中国科学: 技术科学 2024 年 第 54 卷 第 10 期: 2042 ~ 2052
SCIENTIA SINICA Technologica techcn.scichina.com
《中国科学》杂志社 SCIENCE CHINA PRESS

进 展

工业互联网层级架构与安全: 复杂网络新视角

吕金虎[1,2*], 任磊[1,2], 谭少林[1], 赖李媛君[1,2], 孔宇升[1], 王雅哲[1]

1. 中关村实验室, 北京 100094;
2. 北京航空航天大学自动化科学与电气工程学院, 北京 100191
* E-mail: jhlu@iss.ac.cn

收稿日期: 2023-10-16; 接受日期: 2024-01-05; 网络版发表日期: 2024-10-09
国家重点研发计划(编号: 2022YFB3305600)和国家自然科学基金(批准号: T2322023, 61621003, 62141604)资助项目

摘要 工业互联网是新一代信息技术与制造业深度融合的产物. 通过构建人-机-物全面互联的新型工业制造平台, 工业互联网正快速推动着传统工业生产与服务模式朝向数字化、网络化、智能化方向变革与发展. 本文从多层级动态异构复杂网络的视角, 系统阐述制造业工业互联网的层级架构与系统安全. 具体地, 通过详细分析工业制造过程中设备层、产线层、企业层与跨企业层的核心功能组件及其关键技术, 阐明传统工控系统与新一代工业互联网之间的联系与区别. 特别地, 本文将从新型末端设备的智能防护接口、弹性自愈合工控网络、IT/OT跨域信任传递与异常检测、工业数据流通保护与溯源等几个方面, 聚焦工业互联网安全的关键技术与挑战.

关键词 工业互联网, 云网边端, 智能制造, 工控系统, 数据保护

1 引言

工业制造是现代工业生产的核心环节, 通过将原材料或零部件转化为成品, 服务于汽车、电子、纺织等各类关系国计民生的制造行业. 科技的进步推动着工业制造技术的快速发展. 众所周知, 工业制造的发展进程已经经历了三大显著变革的历史阶段: 从18世纪末19世纪初以蒸汽机为代表的机械化时代, 到19世纪末20世纪初以电力与内燃机为代表的电气化时代, 再到20世纪末21世纪初以计算机控制为代表的信息化时代. 随着数字技术和人工智能的蓬勃发展, 物联网、大数据、云计算和人工智能等新兴技术正在不断涌现[1~6], 工业制造正经历新一轮技术变革, 朝向更加高效、灵活、协同的数字化、网络化、智能化时代迈进[7~10].

工业互联网是建设新一代高端制造体系的关键基础设施. 通过互联网、物联网等先进信息技术与工业制造技术深度融合, 工业互联网旨在构建工业制造过程中人、机、物要素的全面互联, 并基于规模化数据、先进算力与智能化算法, 形成覆盖全产业链、全价值链的新型工业网络协同制造与服务体系[11~13]. 工业互联网被誉为产业效率提升倍增器. 据GE工业互联网白皮书分析, 产业效率每提高1%将创造万亿美元级的GDP增量. 而据欧盟预测, 未来15年20%~30%的生产效率提升将由工业互联网带来[14].

工业互联网是数字经济和实体经济深度融合的关

引用格式: 吕金虎, 任磊, 谭少林, 等. 工业互联网层级架构与安全: 复杂网络新视角. 中国科学: 技术科学, 2024, 54: 2042–2052
Lü J H, Ren L, Tan S L, et al. Hierarchical architecture and security of Industrial Internet: A new perspective from complex network (in Chinese). Sci Sin Tech, 2024, 54: 2042–2052, doi: 10.1360/SST-2023-0323

键底座, 是新型工业化的战略性基础设施. 国际上各主要发达国家均发布了相应的工业战略, 将工业互联网作为国家发展长期战略. 例如, 德国提出了工业4.0计划, 推动企业打造以信息物理融合系统为核心的智能制造与智能管理系统; 美国发布了先进制造伙伴计划, 提出建立先进制造基础设施与国家制造创新网络; 日本形成了互联工业愿景, 宣布推进“通过连接人、设备、技术等实现价值创造的互联工业”[15~17].

我国也高度重视工业互联网发展. 从2017年提出深入实施工业互联网创新发展战略以来, 工业互联网已连续六年写入政府工作报告. 当前, 我国工业互联网平台连接设备超过7900万台设备, 工业互联网产业规模突破1.2万亿元. 工业互联网网络、标识、平台、安全体系得到了快速的部署与建设, 有效推进了工业生产制造朝向柔性化、定制化、智能化、绿色化模式转型升级[18,19].

制造工业互联网由传统工业控制系统(industrial control systems, ICS)(简称工控系统)发展而来, 通过将互联网与协同制造理念与技术融入工控系统中, 形成设备互联互通、数据高效流转、生产智能协同的产品制造过程. 当前, 工业互联网技术体系尚处于快速发展过程中的初级阶段, 面临着工业生产设备种类繁多、通信协议不统一; 工业数据复杂多样、数据治理共享难; 生产管理层级化、智能决策层级低等困境. 为了厘清工业互联网发展脉络、当前现状以及未来机遇挑战, 本文基于多层级动态异构复杂网络视角[2~6], 重新审视制造业工业互联网云网边端的体系架构, 阐述各层主要结构与功能, 并着重分析其中存在的安全性风险与挑战, 为进一步构建安全可控的工业互联网协同技术体系提供系统原型与总体框架参考.

2　新一代制造工业互联网

新一代制造工业互联网是工控系统与互联网的有机结合体. 其中, 工控系统是工业生产自动化的核心基础. 通过对传感器、执行器、控制器等各类自动化及其管理系统的软硬件集成, 工控系统可以实现对工业设备、生产线及其工艺过程的自动化控制与检测[20]. 而工业互联网在工控系统的基础上, 通过融入新型数据采集、通信、存储、计算等要素, 实现工业设备之间、设备与系统之间的信息交互和智慧运维. 工业互联网是新一代工业生产制造系统数字化、网络化、智能化转型升级的关键载体, 对于帮助单个企业层甚至整个社会层面生产效率的提升、成本的降低、产品质量的提高以及创新能力的增强至关重要, 有力推动工业生产制造和服务体系新生态的形成与发展.

本节对比性地概述基于传统工控系统架构模型形成的新一代制造工业互联网体系架构.

2.1　制造工业互联网层级架构

传统工控系统架构模型是指用于组织和布局工控系统各个组件、功能和层次的一种结构模式. 它用于描述工控系统中各组件的功能以及不同组件之间的连接关系与信息流动, 已达到组件分工明确、系统灵活可扩展、功能可靠稳定、数据流动共享、确保安全性与隔离性等目的. 其中最为典型的工控系统架构模型是由普渡大学于1990年提出的分层控制系统模型, 通常称为普渡模型[21]. 如图1所示, 普渡模型将工控系统划分为L0~L4等5层.

随着工业互联网相关理念与技术的快速发展, 从不同的视角切入衍生出了多种类型的体系架构. 例如, 美国工业互联网联盟从商业、使用、功能、实现等4个视角界定了工业互联网模型, 侧重于跨行业的通用性与互操作性. 德国工业4.0则从业务层级、生命周期与价值流以及物理层次结构等3个维度, 构建了工业互联网的三维架构模型, 更加侧重于信息物理融合系统的核心特征. 我国工业互联网产业联盟分别在2016年与2019年发布了《工业互联网体系架构1.0》与《工业互联网体系架构2.0》, 从业务指南、功能架构、实施框架与技术体系等4个方面概述了工业互联网体系架构.

下面从一个前瞻性角度, 基于“云网边端”的一体化架构设计思路, 将工业互联网视为一个具有多层复杂网络结构的协同控制系统. 如图1所示, 其架构模型从下至上分为设备层、产线层、企业层、跨企业层等4部分.

(1) 设备层. 对应于普渡模型的现场设备层. 传统工控系统中的现场设备层主要包括各种生产过程相关的传感器、调节器、执行器等. 用于对现场设备以及生产过程的运行数据进行采集, 并基于上层控制信号, 执行相应生产操作. 而工业互联网架构中的设备层扩展地对应云网边端系统的端层, 指生产现场的各类新

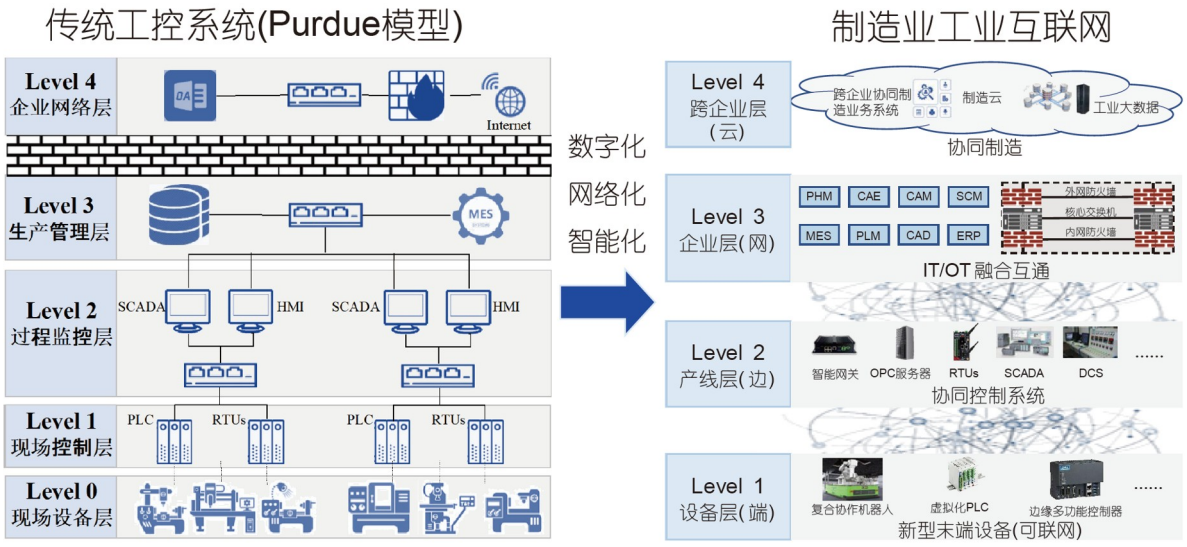

图 1 (网络版彩图)复杂网络视角下的工业互联网层级架构(Copyright©1994, Elsevier)[21]

Figure 1 (Color online) Hierarchical architecture of Industrial Internet from the perspective of complex networks (Copyright©1994, Elsevier) [21].

型工业末端设备，包括复合协作机器人、虚拟化可编程逻辑控制器(programmable logic controller, PLC)、智能传感器、边缘多功能控制器、机械臂、搬运车等. 这些设备贯穿整个产品生产的生命周期, 起到采集数据、实时响应、执行动作等功能. 随着物联网以及微型计算机技术的发展，这些末端设备将被赋予端对端互联以及本地计算的能力，依托智能协同算法，进而实现异构设备的协同作业.

(2) 产线层. 对应于普渡模型的现场控制层和过程监控层. 传统工控系统现场控制层负责对工业生产的各类现场设备，如开关阀、电机、机械臂、传送带、反应炉、传感器等，进行操作与控制. 通过底层传感器所反馈的现场数据，并利用预先编写的控制程序，生产相应的控制信号对底层执行设备进行操控. 根据生产过程类型，该层主要由集散控制系统或可编程逻辑控制器，以及远程终端等组件构成，通过工业总线与现场设备层相连；而过程监控层主要负责对工业产生过程的工艺和设备进行实时监测与控制. 通过对底层所采集的数据进行存储与分析，并基于数据可视化功能，实现对生成过程及其设备状况的监测、诊断等功能. 该层主要由数据采集分析及可视化，以及人机交互界面等软硬件组成，通过工业以太网与现场控制层设备连接.

在工业互联网架构中，产线层融合了上述两层功能，扩展地对应云网边端系统的边缘层，涵盖智能网关、OPC服务器、远程终端单元(RTU)、监控与数据采集系统(supervisory control and data acquisition, SCADA)、集散控制系统(DCS)等组件. 产线层通过对来自不同设备的工业数据进行分析整理，来监测设备层的运行状态并进行调控. 通过边缘计算与智能模块的部署，快速挖掘工业数据的价值，将能够以较低延迟实现突发事件的响应，提高制造过程的灵活性与可靠性. 同时，该层将压缩后的工业数据信息上传至更上一层, 并接受上层指令, 对设备资源进行调度分配.

(3) 企业层. 对应于普渡模型的生产管理层和企业网络层. 传统工控系统中生产管理层负责具体的生产过程和操作控制. 依据所接收的来自企业网络层的生产计划，将其转化为可执行的任务序列. 具体功能包括生产调度管理、产品工艺与质量管理、设备管理、制造过程数据管理等. 该层主要由企业内部数据库以及生产信息化管理系统构成，通过企业内网与下层数据采集与过程控制设备相连. 而企业网络层作为控制系统的最顶层主要负责整个企业的管理与决策. 它与市场需求、供应链网络、能源电力等外部环境以及企业自身战略定位密切相关，基于这些信息进行生产规划、资源分配以及商业决策等. 该层主要由一些能够与企业外网相连的办公自动化系统以及企业资源规划系统等组件构成，并通过企业网络防火墙在企业内外

网之间构建安全防护屏障.

在工业互联网架构中，企业层上升到云网边端系统的网络层，涵盖了生产设计(CAD)、制造执行系统(manufacturing execution system, MES)、企业资源规划(enterprise resource planning, ERP)系统、故障预测与健康管理(PHM)等应用组件. 通过运用企业层级的计算资源、数据资源、存储资源以及网络资源，对整个企业的各类资源进行调度安排，实现生产过程的动态管理, 提高生产效率, 保障系统安全.

(4) 跨企业层. 由于传统工控系统集中于企业内部计划到生产设备的分层管理, 因此, 不具备跨企业协同能力. 而工业互联网架构组织形成了跨企业层级, 由云网边端系统中云服务层体现，主要由跨企业协同制造业务系统、制造云、工业大数据、供应链网络、能源系统等组件构成. 跨企业层打破传统企业界限, 通过市场数据、行业企业运营数据、供应链数据的共享，实现资源与需求的合理高效配置；保障产品可溯源、企业资源优势互补，避免过度竞争；形成产品定制化、制造服务化的商业性模式.

为了满足工业互联网中工业大数据的采集与传输、生产制造过程的实时响应与控制以及数字孪生的新型应用需求，传统工控系统的网络通信技术也在不断革新. 在我国, 5G+工业互联网是着重推广的产业模式. 5G通信技术的高速率、低时延、大连接与高可靠性等优势，能够满足工艺场景中高速、可靠和低时延的数据传输与智能化应用需求，但同时也对工业互联网的网络安全、隐私保护、技术与设备兼容提出了新的挑战[22~24].

综上所示，新一代制造工业互联网是在传统基于普渡模型的工控系统基础上，不断通过网络化、智能化、数字化升级，逐步演化形成云网边端的层级架构, 且各层级构成部件之间也通过数据传输、控制指令等形式交互关联. 具体地, 在端层, 工业互联网具有大量不同类型的新型末端设备，包括智能传感器、摄像头等数据采集装置，射频信号读写器、定位装置等物联网设备，以及工业机器人等，以满足现代复杂工业制造系统的全方位信息感知与柔性协同作业需求. 在边缘层，工业互联网部署了边缘计算与智能模块，通过轻量化智能模型实时挖掘工业数据的价值，规避了数据集中式处理带来的响应延误，提高制造过程的灵活性与可靠性. 在网络层，工业互联网依托工业以太网、5G、Wi-Fi等多种接入方式构成泛在网络，将生产运营技术(OT)层面的异构智能设备与信息技术(IT)层面的网络环境连接起来，打破传统制造过程中的数据孤岛，实现全方位数据循环与流通. 最后，在云层，工业互联网通过构建数字化资源管理系统，将传统工业软件云化并不断开发汇聚各类工业APP，实现生产制造流程的数字化智能化管控.

如果将工业互联网中各设备以及组件视为一个控制节点，那么整个工业互联网的体系结构可以抽象为一个多层复杂网络协同控制系统[25]. 在每一层以及各层级之间的控制节点通过对应的通信网络相连，实现数据与指令的传输. 图2展示了设备层的人-机-物交互网络结构图. 该多层复杂网络协同控制系统具有几个典型的特征: (1) 异构性, 各控制节点对应不同的设备或功能组件、连边之间的信道类型也可能各不相同; (2) 动态性, 根据业务类型以及设备状态, 对应复杂网络的结构在不断切换; (3) 非对称性, 网络结构中的连边双向关系不对等，如上层节点可以对下层节点进行控制, 而下层节点只能向上层传输数据; 同时, 根据设备之间互操作性自由度不同，同一层级之间的链路双向关系也可能不对等. 这为工业互联网结构与功能分析增加了新的困难.

2.2　制造工业互联网关键技术

新型通信与计算组件的融入为工业生产制造过程

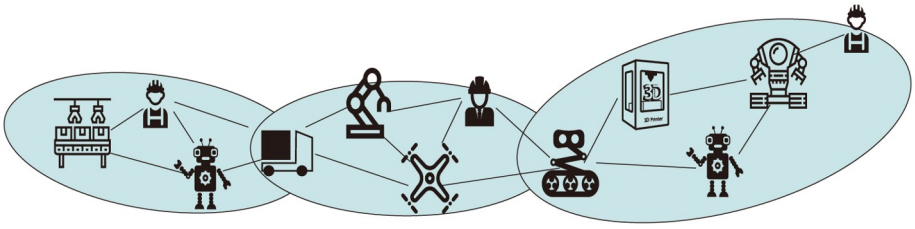

图 2　(网络版彩图)设备层的人-机-物交互网络拓扑示意图

Figure 2　(Color online) Illustration of the interaction network topology in the plant floor.

中的人机物互联互通、全产业链与价值链服务体系构建提供了关键基础设施，也形成了一个包含多个层级的工业互联网复杂网络，横向联通人机物料法环工业生产全要素，纵向联通云端-边缘端-工业终端多个层次. 工业互联网在推动生产制造智能化、协同化、个性化、服务化等产业新生态的同时，也对其形成的复杂网络系统的管理控制、设备的运行维护技术提出了新的挑战. 下面就工业互联网设备层、产线层、企业层与跨企业层, 分别阐述其中最核心的关键技术.

(1) 人机物交互技术. 人机物交互是指在人工、机器与物料之间建立紧密的交互网络，通过智能协同与信息共享，来实现制造过程中人-机-物的高效交互与协作，提升生产过程的性能与效率，保障生产作业安全. 随着机器视觉、触觉、听觉等多方面智能感知与反馈技术的发展，人-机、机-机、机-物等二元交互技术得到了快速发展. 通过设计物理交互(传感器+控制器)以及信息交互(数据+决策)规则，来进行动作规划与行为学习，实现双向适应与协调. 然而随着复杂集群作业环境中人-机-物要素的不断增加，简单的二元交互模式亟需向复杂的集群交互模式拓展，以完成大规模复杂生成任务[26,27]. 基于端对端通信网络，发展智能自主的分布式集群交互技术，实现多样异构设备的分工合作与安全作业，是未来制造工业互联网设备层的核心技术.

(2) 边缘计算技术. 边缘计算技术是指在靠近设备端部署存储与计算资源, 对数据进行分析与处理, 来减少数据传输带来的延迟，提高突发事件响应速度[28,29]. 边缘计算作为云计算的互补，能够有效解决传统云计算模式下的数据传输延迟、带宽瓶颈以及隐私安全等问题. 边缘计算是结合了数据采集传输、大数据计算、人工智能与自动控制等多个领域先进技术的综合性应用技术. 边缘端设备与云端设备和新型异构工业终端设备的动态互联，形成了更加复杂的多层网络结构. 由于工业互联网所面向的工业制造过程的特殊性, 如何平衡云端和边缘端的计算特性实现大规模智能计算，如何通过边缘端设备实现分布式工业现场的快速监控，如何实现人工智能模型轻量化压缩与数据分布计算以支持边缘端对工业终端的实时响应与控制，以及如何组织边缘端设备对大规模工业终端进行多维度数据传输、转发和监控，是工业互联网边缘计算技术面临的新的挑战. 在具有高噪声、强干扰、动态性强和不稳定性强的复杂网络环境下，工业边缘设备连接上层云端设备和底层工业终端设备的协同管控、平衡传输、实时计算技术，是未来工业互联网产线层的核心技术.

(3) IT/OT融合技术. IT/OT融合是指将信息技术(IT)与生产运营技术(OT)相结合，从而形成从工业生产过程到信息的传输处理，再到工业生产过程的数据流动闭环，推动企业销售、研发、调度、运维等各项业务流程的互联互通，提升企业智能决策水平. 然而, IT与OT网络通常具有不同的技术架构与标准. 一方面, 两者的融合互通需要解决技术兼容性问题，以确保各种组件之间能够进行通信和数据交换[30]. 例如，IT与OT系统涉及的数据源和数据格式通常不同, 为了保障数据一致性、互操作性和可理解性，需要建立标准化的数据标识与解析标体系. 另一方面，两个复杂网络的动态融合依赖异构网络节点的安全链接、动态路由和多路交互, 如何维持IT/OT融合复杂网络的连通性、稳定性和时效性，是工业互联网企业层亟需发展的核心技术.

(4) 智能协同制造技术. 智能协同制造是指制造全生命周期过程中生产全要素、供应链和产业链的动态协同, 主要通过将各类信息进行数字化, 通过大数据分析与智能决策算法，实现不同制造环节与参与方之间的紧密协作，共同优化并完成产品设计、生产计划、供应链管理、生产制造与服务等各个过程，以实现整体生产效率的提升和资源的最优利用[31]. 协同过程的智能化主要体现在人工智能技术的应用方面，即通过人工智能技术对产品物料、生产工艺要求、供应链上下游乃至设备本身的性能状态进行分析和推理，使得整个制造系统或部分设备具有自主决策能力. 而制造的协同主要体现多层次复杂网络中海量节点针对不同任务的组合运行模式，主要体现在任务的合理分工与协助以及资源的匹配与适应性等方面，通过复杂网络分析算法和智能优化算法的结合，实现任务的有效执行和资源节点的均衡运行与稳定交互. 从工业互联网复杂网络的视角，智能协同制造技术不仅关联生产过程全要素，进一步关联了跨企业供应链上下游关联关系，是在生产过程自动化基础上进一步融入数字化与智能化的重要技术，对于推动重要装备和定制化产品工艺创新、缩短产品研发周期，形成全新的智能制造模式具有核心支撑作用.

工业互联网及其核心技术体系将工业产生过程中的设备、传感器、计算机系统, 以及互联网等要素进行有机融合, 构建起一个数字化、网络化、智能化的工业生态系统. 工业互联网在构建全新生产制造和服务体系, 为高质量发展和供给侧改革提供支撑的同时, 也打破了传统工业环境相对封闭可信的状态, 形成了一个包含多层异构资源、多维生产要素和多模态数据信息的复杂网络. 这样的复杂网络在信息流、物流、人流的动态交互下, 具有极高的受攻击风险. 因此, 除了上述关键技术之外, 工业互联网安全技术是工业互联网发展的根本保障.

2.3　复杂网络新视角

在工业互联网中, 各类设备、传感器、控制系统、生产设施、软件系统之间, 通过数据通信、控制指令、状态反馈等连接关系, 形成了一个异构、动态、多层级的复杂网络结构. 复杂网络相关理论与方法能够为工业互联网这一复杂信息物理融合系统的理解、分析与优化提供新的工具. 下面从工业大数据深度融合、规模化边缘设备协同控制以及工控网络脆弱性分析与防御等三个典型场景, 分析复杂网络理论方法在工业互联网中的应用.

工业大数据深度融合. 工业大数据深度融合是指将工业生产中所产生的大规模、多源、高维度的数据与深度学习技术相结合, 以实现更高效、智能的工业生产和管理. 工业制造现场存在大量传感器、监控设备等组成的数据采集系统, 用以收集各类设备、产品以及生产环境等各方面数据. 这些数据来源不同、模态不同、结构不同, 但相互之间并不孤立, 而是通过内在的关联关系相互影响相互补充, 呈现出复杂网络式的层次结构特征. 通过将工业生产中各类数据抽象为图数据形式, 其中节点代表生产设备、传感器、边缘模块等元素. 边代表它们之间的物理连接、数据通信等关联关系, 构建适应工业图数据的图神经网络模型, 如图卷积网络、图注意力网络、图自编码器等, 能够在集成节点属性与网络拓扑结构的基础上, 对工业系统中的复杂关系进行学习与推理, 从而实现对工业数据的有效表征与精准分析. 一些典型的任务包括: (1) 故障诊断, 该问题为节点任务, 通过对相邻节点数据的聚合与分析, 对其中若干节点的运行状态进行判定, 预测该节点的标签(如正常或异常); (2) 数据对齐, 该问题为边层级任务, 不同节点对应的数据采集周期、时空基准不尽相同, 通过图神经网络模型挖掘不同节点数据之间的时空以及逻辑关联性, 实现相邻感知信息之间的数据对齐; (3) 健康评估, 该问题为图层级任务, 需要对各个节点数据进行汇聚融合, 评估整个工业制造系统的健康程度, 为工业生产管理提供更科学、更精细的决策依据.

规模化边缘设备协同控制. 规模化边缘设备协同控制是指在工业互联网边缘计算环境中, 多个边缘设备之间通过协同工作, 共同完成复杂的制造任务. 随着工业制造流程的不断发展和优化, 现代工业制造需要大量的终端设备来实现对生产流程的精细化高效化控制, 而这些设备之间的协同控制则是其核心问题. 由于工业边缘设备多样异构、边缘设备间耦合结构复杂, 对其中单个设备的行为控制将影响相邻其他设备的运行状态, 因此需要构建工业生产制造流程的多层级复杂网络建模方法、研究复杂工控网络牵制鲁棒控制技术, 通过边缘设备之间的通信与数据共享, 构建分布式协同控制算法, 实现对多个边缘设备的高效精准控制. 此外, 网络化控制能够提高工业生产系统的可靠性. 一方面, 通过采用网络滤波和攻击重构技术, 基于状态估计、攻击重构和弹性控制等技术方法, 结合复杂网络系统动力学模型, 构建基于状态估计的攻击信号识别与阻断, 对系统运行状态实时估计与补偿, 提高控制策略的稳健性; 另一方面, 基于复杂网络拓扑结构的冗余保护与动态优化机制, 通过增加系统备用节点和冗余路径, 并对控制系统节点进行动态切换与负载优化, 提高工控网络的容错能力和可用性, 避免单个设备故障或通信中断对于系统稳定性和可靠性的影响.

工控网络脆弱性分析与防御. 工控网络是指工控系统中由监控、数据采集、生产控制等各类设备连接构成的网络. 单个设备或模块出现故障后, 通常能够影响相邻设备的运行, 形成连锁式故障传播. 因此, 通过将工控网络抽象为复杂网络模型, 能够为分析工控网络的脆弱性并进行针对性防御, 提供新的技术路径. 首先, 在关键风险点位挖掘方面, 复杂网络理论中的各类节点中心度量, 包括度中心性、介数中心性、接近中心性、特征向量中心性等, 以及一些基于动力学过程的关键节点识别方法, 能够为工控网络中风险点位的评估提供启发式方法; 其次, 在故障传播路径识

别方面, 通过利用复杂网络可视化工具, 能够清晰展示故障传播路径, 同时复杂网络边中心性的相关度量, 也能够为评估工控网络中各个链路的重要性; 最后, 在工控网络结构优化方面, 通过构建网络拓扑结构与功能之间的关联关系, 探索连通度、直径、异质性、无标度等网络拓扑特征对于工控网络性能的影响, 并基于组合优化方法优化工控网络的结构. 在工控网络安全防御方面, 通过布局工控蜜罐、设备隐藏等相关技术, 改变工控网络拓扑结构, 构建有效防御措施, 确保生产系统的安全和稳定运行.

3 工业互联网安全

随着工业互联网的飞速发展, 其面临的安全威胁日益严峻, 针对工业互联网的攻击与破坏事件频发. 据中国信息通信研究院发布的《2020年上半年工业互联网安全态势报告》统计, 仅2020年上半年发现的针对我国工业互联网的恶意网络攻击行为就高达1.356×10^7次, 涉及企业达2039家. 工业互联网是现代化生产制造的核心组成部分, 其安全性直接关系生产过程的稳定运行甚至现场工人的人身安全, 一旦发生安全攻击, 影响十分严重. 安全问题成为制约工业互联网发展的关键因素.

3.1 安全内涵的多面性

工业互联网是一类典型的信息物理融合系统, 其安全内涵包括物理安全、信息安全以及功能安全等多方面[32~34]. 其中, 物理安全是指工业互联网中的基础物理设施, 包括传感器、执行器、网络通信设备的安全, 防止非法负访问恶意修改物理设备的控制功能或劫持操控物理设备, 造成设备停机损毁等破坏性行为. 物理安全是工业互联网安全与传统互联网安全的核心区别. 由于工业互联网的兴起, 越来越多的工业设备、传感器、执行器等连接到网络中, 形成了互联互通的工业物联网系统. 对工业互联网系统中的物理设备和区域实施严格的访问控制和身份验证机制, 并通过安装视频监控、入侵检测和报警系统等设备, 对工业互联网系统的物理环境进行实时监控, 是保护物理设备和基础设施的安全的重要措施.

信息安全是指工业互联网系统中数据与信息的安全, 防止未经授权的访问、篡改、泄露与破坏, 保障数据信息的隐私性、完整性与可用性. 随着工业互联网中IT/OT技术的深度融合, 打通了工业制造系统内部各组件以及与系统外部之间的信息屏障, 工业数据在整个系统中流动共享, 工业数据的价值得以利用和体现. 但是工业互联网在解除传统工业系统中数据孤岛困境的同时, 也对其信息防护带来了新的挑战. 通过对数据进行加密和访问控制, 设计防火墙和安全网关, 实施威胁检测与分析, 是提高工业互联网数据与信息安全的常用措施.

功能安全是指工业互联网中设备与组件关键功能的安全性, 防止局部故障导致的系统性功能失效溃崩, 保障工业生产的可靠性持续性. 工业互联网通过网络化技术将工业生产中的设备与要素紧密连接起来, 在促进数据流动的同时, 也增加了系统组成部分的耦合性, 从而增加了局部故障不断传导, 导致整个系统停机停产的可能性. 加强安全设计与验证, 设计故障监测与诊断机制、并通过冗余机制提供系统故障容忍与恢复能力, 是确保工业互联网在存在故障条件下的关键功能安全性的有效措施.

3.2 关键防护技术

与传统信息技术领域的网络攻击相比, 工业互联网攻击针对工控系统、工业网络及其相关设备展开, 攻击方法更加隐蔽多样, 影响能够持续传导. 攻击者基于目标系统生产过程的业务逻辑, 精心设计攻击策略, 并通过信息域、物理域或者两者融合的手段入侵, 利用工业制造系统的耦合关系和业务逻辑不断扩散, 达到窃取数据、操控设备以及破坏生产的目的.

下面分别从工业设备安全、工控系统安全、IT/OT融合网络安全以及工业大数据安全等4个层面, 分别阐述制造工业互联网亟待突破的关键防护技术.

(1) 智能防护接口. 智能防护接口是指基于人工智能与机器学习等技术, 用于检测和防御工业末端设备各类网络攻击的接口. 该技术属于设备层级的安全防护措施. 通过深度学习等相关算法, 对自身和相邻设备运行状态数据以及南向网络流量进行实时分析, 实现对各种类型网络攻击检测与识别, 自动触发相应的安全决策与响应机制, 根据网络环境动态调整防御策略, 并提供实时的安全监控与报告功能.

(2) 弹性自愈合工控网络. 弹性自愈合工控网络是一种具备自愈合和弹性适应能力的工业控制网络, 能

够在面对故障、攻击、环境变化等异常情况下，自动检测问题并采取措施进行恢复和调整，确保系统的稳定运行和性能优化. 该技术属于产线层级的安全防护措施，要求控制网络能够通过实时检测和分析网络状态，自动检测故障、攻击等异常事件，并进行快速的故障诊断与定位；同时当网络中节点或连接受到攻击时，能够通过重新配置资源、调整控制策略等方式，重新构建控制网络，抑制故障的扩散；此外，为了增强控制网络的可靠性，通常需要采用容错与冗余设计机制，确保故障发生后能够快速地阻断和恢复.

(3) 跨域信任传递与异常检测. 跨域信任传递是指在工业互联网不同安全域之间建立信任传递关系，以解决不同安全域之间的身份验证和访问授权问题，能够简化用户身份验证流程，提高系统之间的互操作性、确保信息交换与资源访问安全. 同时，建立实时的控制流持续监测与分析机制，快速识别异常访问链路，实现IT/OT跨域传输的攻击行为方法与治理，构建跨域融合的边界防护功能. 该技术属于企业层级的安全防护措施.

(4) 数据流通保护与溯源. 数据流通保护与溯源是指确保工业生产制造过程中数据的安全性和隐私保护，同时能够追溯数据的流动路径和使用情况. 该技术属于跨企业层级的安全防护措施. 通过对工业互联网中数据流动特征进行学习与挖掘，发展数据流通共享泄露威胁预警、敏感数据智能识别保护、数据流动异常监测及泄露溯源技术，防止数据泄露和滥用，增加数据的可信度，提高用户对数据流通的信任度.

近年来，随着工业互联网安全需求日益迫切，面向工业互联网安全的攻防博弈理论与方法也得到了快速的发展[35~38]. 首先，基于工业互联网信息物理深度融合的特性，一些新型的信息物理协同异常检测与防御方法被提出来. 例如，文献[39]为工控系统设计了基于物理水印的数据认证机制，来探测数据完整性. 其次，基于工业互联网高度互联的特性，若干新型的基于复杂网络的脆弱性分析与风险识别方法被提出来. 例如，文献[40]分析了网络化线性控制系统的入侵关键节点以及最优监测节点布局；文献[41]提出了基于网络重构的攻击检测方法，并通过控制链路的主动切换，来实现网络控制系统主动防御功能. 最后，基于工业互联网快速发展变化的特性，不少基于深度学习的大数据侦查与应急处置技术被提出来. 例如，文献[42]提出了一个深度神经网络架构来对网络攻击进行识别和分类；文献[43]则基于图神经网络，对工控网络节点的脆弱性进行聚类分析.

安全场景的攻防对抗往往极具策略性，攻击者通过精心策划采取高度优化的攻击方式，来最大化破坏性；而防御者需要充分考虑这些策略性攻击行为，并在有限的安保资源下，进行针对性的防御布局，以最大化安保效能. 工业互联网安全场景具有其特殊性. 工业互联网具有“融”的特性，它由网络空间的信息技术与物理空间的制造技术融合交互形成，对其进行攻防分析，不仅要考虑单一的网络空间与物理空间攻防，更重要的要考虑由物理与信息空间融合带来的增益反馈. 其次，工业互联网具有“连”的特性，它由大量分层异构的功能组件，通过物理或网络线路连接，构成一个统一的协同运行的整体，对其进行攻防分析，不仅要考虑单一功能组件的资产价值及入侵风险，更重要的要考虑该组件失效后所带来的级联效应. 最后，工业互联网具有“变”的特性，其物理构成会随着产业或服务的发展不断延伸，其核心技术会随着通信技术、云计算、大数据等技术的发展不断进步，同样地，潜在攻击者所能使用的攻击手段也会不断地发展，对其进行攻防分析，不仅要考虑单阶段对策，更重要的要考虑防御技术的不断学习与演进.

4　应用与展望

工业互联网通过物联网、大数据、云计算等技术手段，将生产设备、生产过程以及企业内外的各种资源进行互联与信息化，来实现生产系统自动化、智能化和高效化. 目前，工业互联网在企业生产与供应链运营管理等场景取得了有效的应用. 在工业生产方面，通过采集分析产品全生命周期内中的人、机、物、环等关键数据，助力产品设计、工艺优化、质量管理溯源；在供应链协同方面，通过汇聚供应链网络各品类数据，实现产品精准配送、库存管理和生产安排，形成现代化智慧供应链体系；在设备运维方面，通过对系统关键设备与操作的监测，助力工控生产过程的“可视化”，实现工控系统健康状态的态势感知，保障基础设施安全；在能源管理方面，通过对用能设备海量工业数据的采集与挖掘，实现生产能耗的在线监控与优化，提高设备运行效率，助力企业绿色低碳发展[44~46].

工业互联网使得工业大数据的价值与潜能得以释放. 但要充分发挥工业互联网在柔性化定制化生产、协同化服务化制造等新兴工业模式中的作用, 还存在诸多理论技术瓶颈亟待突破, 包括工业互联网组织结构的动态优化方法、面向柔性化生产的弹性控制与智能决策算法以及全产业链价值链的网络协同调控技术等. 同时随着工业互联网应用广度与深度不断拓展, 其安全问题的重要性也更加突出. 当前, 由西门子、施耐德等国外厂商生产的工控系统相关软硬件在我国占比较高, 其通信协议的不可见性和不可控性极大地增加了工业互联网防御难题. 未来, 除了不断发展新的防御技术之外, 工业生产设备的国产化也刻不容缓.

参考文献

1 Misra S, Roy C, Mukherjee A. Introduction to Industrial Internet of Things and Industry 4.0. Boca Raton: CRC Press, 2021

2 Liu K X, Wu L L, Lü J H, et al. Finite-time adaptive consensus of a class of multi-agent systems. Sci China Tech Sci, 2016, 59: 22–32

3 Wang X, Gu H B, Wang Q Y, et al. Identifying topologies and system parameters of uncertain time-varying delayed complex networks. Sci China Tech Sci, 2019, 62: 94–105

4 Fu Z, Yu W W, Lü J H, et al. A distributed normalized Nash equilibrium seeking algorithm for power allocation among micro-grids. Sci China Tech Sci, 2021, 64: 341–352

5 Lv J, Ran M, Wang C, et al. Manned/unmanned aerial vehicle intelligent cooperation: Opportunities and challenges (in Chinese). Sci Sin Tech, 2024, 54: 968–978 [吕金虎, 冉茂鹏, 王成才, 等. 有人/无人机智能协同: 机遇与挑战. 中国科学: 技术科学, 2024, 54: 968–978]

6 Zhang M, Lü J H, Bai Z D, et al. Improving the initialization speed for long-range NRTK in network solution mode. Sci China Tech Sci, 2020, 63: 866–873

7 Karnik N, Bora U, Bhadri K, et al. A comprehensive study on current and future trends towards the characteristics and enablers of Industry 4.0. J Ind Inf Integrat, 2022, 27: 100294

8 Meindl B, Ayala N F, Mendonça J, et al. The four smarts of Industry 4.0: Evolution of ten years of research and future perspectives. Tech Forecasting Soc Change, 2021, 168: 120784

9 Castelo-Branco I, Oliveira T, Simões-Coelho P, et al. Measuring the fourth industrial revolution through the Industry 4.0 lens: The relevance of resources, capabilities and the value chain. Comput Industry, 2022, 138: 103639

10 Li J Q, Yu F R, Deng G, et al. Industrial Internet: A survey on the enabling technologies, applications, and challenges. IEEE Commun Surv Tutorials, 2017, 19: 1504–1526

11 Ciano M P, Dallasega P, Orzes G, et al. One-to-one relationships between Industry 4.0 technologies and lean production techniques: A multiple case study. Int J Product Res, 2021, 59: 1386–1410

12 Pivoto D G S, de Almeida L F F, da Rosa Righi R, et al. Cyber-physical systems architectures for Industrial Internet Of Things applications in Industry 4.0: A literature review. J Manuf Syst, 2021, 58: 176–192

13 Culot G, Nassimbeni G, Orzes G, et al. Behind the definition of Industry 4.0: Analysis and open questions. Int J Product Econom, 2020, 226: 107617

14 Annunziata M, Evans P C. The Industrial Internet Work. General Electric White Paper, 2013

15 Sisinni E, Saifullah A, Han S, et al. Industrial Internet Of Things: Challenges, opportunities, and directions. IEEE Trans Ind Inf, 2018, 14: 4724–4734

16 Lee J, Bagheri B, Kao H A. A cyber-physical systems architecture for Industry 4.0-based manufacturing systems. Manuf Lett, 2015, 3: 18–23

17 Wang J, Xu C, Zhang J, et al. A collaborative architecture of the industrial internet platform for manufacturing systems. Robot Comput-Integr Manuf, 2020, 61: 101854

18 Wei Y Y, Chai X D. Industrial Internet: Technologies and Implementation (in Chinese). 2nd ed. Beijing: Publishing House Electronics Industry, 2021 [魏毅寅, 柴旭东. 工业互联网: 技术与实践. 第2版. 北京: 电子工业出版社, 2021]

19 Zhou X, Song M, Cui L. Driving force for China's economic development under Industry 4.0 and circular economy: Technological innovation or structural change? J Cleaner Product, 2020, 271: 122680

20 Zhang P. Advanced Industrial Control Technology. Oxford: Elsevier Inc., 2010

21 Williams T J. The Purdue enterprise reference architecture. Comput Ind, 1994, 24: 141–158

22 Neumann P. Communication in industrial automation—What is going on? Control Eng Pract, 2007, 15: 1332–1347

23 Pereira C E, Neumann P. Industrial communication protocols. In: Nof S, ed. Springer Handbook of Automation. Berlin: Springer Handbooks, 2009

24 Silva M, Pereira F, Soares F, et al. An overview of industrial communication networks. In: Flores P, Viadero F, eds. New Trends in Mechanism and Machine Science (Vol 24). Cham: Springer, 2015

25 Lü J H, Tan S L. Games and Evolutionary Dynamics on Complex Networks (in Chinese). Beijing: Higher Education Press, 2019 [吕金虎, 谭少林. 复杂网络上的博弈及其演化动力学. 北京: 高等教育出版社, 2019]

26 Tan S, Wang Y, Vasilakos A V. Distributed population dynamics for searching generalized Nash equilibria of population games with graphical strategy interactions. IEEE Trans Syst Man Cybern Syst, 2022, 52: 3263–3272

27 Tan S, Fang Z, Wang Y, et al. Consensus-based multipopulation game dynamics for distributed Nash equilibria seeking and optimization. IEEE Trans Syst Man Cybern Syst, 2023, 53: 813–823

28 Zhang T, Li Y, Philip Chen C L. Edge computing and its role in Industrial internet: Methodologies, applications, and future directions. Inf Sci, 2021, 557: 34–65

29 Qiu T, Chi J, Zhou X, et al. Edge computing in Industrial Internet of Things: Architecture, advances and challenges. IEEE Commun Surv Tutorials, 2020, 22: 2462–2488

30 Ghobakhloo M, Iranmanesh M. Digital transformation success under Industry 4.0: A strategic guideline for manufacturing SMEs. JMTM, 2021, 32: 1533–1556

31 Choo K K R, Gritzalis S, Park J H. Cryptographic solutions for Industrial Internet-of-Things: Research challenges and opportunities. IEEE Trans Ind Inf, 2018, 14: 3567–3569

32 Wei Q, Wang W H, Cheng P. Industrial Internet Security: Architecture and Defence (in Chinese). Beijing: China Machine Press, 2021 [魏强, 王文海, 程鹏. 工业互联网安全: 架构与防御. 北京: 机械工业出版社, 2021]

33 Li Y, Shi D, Chen T. False data injection attacks on networked control systems: A stackelberg game analysis. IEEE Trans Automat Contr, 2018, 63: 3503–3509

34 Wang W, Han Z, Liu K, et al. Distributed adaptive resilient formation control of uncertain nonholonomic mobile robots under deception attacks. IEEE Trans Circuits Syst I, 2021, 68: 3822–3835

35 Zhu C, Rodrigues J J P C, Leung V C M, et al. Trust-based communication for the Industrial Internet of Things. IEEE Commun Mag, 2018, 56: 16–22

36 AL-Hawawreh M, Moustafa N, Sitnikova E. Identification of malicious activities in Industrial Internet of Things based on deep learning models. J Inf Security Appl, 2018, 41: 1–11

37 Wu Y, Dai H N, Tang H. Graph neural networks for anomaly detection in Industrial Internet of Things. IEEE Internet Things J, 2022, 9: 9214–9231

38 Li X, Niu J, Bhuiyan M Z A, et al. A robust ECC-based provable secure authentication protocol with privacy preserving for Industrial Internet of Things. IEEE Trans Ind Inf, 2018, 14: 3599–3609

39 Wazirali R, Ahmad R, Al-Amayreh A, et al. Secure watermarking schemes and their approaches in the IoT technology: An overview. Electronics, 2021, 10: 1744

40 Ghosh S, Bhatnagar M R, Saad W, et al. Defending false data injection on state estimation over fading wireless channels. IEEE Trans Inform Forensic Secur, 2021, 16: 1424–1439

41 Xiong W, Gong K, Wen G, et al. Security analysis of discrete nonlinear systems with injection attacks under iterative learning schemes. IEEE Trans Syst Man Cybern Syst, 2022, 52: 927–935

42 Amanullah M A, Habeeb R A A, Nasaruddin F H, et al. Deep learning and big data technologies for IoT security. Comput Commun, 2020, 151: 495–517

43 Almiani M, AbuGhazleh A, Al-Rahayfeh A, et al. Deep recurrent neural network for IoT intrusion detection system. Simul Model Pract Theor, 2020, 101: 102031

44 Compare M, Baraldi P, Zio E. Challenges to IoT-enabled predictive maintenance for Industry 4.0. IEEE Internet Things J, 2020, 7: 4585–4597

45 Aazam M, Zeadally S, Harras K A. Deploying fog computing in Industrial Internet of Things and Industry 4.0. IEEE Trans Ind Inf, 2018, 14: 4674–4682

46 Khalil R A, Saeed N, Masood M, et al. Deep learning in the Industrial Internet of Things: Potentials, challenges, and emerging applications. IEEE Internet Things J, 2021, 8: 11016–11040

Hierarchical architecture and security of Industrial Internet: A new perspective from complex network

LÜ JinHu[1,2], REN Lei[1,2], TAN ShaoLin[1], LAI LiYuanJun[1,2], KONG YuSheng[1] & WANG YaZhe[1]

[1] *Zhongguancun Laboratory, Beijing 100094, China;*
[2] *School of Automation Science and Electrical Engineering, Beihang University, Beijing 100191, China*

Industrial Internet is the product of deep integration between new-generation information technology and the manufacturing industry. Through constructing a new type of industrial manufacturing platform for human-cyber-physical networks, the Industrial Internet is rapidly driving the transformation and development of manufacturing mode towards digital, networked, and intelligent formulation. From a forward-looking perspective, this paper aims to systematically elaborate the hierarchical architecture and system security of manufacturing Industrial Internet based on the theory and methods of complex network cooperative control systems. In detail, the differences between traditional industrial manufacturing systems and Industrial Internet will be discussed from the aspects of key functional components and their core technologies at the device, production line, enterprise, and cross-enterprise levels, respectively. Furthermore, the paper also highlights key technologies and challenges of Industrial Internet security, including intelligent protection interfaces for new terminal devices, resilient self-healing industrial control networks, IT/OT cross-domain trust transmission and anomaly detection, industrial data circulation protection and traceability.

Industrial Internet, cloud computing architecture, intelligent manufacturing, industrial control system, data proection

doi: 10.1360/SST-2023-0323