工业互联网信息通信安全问题研究

苏泳龙
长讯通信服务有限公司　广东　广州　510030

摘　要：工业互联网是现代信息技术和制造业的有效融合，作为构筑现代化产业体系的核心支撑，已经成为各国发展制造业的重要战略之一，在我国产业发展顶层政策体系逐步构建完善的基础上，加快发展工业互联网有助于融入新一代信息技术革命，推动生产力实现质的飞跃，开辟新道路和拓展新领域，为经济增长提供新动能，进而实现高质量发展。但工业互联网是通过借助互联网、大数据分析等的融合从而实现智能交互，网络是基础，安全是保障。本文主要从信息通信网络传输入手，对工业互联网安全问题进行研究，提出了相应的解决对策。

关键词：工业互联网；信息通信；安全问题

引言

工业互联网包括计算机网、物联网及传感网等多种网络，涉及到的内容也比较广，如智能分析、计算、互联网等，其连接对象延伸范围很广，涵盖机器设备、工业产品服务等。为了进一步推动工业互联网安全技术及安全产品的研发及应用，有必要采取强化政策引导和扶持、强化技术创新及转换、构建产业联合发展体系等策略，进而推动工业互联网安全产业发展，全面提高工业互联网安全防护水平。对此，需要相关从业者详细了解工业互联网网络传输的安全问题，并在此基础上探讨针对这些问题的解决策略。

1 工业互联网概述

1.1 工业互联网的概念

工业互联网是全球工业系统与高级计算、分析、感应技术以及互联网连接融合的一种结果。工业互联网的本质是通过开放的、全球化的工业级网络平台把设备、生产线、工厂、供应商、产品和客户紧密地连接和融合起来，高效共享工业经济中的各种要素资源，从而通过自动化、智能化的生产方式降低成本、增加效率，帮助制造业延长产业链，推动制造业转型发展。

1.2 工业互联网的构成

工业互联网包含网络、平台、数据、安全四大体系，既是工业数字化、网络化、智能化转型的基础设施，也是物联网、大数据、云计算、AI、5G等技术与实体经济深度融合的应用模式，同时也是一种新业态、新产业，将重塑企业形态、供应链和产业链。网络体系是基础，包括网络互联、数据互通、标识解析三部分；平台体系是中枢，包括边缘层（与设备连接）、IaaS层、PaaS层、SaaS层四部分，是工业互联网的“操作系统”；数据体系是要素，是工业互联网价值创造的源泉；安全体系是保障，针对工业互联网涉及范围广、影响大、企业防护基础弱的特点，提供设备、控制、网络、平台、工业应用的整体保护，保障工业互联网平稳运行。

1.3 工业互联网的连接特性

工业互联网的特征是连接节点数量多分布广。终端设备和网关设备共同组成，网关设备作为边缘层的集群节点，可连接多个工业设备，除了完成工业网络数据包抓取和特定通讯协议解析外，还可能包含边缘计算环境。云计算环境构成平台层，为工业大数据存储、管理和计算的中心。人机交互的可视化应用终端构成应用层，用于工业用户的需求输入及工业应用的计算结果显示。工业互联网四个层级（边缘层、网络层、平台层、应用层）包含的多条连接通道承担着边缘数据采集、云控制、人机交互及与其他第三方系统API通信的重要任务。而对于其中的单个通道，可以承接两个端点的数据传输任务，也可以穿越不同层级的多个中间节点，通过单向和双向的数据传输，形成数据链路或回路。由此可见，不同节点通过连接通道形成的关系构成了工业互联网交错复杂的数据网络，若其中一个环节出问题，整个工业互联网将受到冲击，因此确保每个连接通道都得到安全防护非常重要。

2 工业互联网的发展现状

2.1 供应端技术瓶颈多

工业企业各行业数字化改造的需求不同，可供借鉴学习的案例较少；大部分平台对于工业知识、模型和历史数据的沉淀还不够，面向特定行业或工业场景提供服务时，往往难以精准对接工业企业的业务需求；工业设备种类繁杂、数量多、通信协议与数据格式各异，低成本快速接入平台的技术手段少，解决方案移植性差。二

是关键核心技术和元器件受制于人。如F公司反映国内先进制造业在人工智能深度学习平台领域起步较晚，人工智能产业面临被国外厂商“卡脖子”的局面；又如，某智能公司反映，大量制造业核心工业软件过分依赖国外产品，每年企业需要支付高额使用费用。

2.2 行业标准不统一

工业装备仍缺乏行业通用的标准体系，设备与设备、设备与系统之间互联互通困难，打通成本高；同时由于缺乏标识、平台、数据安全等标准，尚未建立统一权威的工业互联网平台能力和安全评估认证体系，用户企业对企业上云心存顾虑。

2.3 专业人才缺口大

工业互联网是工业与信息技术深度融合的新生产物，需要工业与信息技术方面的复合型人才。目前从事工业互联网行业的主要为自动化专业人才，对控制系统、操作平台、大数据、人工智能等新技术掌握不足。实地调查走访的企业均表示，当前最大问题就是很难找到既懂工业生产又精通信息技术的复合型人才，全国高校都缺乏培养工业互联网人才的专业，人才问题已日益成为制约企业应用工业互联网的重要因素。

3 工业互联网数据安全防护思路

根据工业互联网数据安全防护需求，设计了工业互联网数据安全防护框架。其中，安全管理方面包括制度、机构、人员、设备、供应链等安全管理，技术防护方面包括从系统安全角度加强数据安全，主要措施有边界防护、入侵检测、身份鉴别、访问控制和安全审计:另一方面的技术防护是指分类分级防护，针对不同类别、级别的数据实施差异化防护措施。在分类施策方面，主要是要根据不同类别工业互联网数据的特征，有针对性地提出工业互联网数据分类防护要求，解决适应各类数据合规性、保密性、完整性、可用性、可追溯性等需求下的差异化安全防护问题[1]。

4 工业互联网网络传输中存在的安全问题

4.1 密钥管理设计问题

在工业互联网环境中依然可以应用Kerckhoffs这一传统信息系统中的密钥设计，其核心在于：密钥保护会直接决定密码系统的安全性而不是密码系统保护，且密钥有必要得到通信双方的事先约定，按照指定协议还需定期进行更换，因此在工业环境中必须密切留意密钥保护、安全管理问题。

4.2 工控环境漏洞多

工控环境中，工控设备种类繁多、数量庞大且普遍无法及时升级系统、修复漏洞、加固补丁，且大多采用私有工业协议且标准不统一，协议本身漏洞难以及时发现和加固。

4.3 存储阶段分类分级难

存储阶段极易形成数据的汇聚，需要根据数据的类别和等级采用划分区域、设置访问权限、加密存储等多种手段。然而工业互联网数据形态多样、格式复杂，使得数据分类分级管理与防护难度大。

5 工业互联网网络传输安全的控制策略

5.1 强化政策引导和扶持

政策引导和扶持有助于工业互联网网络传输安全建设形成循环发展的新格局。第一，加大对工业互联网安全产业的顶层设计力度。例如，健全现有法律法规、建立与政策相匹配的基础设施体系、完善产业发展战略等，进而建立工业互联网安全建设需要的长效机制[2]。第二，深入贯彻可持续发展和防患于未然的管理理念，将工业互联网安全防护关口向前移动，提高安全防护效果。

5.2 构建工业互联网网络传输安全机制

在工业互联网网络传输过程中有必要对各个传输节点、链路、端到端的加密过程进行强有力的控制，还需选择一种科学、合理的对称加密、公钥加密算法，借助其中所具有的保密性可以更好的加密传输数据流，对通信链路上有效的防范各种问题，[3]。

在传输协议方面，为支持IPSec来实现远程通道的安全加密可以借助HTTPS、SSL/TLS，并能够兼容IPv4协议、IPv6协议。在工业网络通信传输过程中为满足最低安全基线，可以在特定安全域中设置一个可以启动的安全通道流量，加密那些使用安全通道进行传输的全部用户数据，以此可以更好的验证身份，有效规避中间人攻击与重放攻击等。

5.3 优化通信传输设备

在工业互联网网络传输中，设备是不可缺少的一部分。设备性能越优良，传输效果越好。目前，设备性能还有待加强。因此，要鼓励创新型设备的研发。相比较之下，新设备的造价更高。如果不解决这个问题，就会导致应用率提高缓慢。在实际使用中，设备问题就会浮出水面，在消灭问题的同时，促进厂商实力的提升。长此以往，整体生产水平就会有质的提升，设备升级换代更加频繁，随之带来的是工业互联网网络传输安全效果越来越强。

5.4 密钥管理

工业环境当中，密钥保护及安全监管较为关键。工业领域互联网密钥管理层面设计原则：一是，在密文存储层面。密码装置除非是极具安全性，否则切勿明文

实施密钥存储。工业控制层面，以密钥人工分配较为常见，需注意的是密钥严禁实施明文存储、传递及把控。可以密钥的分量形式，若干信任关系实现实体的共同监管；二是，注重密钥有效分离。各个通信实体相互间，切勿选定有密切关联或者是相同密钥，防止通信实体潜在的安全通信层面问题，对其他实体整体通信安全产生威胁。

5.5 构建风险评估预警机制

现阶段全球经济发展趋势和政治局面不断变动，工业互联网网络传输安全的发展不确定因素在不断增多，有必要构建风险评估预警机制来防范主要安全风险。第一，将风险评估预警机制建设纳入法律法规中，出台针对性建设规划和标准，尽快建立较为准确和规范的评估预警机制，为各个部门及机构识别工业互联网运行风险提供准确依据。第二，建立动态跟踪机制，对工业互联网建设进行全过程监管，及时发现潜在安全隐患，采取针对性控制和解决策略，形成全面的危机应对联动机制。

结束语

综上所述，工业互联网是当前新一代信息通信技术与工业经济的深度融合，为工业乃至产业数字化、网络化、智能化发展提供了实现途径，是第四次工业革命的重要基石。当前发达国家采用的信息智能化大大降低了劳动力成本，在制造生产过程中极大地提高了生产率。建立动态的防护机制，加强应急响应能力，构建工业互联网安全评测体系，积极推动工业互联网的安全建设，最重要的是将工业互联网安全防护技术与科学管理相结合，及时应对内部和外部的各种安全威胁以及安全风险，才能真正实现新时代、新环境下工业互联网的安全防护目标。

参考文献：

[1]吴画斌，张静. 高质量发展背景下工业互联网发展途径及保障措施研究[J]. 现代管理科学，2021(1)：109-113.

[2]严方舟.工业互联网网络传输安全问题研究探析[J].中国宽带,2021(7):1.

[3]任保平. 工业互联网发展的本质与态势分析[J].人民论坛，2021(18)：4.