DOI 10.15302/J-SSCAE-2021.02.009

工业互联网安全技术发展研究

董悦[1]，王志勤[2]，田慧蓉[1]，李姗[1]，秦国英[1]，吾守尔·斯拉木[3]

（1. 中国信息通信研究院安全研究所，北京 100191；2. 中国信息通信研究院，北京 100191；
3. 新疆大学信息科学与工程学院，乌鲁木齐 830046）

摘要：随着云计算、大数据等新一代信息技术与传统工业运营技术的深度融合，工业互联网已成为工业企业数字化转型升级的新动能；与此同时工业互联网安全问题日趋凸显，提升工业互联网安全技术保障能力成为我国工业互联网高质量发展的前提和保障。为深入了解我国工业互联网安全技术的发展情况，本文研判了我国工业互联网的发展需求，系统梳理了工业互联网安全防护技术、安全评测技术、安全监测技术的发展现状，剖析了工业互联网安全技术的发展趋势、技术难点和面临的挑战，提出了工业互联网安全关键技术的攻关路径。研究建议，工业互联网安全技术需结合工业特点及场景，开展定制化服务；紧密融合大数据、人工智能等新技术，实现主动防御；打造内生安全能力，助力工业互联网安全建设，推动我国工业互联网安全健康发展。

关键词：工业互联网安全；安全防护技术；安全评测技术；安全监测技术

中图分类号：TP393.08　　**文献标识码：**A

Development of Industrial Internet Security Technology in China

Dong Yue[1], Wang Zhiqin[2], Tian Huirong[1], Li Shan[1], Qin Guoying[1], Wushour Silamu[3]

(1. Institute of Security Research, China Academy of Information and Communications Technology, Beijing 100191, China; 2. China Academy of Information and Communications Technology, Beijing 100191, China; 3. College of Information Science and Engineering, Xinjiang University, Urumqi 830046, China)

Abstract: As the new-generation information technology, such as cloud computing and big data, integrates in depth with traditional industrial operation technologies, the industrial Internet becomes a new driving force for the digital transformation of industrial enterprises. Meanwhile, industrial Internet security problems have increased; therefore, improving the technological capabilities for guaranteeing industrial Internet security becomes the prerequisite for the high-quality development of the industrial Internet. In this study, we first analyze the demand for industrial Internet development and summarize the development status of industrial Internet security protection, evaluation, and monitoring technologies. Subsequently, we investigate the development trend, technological difficulties, and challenges for the industrial Internet security technology, and propose the key technologies and their development approaches. To promote the safe and healthy development of industrial Internet in China, the industrial Internet security technologies need to be customized in accordance with industrial characteristics and scenarios, and closely integrate with new technologies such as big data and AI, to achieve active defense and create endogenous security capabilities.

Keywords: industrial Internet security; security protection technology; security evaluation technology; security monitoring technology

收稿日期：2021-01-22；**修回日期：**2021-03-17

通讯作者：田慧蓉，中国信息通信研究院安全研究所高级工程师，研究方向为工业互联网安全；E-mail: tianhuirong@caict.ac.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

随着计算机和网络技术的发展，新一代互联网、大数据、人工智能（AI）等技术正逐步与实体经济进行融合。基于这种发展背景，工业互联网已成为诸多传统发达国家、新兴发展中国家抢占发展机遇、加快战略布局的关键支撑 [1,2]。我国高度重视工业互联网的安全高效发展，2021 年政府工作报告提出，发展工业互联网，搭建更多共性技术研发平台。与传统工业生产相对封闭可信的环境不同，随着工业互联网的发展，工业制造业的工作环境也在逐步开放，传统互联网安全威胁向工业领域逐步渗透，导致安全问题交织、安全形势复杂、安全风险日益加大 [3,4]。

以美国、德国等为代表的工业发达国家和一些国际知名企业已在积极推进工业互联网安全技术从战略布局到部署实施转变，聚焦工业互联网安全技术的实际应用 [5,6]。美国为推动工业互联网安全框架在产业中的应用，发布了一系列白皮书和使用指南，指导相关企业部署工业互联网安全防护措施。德国、日本分别推出工业 4.0 参考架构、工业价值链参考架构，将工业互联网安全作为重要内容进行整体设计。以色列工业网络安全领域的 CyberX 公司推出了工业控制系统攻击途径预测的安全服务。卡巴斯基实验室发布了 2019 年工业安全威胁预测，关注工业领域面临的网络安全挑战 [7]。

我国工业互联网安全技术的研究起步较晚，但跟进较快，注重完善工业互联网安全的顶层设计，引导安全技术和产业发展。2019 年，工业和信息化部等十部委联合印发《加强工业互联网安全工作的指导意见》，要求针对工业互联网安全，加强攻击防护、漏洞挖掘、态势感知等安全产品研发，探索利用 AI、大数据、区块链等新技术提升安全防护水平。我国除依托传统网络安全技术进行安全技术产品功能的拓展外，着重基于新兴互联网技术，开展新一代网络安全技术产品的研发创新。相关研究主要有：工业互联网边缘端点的防护技术 [8]、工业防火墙技术 [9]、工业互联网漏洞挖掘技术 [10]、渗透测试技术 [11]、安全态势感知技术 [12] 等；多为针对某一种技术的分析及应用研究，缺乏对工业互联网安全技术的系统梳理和分类研究。为此，本文通过深入剖析工业互联网安全技术发展需求，系统梳理相关发展现状，总结分析发展趋势、存在问题及关键技术攻关路径，据此提出对策建议。

二、工业互联网安全技术需求分析

传统的工控系统处于封闭可信环境，采用“两层三级”的防御体系、分层分域的隔离思路，对网络攻击防护能力普遍不足。随着工业互联网的发展，工业设备逐渐智能化，相关业务上云、企业协作等不断推进，互联网与工业企业中的生产组件和服务深度融合，使传统的互联网安全威胁如病毒、木马、高级持续性攻击等蔓延至工业企业内部（见图 1）。不同于传统互联网中的信息安全防护，工业互联网安全需要有机融合信息安全和功能安全，还要叠加交织传统工控安全和互联网安全，因而更显复杂。

（一）网络攻防对抗持续升级，工业互联网成为重点攻击目标

工业互联网相关系统被成功攻击的概率为 12%，远高于电子政务系统的 1% 和通信行业的 5% [13]。随着网络攻防对抗的不断升级，网络攻击也呈现出一些新特性：①攻击技术复杂化，从单一攻击向多种复杂技术结合的方式转变；②攻击形式定向化，以往多为获取利益、没有固定目标，而现在高级可持续威胁攻击（APT）成为主要攻击方式，攻击多为定向、长期潜伏难以发现；③攻击行为国家化，国家层面的网络攻击安全隐患加剧，针对能源、电力等重要领域的攻击行为频繁发生，对工业生产、居民生活、经济社会稳定运行乃至国家安全构成直接影响 [14]。

为有效应对来自外部的网络攻击，工业互联网需要不断提升技术能力来进行防御。此外，工业互联网安全防护技术在工业企业安全防护需求的驱动下创新发展，如边界防护采用工业防火墙、白名单机制等边界控制技术，工业主机防护需采取融合身份鉴别与访问控制的主机加固技术等。鉴于工业互联网数据存在泄露安全风险，应采用数据机密、数据防泄漏等工业互联网数据安全防护技术。

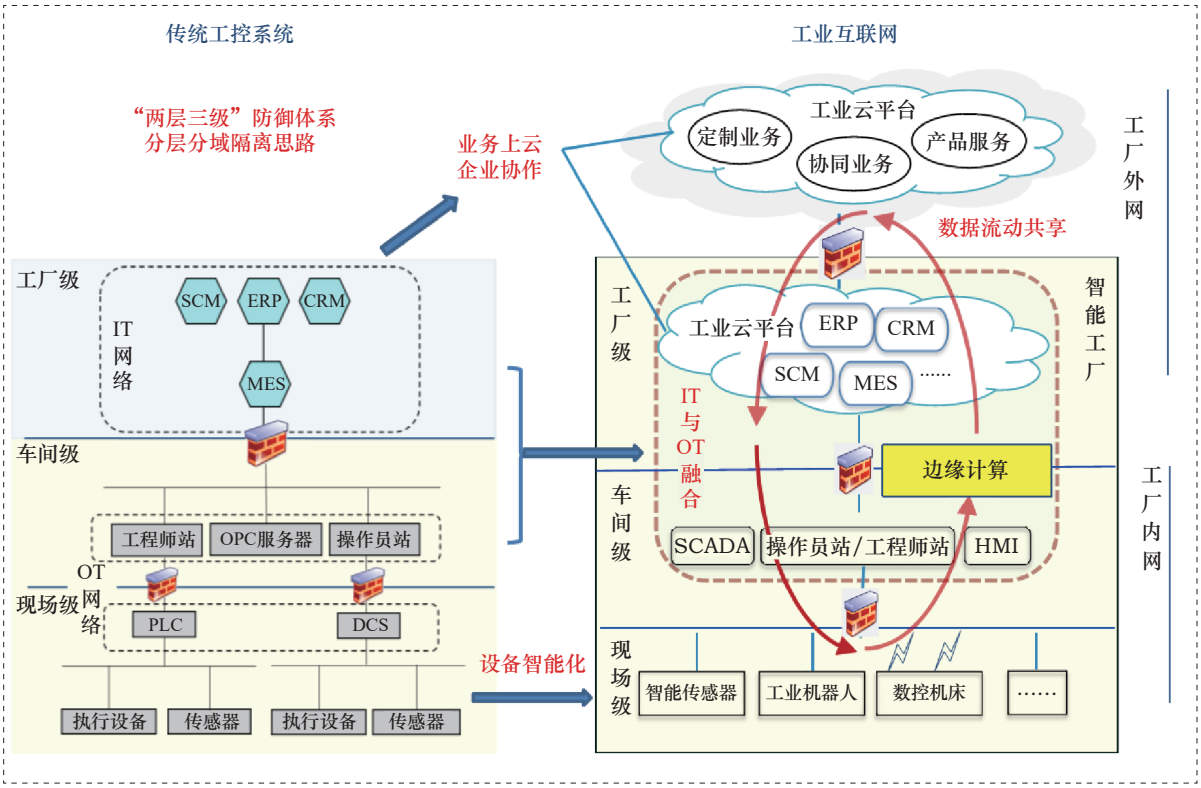
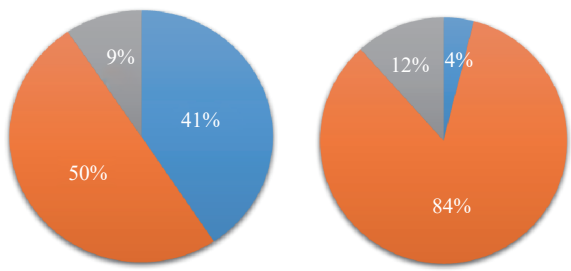


图 1　传统工控系统向工业互联网的转化示意图

注：SCM 表示软件配置管理；ERP 表示企业资源计划；CRM 表示客户关系管理；MES 表示制造企业生产过程执行管理系统；OPC 表示用于过程控制的对象连接与嵌入（OLE）；PLC 表示可编程逻辑控制器；DCS 表示分散控制系统；SCADA 表示数据采集与监视控制系统；IT 表示信息技术；HMI 表示人机交互界面；OT 表示运营技术。

（二）联网工业设备和平台的漏洞数量多、级别高，潜在威胁不容忽视

网络互通互联之后，原来封闭的工控系统大多存在安全脆弱性、漏洞难以修补、安全问题短期难以解决等问题。截至 2020 年 6 月 30 日，国家工业互联网安全态势感知与风险预警平台（简称“国家平台”）累计监测发现联网工控设备漏洞隐患共有 946 个，其中高危漏洞有 385 个，中危漏洞有 472 个，中、高危漏洞占漏洞总数的 90.6% [13]。此外，工业互联网平台与企业内大量关键设备之间的直连也存在严重的漏洞隐患，且安全漏洞大多为中高危漏洞。截至 2020 年 6 月，通过对 136 个重点工业互联网平台进行扫描，累计共发现漏洞为 3381 个，其中高危漏洞有 133 个，中危漏洞有 2852 个，中高危漏洞占比为 88% [12]（见图 2）。



(a) 联网工控设备　(b) 工业互联网平台

图 2　工业企业中的网络漏洞危害等级分布

工业设备和工业互联网平台中存在的漏洞数量多、级别高，需采用漏洞扫描、漏洞挖掘技术及时发现潜在威胁。工业互联网平台或相关系统在正式投入使用前，需进行安全评测。然而，目前工业互联网资产众多且不明晰、安全风险不可知；建设工业互联网安全态势感知平台之后才能实现工业互联网安全风险的可视、可知、可感。因此，在企业安全合规和政府监管需求的驱动下，亟需大力发展工业互联网安全评测和监测技术。

（三）工业互联网安全架构改变与新技术应用不断引入新的安全风险

关键工业设备入网、企业平台云端化等措施使得安全风险的传导与延展进一步加速，原有网络安

全边界瓦解，传统安全防护措施失效，遭受网络攻击的范围由边界向核心不断扩大。标识解析体系面临分布式拒绝服务攻击（DDoS）、域名劫持等风险，而且不同标识体系如 Handle、OID、Ecode、GS1 等在兼容过程中也引入了新的安全风险。第五代移动通信（5G）、互联网协议第六版（IPv6）等新技术在工业互联网中的普及应用，也带来了更多的网络安全挑战。

随着信息通信技术（ICT）、AI、区块链的不断发展，IT 架构出现了颠覆性变革，为工业互联网安全技术提供了底层技术支撑。例如，密码技术经历了古典密码、近代密码、现代密码的发展历程，未来将面临由大数据、区块链等新技术、新业务发展带来的重大挑战。安全技术自身发展到一定阶段，面对新的应用环境和需求，将不断追求技术瓶颈突破，进一步与新技术融合发展。

针对设备、控制、网络、应用、数据等不同的工业互联网防护对象，应分别采取相应的安全技术措施，对技术进行分类，形成工业互联网安全技术视图（见图 3），主要分为底层技术、安全防护技术、安全评测技术、安全监测技术 4 类。①底层技术包括密码算法、AI、区块链等技术，通过提供基础技术手段，为工业互联网安全防护、安全评测、安全监测提供技术支撑。②工业互联网安全防护技术是对工业互联网各层级部署边界控制、身份鉴别与访问控制等的技术措施，覆盖工业互联网安全体系架构 4 个层级的五大安全防护对象（设备、控制、网络、应用、数据），是工业互联网安全技术的核心。③工业互联网安全评测技术主要对工业设备和系统进行漏洞扫描、漏洞挖掘、渗透测试、上线测试等。④工业互联网安全监测技术主要对工业互联网防护对象采取资产安全管理、安全监测与审计、态势感知等技术措施。

三、工业互联网安全技术发展现状

（一）工业互联网安全防护技术

工业互联网安全防护技术是以攻防对抗为核心的基础技术，主要包括白名单技术、网络边界防护、工业主机安全防护等关键技术 [15]。

1. 安全机制

工业互联网涉及工业生产的重要环节，对系统可用性和实时性要求高。原有的工控网络相对封闭，工控设备缺乏灵活的安全策略，无法保证接入工业

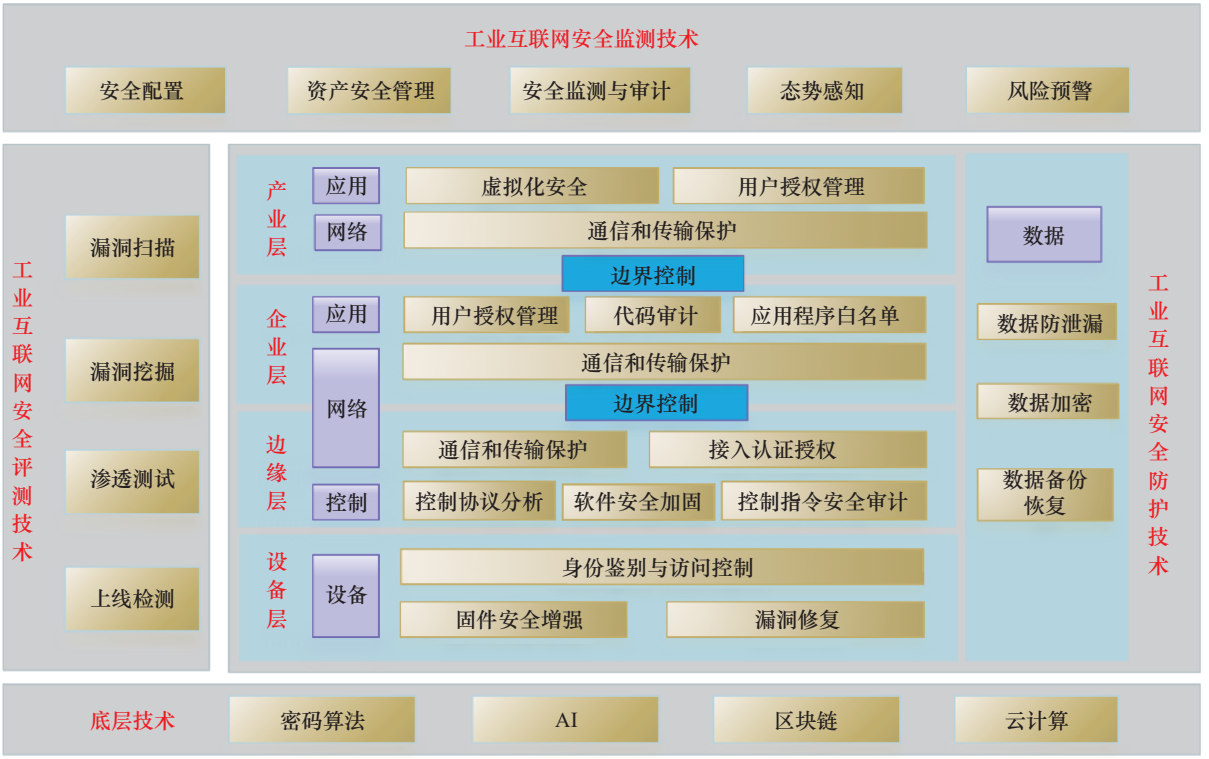


图 3　工业互联网安全技术视图

互联网中的设备和运行软件安全可信。在传统 IT 网络中，安全机制一般采取黑名单技术，可以有效阻止已知威胁，但不能阻止未知攻击行为。在传统工控系统中，工业业务流程相对固定，不需要频繁升级，采取白名单技术允许信任且正确的内容通过；如果信任内容发生变化，则重新调整安全策略。在工业互联网中，可采取以白名单技术为主、以黑名单技术为辅的安全防护机制。这是因为工业控制工艺流程、业务等相对固定，且对可用性和实时性的安全需求高，白名单技术更加适用，同时在开放网络中引入黑名单技术进行辅助防护。

2. 边界防护

传统工控系统发展到网络互通互联的工业互联网阶段，OT 与 IT 不断融合，OT 网络不再封闭可信，涉及多种网络边界。在传统 IT 网络中，通常采用 IT 防火墙技术进行边界防护，但传统 IT 防火墙技术不支持 OPC 协议（用于过程控制的 OLE）的任何解析；为确保 OPC 客户端可以正常连接 OPC 服务器，防火墙需要配置全部端口可访问，使生产控制网暴露在攻击者面前。在工控网络边界部署的工业防火墙，可以对 OPC 协议进行深度解析，跟踪 OPC 连接建立的动态端口并对传输指令进行实时监测。因此，工业互联网边界防护需要针对不同网络边界的防护情况部署不同的防火墙。为适应工业环境下的部署要求，支持常见工业协议的深度解析，边界防护产品应具有高可靠性和低时延。

3. 工业主机防护

工业主机是工业互联网安全事件的突破口、众多工业病毒的传播载体。由于工业组态软件等的稳定性要求高，工业主机若未及时更新系统补丁，将无法获得全面的安全防护。在互联网中，传统 IT 主机通常采用防病毒技术，通过接入互联网进行病毒库升级；“云”查杀技术逐步推广，新病毒发现和查杀的效率不断提高，但需要实时更新升级病毒库。在工业互联网中，工业主机可以采取基于关闭无关端口、进行最小权限的账号认证、设置强制访问控制等措施的主机加固技术，提高主机操作系统的安全性。因此，以主机加固技术为基础，以防病毒技术为重要补充手段，综合利用防护技术来提高工业主机的安全防护水平。

（二）工业互联网安全评测技术

工业互联网安全评测技术指采取技术手段对工业互联网安全防护对象进行测试和评价，了解其安全状态；主要包括漏洞挖掘、渗透测试等技术。

1. 漏洞挖掘

随着工控系统开放性的逐步提高，利用漏洞、后门等攻击行为和窃密方式成为工业互联网安全面临的巨大威胁。传统 IT 系统漏洞主要包括恶意软件、密码攻击、拒绝服务等，而工控系统漏洞不同于传统 IT 系统漏洞，具体原因为：①大部分工控系统来自国外进口，相关系统的运营维护无法实现自主可控；②工控系统漏洞来源范围广，涵盖网络安全中的安全计算环境漏洞、控制协议自身漏洞、应用系统漏洞、PLC 等控制器的自身漏洞与后门等；③工控系统相对封闭，系统通信协议相对私有，难以深度研究其通信协议和安全特性。因此，工业互联网中的漏洞挖掘技术，需对工控系统网络特性、生产过程控制及其控制协议进行分析，采取有针对性的模糊测试技术 [16]。在工业互联网中，需采用 IT 和 OT 融合环境下的漏洞挖掘思维，运用多种组合且深度融合的漏洞挖掘技术。

2. 渗透测试

渗透测试通过模拟来自网络外部的恶意攻击者常用的攻击手段和方法，检测并评估工业互联网的网络系统安全性。工业互联网中的渗透测试技术，要以工控系统中渗透测试的实际需求为出发点，辅以渗透测试执行标准（PTES）、《信息安全测试评估技术指南》（NIST SP800-115）、开源安全测试方法（OSSTMM）、《开放式网页应用程序安全项目测试指南》（OWASP Test Guide）等渗透测试和安全测试流程指南，完成对工控系统渗透测试的检测与分析，提取关键流程、步骤、技术。工业互联网安全渗透测试并不是将多种渗透测试安全工具进行拼装应用，而是将多种渗透工具高度融合后进行使用。

（三）工业互联网安全监测技术

工业互联网安全监测技术通过技术手段实现对安全威胁的发现识别、理解分析、响应处置，主要包括安全监测审计、安全态势感知等关键技术。工业互联网的设备资产和软件系统众多，生产人员的管理运维工作复杂且繁重，相关设备和平台存在安全漏洞多、安全威胁难以掌握、易受网络攻击等问

题。工业互联网安全态势感知技术在网络空间搜索引擎的基础上，添加工业控制系统及设备的资产特征，利用软件代码的形式模拟常见的工业控制系统服务或工控专用协议（如 Modbus、Profinet、FINS 等），利用深度包检测（DPI）技术，对网络及应用层协议（如工控专用协议、通用协议等）进行逐层解析与还原工作，最终完成访问日志合成、工控设备资产检测、工控漏洞及安全事件识别等安全检测工作 [17]。后续，工业互联网安全态势感知技术在传统在线监测、蜜罐仿真、网络流量分析技术的基础上，加强对工业互联网协议与设备的识别能力，构建对工业互联网安全事件监测预警、处置溯源、安全态势分析等能力。

四、工业互联网安全技术发展趋势

（一）工业互联网安全架构从边界安全向零信任安全方向发展

传统的工厂网络边界安全架构默认边界内部是安全的，防火墙、杀毒软件、入侵检测系统（IDS）、数据泄露防护系统（DLP）等边界设备作用在物理边界上，根据在边界上的行为开展防护和监视。随着工业互联网在计算能力下沉、业务上云等方面的不断发展，工业互联网安全边界发生改变，需要重构网络安全架构（见图 4）。后续，工业互联网安全架构着重构建以身份为基石，以业务安全访问、持续信任评估、动态访问控制为主要关键能力的“云管边端”一体化零信任安全架构。

（二）工业互联网安全防护理念从被动防护向主动前瞻防护转变

工控系统虽已设置了相关安全设备来提升系统安全性，但网络攻击手段不断增多，被动防御存在一定的局限性。主动防御可以在恶意入侵行为对工业互联网中信息系统产生影响之前来避免、降低或转移风险，体现一对多防御特征；结合主动探测、流量分析、被动诱捕等技术，可以支持工业互联网的安全态势感知和风险预警，最终实现从被动安全防护向主动防御转变。

（三）工业互联网安全技术从传统分析向智能感知发展

在发展初期，态势感知技术主要通过采集和分析海量安全数据，发现其中有价值的信息，汇总成易于理解的报告和图表，从而明确可能会对系统安全造成威胁的漏洞 [18]。当前，安全技术与大数据、AI 技术不断融合，增强了系统的安全检测和分析能力，推动了安全态势感知的发展，主要表现在 APT 截获、威胁感知、威胁情报共享等。工业互联网安全技术朝着智能感知方向发展，开展基于逻辑和知识的推理，从已知威胁推演未知威胁，实现对安全威胁事件的预测和判断。未来借助 AI、大数据分析等新兴技术，不断提升安全风险精确预警与准确处置的水平，实现网络攻击和重大网络威胁的可知化、可视化、可控化。

五、工业互联网安全技术难点及面临的挑战

（一）工业互联网安全技术难点

整体来看，目前我国工业互联网安全技术的发展处于在传统网络安全技术基础上加以改进和融合的阶段，存在的技术难点有：①工业协议复杂多样，深度解析难度大；工业安全防护产品在深度感知工业互联网业务流量、深度解析流量中的工业协议的

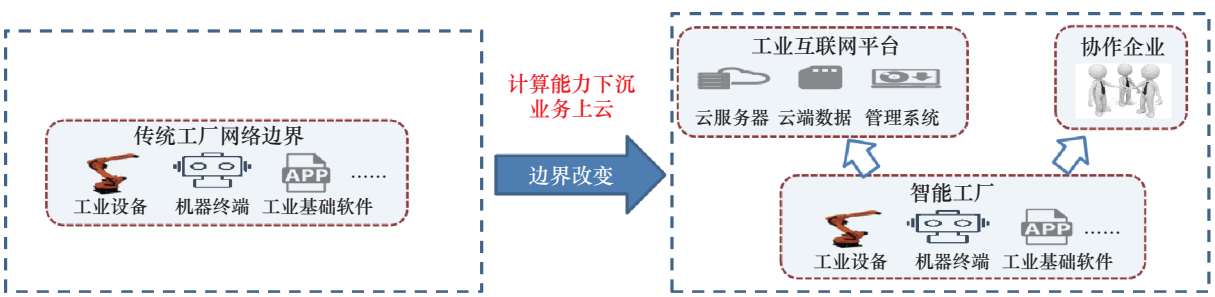


图 4　工业互联网安全边界的变化

基础上，才能实现对工业协议指令级别和值域级别的安全防护。②行业壁垒明显，难以形成覆盖面广的安全模型；工业行业领域众多，甚至同一行业的业务也会千差万别，工业互联网安全技术产品要与具体工业场景紧密结合，必要时需进行定制化开发。③针对 5G 等新技术的安全技术储备不足，存在利用 5G 相关协议、终端漏洞控制工业互联网终端和工厂等风险。

（二）工业互联网安全技术面临的挑战

工业互联网的深入应用，增加了工业企业联网设备遭受网络攻击、病毒传播的安全风险；加之部分企业安全意识薄弱、防护水平普遍较低、安全产业支撑能力不足等客观因素，工业互联网安全技术面临诸多挑战。①工业企业安全意识不足，对工业互联网安全的投入不充分；普遍重发展、轻安全，只关注对传统生产系统、制造模式的升级改造，而对网络安全风险认识不足，安全投入低；较少整体考虑建设IT与OT安全，多为分开建设，不利于工业互联网安全防护。②工业互联网安全产业在工业互联网核心产业中占比较低，存量规模虽由 2017 年的 13.4 亿元增长至 2019 年的 27.2 亿元（年复合增长率为 42.3%），但在工业互联网核心产业中的占比仅为 0.5% [19]；同时缺乏龙头企业引领，相关产品和服务较为松散，多以边界和终端安全防护为主。③安全复合人才紧缺，不足以支撑以工业和信息化深度融合为特征的工业互联网发展需求；这些安全人才不仅要掌握网络安全专业知识，还要熟悉工厂环境的应用场景，相应人才缺口较大。

六、工业互联网安全关键技术攻关路径

工业互联网安全关键技术主要由工控核心安全技术、在工业领域应用的互联网安全核心技术两部分构成，具体包括密码技术、安全编排与自动化响应（SOAR）技术、工业高交互仿真技术等。

（一）应用密码技术

在工业互联网领域，国外密码技术起步早、应用广、成本低。国内密码技术起步较晚，部分工业产品尽管预先集成了国外密码算法（如更换密码技术），但存在更换成本高、市场接受周期长等问题。为此，国内信息安全企业提出了基于国产密码技术的工业互联网安全解决方案，即通过使用 SM9 国产密码算法，实现工业终端数据、云端服务器数据的加密传输和存储；建设相应的工业信息安全密码支撑系统，为工业互联网平台提供安全可靠的网络环境、数据加密服务的整体解决方案。针对工业互联网标识解析体系的身份认证、敏感数据保护、隐私保护等应用需求，研究攻关基于 SM9/SM2 算法的密码模块、数字签名、隐私数据脱敏等技术，构建基于数字认证、基于身份标识的密码系统（IBC）、无证书技术等体制融合的工业互联网标识解析安全体系。

（二）应用 SOAR 技术

SOAR 是人员、流程、技术融合的智能协作系统，核心是实现跨产品、跨组件的安全能力编排，缩短安全事件响应时间，提高安全事件响应的准确率。SOAR 技术在工业领域面向异构企业、异构安全设备，构建统一化、标准化的安全接口体系，打破各个安全企业安全设备的孤岛形态，建立可信任的安全联动体系。

国外已在工业安全领域实际应用了 SOAR 技术，如西门子股份公司实现了不同业务场景的安全策略定制、不同安全需求及业务的安全策略选择和部署，以色列 Cyberbit 公司的 SOAR 产品也在工控安全领域得到应用。目前，我国以制造业为代表的各大企业虽已部署相关安全设备，但没有统一、标准的安全接口，无法整合设备和产品的安全能力以实施自动化的响应和处置。因此，亟需应用 SOAR 技术，通过各类安全能力的协同，为网络安全领域的一体化响应奠定基础。

（三）应用工业高交互仿真技术

工业高交互仿真技术指对工业互联网主机、控制及边缘设备、工业协议、工业互联网平台、相关业务和应用进行高交互虚拟仿真；提供更真实的攻击系统，采集和分析攻击数据，准确掌握工业互联网攻击行为特征，为开展安全防护工作提供决策支撑。国外在工业互联网设备和协议仿真方面已有相关成熟产品的部署应用，如 CryPLH、Xpot 等高交

互工控蜜罐，支持监管部门有效掌握威胁情报信息。我国相关技术处于研发和产品试点应用阶段，但成熟产品仍为空白。

工业互联网设备参与的协议种类繁多、技术性壁垒强，如设备多采用无线协议进行通信而难以进行高交互仿真。工业高交互仿真技术的核心在于支持 Modbus、Dnp3、Siemens S7 等多种工控协议以及 SCADA、DCS、PLC 等工控设备的高交互模拟能力；相对全面地捕获攻击者的访问流量，分析取证攻击行为，为工业互联网安全事件的预警、预测提供数据支撑。

七、对策建议

（一）结合工业特点及场景，开展定制化服务

工业互联网安全技术应结合工业场景特点，借鉴传统互联网安全技术的相关方法，定制适合工业互联网防护对象的安全技术。建议实行工业协议指令级防护，部署于企业管理网和生产控制网边界处的指令级工业防火墙；深度解析 OPC 协议并拓展至指令级别，跟踪 OPC 服务器和 OPC 客户端之间协商的动态端口；最小化开放生产控制网的端口，提升基于 OPC 协议的工业控制系统的网络安全。针对不同行业和工业场景，定制适合的安全技术。例如，电力行业安全技术的部署遵循“安全分区、网络专用、横向隔离、纵向认证”的总体原则；在石油炼化工业控制系统中对网络边界、区域、主机等进行安全防护，提升生产网防攻击、抗干扰能力，保护生产系统的安全、稳定运行。

（二）不断融合新技术，实现主动防御

区块链、AI、大数据、可信计算等技术的发展，为工业互联网安全助力赋能，在发现高级威胁、检测恶意文件、判定恶意家族、监测加密攻击、主动发现威胁、辅助快速调查，保障工业互联网安全等方面具有潜在优势。工业互联网安全技术应与这些新技术进行有机融合，定制适用的安全策略。建议快速发展基于技术大数据的工业互联网安全态势感知技术，通过海量工业数据检索、日志采集、流量分析、自动定位、可视回溯等环节实现工业互联网安全态势感知；利用 AI 等技术智能化、自动化地发现高级威胁和潜在安全问题，保障工业互联网安全。

（三）打造内生安全能力，助力工业互联网安全建设

传统局部与外挂的安全防护能力已不能满足安全需求，亟需提升工业互联网的内生安全能力，实现网络安全能力和工业信息化环境的融合。建议在工业互联网系统规划、建设、运维的过程中考虑安全能力的同步建设；网络安全企业与系统设备提供商、工业龙头企业强强联合，打造具备内嵌安全功能的设备产品，更好实现工业生产系统和安全系统的聚合；企业结合业务特性，立足自身安全需求开展安全能力建设，实现工业互联网安全的自适应与自成长，动态提升工业互联网安全能力。

参考文献

[1] 许可, 秦锐, 王圆, 等. 互联网+下的产业大变局: 赢战产业互联网 [M]. 北京: 人民邮电出版社, 2015.
Xu K, Qin R, Wang Y, et al. Industrial game-changing strategy in the Internet+ area：Win the war of industrial Internet [M]. Beijing: Posts & Telecom Press Co., Ltd., 2015.

[2] 张尼, 刘廉如, 田志宏, 等. 工业互联网安全进展与趋势 [J]. 广州大学学报(自然科学版), 2019, 18(3): 68–76.
Zhang N, Liu L R, Tian Z H, et al. Progress and trend of industrial Internet security [J]. Journal of Guangzhou University(Natural Science Edition), 2019, 18(3): 68–76.

[3] 杜霖, 陈诗洋, 姜宇泽, 等. 工业互联网安全关键技术研究 [J]. 信息通信技术与政策, 2018 (10): 10–13.
Du L, Chen S Y, Jiang Y Z, et al. Research on the protection of national basic data [J]. Information and Communications Technology and Policy, 2018 (10): 10–13.

[4] 李涛. 对工业互联网安全态势分析及安全防护建议思考 [J]. 网络安全技术与应用, 2020 (4): 126–128.
Li T. The consideration on security posture analysis and security defense suggestion in the industrial Internet of Things [J]. Network Security Technology & Application, 2020 (4): 126–128.

[5] 李强, 田慧蓉, 杜霖, 等. 工业互联网安全发展策略研究 [J]. 世界电信, 2016 (4): 16–19.
Li Q, Tian H R, Du L, et al. The strategic research on industrial Internet of Things [J]. World Telecommunications, 2016 (4): 16–19.

[6] 刘晓曼, 杜霖, 杨冬梅. 2019年工业互联网安全态势简析 [J]. 保密科学技术, 2019 (12): 27–31.
Liu X M, Du L, Yang D M. The analysis on security posture of industrial Internet of Things in 2019 [J]. Secrecy Science and Technology, 2019 (12): 27–31.

[7] 郭娴, 刘京娟, 余章馗, 等. 2019年工业信息安全态势展望 [J]. 中国信息安全, 2019 (6): 51–52.
Guo X, Liu J J, Yu Z K, et al. The security expectation on industrial Internet of Things in 2019 [J]. China Information

Security, 2019 (6): 51–52.

[8] 万明, 张世炎, 李嘉玮, 等. 工业互联网安全浅析: 边缘端点的主动防护 [J]. 自动化博览, 2021, 38(1): 62–66.
Wan M, Zhang S Y, Li J W, et al. Analysis on security in industry Internet of Things [J]. Automation Panorama, 2021, 38(1): 62–66.

[9] 孙晓东, 秦焕亮, 梁志军, 等. 智能工业防火墙新技术 [J]. 自动化博览, 2018, 35(5): 80–83.
Sun X D, Qin H L, Liang Z J, et al. New technology of intelligent industrial firewall [J]. Automation Panorama, 2018, 35(5): 80–83.

[10] 赵振学, 石永杰, 于慧超, 等. 工业互联网环境下的漏洞挖掘技术研究 [J]. 化工自动化及仪表, 2020, 47(2): 160–164.
Zhao Z X, Shi Y J, Yu H C, et al. Research on vulnerability discovering in IIOT system [J]. Control and Instruments in Chemical Industry, 2020, 47(2): 160–164.

[11] 陈坤华. 工业互联网网络安全渗透测试技术研究 [J]. 网络安全技术与应用, 2020 (4): 124–126.
Chen K H. The research on security permeation test in industrial Internet of Things [J]. Network Security Technology & Application, 2020 (4): 124–126.

[12] 解旭东. 工业互联网安全监测审计及态势感知技术研究 [J]. 信息安全研究, 2020, 6(11): 996–1002.
Xie X D. Research on industrial Internet security monitoring audit and situation awareness technology [J]. Journal of Information Security Research, 2020, 6(11): 996–1002.

[13] 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报告 [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 Communications Technology, Alliance of Industrial Internet. Report on industrial Internet security situation for the first half of 2020 [R]. Beijing: China Academy of Information and Communications Technology, Alliance of Industrial Internet, 2020.

[14] 刘晓曼, 全湘溶, 李姗. 国外工业互联网安全发展概况 [J]. 保密科学技术, 2020 (5): 20–26.
Liu X M, Quan X R, Li S. The development on security of overseas industrial Internet of Things [J]. Secrecy Science and Technology, 2020 (5): 20–26.

[15] 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 on the development of industrial Internet security industry in China [J]. Secrecy Science and Technology, 2020 (5): 27–31.

[16] 孙易安, 胡仁豪. 工业控制系统漏洞扫描与挖掘技术研究 [J]. 网络空间安全, 2017, 8(1): 75–77.
Sun Y A, Hu R H. Research on vulnerability scanning and discovering technology of industrial control system [J]. Cyberspace Security, 2017, 8(1): 75–77.

[17] 南京中新赛克科技有限责任公司. 工业互联网安全监测与态势感知解决方案 [J]. 自动化博览, 2020, 37(2): 28–31.
Nanjing Sinovatio Technology Co., Ltd. The solution on security detection and situation awareness in industrial Internet of Things [J]. Automation Panorama, 2020, 37(2): 28–31.

[18] 陶源, 黄涛, 张墨涵, 等. 网络安全态势感知关键技术研究及发展趋势分析 [J]. 信息网络安全, 2018 (8): 79–85.
Tao Y, Huang T, Zhang M H, et al. Research and development trend analysis of key technologies for cyberspace security situation awareness [J]. Netinfo Security, 2018 (8): 79–85.

[19] 中国信息通信研究院. 工业互联网产业经济发展报告(2020) [R]. 北京: 中国信息通信研究院, 2020.
China Academy of Information and Communications Technology. Report on industrial Internet industry economic development (2020) [R]. Beijing: China Academy of Information and Communications Technology, 2020.