



专题：工业互联网平台及安全

工业互联网平台及其安全技术发展

蒋融融^{1,2}, 翁正秋^{3,4}, 陈铁明⁴

(1. 浙江广播电视大学, 浙江 杭州 310012;

2. 北京航空航天大学计算机学院, 北京 100191;

3. 温州职业技术学院信息技术系, 浙江 温州 325035;

4. 浙江工业大学计算机科学与技术学院, 浙江 杭州 310023)

摘要: 互联网与传统产业的深度融合促进工业互联网的飞速发展, 数字化、网络化、智能化等关键要素使工业互联网平台成为新的基础建设项目, 标识体系、边缘计算、数字孪生等新技术不断涌现, 同时工业互联网平台也带来终端安全、控制安全、业务安全等新的安全威胁。从工业互联网现状出发, 梳理工业互联网平台的技术发展, 分析总结安全技术挑战, 并阐述工业互联网安全发展趋势。最后提出工业互联网“泛安全”保障框架。

关键词: 工业互联网; 数据; 计算; 服务; 平台; 安全

中图分类号: TP393

文献标识码: A

doi: 10.11959/j.issn.1000-0801.2020067

Development of industrial internet platform and its security challenges

JIANG Rongrong^{1,2}, WENG Zhengqiu^{3,4}, CHEN Tieming⁴

1. Zhejiang Open University, Hangzhou 310012, China

2. College of Computer Engineering, Beihang University, Beijing 100191, China

3. Department of Information Technology, Wenzhou Polytechnics, Wenzhou 325035, China

4. College of Computer Science and Technology, Zhejiang University of Technology, Hangzhou 310023, China

Abstract: The deep integration of the internet and traditional industries promotes the rapid development of the industrial internet. Key factors such as digitization, networking, and intelligence have made the industrial internet platform a new infrastructure project, and new technologies like identification systems, edge computing, and digital twin have emerged. Industrial internet platforms also bring new security challenges (e.g., terminal security, control security, and business security). Starting from the current situation of industrial internet, the technological development of the industrial internet platform was sorted out, the security challenges were analyzed, the new trends of the industrial internet security were elaborated, and a framework of “ubiquitous security” for industrial internet was proposed.

Key words: industrial internet, data, computing, service, platform, security

收稿日期: 2019-12-20; 修回日期: 2020-03-12

通信作者: 翁正秋, derisweng@163.com

基金项目: 2019 年工业互联网创新发展工程-工业互联网网络安全公共服务平台资金资助项目 (No.TC190H3WN)

Foundation Item: 2019 Industrial Internet Innovation and Development Project of the Ministry of Industry and Information Technology-Industrial Internet Network Security Public Service Platform (No.TC190H3WN)



1 引言

工业互联网作为产业互联网的支撑,极大扩展了网络空间的边界和功能,但由于工业化和信息化的深度融合^[1-3],打破了工业控制系统的封闭格局,增加了设备安全、控制安全、网络安全、平台安全和数据安全等多个领域的安全风险^[4-6]。近年来,电力、交通、石油、取暖、制药等关键信息基础设施系统遭受攻击的事件频发,例如伊朗核设施遭遇震网病毒攻击、乌克兰电厂受到黑客攻击导致大面积停电、“永恒之蓝”勒索病毒致使全球多家车企停产等,工业互联网安全已威胁到国计民生和国家发展的安全。由于工业系统自身安全建设的不足,许多工控设备缺乏安全设计,设备联网机制缺乏安全保障,生产数据面临丢失、泄露、篡改等安全威胁,传统的保密性、完整性、可用性等信息安全技术无法直接适用,工业互联网平台安全保障面临全新的挑战^[7-8]。

本文从全球工业互联网技术现状出发,介绍工业互联网平台发展情况,分析其面临的安全威胁,并阐述安全技术创新趋势,最后提出一种工业互联网“泛安全”保障框架。

2 工业互联网发展概况

2011年,以美国通用电气为代表的企业确立了将工业互联网作为制造业升级核心,首次提出了“工业互联网”的概念;2013年,在德国汉诺威工业博览会上,德国提出了“工业4.0”概念;2014年,中国提出“中国制造2025”计划,为实施制造强国战略提供了行动纲领。新一轮工业革命在全世界同时发生,工业互联网成为第四次工业革命的主驱动和智能制造变革的关键支撑力量。工业互联网通过开放的通信网络平台,利用新一代信息化技术与传统工业系统全方位深度融合,管理工业生产全流程的各种要素,使其网络化、数字化、自动化、智能化,实现智能控制、

运营优化和生产组织方式的变革,从而提升效率和降低成本。

德国“工业4.0”战略计划强调通过信息网络与工业生产系统的融合,将传统工厂转化为智能工厂,保持其装备制造业在全球市场中的领导地位,以使德国成为智能制造技术的主要供应国。与德国强调的“硬”制造不同,美国的“工业互联网”侧重于软件和互联网等“软”服务,以政府战略为推动,通过新的技术、标准、商业模式重新定义制造业,提升整个工业的价值创造能力。

2014年提出“中国制造2025”计划、2017年国务院审议通过《关于深化“互联网+先进制造业”发展工业互联网的指导意见》、2018年在国家制造强国建设领导小组下设立工业互联网专项工作组以及提出工业互联网发展四大战略部署等一系列政策和措施的制定,说明工业互联网工作受到了国家极大的关注与重视,成为国家战略中重要的组成部分。在政策与市场的双重驱动下,深入推进制造业转型升级,以提高国家制造业的创新能力,使中国在新一轮产业革命中抢占先机。

3 工业互联网平台现状

随着工业数据的爆发式增长以及企业对智能化决策需求的不断提高,工业互联网平台成为工业全要素链接的枢纽,成为工业资源配置的核心。工业互联网平台是面向制造业数字化、网络化、智能化需求,构建基于海量数据采集、汇聚、分析的服务体系,支撑制造资源泛在连接、弹性供给、高效配置的工业云平台^[3]。

国际上主要依托行业巨头主导工业互联网平台建设,中国的工业互联网平台则在政府的引导下,呈现制造企业、自动化企业、互联网公司、ICT企业等多元化优势互补的发展态势。如航天云网的INDICS平台、海尔的COSMOPlat平台、三一重工的根云平台、华为的FusionPlant平台、阿里巴巴的supET平台等积极推进大企业平台化

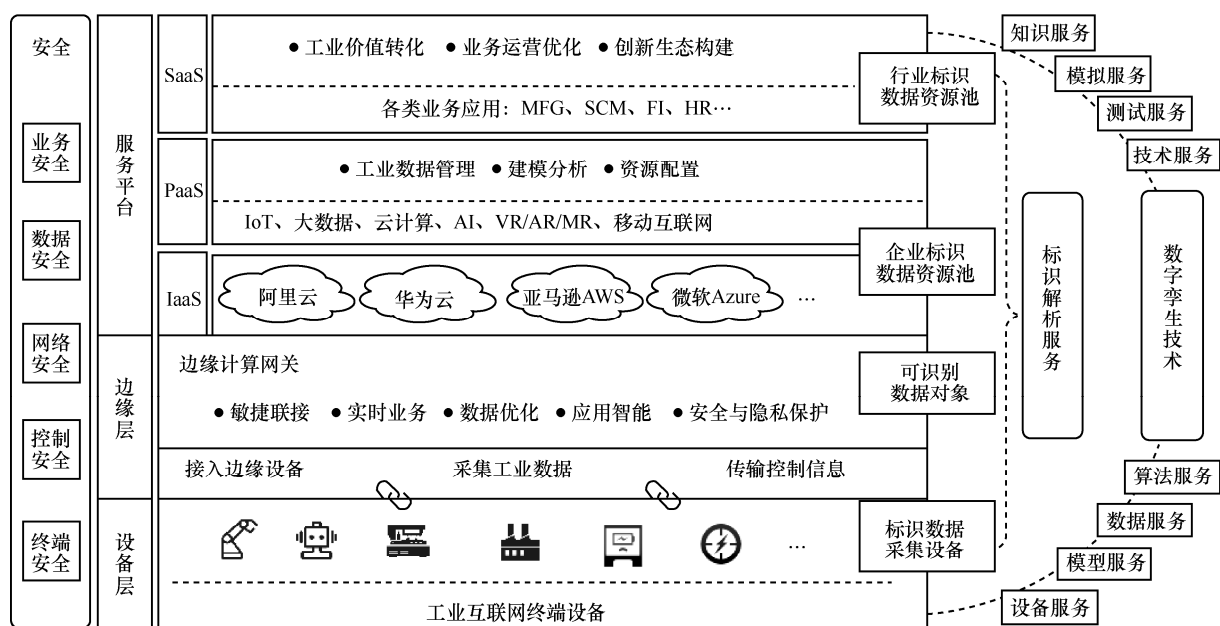


图1 工业互联网平台发展的通用技术框架

转型，用友的“精智”、石化盈科的 ProMACE、东方国信 Cloudiip 平台等助力企业软件云化与工业 App 的应用部署^[3-4]。

根据当前的技术现状及发展趋势，给出如图1所示的工业互联网平台发展的通用框架，主要涵盖标识解析服务、边缘计算网关、数据处理平台、数字孪生技术、计算服务平台等关键技术体系。

3.1 标识解析服务

工业互联网以网络为基础，标识解析服务体系则是网络的基础设施。利用标识编码技术与标识解析技术建立工业互联网中工业设备与标识、地址与标识、内容与标识等之间的映射关系，通过标识控制工业设备、获取和处理工业数据，实现工业智能化^[9-10]。

目前，全球范围内标识解析技术方案种类繁多，包括 GS1、Handle、OID、Ecode、DNS 等。2017 年中国开放对象标识（OID）应用联盟发布了“工业大数据和标识服务平台”。通过提供统一标识解析服务，与各类智能制造企业信息系统进行安全高效对接，实现了各类制造产品的全生命周期信息追溯查询。2018 年 12 月，工业和信息

化部推出以国家顶级节点为核心的工业互联网标识解析体系，探索更为丰富的标识应用场景，推进新型标识体系研制，推进区块链等创新技术在标识解析体系中深度应用。

3.2 边缘计算网关

边缘计算是在靠近物或数据源头的网络边缘侧，构建融合网络、计算、存储、应用核心能力的分布式开放体系。通过就近提供边缘智能服务，降低网络与 IT 资源的消耗，满足工业在敏捷联接、实时业务、数据优化、应用智能、安全与隐私保护等方面的关键需求，解决工业环境中海量异构设备和复杂网络环境带来的问题，解决工业生产的实时性和可靠性问题。

现阶段边缘网关的主流架构为“通用处理器+通用操作系统”，而“专用处理器+通用处理器”混合结构将成为未来的发展趋势，可满足实时控制和数据分析功能，形成边缘数据分析从简单规则向复杂分析延伸，通用化软硬件架构向边缘侧下沉的趋势，并利用虚拟化、软件定义等技术强化工业互联网边缘侧能力。边缘侧的智能化能力是目前业内探索和布局的重点方向。



目前全球范围内,工业互联网边缘计算的发展正处于技术创新的关键期和企业抢占主导权的机遇期^[11-12]。推进工业互联网边缘计算主要有以下三大发力点:持续推进理论技术创新,加速边缘智能、云边协同等核心技术研发;突出应用引领,推动工业互联网边缘计算成熟方案的部署和应用;依托产业联盟,推进技术标准制定与开源软件开发。

3.3 数据处理平台

数据作为工业互联网平台的核心要素,驱动平台业务发展和模式创新改革。全球主要的工业互联网平台都在积极争夺数据资源和数据能力合作,制造企业与平台商、组件商、集成商合作构建合作伙伴关系和生态系统,聚焦工业特色需求,构建海量工业大数据分析体系。区别于传统数字化、网络化、智能化解决方案,工业互联网平台更强调工业数据管控能力,特别是针对工业数据的 3B 问题(隐匿性(below surface)、碎片化(broken)、低质性(bad quality)),强调包括数学、物理、机器学习、控制、人工智能等跨学科的技术融合,亟需高水平的数据模型和大数据分析能力,利用定制化开发、批流融合处理、数据质量控制等进一步提升数据处理效率、读写性能以及支撑生产数据和业务数据的综合分析,提升平台核心竞争力。

3.4 数字孪生技术

数字孪生技术通过数字化的手段,将物理实体映射成数字模型,形成可拆解、可复制、可转移、可修改、可删除、可重复操作的数字镜像,提供建模、分析及行为预测等功能。

数字孪生作为工业互联网平台的知识萃取工具,将工业系统中的碎片化知识传输到工业互联网平台中。数字孪生技术可作为构建数字/虚拟工厂的基础技术,连接组件、装备与生产线并进行系统性的管理,避免碎片化模式,有效融合设计仿真、物联网、虚拟现实等信息技术与工业制造

技术,形成制造与产品设计、智能服务等闭环优化。数字孪生技术衍生出来的服务内涵包括知识服务、模拟服务、测试服务、技术服务、算法服务、数据服务、模型服务、设备服务等。

3.5 计算服务平台

目前,工业互联网平台 IaaS 发展相对成熟,亚马逊 AWS、微软 Azure、阿里云、腾讯云、华为云等占据了全球主要市场。工业 PaaS 建设处于起步阶段,主要以专业性为基础拓展通用性,GE、西门子等信息化水平高的龙头制造企业设备数字化率、联网率具有领先优势。SaaS 正逐步深入制造业细分行业领域,专注专业纵深,中小企业的 SaaS 应用需求最迫切、服务量最大、价值创造最直接。PaaS 赋能 SaaS 平台,提升 PaaS 的成熟度和能力将加速 SaaS 的发展。

4 工业互联网安全挑战

随着工业互联网的不断发展,传统的安全防御技术已无法抗衡新的安全威胁,工业互联网将面临严峻的安全挑战。下面主要介绍终端安全、控制安全、数据安全、业务安全和网络安全五大方面的安全问题^[13-17],具体如图 2 所示。

4.1 终端安全

工业互联网中的终端包括工业领域应用的产品、系统、设备等,传统生产设备安全重点关注物理和功能安全,而随着海量工业互联网设备集成到平台中,传统设备在设计上存在的安全漏洞将直接暴露在网络攻击之下,一旦被攻击,木马病毒将以指数级增长的方式在设备之间传播。另外,多数国家的工业设备依赖于国外先进厂商,没有自主可控的核心技术,存在被境外控制的风险,设备的终端安全问题形势严峻。

设备的安全管理可以从软件与硬件两方面考虑。硬件方面主要体现在以下方面。

(1) 硬件安全增强

针对工业互联网的现场设备,支持基于硬件

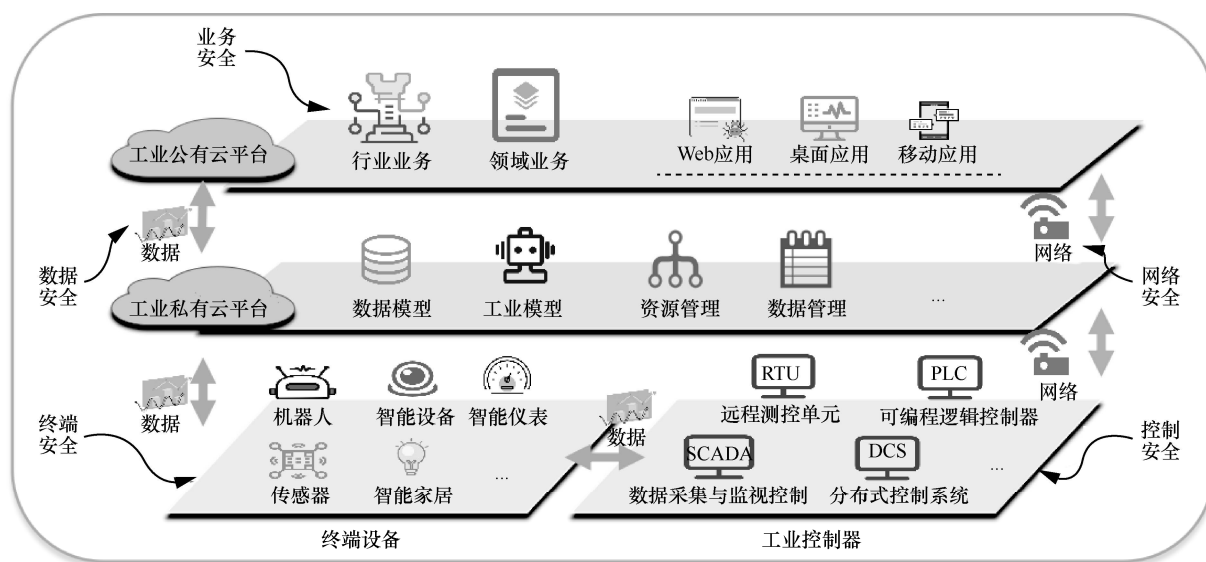


图2 工业互联网平台面临的五大安全挑战

特征的唯一标识符，将硬件级部件作为系统信任根。

(2) 运维管控

工业现场网络重要控制系统部署运维管控系统，实现对外存、键盘和鼠标等使用USB接口的硬件设备的动态智能识别。

(3) 自主可控

加大科研投入，研发自主可控的工业设备。软件安全方面主要体现在固件安全增强、漏洞修复加固、补丁升级管理等方面。

4.2 控制安全

大量的工业物联网设备接入互联网，通过一定的协议与云端服务器进行通信，比较常见的协议有MQTT、AMQP、XMPP等，如果通信过程没有采取加密措施，容易被攻击者截获信息、篡改数据，或者进行中间人攻击，发布伪造的控制指令，导致设备损坏、系统瘫痪等严重后果，需要有效的APT攻击检测和防护手段。

生产控制的安全管理可从控制软件安全、控制功能安全、控制协议安全等方面考虑。控制软件安全主要包括软件防篡改、恶意软件防护、补丁升级更新、安全监测审计。控制功能安全主要包括：确定控制软件与其他设备相互作用可能引

发的危险；考虑自动化、信息化可能导致的安全失控状态；明确操作人员执行操作过程中可能产生的合理可预见的误用以及智能化系统对于人员恶意攻击操作的防护能力。控制协议安全方面则主要包括身份认证约束、访问控制、传输加密、稳健性测试等。

4.3 数据安全

工业互联网数据安全主要包括工厂内部重要的生产管理数据、生产操作数据以及工厂外部数据等各类数据的安全。工业领域业务复杂，工业数据体量大，数据在工厂内外双向流动共享，数据保护难度增大。另外，二次开发服务、个性化定制等服务的延伸也带来用户隐私数据外泄的风险。

数据的安全管理贯穿数据的4个阶段：数据收集、数据传输、数据存储及数据处理。

- 数据收集要遵循合法、正当、必要的原则。
- 数据传输需根据不同的数据类型以及业务部署情况，采用有效手段确保数据传输安全。
- 数据存储涉及访问控制、分级存储加密、备份和恢复等。
- 数据处理则需解决使用授权、数据销毁、



数据脱敏等关键问题。

4.4 业务安全

网络化协同、服务化延伸、个性化定制等新模式打破了传统工控系统相对封闭的业务环境，将业务逻辑暴露在公网中，对工控系统防范非法业务的能力提出了更高要求。

业务安全管理主要考虑业务隔离、协议加密与混淆、配置安全策略、业务监控、人员培训、业务审计等问题。

4.5 网络安全

工业互联网的网络安全威胁来源于工厂内部网络、外部网络及标识解析系统等方面，主要隐患在于网络结构、边界安全、接入认证、通信内容、通信设备、安全监测等的安全防护及管理机制，一般需构筑立体化的防护管理体系。

网络安全防御主要从以下几方面考虑：优化网络结构设计、网络边界安全、网络接入认证、通信和传输保护、网络设备安全防护、安全监测审计。

5 工业互联网安全趋势

5.1 工业互联网安全的技术创新

(1) 密码技术

利用标识密码技术对工业互联网设备进行加密认证，确认身份后建立数据加密通道，同时研究密码的轻量级实现，降低设备身份认证的时间消耗。针对工业互联网的体系架构，通过统一可信的密钥安全管理中间服务层，实现与应用系统或第三方认证服务的无缝集成。

(2) 人工智能

利用人工智能技术进行状态检测与报警、故障诊断及远程运维、预测性维护等设备安全管理；进行身份识别、安全穿戴、行为识别等员工安全管理；进行异常预警、事故预测等设备安全管理；进行危险源识别、环境监测等环境安全管理。人工智能赋能工业互联网安全，助力制造业转型升级^[18]。

(3) 区块链

区块链技术可利用去中心化存储策略，将设备安全信息存放到网络节点中，同时将流程管理信息以云端开放的方式分而治之，将工业软件与云平台结合，依托云平台实现端到端直连、网络节点互联、数据互为备份，避免工业数据被恶意篡改，从而有效控制产品质量。利用区块链的加密技术、共识算法、可信身份认证技术、P2P 技术，有效保障工业设备终端安全、数据安全和网络安全^[19-21]。

(4) 隐私保护

利用隐私保护技术，加强对工业设备数据的防护，实现对工业设备数据的脱敏与混淆，防止隐私泄露引发的恶意攻击、网络犯罪，保证工业互联网的数据安全。技术方案上可以采用安全多方计算 SMC、分布式匿名化数据加密技术在数据挖掘过程中隐藏敏感数据；采用限制发布的技术有选择地发布原始数据、不发布或者发布精度较低的敏感数据，保证对敏感数据及隐私的披露风险在可容忍范围内；采用差分隐私方法量化和评估隐私保护水平。

(5) 数据驱动安全

利用工业设备传感器等大量采集工控设备数据。利用大数据平台，构建工业设备的威胁感知中心、智慧分析系统。采集内部的各类数据和日志，收集外部的各类威胁情报，将其相互关联，运用大数据和人工智能技术，从多维度中分析、发现、判断、挖掘潜在的安全问题和风险，实现工业设备的系统安全。

5.2 工业互联网“泛安全”保障框架

本文提出如图 3 所示的“泛安全”保障框架，以“人”“工控系统”“信息系统”为三要素，打造工业互联网应用层、数据层、服务层融合的“泛安全”可信环境。

研究工业互联网应用层、数据层、服务层的多源异质异构数据融合、面向人机物协同环境的

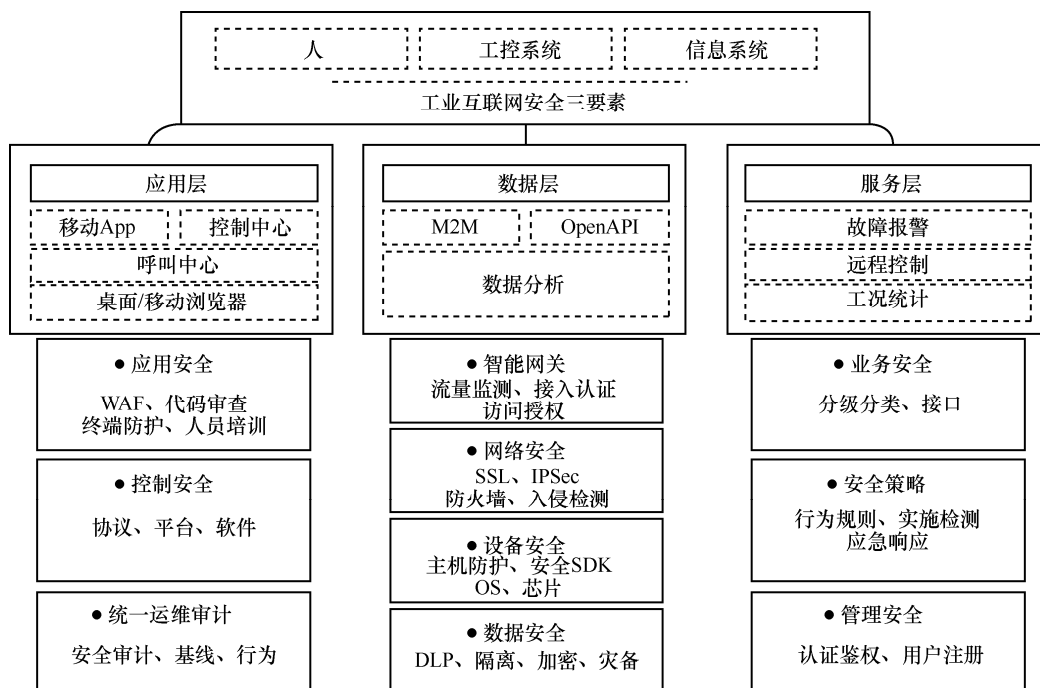


图3 工业互联网“泛安全”保障框架

跨领域数据的一体化表示表征机理、面向不确定条件下的多源时空数据融合及时序模式挖掘方法、可解释的异常检测和态势预测方法、信息物理融合系统的安全知识模型、数据模型双驱动的安全态势感知等关键技术，为面向工业互联网“人”“工控系统”“信息系统”融合的安全防御提供决策依据。

工业互联网“泛安全”保障框架建立涵盖终端安全、控制安全、数据安全、业务安全和网络安全的多层次工业互联网安全保障体系，构建工业互联网全产业链数据安全管理体系和数据流动管理机制，加强数据收集、存储、处理、转移、删除等环节的安全防护能力。同时，可推动安全技术手段建设，督促工业互联网相关企业落实网络安全主体责任，引导企业提升自身安全防护能力。鼓励相关产业联盟整合行业资源和创新服务模式，开展工业互联网安全试点示范，为建设国家级工业互联网安全技术提供有效支撑。

6 结束语

工业互联网平台建设是一项具有前瞻性、融合性、基础性、全局性的重大系统工程，工业互联网安全技术则是重中之重的基础保障。未来，应当充分认识工业互联网平台安全的重要性和特殊性，通过落实工业互联网“泛安全”保障计划，着力增强网络安全技术能力，在保障安全的前提下，大力推进工业系统中的各种元素与传感器技术、高级计算、深度分析、互联网深度融合，重构工业格局，提升生产力，实现实体经济数字化转型，为制造业的“弯道超车”提供重要保障。

参考文献：

- [1] 王俊文. 未来工业互联网发展的技术需求[J]. 电信科学, 2019, 35(8): 26-38.
WANG J W. Technical requirement of future industrial internet[J]. Telecommunications Science, 2019, 35(8): 26-38.
- [2] ZHANG J, HUANG S, WANG Y J. Future internet: trends and challenges[J]. Frontiers of Information Technology & Electronic Engineering (English), 2019(9): 1185-1194.



- [3] 前瞻产业研究院. 2020 年工业互联网发展现状与趋势分析[EB]. 2020.
Prospective Industrial Research Institute. Analysis on the development status and trend of industrial Internet in 2020[EB]. 2020.
- [4] 全球工业互联网大会. 全球工业互联网平台创新发展白皮书 (2018-2019) 摘要版[R]. 2019.
Global Industrial Internet Conference. Abstract edition of white paper on innovation and development of global industrial internet platform (2018-2019) [R]. 2019.
- [5] 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(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(3): 68-76.
- [6] 陶耀东, 李强, 李宁. 工业互联网的安全挑战及应对策略[J]. 中兴通讯技术, 2016, 22(5): 36-41.
TAO Y D, LI Q, LI N. Security challenges and countermeasures of the industrial internet[J]. ZTE Technology Journal, 2016, 22(5): 36-41.
- [7] REHMAN M H U, AHMED E, YAQOOB I. Big data analytics in industrial IoT using a concentric computing model[J]. IEEE Communications Magazine, 2018, 56(2).
- [8] MOURATIDIS H, DIAMANTOPOULOU V. A security analysis method for industrial internet of things[J]. IEEE Transactions on Industrial Informatics, 2018(14).
- [9] 任语铮, 曾诗钦, 霍如, 等. 新型工业互联网标识解析体系探讨与实践[J]. 信息通信技术与政策, 2019(8): 74-77
REN Y Z, ZENG S Q, HUO R, et al. Discussion and practice of new industrial internet identity analysis system[J]. Information and Communications Technology and Policy, 2019(8): 74-77
- [10] 杨震, 张东, 李洁, 等. 工业互联网中的标识解析技术[J]. 电信科学, 2017, 33(11): 134-140.
YANG Z, ZHANG D, LI J, et al. Identifier technology in industrial internet[J]. Telecommunications Science, 2017, 33(11): 134-140.
- [11] LI Z, ZHOU X, QIN Y Y. A survey of mobile edge computing in the industrial internet[C]//Proceedings of 2019 7th International Conference on Information, Communication and Networks (ICIN). Piscataway: IEEE Press, 2019.
- [12] SATHYADEVAN S, ACHUTHAN K, DOSS R, et al. Protean authentication scheme—a time-bound dynamic keyGen authentication technique for IoT edge nodes in outdoor deployments[J]. IEEE Access, 2019: 92419-92435.
- [13] 刘晓曼, 李艺, 吴昊. 工业互联网安全架构及未来发展思考[J]. 保密科学技术, 2019, 102(3): 14-21.
LIU X M, LI Y, WU H. Industrial internet security architecture and future development[J]. Secrecy Science and Technology, 2019, 102(3): 14-21.
- [14] WANG Z, HU H, CHENG G. Design and implementation of an SDN-enabled DNS security framework[J]. China Communications, 2019, 16(2): 233-245.
- [15] 郭贺铨. “互联网+”行动计划：机遇与挑战[J]. 人民论坛·学术前沿, 2015(10): 6-14.

WU H Q. The “Internet Plus” action plan: opportunities and challenges[J]. People’s Forum·Academic Frontiers, 2015(10): 6-14.

- [16] 张云勇. 5G 将全面使能工业互联网[J]. 电信科学, 2019, 35(1): 1-8.
ZHANG Y Y. 5G will fully enable the industrial internet[J]. Telecommunications Science, 2019, 35(1): 1-8.
- [17] 国务院. 关于深化“互联网+先进制造业”发展工业互联网的指导意见[R]. 2017.
The State Council. Guidance on deepening the development of industrial internet in the “internet+ advanced manufacturing industry”[R]. 2017.
- [18] TIAN W, HAO L, WEI J J, et al. MTES: an intelligent trust evaluation scheme in sensor-cloud-enabled industrial internet of things[J]. IEEE Transactions on Industrial Informatics, 2020(16).
- [19] ALI M S, VECCHIO M, PINCHEIRA M. Applications of blockchains in the internet of things: a comprehensive survey[J]. IEEE Communications Surveys & Tutorials, 2019(21).
- [20] HUANG J Q, KONG L H, CHEN G H, et al. Towards secure industrial IoT: blockchain system with credit-based consensus mechanism[J]. IEEE Transactions on Industrial Informatics, 2019(15).
- [21] DI PIETRO R, SALLERAS X, SIGNORINI M, et al. A blockchain-based trust system for the internet of things[C]//Proceedings of 23rd ACM on Symposium on Access Control Models and Technologies (SACMAT). Piscataway: IEEE Press, 2018: 77-83.

[作者简介]



蒋融融 (1979—), 女, 浙江广播电视大学副教授, 北京航空航天大学计算机学院访问学者, 主要研究方向为网络安全。



翁正秋 (1981—), 女, 温州职业技术学院副教授, 浙江工业大学计算机科学与技术学院博士生, 主要研究方向为数据安全与大数据技术。



陈铁明 (1978—), 男, 浙江工业大学计算机科学与技术学院教授、博士生导师, 主要研究方向为网络空间安全、大数据分析。