

工业互联网时代的 PLC 发展趋势研究

原崇蛟, 郭肖旺, 贡春燕

(中电智能科技有限公司, 北京 102209)

摘要: 近年来, 工业互联网、物联网、智能制造等发展趋势迅猛, 工业控制领域呈现出新型工业业态模式。在新业态模式下, PLC 在设备通信、控制、数据采集等功能上得以提升。通过与云计算、大数据、5G、AI 等新技术结合, 实现与“智能制造”的融合, PLC 将发展成为一种可编程智能终端, 推动制造生产控制系统的自动化, 进而助推工业企业的信息化、智能化进程。针对当前 PLC 技术特点和市场现状进行了分析, 对新业态模式下 PLC 发展路线进行了研究, 提出 PLC 核心技术体系、先进制造能力、产业生态协作三方面发展思路, 为我国自主安全 PLC 产业发展研究提供了支撑。

关键词: 工业互联网; 智能制造; PLC; 可编程智能终端

中图分类号: TP314

文献标识码: A

DOI: 10.19358/j.issn.2097-1788.2022.05.003

引用格式: 原崇蛟, 郭肖旺, 贡春燕. 工业互联网时代的 PLC 发展趋势研究[J]. 网络安全与数据治理, 2022, 41(5): 16-21.

Research on PLC development trend in industrial Internet era

Yuan Chongjiao, Guo Xiaowang, Gong Chunyan

(Intelligence Technology of CEC Co., Ltd., Beijing 102209, China)

Abstract: In recent years, as the industrial Internet, the Internet of Things and intelligent manufacturing develop rapidly, industrial control field presents a new pattern of industrial forms. Under the mode of new formats, the PLC function in communications equipment, control and data acquisition was improved. By combining with cloud computing, big data, 5G, AI and other new technologies, it realizes the integration with “intelligent manufacturing”. PLC will develop into a programmable intelligent terminal, promote the automation of manufacturing control system, and then boost the information and intelligent process of industrial enterprises. In this paper, the current technical characteristics and market status of PLC are analyzed, and the development route of PLC under the new format mode is studied. The development ideas of PLC core technology system, advanced manufacturing ability and industrial ecological cooperation are proposed, which provides support for the development of China's independent security PLC industry.

Key words: industrial Internet; intelligent manufacturing; PLC; programmable intelligent terminal

0 引言

在风电、水电、石油、管网等国家关键基础设施领域, 以及电子设备、汽车、电器、食品、医药、专用设备制造、化学原料及制品等智能制造领域, PLC 控制系统正得到大量应用, PLC 控制系统成为工业自动化领域的“关键大脑”“神经中枢”。随着工业互联网、云计算、人工智能、大数据等新技术的发展和运用, 工控系统从“相对封闭”加速走向“开放互联”。

工控系统为五层结构, 从底向上依次为现场设

备层、控制层、监控层、管理层、决策层。设备层是执行层, 具有通信和控制能力, 一般不具备或只具备简单的智能; 控制层是一系列具有可编程能力的智能终端, 包括 PLC、DCS、FCS、RTU、运动控制器、HMI 等, 具有可编程、高可靠、强实时、多连接等特性; 监控层部署工业软件; 管理层通过 5G、OPC UA 等通信技术, 实现整个工业系统的纵向贯通, 实现数据的互联互通; 决策层通过云计算、大数据、5G、AI 等新技术融合, 提供智能分析、协同管理等决策能力。本文重点分析控制层可编程终端的发展, 未

来发展进程中,PLC 控制系统也会在智能制造时代中向着安全可信、自主自控、智能化方向发展^[1],通过与新技术的融合,PLC 将发展成为新一代的可编程工业智能终端。

1 技术发展趋势

细数工业控制系统发展过程,工业生产自 1952 年由传统电气控制转为模拟信号为主的单 PID 控制,1985 年进入现场总线为主的集散控制,发展到如今工业以太网为主的协同控制,已基本实现工业数据集成和数字化、信息化建设。在当前工业互联网时代,工业生产面临管控范围扩大、接入点规模增加、智能总线信号比例提升、高级算法算力需求难以满足等新挑战。下一阶段工业生产将建设面向多种控制需求的新型网络架构以及工业数据复合应用平台,最终实现智能控制。在智能控制中,因具备高性价比、高可靠性、高易用性特点,PLC 通过加入分布式 I/O、嵌入式智能、无缝通信等升级,得到了性能的提升和形态的改进。通过工业软件赋能,PLC 将以工业智能终端的形式继续活跃在工业自动化领域中。

随着 IT 技术的发展,PLC 的性能指标从速度转向安全性、可靠性、运动控制、实时通信、数据处理、流程优化、故障诊断等更加综合的指标^[2]。本文分析 PLC 在工业互联网时代的发展趋势,其技术发展特点总结为可编程、高可靠、强实时、多连接、高安全和智决策六个方面,如图 1 所示。

1.1 可编程:协同处理能力、软件定义能力

软件是信息系统技术与工控系统技术快速融合发展的支撑,工业软件分为两个类型:嵌入式软

件和非嵌入式软件。嵌入式软件是嵌入在控制器等设备中的软件,具有采集、控制、通信等功能;非嵌入式软件是装在通用计算机或者工业控制计算机之中的设计、编程、工艺、监控、管理等软件^[3]。工业互联网和智能制造推动了工业软件的快速发展,通过工业软件实现 PLC 的软件定义、增加多系统之间的协同处理能力,增强其灵活性,通过工业网络采集到大量的现场数据,在云平台集中强大的计算能力进行大数据分析,提升和优化生产效率,使得控制系统越来越智能化。

2020~2021 年中国频繁发布多项政策支持工业软件方面的发展和应用,力争尽快补齐工业软件技术短板,可以预见工业软件产业在“十四五”期间将迎来快速发展。根据“十四五”规划和 2035 年远景目标纲要,积极稳妥发展工业互联网、加快补齐基础软件等瓶颈短板成为“十四五”时期的主要任务之一^[4]。

1.2 高可靠:连续无故障稳定运行、适应复杂环境

工业控制系统对 PLC 的可靠性有较高的要求,一般 PLC 控制器的使用寿命在 15~20 年^[5],且在使用过程中基本不停机,其平均故障间隔时间长,故障修复时间短。随着硬件技术的进步,PLC 采用严格的工艺制造过程,在屏蔽措施、滤波、故障电路、光电隔离等方面都有很成熟的设计方法,PLC 的电磁兼容性、环境适应性、可靠性等方面都能满足复杂环境的应用需求,另外,在软件设计方面,也增加了功能安全等机制,保障其可靠工作。

1.3 强实时:微秒级、高精度、低延迟、多任务协同

PLC 控制系统的实时性要求体现网络通信、数

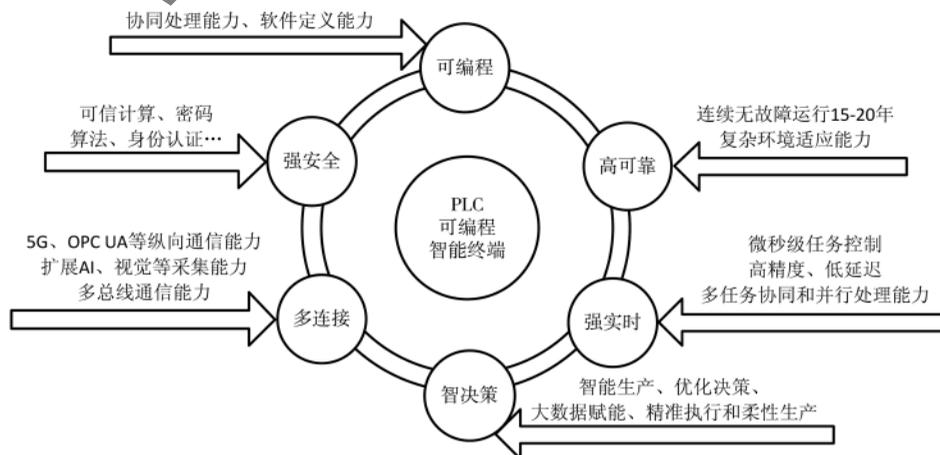


图 1 PLC 技术发展特点

据采集、任务控制等方面,一般采用响应时间来描述实时性指标,以微秒(μs)、毫秒(ms)、秒(s)等为计量单位。响应时间越短,就标志着系统的实时性越好^[6]。现代 PLC 选用嵌入式实时操作系统和工业以太网总线,可以实现微秒级任务控制、高精度低延迟、多任务协同并行处理能力,在运动控制尤其是大惯量设备控制领域应用较多。

1.4 强安全:数据安全和系统安全

随着工业互联网和智能制造的发展,PLC 系统逐渐走向开放化,也引入了以前在工业领域从未面临的安全问题,自从 2010 年震网病毒爆发之后,攻击者对工控系统不断深入研究,攻击花样越来越多,攻击手段也更加复杂,PLC 作为工业生产的重要基础性设备,面临的安全问题更加突出,也日益成为遭受攻击的目标^[7]。目前在工控系统中通过可信计算、密码算法、身份认证、深入检测等技术进行了安全防护,但由于增加防护带来的延迟将会影响控制系统的实时性,因此如何解决安全性和实时性之间的矛盾也是当前研究的难点之一。

1.5 多连接:纵向通信、智能采集、异构通信

通过 5G、OPC UA 等通信技术的应用,实现 PLC 控制终端数据直接与决策层交互的纵向通信能力。在智能化方面,通过 PLC 连接 AI、机器视觉等设备,将智能化引入到终端中。通过本地服务器机房部署云化控制器、现场部署多协议网关,可将现场传统 PLC 接入云 PLC,实现与工业互联网和云计算结合,借助云 PLC 具备的实时任务处理能力和大算力,以 5 ms 的连锁响应速度实现厂内多控制系统间的协同控制、协同调度以及协同管理,为 PLC 和控制系统实现大数据赋能。工信部于 2019 年底印发《“5G+工业互联网”512 工程推进方案》,文件要求到 2022 年,突破一批面向工业互联网特定需求的 5G 关键技术,“5G+工业互联网”的产业支撑能力显著提升^[8]。

1.6 智决策:智能控制、优化决策、大数据赋能、柔性生产

将人工智能应用到工业自动化控制系统的应用和发展中具有很强的可行性^[9]。传统工业控制系统在新型工业业态模式下存在以下问题:生产规模和工艺复杂度迅速提升,被控对象系统辨识和建模难度大;基于简化机理模型的控制策略难以解决分布参数、非线性、时变、多变量耦合的复杂对象优化

问题;工业现场调试完全依赖调试人员的知识和经验。智能控制是一种模仿人类智能的控制方法,必须具有模拟人类学习和自适应能力。工业控制系统在人工智能、机器视觉、AR/VR、大数据、云计算等技术加持下,可以实现基于大数据的机器学习能力,系统通过训练建立控制模型可以实现优化控制。更进一步,智能控制系统具备基于小数据集的知识迁移能力,使系统能在不确定情况下继续工作。在大算力和大数据赋能下,实现软测量、预测诊断、预测维护、实施优化探索和柔性生产。

2 市场发展趋势

在工控自主市场方面,2019 年中国工控行业控制系统市场规模为 372.6 亿元,2020~2025 年预计年增长率为 10%~15%。自 20 世纪 70 年代引进 PLC 以来,PLC 在我国的应用已有 40 多年的历史,我国 PLC 本土品牌的发展却一直步履维艰,国内 PLC 市场外资品牌整体占比达 90%^[10],主要由西门子、三菱、欧姆龙、罗克韦尔等欧美和日系巨头占据,西门子在国内 PLC 市场的综合市占率超 40%,第二大品牌三菱市占率 14%,国产化率仅 10%,而且国产品牌大都不是“国产芯”。面对新冠疫情对供应链的巨大冲击以及国际形势潜藏的安全威胁,工业控制系统国产化替代需求日益迫切。

对国内 PLC 市场进一步细分,可以明显看出因技术难度与应用场景不同,大、中、小三型 PLC 市场呈现不同的竞争态势,如表 1 所示。

大型 PLC 市场头部位置一直由罗克韦尔(Rockwell)占据,其产品主要应用在冶金、电力、交通等,产品需要具备强大的计算处理能力、控制能力和通信能力,用户对其产品的安全性、可靠性和抗干扰性要求也比较高。另外,应用大型 PLC 的场合一般来说工艺比较复杂,需要多样和灵活的通信方式以及较好的网络拓展能力,所以对大型 PLC 的网络通信能力要求较高^[10]。因此大型 PLC 具有较高的技术壁垒,是厂商竞争难度最大的领域。凭借产品优势罗克韦尔一度占有 39.8% 的国内大型 PLC 市场份额。在自主安全提升到国家战略的背景下,国内品牌厂商陆续推出大型 PLC 产品,并在市场竞争中开始发力。以和利时公司为例,该公司 2021 年大型 PLC 市场份额增加 0.4%,整体市场占比达 4.9%,如图 2 所示。

中型 PLC 产品主要应用于项目型市场,因此该

表 1 PLC 市场特点比较

	大型 PLC	中型 PLC	小型 PLC
外资品牌市场占有率/%	93	95	75
外资品牌代表厂商	罗克韦尔、施耐德、西门子	西门子、欧姆龙、三菱	西门子、三菱、欧姆龙
应用特点	计算能力、通信能力、安全性、可靠性和抗干扰性要求高	通信能力、组网便利性、CPU 指令处理速度、程序容量、运动控制精度要求较高	集成度高、能耗低、经济易用
技术难度	高	高	低
产品价格	高	高	低
客户粘性	高	高	低
可替代性	低	低	高

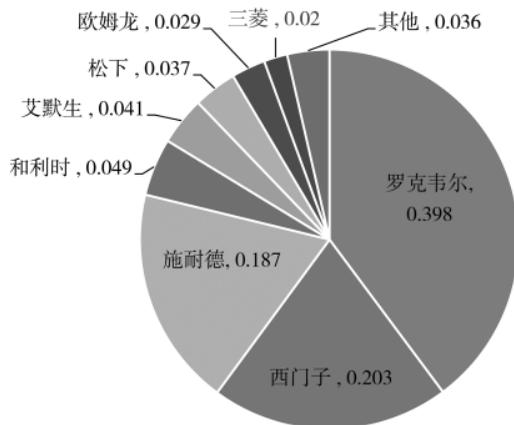


图 2 2021 年大型 PLC 市场分布

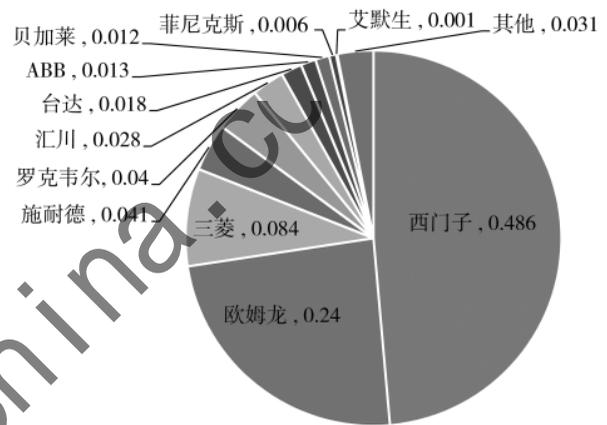


图 3 2021 年中型 PLC 市场分布

市场是竞争格局最为集中的领域，而西门子 (Siemens) 凭借 S7 系列 PLC 产品占据国内 48.6% 的市场份额，已成为中型 PLC 市场国内第一品牌。中型 PLC 应用场景一般需要建立小规模的网络，因此通信能力和组建网络的便利性成为中型 PLC 的技术发展趋势。另外在 OEM 应用中，由于采用中型 PLC 的应用在 OEM 应用中通常属于高端应用，机器的复杂程度较高，在 PLC 的 CPU 指令处理速度、程序容量、运动控制精度、通信方式等方面有较高要求。这成为中型 PLC 技术发展的另一个趋势^[11]。国产中型 PLC 厂商方面，受益于电子、机床等行业国产化需求增长，汇川公司中型 PLC 市场份额增加 0.6%，整体市场占比达 2.8%，如图 3 所示。

小型 PLC 市场相对分散，国内市场主要由西门子、三菱 (Mitsubishi)、欧姆龙 (Omron) 等国外厂商占据优势地位，三家厂商合计占据国内 57% 的市场份额，其中西门子依靠产品突出的性价比优势领先于三菱、欧姆龙，占有 40.8% 的市场份额。小型 PLC 产

品主要应用于电力电子、机械制造、汽车生产、环保文娱等行业，要求产品集成度高、能耗低、经济易用，因其技术难度小、竞争壁垒相对较低，如台达、信捷、汇川、合信等国内品牌厂商近些年迅速崛起，已开始与国外厂商同台竞技，在市场上已占据一席之地。以信捷电气公司为例，信捷的 PLC 业务从 2011 年的 0.8 亿元提升到 2021 年 5.16 亿元，年均复合增速达到 20.49%，小型 PLC 市场份额达到 6.6%，如图 4 所示。

国产自主安全 PLC 品牌以中国电子超御系列、浙江中控研究院、南大傲拓等公司为主，其市场主要面向军工、高新电子和关键基础设施等领域，在自主性、安全性方面独具优势，但这些品牌还处在发展初期，市场占有率较低。造成这些国内 PLC 企业在市场竞争中处于劣势的主要原因有三个方面：其一，能力分散，无法形成竞争合力；其二，技术水平落后，仅能设计生产低端的硬件模块，编程软件大部分依靠国外成熟技术，处理器芯片大多“借用”

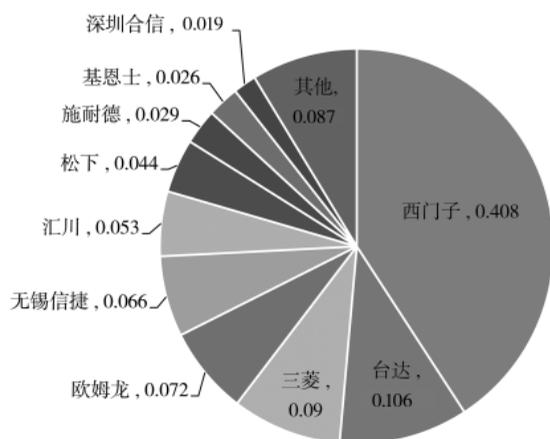


图4 2021年小型PLC市场分布

国外嵌入式信息处理类CPU;其三,产业生态发展差,未形成可持续健康发展的产业生态^[12]。

3 我国PLC未来发展思路

3.1 掌握核心技术

我国PLC向智能化发展应对复杂控制技术、智能控制技术、内置安全技术、通用编程编译技术、面向泛在互联的广域控制技术进行攻关,掌握核心关键技术,形成可编程智能终端技术体系。

(1) 复杂控制技术

针对风电、水力发电、新能源发电、核电等能源行业应用的大规模、高性能、高可靠需求,突破多重冗余控制、故障自诊断、事件分析、复杂环境适应等技术。

(2) 智能控制技术

研制运动控制、AI接入、云边融合、协同互联等智能控制技术,实现系统通用性强、可拓展性强、抗干扰能力和开放性强,能够满足复杂制造的智能控制系统。

(3) 内置安全技术

突破在运行空间隔离与保护、内置可信、动态防护等技术,解决单一加密保护机制无法实现动态防护、通用加密防护技术对工业控制系统资源分配和通信调度性能产生影响的问题,在保证安全性的同时,应该满足计算速度、能耗等需求,实现保障安全的同时,满足工控高可靠、高可用的要求。

(4) 通用编程编译技术

构建具有统一技术体系的工控系统编程环境,突破多语言编程、多平台异构编译、多终端同时开发、多总线异构接入等技术,建立国产工控系统通

用开发平台和工业级实时运行系统通用架构,形成一体化开发环境解决方案,可应用于多种可编程工业智能终端。

(5) 面向泛在互联的广域控制技术

以分散控制、泛在互联、广域协同提升全域协同控制能力,以控制模型智能构建和智能前移提升末端智能水平,解决控制系统的快速部署、联合决策、动态恢复难题,实现分散化控制部署、快速化动态重构、泛在化广域互联、集群化协同控制的目标。

3.2 实施先进制造

集中优势力量,利用国内芯片企业如飞腾、龙芯、华大等,元器件供应商如安路、振华等企业,工业互联网企业如中电互联、东方国信、树根互联、航天云网、浪潮云、华为、工业富联、阿里云、徐工等企业^[13]的合作,在国内形成批量优势,以先进制造的思路,在成本集中控制、供应链、产能保障、质量提升进行全方位的谋划。应在三个方向上努力:(1)稳链强链,构建基于元器件、原材料供应链,确保供应链的健壮性和稳定性。(2)保供降本,建立基于元器件的集采平台和相应的金融保障体系,最大限度降低原材料的采购成本。(3)提质增效,对PLC产品实施PCBA及生产制造,确保产能与质量稳定可靠。

3.3 强化协同和扩大生态

行业上游负责提供生产PLC所需的电子元器件、电力电子器件、钣金结构件等零部件^[14],用于运行环境的操作系统和计算机等软硬件产品。行业下游广泛分布于各个工业应用,包括高新电子、风电、水电、天然气、石油、管网、智能制造、加工产线等领域。依托国内央企深化合作,加大规模化应用,形成技术、产品、应用等多方面的良好合作生态,如图5所示。

(1)加强与上游产品的技术交流合作,联合开发工控专用SoC处理器、微内核嵌入式操作系统等关键产品,双向促进产品能力提升。加强相关企业技术联动,形成一体化解决方案,加快应用推广。

(2)基于国产元器件和软硬件技术打造先进产品,研究具有内置安全的可信终端控制产品,在关键基础设施领域进行应用,建立自主安全的关基控制系统。研究复杂控制终端、智能制造终端,应用于能源、轨道交通、智能制造等领域。

(3)基于PLC系统应用形成整体解决方案,依托例如“PKS”体系国产化全产业链信息系统生态环

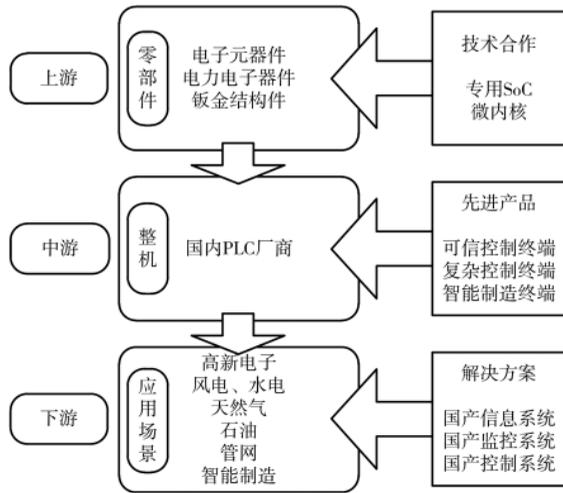


图 5 PLC 行业产业链

境,带动国产计算机、交换机、服务器、操作系统、数据库、云平台等自主安全产品进行整体系统建设,进而推动国内工控行业整体发展。“PKS”是基于飞腾 CPU 和麒麟操作系统构建的一个开放的安全架构,体现了安全和可信,主要是要解决现有计算机先天缺乏免疫的问题及漏洞和效率问题。其中“P”为 CPU、内存、网络交换芯片内置可信核安全机制,内置密码体系;“K”为操作系统、数据库等基础软件内置白名单、访问控制、未知漏洞防护等安全增强机制;“S”为可信策略管理、安全控制中心、安全软件应用商店等立体防护和管控体系。

4 结论

工业互联网、云计算、人工智能、大数据等技术蓬勃发展,第四次工业革命下形成了新型工业业态模式,作为物理世界与数字空间双向实时连接的桥梁,PLC 将会在工业互联网、物联网、智能工厂等发展大势下,突破核心关键技术,形成可编程智能终端产业生态,在设备通信、控制、数据采集、信息安全等功能上进一步提升,通过与云计算、大数据、人工智能等新技术结合,实现 PLC 终端与“智能制造”的融合发展,推动工业控制系统的自动化,进而助推工业企业的信息化、数字化、智能化进程。

参考文献

- [1] 王诗豪.PLC 控制系统在智能制造中的应用及发展趋势[J].造纸装备及材料,2021,50(7):36-37.
- [2] 王德吉.智能时代 PLC 应用及发展趋势[J].自动化博览,2019(6):34-36.
- [3] 顾硕.自动化软件为创新代言[J].自动化博览,2013(11):1.
- [4] 汪涛.2035 年远景目标和“十四五”规划要点[J].企业观察家,2021(2):1.
- [5] 康天娇,邹春明.工业控制系统网络安全产品研究分析[J].网络空间安全,2020,11(1):6.
- [6] 杜品圣,张龙.工业以太网和工业实时以太网的安装,调试和诊断技术(二)[J].自动化博览,2007,24(2):4.
- [7] 徐震,周晓军,王利明,等.PLC 攻防关键技术研究进展[J].信息安全学报,2019,4(3):48-69.
- [8] 佚名.“5G+工业互联网”512 工程推进方案[J].金川科技,2020(4):1.
- [9] 孙敏,李森.人工智能在工业自动化控制系统的应用分析[J].新型工业化,2020,10(1):106-109.
- [10] 工控研究.2020 中国 PLC 市场研究报告[Z].2020.
- [11] 佚名.创新将成为制造业转型升级主引擎[J].现代制造,2017(36):1.
- [12] 宋慧欣.中电智科:聚合中国力量 超御自主可靠[J].自动化博览,2019(6):3.
- [13] 高晓雨.2019~2020 年中国工业互联网发展报告[R].北京:社会科学文献出版社,2020.
- [14] 佚名.2019 年中国 PLC 可编程逻辑控制器行业概览[Z].2019.

(收稿日期:2022-06-10)

作者简介:

原崇蛟(1994-),男,本科,助理工程师,主要研究方向:工业自动化、智能制造。

郭肖旺(1986-),女,硕士,高级工程师,主要研究方向:工业软件、工控安全。

贡春燕(1987-),女,硕士,工程师,主要研究方向:工业软件、项目管理。

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

www.pcachina.com