式转向基于工业互联网平台的开放式服务模式，业务和价值链条也由车间生产向企业运营、产业协同延伸，数据要素驱动和人工智能赋能将成为新型工业化的重点，云安全、数据

安全、人工智能应用安全等新生安全问题如影随形。因此，需要同步建设符合我国国情的工业网络安全治理体系，形成统领全局的安全制造解决方案，指导企业根据组织的任务目标和期望来配置安全资源。

4.3 多层级网络安全保障是制造业数字化转型的基础

LMT 公司的信息系统是吸引网络入侵和攻击的热点对象，2022 年 8 月，受俄乌战争影响，该公司网站受到“Killnet”黑客组织大规模攻击，但并未有证据显示攻击产生实质性破坏效果。该公司至今没有遭受重大信息安全事故，除保障自身数字化转型创新和业务的稳定发展，还利用在通信、电磁、网络方面的技术优势，成为国际重要网络安全服务商。主要得益于其对网络安全多重防护和系统性安全治理的重视，得益于其对合规性的遵守、与服务商共建信息安全设施、实施 DevSecOps 模式、设备认证接入和多级安全人才资源配置的整体性安全风险管理框架。

我国重点工业企业数字化转型过程中，安全策略对业务需求的考量普遍存在差距，尚没有形成清晰的安全体系化建设路径[17]，建议从以下几个方面强化网络安全防护能力：

（1）构建和完善多方位的法律法规及制度框架体系。在网络安全法、数据安全法、系统等级保护制度、网络安全人员认证制度以及各行业部门信息安全规章制度基础上，面向不同类型的产品和服务，制定适用的安全风险管控框架。

（2）建立物联网设备接入认证制度。重点工业企业建设数字化工厂时，应采用类似于智能工厂框架的物联网和数字化设备接入标准和工具，建立工厂数字化设备可信环境，确保所有的接入设备通过认证、运行顺畅、维护便利。

（3）建立工业物联网接入技术标准联盟。依托联盟开发各类设备数据采集交互模型和标准化通信协议，形成适用于我国境内的物联网设备接入认证标准体系，采取开放式的入网认证机制，不断丰富接入设备的品牌和种类，为工厂数字化可信环境提供基础保障。

4.4 加强技术融合，形成相互促进的新型安全模式

LMT 公司、波音、通用电气、ABB 等企业在保障业务安全运营的同时，也利用人工智能、大数据等新技术加强网络安全保障。例如，通用电气利用 AI 和工业数字孪生技术建设网络安全预警模型，在能源、交通等领域形成新的增值业务。美国能源部网络安全制造创新研究所（CyManII）发布的《2022 制造业网络安全路线图》提出，应将网络风险管理融入制造流程，利用安全数字线程来保障老旧系统与网络安全要求兼容，并同时满足维持制造业供应链和生态系统能力[18]。这也是国内外网络安全技术与制造业深度融合的发展方向，一方面，传统的安全技术主要应对和解决具体的问题，比如利用大数据技术对工厂网络活动进行实时监控分析；另一方面，在安全策略上，越来越关注全局的风险影响以及业务功能和安全的多目标平衡问题[19-20]。

我国工业企业或行业主管部门可推广建立重点工业产品和服务的全生命周期安全管控指导框架，包括基于 DevSecOps 的研发安全管理、产品数字孪生（数字线程）及数字化交付安全管理、供应商安全审查、关键数控设备操作员认证等，将网络信息安全向技术纵深和业务延伸覆盖。

4.5 加强规划引导，形成统一的基础性安全技术设施

政府及相关非政府组织出台的网络信息安全规范是企业开展网络信息安全工作的合规性依据，相关行业研究机构或联盟出台的指导性路线图等，可以有效指导企业制定具体的安全策略和方案措施。同时，国家层面出台网络安全战略规划，对于数字化转型、智能制造战略的安全实施具有不可替代的方向指引作用和协调功能。

结合我国现阶段发展现状，要重视新兴技术和新兴产业模式给制造业安全带来的潜在性风险挑战。可面向数字化工厂建设制定国家或行业层级的网络安全战略性指导文件，统筹社会各方建立合作机制，保障产业链供应链安全，并促进安全信息共享，形成全方位的安全风险快速应急能力，保障我国制造业实现高质量发展。

5 结论

我国《“十四五”智能制造发展规划》着重强调，要依托制造单元、车间、工厂、供应链等载体，推动制造业实现数字化转型，实现泛在感知、数据贯通、集成互联、人机协作和分析优化，建设智能场景、智能车间和智能工厂，并将安全可控贯穿智能制造创新发展全过程；加强安全风险研判与应对，加快提升智能制造数据安全、网络安全、功能安全保障能力，实现发展与安全相统一。因此，应在现阶段及未来相当长一段时间内，深度研究数字化工厂的核心机理、基础技术结构和基础功能架构，理解数据要素的资源性支撑作用内涵，系统性识别和分析面临的脆弱性风险，建立集业务功能安全和数据安全于一体的安全策略体系，对于实现我国重点领域数字化工厂发展和安全的高度协同，具有重大的现实意义和紧迫性。

参考文献

[1] 单忠德，汪俊，张倩. 批量定制柔性生产的数字化、智能化、网络化制造发展 [J]. 物联网学报，2021，5（3）：1-9.

[2] 李阳春，王海龙，李欲晓，等. 国外工业互联网安全产业布局

及启示研究［J］. 中国工程科学，2021，23（2）：112－121.

［3］BRAVERMAN-BLUMENSTYK M，GEORGE S. Microsoft acquires cyberX to accelerate and secure customers′IoT deployments［EB/OL］.（2020－06－22）［2024－03－28］. https：//blogs. microsoft. com/blog/2020/06/22/microsoft-acquires-cyberx-to-accelerate-and-secure-customers-iotVdeployments/.

［4］Lockheed Martin. Manufacturing gets a systemic upgrade with the digital factory［EB/OL］.（2021－11－22）［2024－03－28］. https：//www. lockheedmartin. com/en-us/news/features/2021/manufacturing-gets-systemic-upgrade-intelligent-digital-factory. html.

［5］ISO/TC 184/SC5. IEC 62264-2：2015 Enterprise-control system integration-part 2：objects and attributes for enterprise-control system integration（Edition 2.0）［S/OL］.（2015－04－XX）［2024－03－28］. https：//www. iso. org/standard/57310. html.

［6］ARC Advisory Group. ARC industrial digital transformation top 25 report［EB/OL］.［2024－03－28］. https：//www. arcweb. com/arc-industrial-digital-transformation-top-25-report.

［7］张京男. 洛马公司2021年航天发展研究［J］. 卫星与网络，2022（1&2）：20－30.

［8］ROSS R，PILLITTERI V. Protecting controlled unclassified information in nonfederal systems and organizations，NIST SP 800-171r3 fpd［R/OL］.（2023－11－XX）［2024－03－28］. https：//doi. org/10. 6028/NIST. SP. 800－171r3. fpd.

［9］IPC-CFX Standard Task Group（2－17a）of the Electronic Product Data Description Committee（2－10）of IPC. IPC-2591-Version 1.5 connected factory exchange（CFX）［S/OL］.（2022－07－XX）［2024－03－28］. https：//www. ipc. org/TOC/IPC-2591-Version%201. 5_ TOC. pdf.

［10］穆超，王鑫，杨明，等. 面向物联网设备固件的硬编码漏洞检测方法［J］. 网络与信息安全学报，2022，8（5）：98－110.

［11］Carnegie Mellon University and The Johns Hopkins University Applied Physics Laboratory LLC. Cybersecurity maturity model certification（CMMC）model overview（Version 2.0）［S/OL］.（2021－12－XX）［2024－03－28］. https：//dodcio. defense. gov/ Portals/0/Documents/CMMC/ModelOverview _ V2. 0 _ FINAL2 _ 20211202_ 508. pdf.

［12］张晓菲，李斌. 国外信息安全从业人员管理的几点研究体会——以美国、英国为例［J］. 信息安全与通信保密，2014（5）：56－57.

［13］Lockheed Martin. Softwarefactory［EB/OL］.［2024－03－28］. https：//www. lockheedmartin. com/en-us/capabilities/space/software-factory. html.

［14］MULLET V，SONDI P，RAMAT E. A review of cybersecurity guidelines for manufacturing factories in industry 4.0［J］. IEEE Access，2021（9）：23235－23263.

［15］李婧文，李雅文. 深度合成技术应用与风险应对［J］. 网络与信息安全学报，2023，9（2）：184－190.

［16］National Institute of Standards and Technology. The NIST cybersecurity framework（CSF）2.0，NIST CSWP 29［R/OL］.（2024－02－26）［2024－03－28］. https：//nvlpubs. nist. gov/nistpubs/CSWP/NIST. CSWP. 29. pdf.

［17］张格. 我国工业关键信息基础设施安全产业链供需角度分析与建议［J］. 中国信息安全，2022（9）：38－41.

［18］The U. S. Department of Energy（DOE）Cybersecurity Manufacturing Innovation Institute（CyManII）. Cyber-security manufacturing roadmap 2022（public version）［R］. 2022－05－26.

［19］MAHESH P，TIWARI A，JIN C L，et al. A survey of cybersecurity of digital manufacturing［J］. Proceedings of the IEEE，2021，109（4）：495－516.

［20］QIU JH，SUN J，ZHONG ZM. Multi objective green vehicle path optimization algorithm based on distribution revenue balance［J］. Control and Decision，2023，38（2）365－371.

（收稿日期：2024－03－31）

作者简介：

杜洪涛（1979－），男，博士，副研究员，主要研究方向：数字化转型、网络信息安全、数字治理。

李云志（1977－），通信作者，男，博士，高级工程师，主要研究方向：信息安全、数据治理。

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，即视作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，本刊支付的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