DOI 10.15302/J-SSCAE-2021.02.011

工业互联网设备的网络安全管理与防护研究

马娟[1]，于广琛[1]，柯皓仁[1]，杨冬梅[1]，吾守尔·斯拉木[2]

（1. 中国信息通信研究院安全研究所，北京 100191；2. 新疆大学信息科学与工程学院，乌鲁木齐 830046）

摘要：新一代信息通信技术与工业体系深度融合，工业互联网推动“人、机、物”的泛在深度互联和全面感知；工业互联网设备的网络化、数字化、智能化应用不断泛化，设备自身网络安全设计、应用过程管理与防护成为关注重点。本文从工业互联网设备的安全防护视角出发，明晰了工业互联网设备的内涵、防护范畴及需求，梳理了国内外工业互联网在安全监管和审查、安全检测认证等方面的发展现状；结合工业互联网设备的网络安全相关实践，剖析了我国工业互联网设备网络安全面临的问题。本文论证了我国工业互联网设备网络安全管理与防护的具体实施路径，并提出发展建议：从国家层面完善工业互联网设备的网络安全准入机制，建立设备网络安全检测认证体系，促进设备的网络安全架构研究和工程应用，强化设备的网络安全风险监测感知。

关键词：工业互联网设备；网络安全；管理；防护；认证

中图分类号：TN915.08　　**文献标识码：**A

Network Security Management and Protection of Industrial Internet Equipment

Ma Juan[1], Yu Guangchen[1], Ke Haoren[1], Yang Dongmei[1], Wushour Silamu[2]

(1. Security Research Institute, China Academy of Information and Communications Technology, Beijing 100191, China;
2. College of Information Science and Engineering, Xinjiang University, Urumqi 830046, China)

Abstract: The new generation of information and communications technology is deeply integrated with the industrial system. The industrial Internet promotes the ubiquitous and deep interconnection and comprehensive perception of human, machines, and things. The industrial Internet equipment becomes increasingly networked, digital, and intelligent; therefore, the network security design, application management, and protection of these equipment become increasingly important. In this study, we clarify the connotation, protection scope, and requirements of the industrial Internet equipment, and summarize the development status of industrial Internet in China and abroad from the aspects of security control and security certification. Moreover, the problems regarding the network security of industrial Internet equipment in China are analyzed, and the specific implementation paths regarding the network security management and protection for the industrial internet equipment in China are discussed. Furthermore, several development suggestions are proposed. Specifically, the network security access mechanism of the industrial Internet equipment should be improved at the national level, a network security testing and certification system for the equipment should be established, research on the network security architecture and engineering application of the equipment should be promoted, and the network security risk monitoring and perception of the equipment should be strengthened.

Keywords: industrial Internet equipment; network security; management; protection; certification

收稿日期：2021-02-05；**修回日期：**2021-03-09

通讯作者：马娟，中国信息通信研究院安全研究所工程师，研究方向为工业互联网、物联网安全技术；E-mail: majuan@caict.ac.cn

资助项目：中国工程院咨询项目“新一代工业互联网安全技术发展战略研究”(2020-XZ-02)

本刊网址：www.engineering.org.cn/ch/journal/sscae

一、前言

工业互联网是新一代信息通信技术与工业体系融合的产物，做好产业融合转型保障，建设工业互联网安全保障体系，是工业互联网安全的发展前提。网络连接、数据互通趋势下的工业体系加速开放融合，传统工业体系相对封闭隔离环境下以生产安全为导向的安全管理、运维模式，无法适应复杂多变的工业互联网应用环境。与此同时，工业控制系统、设备本身也存在漏洞和后门，加之工业控制系统与设备的脆弱性、高的实时性要求，难以像传统信息系统那样进行安全防护，因此相关网络安全能力建设成为关键内容。

信息技术与传统工业运营技术的融合日益深化，工业互联网设备的网络安全防护能力将直接影响工业生产和业务运行，成为网络安全政策管控、产业保护实践的重要组成部分。近年来，设备产品安全逐渐成为传统工业强国的关注重点，被视为强化网络安全管控、保障供应链安全及产业发展的关键内容。例如，美国建立了以网络安全审查为手段的供应链管控体系，制定了《物联网网络安全改进法案》。当前，在工业设备测量、运营、维护、质量管理方面开展了较多的研究与应用，注重利用设备质量控制、预测性维护、高精度测量、故障分析、远程监控等手段来保障设备的功能安全及性能[1~4]；在设备功能安全应用方面积极开展工业大数据、人工智能（AI）等新技术应用研究[5~8]。从已有进展来看，工业互联网设备的网络安全研究整体上依然缺乏；无论是设备自身功能性能的安全保障，还是利用新技术强化设备健康管理和监控，都不应忽视工业设备面临的网络安全问题。

本文着眼于工业互联网设备的网络安全问题，分析需求、梳理现状、研判问题、论证路径，提出具体的发展建议，以期为领域内的基础与政策研究提供思路参考。

二、工业互联网设备的安全防护概念及需求分析

（一）工业互联网设备的安全防护概念

工业互联网设备指在新一代信息技术与工业生产、制造、运营、管理等环节的融合应用过程中，通过有线或无线方式接入工业互联网网络的装置或设备，具有类型、功能、应用形态多样的特点。工业互联网设备分为：工业控制设备，如可编辑逻辑控制器（PLC）、远程终端单元（RTU）；工业网络和安全设备，如工业交换机、工业防火墙；工业智能终端设备，如数据采集网关、视频监控设备、物联网相关设备。从设备安全性及其应用过程防护的角度来看，工业互联网设备的安全防护细分为硬件安全、网络通信安全、系统服务安全、应用开发安全、数据安全等（见图 1）。

硬件安全，包括设备调试接口权限控制、芯片安全保护、防范针对设备功耗等信息进行统计分析所伴生的威胁风险。目前多数的网络设备、物联网设备保留了硬件调试接口，部分接口甚至无需验证即可获取权限操作，极有可能成为恶意攻击、数据窃取的入口，进而导致设备密钥、认证等信息泄漏。

网络通信安全，包括通信认证鉴权、通信加密，后者进一步划分为网络层加密、传输层加密、应用层数据加密等。若设备网络通信的访问权限控制不足，攻击者即可通过身份伪造在设备间、设备与主机系统间实施“中间人攻击”，极有可能快速传播形成僵尸网络，僵尸网络进而作为被控端对网络实施大规模攻击。此外，设备的通信加密能力不足，容易出现黑客窃取用户或设备的身份信息、重要工业数据泄露等情况。

系统服务安全，包括设备操作系统的权限控制、基线安全配置，系统更新的安全机制保护，系统入侵防范、恶意代码防范等。攻击者可利用设备系统（或固件）存在的漏洞或缺陷入侵设备，在升级过程中植入恶意代码，增加了事后溯源与排查难度。

应用开发安全，包括组件资源间的访问控制与用户的认证授权、外部接口安全、配置文件及重要

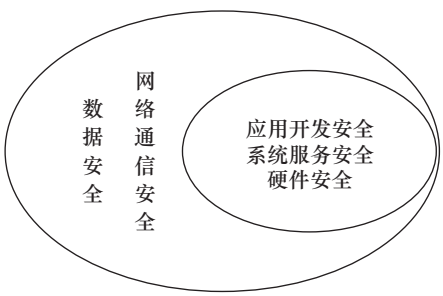

图 1　工业互联网设备的网络安全防护范畴

数据的安全保护、通信协议加密、第三方组件库漏洞隐患排查、代码自身安全设计等。若设备自身安全机制不足，攻击者即可利用应用安全漏洞或缺陷入侵设备和系统，发起针对性攻击。

数据安全，包括数据完整性、隐私性、可用性保护，防范数据不被窃取、监听、篡改。工业企业加快数字化转型，开始规模化部署数据采集、边缘计算等物联和智能化设备，工业生产过程及业务数据、用户信息的开放共享和流动利用呈指数型增长的趋势。不少工业设备、工业网络中依然存在着明文传输数据的现象，难以发现针对设备进行的非侵入、被动式数据监听活动；若设备本身的数据防护、隐私保护机制不足，关键工艺参数、流程数据等信息存在被泄露或被恶意控制篡改的风险。

（二）工业互联网设备的安全防护需求分析

工业互联网设备的功能安全、网络与数据安全等，需要结合实际应用形态下的网络安全漏洞隐患防范排查与解决，基于设备的应用周期、智能化属性等实施差异化的管理防护。

部分设备在设计开发环节没有周到考虑网络安全问题，长期不间断运行的工作方式导致难以进行深度安全检测或部署安全防护措施，存在不同程度的漏洞及隐患。根据中国国家信息安全漏洞共享平台（CNVD）统计 [9]，与工业控制系统设备相关的漏洞数量为 2955 个（截至 2020 年 12 月），年度新增工业控制系统设备漏洞数量为 593 个。根据中国信息通信研究院工业互联网设备安全评测和相关监测结果，有相当数量的工业互联网设备存在指令篡改、敏感信息获取、权限绕过等中高风险漏洞，部分工业安全设备甚至存在高危漏洞，安全防护能力明显不足。我国部分工业互联网设备系统持续遭受了来自境外的定向扫描和恶意感染，僵尸网络、木马、蠕虫、病毒等攻击感染，网页攻击、系统攻击的频率和数量不断加大；在我国工业领域应用广泛的罗克韦尔 PLC、西门子视窗控制中心等均存在严重高危漏洞。因此，工业互联网设备的漏洞深度安全检测，尤其是无损安全检测与防护，成为工业企业、设备供应商普遍性的迫切需求。

从设备应用周期、适用的网络安全防护措施角度看，工业互联网设备需要开展差异化、分类分级的网络安全管理与防护。一类是已经应用部署的“存量”设备，由于自身资源、性能受限，加之长时间运转，极有可能长期未开展网络安全检测，威胁隐患难以完全掌握；针对这类设备的安全防护需要具体分析实际应用情况，通过防护措施叠加、监测感知等手段强化风险防控。另一类是新投入应用的“增量”设备，尤其是具有远程控制、数据采集分析、计算处理功能的智能化设备，多使用通用操作系统（如嵌入式 Linux 等），一定程度上降低了攻击者的入侵难度；部分智能化设备若遭受恶意控制和攻击，可能具备大规模主动扩散能力、变成“跳板”后成为智能化攻击的一环；针对这类设备的安全防护需要融合设备自身功能、应用场景、支撑业务需求，强化自身硬件安全保护、网络通信、数据安全等机制设计，采取网络安全感知、监测预警、应急处置等措施。

三、工业互联网设备安全领域的国际进展

（一）安全监管和审查

传统工业强国的网络安全法律、监管措施持续升级，逐步强化网络安全审查，涉及相关设备产品安全性和安全能力审查，设备产品开发、设计、应用等全周期及各环节的安全机制。

美国将网络安全审查上升为国家战略和国际竞争手段，其网络安全审查覆盖了政府采购、关键信息基础设施保护、外国投资、供应链，建立了较完备的审查机构、程序、标准规范。其中，供应链审查制度是美国网络安全审查的重点方面，具有代表性；针对相关技术、设备产品等供应链的安全审查内容和范围逐渐完备，发布了一系列强制性安全审查规范并要求企业签署网络安全协议。2000 年，美国国家电信与信息系统安全委员会发布了《国家信息系统安全保障采购政策》，要求入侵检测、防火墙、操作系统、数据库管理等方面的产品，必须经过国家信息保障联盟（NIAP）通用准则评估与认证体系框架下的风险评估和认证 [10]。2015 年，美国财政部、商务部要求国家标准技术研究院（NIST）依据相关技术标准开展供应链安全风险审查 [11]。2020 年，美国颁布《物联网网络安全改进法案》，禁止联邦机构购买任何不符合最低安全标准的物联网设备，要求 NIST 发布联邦政府使用物联网设备的标准和指南 [12]。

英国要求相关设备产品通过政府通信总部制定的通信电子安全小组安全认证后才能销售。俄罗斯工业和贸易部重点针对外资进入的战略性产业交易进行安全审查 [13]。

（二）安全检测认证

网络安全检测认证是设备产品进入市场应用前的重要环节，在部分国家也属于法律强制要求的环节。目前，国际网络信息安全认证测评体系趋于稳定，国际通用认证准则逐步建立，国际通用认证规则（CC）和欧洲创建的信息技术安全评估准则（ITSEC）并存。

各国的网络安全检测认证多由相关机构或协会负责，委托实验室、企业、专业机构具体实施。测评体系通常由 1 个测评认证协调组织、1 个测评认证实体、多个技术检测机构组成。例如，美国由 NIAP 管理，授权给相关实验室、公司等测评机构，目前只颁发通用准则证书；英国由通信电子安全局管理，德国由信息安全局管理，均将检测认证授权给商业性评估机构，颁布 ITSEC、CC 两种证书。

各国重点围绕设备产品的安全合规、功能、安全保证、可控等方面开展测评认证标准建设，划分功能级别、保证级别以满足不同部门、行业、用户的需求，其中功能、安全保证评估是测评认证的核心内容。美国、欧洲、国际标准化组织都在建立基于测评的“保护轮廓”，强调功能评估、安全性评估并分别开展定级。国际标准化组织推出的国际通用准则是目前最全面的评价准则，与 ITSEC 一起成为通用测评方法。此外，美国、德国等注重推行国防、政府、商用共享的测评体系，通过划分级别和轮廓，满足不同对象的安全要求。

在工业互联网设备安全测评认证方面，国际性机构和一些国家分别建立了各有侧重的认证体系。① ISA Secure 认证体系是国际自动化协会安全合规学会（ISCI）推动建立的一套国际认可体系，旨在提供通用的工业设备认证、处理工业设备安全方面需求、简化业主设备采购流程和设备供应商设备保险流程 [14]；ISA Secure 对工业自动化、控制类产品及系统进行独立认证，确保网络攻击防护能力并消除已知漏洞。② NIST 认证体系指由 NIST 牵头、相关行业主管机构和行业协会参与建立的标准认证体系，涵盖国家标准、行业规范、检测认证；在实施方面，推动形成覆盖电力、天然气、石油、核能等行业的安全标准认证体系，成为美国乃至国际安全界广泛认可的事实标准和权威指南。③莱茵认证体系指由德国技术监督协会（经德国政府授权和委托）开展的工业设备、技术产品安全认证及质量保证评估审核；提供嵌入式系统及设备、智能电子设备的认证服务，工业信息技术安全检查、渗透测试、风险分析、安全手册、安全培训等服务，覆盖航空航天、汽车交通、化工、能源、制造业与工业机械、电力等领域。

四、我国工业互联网设备安全领域的发展情况与面临问题

（一）安全监管和审查方面的基本情况

在安全监管方面，《网络安全法》《网络安全审查办法》等国家法律规章陆续出台，逐步建立了针对关键信息基础设施的网络安全审查办法、针对网络关键设备和网络安全专用产品的强制性检测认证要求。《网络关键设备和网络安全专用产品目录（第一批）》要求，列入目录的设备或产品，应按照相关国家标准的强制性要求，由具备资格的机构安全认证合格或安全检测符合要求后方可销售或提供 [15]。在政策要求方面，《加强工业互联网安全工作的指导意见》要求，加强工业生产、主机、智能终端等设备安全接入和防护，强化控制网络协议、装置装备、工业软件的安全保障，推动设备制造商、自动化集成商与安全企业加强合作，提升设备和控制系统的本质安全 [16]。

（二）安全检测认证方面的基本情况

网络和信息安全测评认证体系主要由国家认证认可监督管理委员会管理，国家信息安全测评认证管理委员会、中国网络安全审查技术与认证中心、相关实验室及测评机构等共同推进实施，基本形成了监管机构、国家认证实体、授权测评机构的综合推进体系。也要注意到，现有的测评认证体系重点关注通用基础设备产品、以医疗为代表的部分行业领域专用关键设备，缺乏对工业控制设备、大型自动化设备、工业网络通信设备等关键工业互联网设

备的规范性、通用性网络安全测评认证。

在工业互联网设备安全相关的标准和评测方面，我国发布了《工业控制系统专用防火墙技术要求》《信息安全技术 工业控制系统测控终端安全要求》《电力监控系统安全防护规定》等国家及行业相关标准；在物联网设备终端安全防护方面，我国发布了《信息安全技术 智能联网设备口令保护指南》《信息安全技术 网络和终端设备隔离部件安全技术要求》等标准或指南。近年来，中国信息通信研究院等单位结合工业互联网行业的应用保障需求，推动了《工业互联网设备安全防护要求》等标准的发布，开展了工业互联网设备安全测试评估工作，建立了工业互联网安全评估机构和队伍。

（三）存在问题分析

一是工业互联网设备安全的专门管理办法、检测认证体系缺乏。尽管行业主管部门制定了相关政策标准，但强制要求和体系化程度不足，缺乏对新技术、新应用形态的网络安全适应性要求。工业互联网设备安全防护还基本处于行业自律的层次。

二是“网络关键设备和安全产品目录”对工业互联网关键设备覆盖不足，未纳入目录的产品缺乏必要且体系化的网络安全审查。工业生产装备、关键设备、工业互联网安全专用产品等关键设备产品的安全性、防护能力难以保证，使得工业生产、业务运行面临安全威胁，设备供应链存在未知风险。

三是工业互联网设备种类多、数量大，目前的安全防护能力和保障水平无法适应产业转型升级需求。PLC、工业主机、工业防火墙等工业设备自身的安全运行要求尚未明晰，设备在网络化、数字化应用过程中的安全标准规范等比较缺乏，专门的评估评测规范和实施体系有待完善。已有网络安全检测认证体系无法满足实际应用、市场需求、他国网络安全审查等的要求。

四是工业互联网设备及产品安全相关的国家标准较少，强制性网络安全标准缺乏，评估检测流程方法、机构人员、认证体系明显缺失。目前，工业互联网设备自身的安全性难以满足不同行业要求、市场级别需求，同时国产工业互联网设备产品在走向国际市场时也缺乏权威测评认证，难以适应国际互认、他国网络安全审查的要求。

五、我国工业互联网设备的安全防护实施路径

鉴于工业互联网设备类型多样、体量较大，安全管理较为分散、行业自律水平不一等实际情况，应从国家、行业、应用等角度统筹规划，强化国家监管、行业认证、网络安全工程应用。本文论证了我国工业互联网设备网络安全管理与防护的具体实施路径（见图 2），旨在健全工业互联网设备的适应性策略与能力，分类分级实施安全评估和管理，完善标准规范、检测认证、风险管理应急处置等机制。

一是建立设备自身安全策略和基础能力集，包括设备安全架构设计、安全基线配置、可信根验证和分类分级防护的基本要求。构建设备自身的安全“基线”，强化设备的内生安全能力。

二是结合设备的网络安全风险、保护价值、发生事件的安全影响，针对不同种类、应用场景的工业互联网设备开展分类分级评估。建立分类分级目录，形成重点保护设备及其安全策略并纳入网络关键设备和网络安全专用产品目录，高效开展强制性安全检测认证和审查。

三是完善工业互联网设备的安全防护规范、分类分级防护要求。针对不同类别和防护级别的设备，做好应用开发安全、系统服务安全、硬件安全、网络通信安全、数据安全等技术防护要求，形成设备的网络安全差异化、精细化管理模式。

四是建立工业互联网设备网络安全检测评估体系。加强设备进入市场前的网络安全试验验证、准入审核、测试认证以及应用过程中常态化的安全风险评估，以评促建，形成设备安全防护闭环。

五是强化工业互联网设备安全风险管理和应急处置，包括针对关键工业互联网设备的网络安全态势感知与监测预警，行业侧 / 企业侧的应急响应、事件处置的工具平台及机制方法。实时掌握设备安全态势和风险视图，为风险预警和应急工作提供常态化技术手段。

六、对策建议

（一）从国家层面完善工业互联网设备的网络安全准入机制

建议主管部门研究制定工业互联网设备安全相

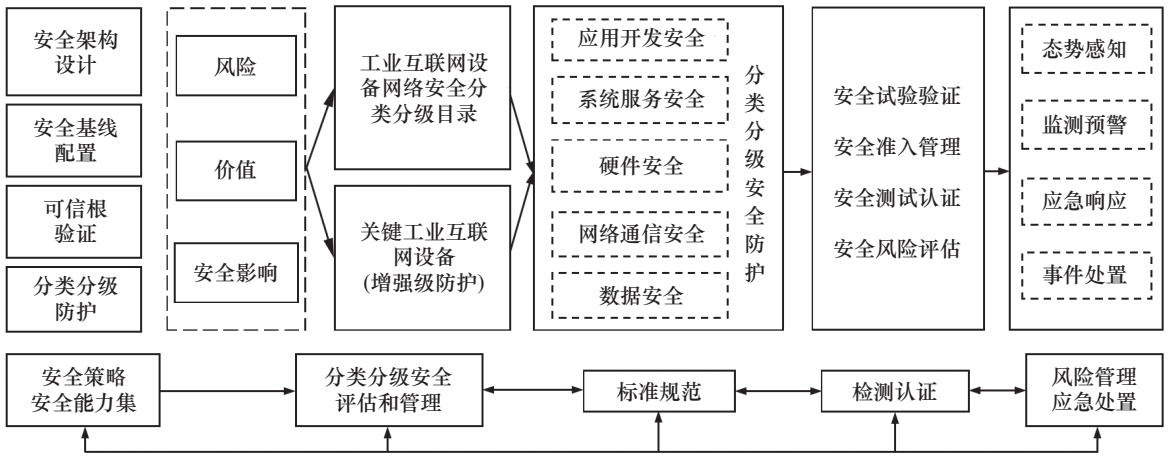

图 2　工业互联网设备安全防护实施路径示意图

关管理办法，颁布工业互联网设备安全强制标准和行业规范。强化工业互联网设备的设计、开发、实施、运行维护等全生命周期过程的网络安全规范要求，为企业产品安全开发、第三方机构测试认证、设备部署运行提供依据。《网络关键设备和网络安全专用产品目录（第一批）》发布后，目录中的设备产品检测认证工作已逐步展开，但工业互联网设备等暂未提及的设备仍处于监管盲区。建议研究梳理工业互联网关键设备并将之列为“网络关键设备和网络安全专用产品”，对设备进行分类分级；完善相关安全标准规范，建立体系健全的工业互联网设备安全监管和安全准入机制，保证设备在进入市场销售或使用前进行严格的安全检测。

（二）建立设备网络安全检测认证体系

建议建立工业互联网设备安全测试认证体系，加强安全测试验证，特别是针对工业设备在工业现场环境下的安全试验验证、无损检测、工业级安全防护应用。推动工业互联网设备安全相关测评认证中心建设，围绕设备安全性、防护水平等设计安全认证级别，开展设备的网络安全分类分级管理和差异化防护。向不同部门、行业、企业，提供安全级别选择，准确划分设备安全能力层级，提升市场良性竞争环境，促进厂商升级自身设备的安全性。推动安全检测认证和设备能力提升，匹配工业互联网设备的工业环境适用性、硬件安全、系统 / 固件安全、应用安全、数据安全、接入安全等要求，构建设备安全功能、抗渗透、恶意代码防范、抗分布式拒绝服务攻击、漏洞隐患防护等能力。

（三）促进设备网络安全架构研究和工程应用

建议在工业互联网设备设计阶段，充分考虑安全性因素，增强包括硬件安全、接入认证安全、数据传输安全、代码安全、系统服务安全在内的设备安全防护综合能力；建立设备的可信计算环境，引入硬件信任根对系统启动、应用运行、参数修改等行为进行可信验证。在设备安全基线配置方面，建议督促设备厂商在产品部署时向用户明示安全使用准则，使用技术手段保证设备的基线配置安全。工业相关设备制造商、自动化集成商与研究机构、安全企业等应加强合作，加快区块链、国产密码、可信计算等新技术应用进度，推动设备本质安全和技术产品研究创新。

（四）强化设备的网络安全风险监测感知

工业互联网设备种类多，适用不同行业和场景的防护技术能力差异较大。建议对于工业（尤其是制造业），推动行业性的设备采购与应用、网络化改造等安全测试评估，加强工业生产装备、工业主机、相关智能终端的安全监测和管理。建议主管部门引导行业加强工业互联网设备的安全监测和应急处置能力，加强设备的安全监测感知、态势研判、信息共享通报、应急处置，及时预警木马感染、病毒或主机受控等网络攻击事件；建立工业互联网设备安全检测、应急响应工具库，漏洞库、威胁情报

库等安全知识库，快速实施应急处置，防止黑客利用漏洞进行更广泛的攻击。

参考文献

[1] 张跃. 工业设备安装中的高精度测量方法探讨 [J]. 科技经济导刊, 2019, 27(24): 72.
Zhang Y. Discussion on high-precision measurement methods in the installation of industrial equipment [J]. Technology and Economic Guide, 2019, 27(24): 72.

[2] 张斌, 滕俊杰, 满毅. 改进的并行fp-growth算法在工业设备故障诊断中的应用研究 [J]. 计算机科学, 2018, 45(S1): 508–512.
Zhang B, Teng J J, Man Y. Application research of improved parallel fp-growth algorithm in fault diagnosis of industrial equipment [J]. Computer Science, 2018, 45(S1): 508–512.

[3] Samigulina G, Samigulina Z. Diagnostics of industrial equipment and faults prediction based on modified algorithms of artificial immune systems [J]. Journal of Intelligent Manufacturing, 2021 (1): 1–18.

[4] Compare M, Baraldi P, Bani I, et al. Industrial equipment reliability estimation: A bayesian weibull regression model with covariate selection [J]. Reliability Engineering & System Safety, 2020, 200: 1–10.

[5] 余骋远. 基于工业大数据的设备健康与故障分析方法研究与应用 [D]. 沈阳: 中国科学院大学(硕士学位论文), 2017.
Yu P Y. Research and application of equipment health and failure analysis based on industrial big data [D]. Shenyang: University of Chinese Academy of Sciences(Master's thesis), 2017.

[6] 金洪吉. 基于物联网的工业设备远程监控系统研究 [J]. 产业与科技论坛, 2020, 19(14): 35–36.
Jin H J. Research on remote monitoring system of industrial equipment based on Internet of things [J]. Industrial & Science Tribune, 2020, 19(14): 35–36.

[7] 戴认之. 人工智能技术在工业设备和系统智能运营维护的应用 [J]. 中国信息化, 2020 (7): 52–53.
Dai R Z. The application of artificial intelligence technology in the intelligent operation and maintenance of industrial equipment and systems [J]. China Information, 2020 (7): 52–53.

[8] Mourtzis D, Angelopoulos J, Panopoulos N. Intelligent predictive maintenance and remote monitoring framework for industrial equipment based on mixed reality [J]. Frontiers in Mechanical Engineering, 2020, 6(12): 1–12.

[9] 关键基础设施安全应急响应中心. 工控系统行业漏洞 [EB/OL]. (2020-12-01)[2021-01-05]. https://ics.cnvd.org.cn/.
Critical Infrastructure Security Response Center. Industrial control system vulnerabilities [EB/OL]. (2020-12-01)[2021-01-05]. https://ics.cnvd.org.cn/.

[10] Committee on National Security Systems. Frequently asked questions (FAQ) [EB/OL]. (2001-10-16)[2021-01-05]. https://www.niap-ccevs.org/Ref/FAQ.cfm#cat32.

[11] Department of Homeland Security. National strategy for global supply chain security [EB/OL]. (2017-07-13) [2021-01-05]. https://www.dhs.gov/national-strategy-global-supply-chain-security.

[12] Warner S, Mark R. S.734 - Internet of Things cybersecurity improvement act of 2019 [EB/OL]. (2019-06-19)[2021-01-05]. https://www.congress.gov/bill/116th-congress/senate-bill/734.

[13] 中华人民共和国国家互联网信息办公室. 各国网络安全审查制度及案例分析 [EB/OL]. (2015-04-17)[2021-01-05]. http://www.cac.gov.cn/2015-04/17/c_1114990146.htm.
Cyberspace Administration of China. Cyberspace security review system and case analysis for several countries. [EB/OL]. (2015-04-17)[2021-01-05]. http://www.cac.gov.cn/2015-04/17/c_1114990146.htm.

14] ISA Secure. IEC 62443 conformance certification certifying industrial control system equipment and systems [EB/OL]. (2021-01-05)[2021-01-05]. https://www.isasecure.org/en-US/Certification.

[15] 中华人民共和国国家互联网信息办公室. 关于发布《网络关键设备和网络安全专用产品目录（第一批）》的公告 [EB/OL]. (2017-06-09)[2021-01-05]. http://www.cac.gov.cn/2017-06/09/c_1121113591.htm.
Cyberspace Administration of China. Announcement on the issuance of the *Critical network equipment and special network security products catalog (first batch)* [EB/OL]. (2017-06-09)[2021-01-05]. http://www.cac.gov.cn/2017-06/09/c_1121113591.htm.

[16] 中华人民共和国工业和信息化部. 加强工业互联网安全工作的指导意见[EB/OL]. (2019-08-28)[2021-01-05]. https://www.miit.gov.cn/zwgk/zcwj/wjfb/txy/art/2020/art_c41cb8a2f6e74e239bae96068a2dc024.html.
Ministry of Industry and Information Technology of the People's Republic of China. Guiding opinions on strengthening industrial Internet security work [EB/OL]. (2019-08-28)[2021-01-05]. https://www.miit.gov.cn/zwgk/zcwj/wjfb/txy/art/2020/art_c41cb8a2f6e74e239bae96068a2dc024.html.