“人工智能+工业信息安全”初探

Research on AI + Industrial Information Security

程　媛[1]，余文科[1]，宫玲琳[2]（1. 中国电子学会，北京 100036；2. 中国电力科学研究院有限公司，北京 100085）
Cheng Yuan[1]，Yu Wenke[1]，Gong Linglin[2]（1. Chinese Institute of Electronics，Beijing 100036，China；2. China Electric Power Research Institute Co.，Ltd.，Beijing 100085，China）

摘　要：
近年来，工业控制系统展现出新型发展态势，面对日益严重的工业信息安全威胁，从我国工业信息系统发展现状与存在的主要问题出发，剖析人工智能技术架构与产业结构，对“人工智能+工业信息安全”的解决方案进行研究，提出基于人工智能的应用场景，保护工业领域的信息安全，保障工业生产的安全、稳定。

关键词：
人工智能；工业控制系统；信息安全；技术架构
doi：10.12045/j.issn.1007-3043.2019.04.020
中图分类号：TN915.08
文献标识码：A
文章编号：1007-3043（2019）04-0090-03

Abstract：
Industrial control systems have shown a new development trend in recent years. Faced with the increasingly serious threats of industrial information security，starting from the current situations and problems of the industrial information system，the technical and industrial structure of AI is analyzed，the solution of "AI + industrial information security" is studied，and the application scenario based on artificial intelligence is proposed to protect the information security in the industrial field and ensure the safety and stability of industrial production.

Keywords：
AI；Industrial control system；Information security；Technical architecture

引用格式：程媛，余文科，宫玲琳. “人工智能+工业信息安全”初探[J]. 邮电设计技术，2019(4)：90-92.

0 引言

近年来，以美国、德国、中国、日本为首的世界各国都在加速布局工业发展的新战略。在工业领域快速发展的同时，工业系统的网络化、信息化和智能化带来了一系列网络安全问题，全球重大网络事故已为各国带来了巨大的损失，工业信息安全发展至关重要。工业信息安全涉及到工业控制系统的各个环节，包括公共系统的安全、工业互联网的安全、工业大数据的安全、工业云服务的安全、工业电子商务的安全以及基础设施的安全等，它直接关系到了社会经济的发展稳定。

收稿日期：2019-03-07

1 工业信息安全发展态势

2006年，美国提出《美国竞争力计划》，最早将信息物理系统列为重要的研究项目，各国给予了高度重视，先后提出相应发展战略规划。2012年，美国提出《工业互联网计划》，力图利用工业大数据带动工业革命和网络革命两大革命性转变。2013年，德国提出《“工业4.0”战略》，开展以智能制造为主导的第4次工业革命。2015年，我国提出《中国制造2025》，提出成为制造强国的“三步走”战略以及十年行动纲领。同年，日本提出《机器人新战略》，大力发展日本机器人产业，支持工业智能化。伴随着工业系统的快速发展以及工业系统的信息化、智能化，系统的安全隐患也日益突出，市场普及的机器人、物流仓储控制系统、数

控加工系统、PLC控制系统、DCS系统等智能制造系统极容易遭到网络攻击，虚拟空间信息重构技术为智能制造带来沉浸性和预知优化等功能的同时，也暴露了位置、要素、参数等隐私，并易于传播僵尸网络病毒，云服务监测平台也面临着网络攻击、物理篡改攻击等危险。

当前我国工业信息化快速发展，传统制造业与工业企业都在寻求外部协同。市场对工业系统的升级改造、设计算法与方案提出了更高的要求。目前，工业控制系统的整体方案主要是基于传统的工业防火墙、旁路异常检测、安全态势的基础层到服务层和管理层的分层次的解决方案，缺乏体系化的标准和制度的构建，市场迫切需要展开全面的标准化体系建设。

2 人工智能

2.1 关于人工智能

人工智能的概念最早在1956年的达特茅斯会议上被提出，根据中国电子技术标准化研究院在2018年1月最新发布的《人工智能标准化白皮书》，人工智能的定义是：为利用数字计算机或者数字计算机控制的机器模拟、延伸和扩展人的智能，感知环境、获取知识并使用知识获得最佳结果的理论、方法、技术及应用系统。

近年来，人工智能产业发展迅速，全球各国均在利用人工智能技术占领新一轮科技发展的制高点，人工智能快速发展的主要归因于3点：其一，随着云计算、物联网和大数据技术的日趋完善，市场为人工智能提供了丰富的数据资源，提高了算法与学习的有效性；其二，随着后摩尔时代的到来，计算技术硬件成本降低，运算时间大幅缩短，提高了人工智能的效率；其三，基础硬件、算法和平台的更迭降低了人工智能的错误率，大幅提升了AI算法的准确性与有效性。

2016年5月国家发展改革委、科技部、工业和信息化部、中央网信办制定了《推出“互联网+”人工智能三年行动计划》，2017年7月，国务院印发《新一代人工智能发展计划》，同年12月工信部推出《促进新一代人工智能产业发展三年行动计划》，2018年，北京、上海、重庆陆续出台人工智能产业支持政策，可以看出国家正在快速布局人工智能。国家近年来密集地出台了人工智能相应的行动规划，人工智能的加入将工业体系的发展提高到了新的层次。

2.2 人工智能体系

人工智能是我国新一代信息技术的核心之一，是推动科技变革和产业变革的重要抓手，目前我国人工智能技术体系已经逐步形成，如图1所示。

图1　人工智能技术体系逐步形成

基于数据、计算系统技术和芯片的基础性技术持续突破，各行业百花齐放，边缘智能技术快速突破，产学研用联盟共同开发，算法理论、开发平台、开发框架与应用软件日趋完善，产业链正在形成，融合应用成效突出。在制造、交通、医疗、安防、教育、金融、家居领域成效显著。与此同时，我国人工智能产业也存在发展不均衡的现象，基础支撑层特别是芯片领域短板明显，与国外先进技术仍有5~10年的技术差距。在软件算法层面，技术创新速度与应用配套速度不匹配，偷换概念现象明显，人工智能标准欠缺，产业协同创新的局势尚未形成。人工智能当前处于依赖海量数据样本的有监督学习阶段，未来将以海量数据驱动模型学习、以认知仿生驱动类脑计算。在行业应用层面，产业链上下游环境建设尚不健全，仍存在较多问题与挑战。

3 人工智能在工业信息安全的应用

工业信息系统已经历了5个阶段的演进，如图2所示，从最初的孤立封闭向协同开放的互联网架构发展。在应用端，生产厂家不仅仅局限于工业机械化，而开始转向智能化、互联网化和生态化的综合管理体

图2　工业信息系统演进

系，一定程度上希望实现逻辑隔离，实现工业设计网与生产网的双向互联。供应商需要将“向制造企业销售机械设备”转变为“向制造企业提供服务”，通过数据分析和配套智能体系帮助制造企业提高收益。安全产品要具备流内容解析、态势感知与行为预测等数据与场景双驱动的防护能力。现有的国家法规、措施、技术和产品无法完全满足这样的要求，研究人员亟需基于现有的基础状态和发展趋势，提出改进措施，实现工业设计网和工业生产网之间的互联。

人工智能虽然为工业信息安全系统的发展带来了问题与挑战，但也为其升级提供了新的解决思路。工业信息安全与人工智能结合，主要以数据驱动模型为主，在进行工业防护的过程中利用人工智能技术在各个防护阶段进行学习，构建系统核心算法、开发框架以及相应的工业信息环境的识别、理解和交互的应用软件。通过纵向结合，促进产业链的深层次融合，ICT供给能力将产生质的飞跃。人工智能与信息安全的横向结合贯穿消费到生产全产业链，助推实体经济的网络化、数字化、智慧化发展。人工智能在工业信息安全领域得到了初步应用，包括内容分析、态势感知、行为预测等诸多方面。

a）基于人工智能的安全域隔离：截至2017年，超过10万个工业信息系统接入互联网，工业信息系统利用人工智能技术，可以有效利用大规模工业数据，实时监测系统面临的网络攻击，分析网络安全态势，检测恶意代码，减少工业控制系统误报等问题。

b）基于深度学习的智能异常检测：工业信息系统的良性运行离不开异常检测与处理，利用深度学习技术，可以挖掘跨协议相关性，分析内外部网络流量中海量元数据之间的相关性，对可能指示恶意活动的异常流量进行检测，实现异常与常态间的分类识别。

c）基于内容分析的信息集成系统：工业信息系统累计了大量的信息源与数据源，将多个信息源之间的内部日志和具有外部威胁情报服务的监视系统的信息进行集成，对其中高度相关的事件进行自动分类与梳理，可以显著提高安全运营中心的运营效率，增加数据的利用率，减少时延。

d）基于自主学习的漏洞预测与防护：针对工业信息系统中各类风险，可以结合深度学习以及强大的数据库分析能力，开发智能化事件响应系统，当遭受攻击时，系统能够识别切入点，修补漏洞，优化安全防护体系，进行漏洞预测、风险拦截与精准响应，减少企业的损失。

4 结语

综上所述，基于人工智能的工业控制系统因其智能化、虚拟化、数字化以及实时性等特点，能够更加高效地识别工业信息系统风险，隔离网络攻击，预警系统漏洞，监测异常信息，减少系统误报，梳理工业数据，加强系统效率，降低维护成本，减少企业损失，快速满足企业与行业的定制化需求，有着较好的应用前景。

人工智能在给工业控制系统和工业信息安全带来更多技术上的变革的同时，也存在着众多安全隐患。在人工智能2.0时代，应正视风险，理性看待人工智能的发展与应用。进一步发展和完善人工智能技术，才能将人类引入更加光明和幸福的未来。

参考文献：

[1] 王喜文. 图解工业4.0的核心技术——信息物理系统(CPS)[J]. 物联网技术，2017，7(4)：4-5.
[2] 张雷. 人工智能时代下的信息安全[J]. 电子技术与软件工程，2019(2).
[3] 王涵彬. 人工智能技术在网络安全领域的应用思考[J]. 通讯世界，2019，26(2)：69-70.
[4] 张滨. 人工智能在安全领域的应用[J]. 电信工程技术与标准化，2018，31(12)：1-6.
[5] 张建晓. 我国工业控制信息安全现状及其对策探析[J]. 信息与电脑(理论版)，2018(22)：212-213.
[6] 孙鸿宇，何远，王基策，等. 人工智能技术在安全漏洞领域的应用[J]. 通信学报，2018，39(8)：1-17.

作者简介：
程媛，工程师，硕士，主要研究方向为新一代信息技术等相关领域；余文科，高级工程师，博士，主要研究方向为新一代信息技术等相关领域；宫玲琳，工程师，硕士，主要研究方向为电网调度自动化软件测试相关领域。