浅析我国工业互联网安全相关法律体系建设面临的挑战

肖泱枘，洪　晟
（北京航空航天大学 网络空间安全学院，北京 100083）

摘　要： 在工业互联网不断应用延伸的同时，各类安全问题接踵而至，诸如信息嗅探、数据泄露和设备故障等。如何在现存安全框架下降低安全风险成为各国关注的焦点。通过对比中外互联网安全框架，从我国工业互联网安全框架和相关标准的角度出发，分析存在的主要问题并提出有关法律体系建设的建议。

关键词： 工业互联网；安全框架；法律
中图分类号： TP391；D922　　**文献标识码：** A　　**DOI：** 10.19358/j.issn.2096-5133.2021.09.012
引用格式： 肖泱枘，洪晟. 浅析我国工业互联网安全相关法律体系建设面临的挑战[J].信息技术与网络安全，2021，40(9)：71-76.

Brief analysis of challenges faced by the construction of industrial Internet security related legal system in China

Xiao Yinan，Hong Sheng
（School of Cyber Science and Technology，Beihang University，Beijing 100083，China）

Abstract： With the vigorous development of industrial Internet，the corresponding security problems come one after another. How to reduce the security risks in the industrial Internet has become very important. By comparing the security framework of industrial Internet between China and foreign countries，this paper analyzes the existing problems of China′s industrial Internet security framework and related standards，puts forward some suggestions on the construction of the legal system.
Key words： industrial Internet；security framework；legal system

0 引言

“工业互联网”的概念于2012年由通用电气董事长伊斯梅尔提出。工业互联网的本质是通过网络将生产销售过程中的各个环节连接在一起，关联不同地区的设备和系统，继而推动工业体系智能化发展。从网络、平台和安全三个角度看，网络是工业互联网各要素互联的基础，平台是工业互联网汇集分析数据的核心，安全是工业互联网正常运作的保障[1]。新一代信息技术与工业经济深度融合过程中催生的工业互联网，驱动着经济社会的数字化转型，是第四次工业革命发展的基础[2]。

世界各国都非常关注工业互联网推动传统工业制造变革以及提升未来产业竞争力的潜力[3]。然而，传统的网络安全防护手段和安全框架无法满足高速发展下的工业互联网安全需求。我国34%的联网工业设备存在高危漏洞，仅2019年上半年就有高达5 151万起嗅探事件发生[4]。国外工业互联网方面的安全事件也屡见不鲜。以色列水利设施的SCADA系统曾多次遭受网络攻击。伊朗重要港口调节船只、卡车、货车流通的计算机系统遭到攻击，致使港口发生严重混乱。类似的事件还有许多。工业互联网安全法律保障体系建设还有待改进。2018年，习近平总书记在全国网络安全和信息化工作会议上指出，要“加强信息基础设施网络安全防护”[5]。2020年，工信部发布了《关于工业大数据发展的指导意见》，从宏观和微观两个层面布置多项重点任务，涉及数据汇聚、共享、应用等六个方面，针对我国工业大数据现存主要问题对症下药，补齐短板[6]。由此可见提升工业互联网安全框架的安全保障能力，完善相关法律体系建设迫在眉睫。

本文简要介绍了国内和国外工业互联网安全框架[7-11]，对比分析了两者的异同点[7,12-18]，并结合

工业互联网目前存在的问题[12,19-24],提出完善相应安全法律体系建设的建议。

1 工业互联网安全框架

工业互联网安全框架作为工业互联网安全体系的顶层设计和实施纲要,从全局的视角,对保障工业企业安全生产、发展进行统筹规划,为基层部署、实施安全防护措施提供思路,进而促进工业企业系统性安全防护能力提升[7]。工业互联网的诞生使得网络安全威胁不再局限于传统的信息安全,而是扩展到工业生产安全、人身安全、城市安全甚至影响到国家安全[8]。提升工业互联网安全保障是稳定发展现代化工业的必要条件。

1.1 传统网络安全框架

传统的网络安全框架包括 OSI 安全体系结构、P2DR 模型、IATF、IEC62443 等。根据系统对安全的需求,OSI 安全体系结构定义了 5 类安全服务,不同协议层需要提供不同安全服务,采取不同安全机制,达到保障资源安全的目的,该模型指导着安全标准的设计,并提供了通用的术语平台[9]。作为动态网络安全模型的雏形,P2DR 为之后动态模型的研究发展奠定坚实基础,在策略的指导下通过防护、检测和响应三个阶段实现闭环控制[9-10],但 P2DR 模型存在忽略了人员流动、人员素质及策略贯彻的不稳定性等内在的变化因素。IATF 强调从边界的角度划分信息系统,从在端系统、边界系统、网络系统以及支撑系统四方面入手,形成了对网络系统的纵深防御,最大限度降低安全风险,保障系统安全[11]。IEC62443 针对工业生产活动中涉及到不同利益相关者,提出不同安全要求,其中根据抵御威胁的能力将控制系统按等级划分成相对封闭的区域,通过管道实现区域之间的数据通信[9]。

然而,以上模型除 P2DR 外,仅采取了静态安全防护措施,而没有部署主动的安全防护措施,对入侵行为无法实时动态监测,对系统中的漏洞无法及时检查更新,无法满足当前工业互联网的安全需求[9]。

1.2 国外工业互联网安全框架

美国在“国家先进制造战略计划”中将工业互联网列为确保国家优势的重要手段,对工业互联网安全高度重视。2016 年,美国工业互联网联盟发布工业互联网安全框架 1.0 版本,定义了 3 个层次、6 个安全功能。安全功能中底层的安全模型策略和中层的数据保护支撑着顶层的 4 个核心功能,分别是端点保护、通信与连接保护、安全监控与分析、安全配置管理。同时框架明确将信息安全、功能安全、可靠性、弹性和隐私安全定义成为工业互联网提供安全可信环境的五大关键要素。该框架侧重于安全实施,通过分层确定了各层需要提供的安全服务,为工业互联网框架的深入研究与实施提供了理论指导[9]。

2013 年德国工业 4.0 平台在汉诺威工业博览会上正式发布。在工业 4.0 参考架构(RAMI4.0)中定义了一个三维描述模型,分别从 CPS 功能视角、价值链视角和工业系统视角衡量安全性,并因此串联起框架中的各结构元素。该框架采用了分层思想,旨在实时保障所属不同层次的资产在全生命周期中的安全性[9]。

总结分析上述框架,可以得到三个共性:首先根据具体系统和安全需求分类部署对应安全防护措施和对应分类标准,其次安全框架需采用动态安全分析模型,即不仅需要采用防火墙、入侵检测等静态安全技术,还应将时间等动态要素引入到模型中;第三需要从技术手段和管理手段出发,双管齐下,将安全管理机制融入安全模型中,规范工业互联网参与者的行为,使模型的安全保障能力发挥到最大化[9]。

1.3 国内工业互联网安全框架

2016 年,我国工业互联网产业联盟发布了《工业互联网体系架构(版本 1.0)》(下称:架构 1.0),围绕设备、控制、网络、应用、数据五大安全重点,建立工业互联网安全架构。架构 1.0 以明确安全防护对象、落实安全防护措施、提升安全防护管理为抓手构筑工业互联网安全防护体系[7]。工业互联网安全防护工作的基础是明确安全防护对象,即明确防护的范围和方向。架构 1.0 采用静态防护与动态防护相结合的安全防护措施,当发生安全事件时,系统能及时响应、处置并恢复还原。安全防护管理将技术融入管理手段中,在技术层面上对面临的安全威胁和风险进行评估,并提出对应安全策略;在管理层面上通过设定安全目标,制订管理原则,结合管理方法,搭建完备的管理流程,从管理和技术两方面入手,全面提升安全防护水平,保障安全防护措施的实施[7]。架构 1.0 的三个防护视角相互补充,技管结合,部署安全防护措施、协同安全防护管理共同保护防护对象,形成一个多维立体的防护体系[7]。

对比分析美国 IISF1.0 版本和中国的架构 1.0,

虽然前者从功能角度出发，后者从工业互联网安全实施角度出发，呈现视角有所差异，但设计的思路是一致的。两者都采用技术与管理手段相结合的方式，全面持续提升工业互联网安全防护能力。

2019 年，我国《工业互联网体系架构(版本 2.0)》发布，在继承架构 1.0 核心理念、要素和功能体系的基础上，从业务、功能、实施三个视图重新定义了工业互联网的参考体系架构。架构 2.0 较架构 1.0 提供了一套可供企业开展实践的方法论，从战略层面为企业开展工业互联网实践指明方向，并结合规模化应用需求对功能架构进行升级和完善，提出更易于企业应用部署的实施框架[12]。为防范针对工业互联网的网络攻击，维持工业互联网有序健康发展，架构 2.0 统筹考虑工业互联网在信息、功能与物理三方面的安全。在架构 2.0 中，安全实施框架包括边缘安全防护系统、企业安全防护系统、企业安全综合管理平台、行业安全平台及国家级安全平台，体现了工业互联网安全功能在“设备、边缘、企业、产业”的层层递进，全方位保障工业互联网的安全实施[12]。

2 工业互联网安全相关法规

工业互联网连接着大量的设备和系统，拥有企业、个人信息和重要的相关数据[13]。这些信息涉及大量个人信息、商业信息乃至国家机密的数据，使得网络攻击从公共互联网向重要领域工业互联网转移[14]。工业互联网逐渐成为国家级网络空间安全对抗的新重点。

面对不断升级的攻击方式，为营造健康工业互联网发展环境，各国高度重视，积极采取行动。2014 年，美国发布《国家网络安全保护法案》，从法律层面上鼓励社会、企业积极开展对关键基础设施信息共享、标准制定、技术队伍建设和教育培训等方向的研究[15]。美国时任总统特朗普在 2017 年签署的《增强联邦政府网络与关键基础设施网络安全》行政令提出要明确各机构职权，通过市场透明度提高关键基础设施的网络安全防护水平[15-16]。欧盟 2016 年通过的《网络和信息系统安全指令》规定了网络运营者与参与者在关键基础设施遭遇安全风险时的义务，以方便更好地应对处置相关网络攻击[15]。

我国也在逐步推进和工业互联网安全相关的法律、标准。2019 年《工业互联网综合标准化体系建设指南》发布，为工业互联网标准体系建设指明方向，该指南涉及设备安全、工控系统安全、数据安全、网络安全、平台安全等方面[17]。同年发布《中华人民共和国密码法》，该法增加了工业控制系统安全的相关要求，对提升工业互联网安全保护能力有重要意义[13]。工业和信息化部发布的《工业互联网企业网络安全分类分级指南(试行)》提出建立企业分类分级安全管理制度，进一步完善了政府监管与企业责任制相结合的安全管理体系，为企业开展工业互联网安全工作提供了指引[18]。我国工业互联网产业政策体系不断向前推进，2019~2020 年我国工业互联网相关政策进展如表 1 所示。

表 1 2019~2020 年我国工业互联网相关政策

2019	《工业互联网网络建设及推广指南》、《加强工业互联网安全工作的指导意见》、《关于加快培育共享制造新模式新业态 促进制造业高质量发展的指导意见》、《制造业设计能力提升专项行动计划(2019-2022 年)》
2020	《关于推动工业互联网加快发展的通知》、《工业互联网创新发展行动计划(2021-2023 年)》、《工业数据分类分级指南 (试行)》、《智能汽车创新发展战略》

3 工业互联网中存在的风险

当前，我国工业系统安全保障体系建设已经较为完备，但是面对日益多样化、复杂化的各类攻击方式，目前采用的工业互联网安全保障体系还不够完善[19]。工业互联网安全的范畴包含工业互联网平台安全、网络安全、工业控制系统安全等。以工控系统为例，根据国家信息安全漏洞共享平台工控漏洞子库 CNVD 的数据，我国 2015~2020 年新增工控系统漏洞数量及等级分布如表 2 所示。从 2017~2020 年，高、中危漏洞爆发次数明显增涨，我国《工

表 2 2015~2020 年新增工控系统漏洞数量及等级分布(个)

年份	新增高危漏洞	新增中危漏洞	新增低危漏洞	新增漏洞
2015	37	71	11	119
2016	85	90	9	184
2017	201	172	14	387
2018	242	192	14	448
2019	201	221	26	448
2020	259	346	47	652

业互联网体系架构(版本 2.0)》2019 年才发布实施，仍存在不少问题有待解决。

3.1 新技术的安全性面临考验

大数据技术、5G、人工智能和边缘计算等新技术为工业互联网中带来充沛活力的同时，也带来了许多安全隐患。大数据技术在工业互联网平台中的广泛应用使得平台上的用户数据、企业生产资料、商业秘密等敏感信息存在泄露隐患，工业大数据应用存在安全风险[12]。在 5G 环境中进行延时边缘计算时，由于数据传输效率更快且数据会在传输的同时完成处理，为了完成边缘计算指令，系统会弱化系统安全保护[20]。5G 网络可以兼容工业互联网中使用的各种软件系统，但网络环境需要具有良好的开放性，这种需求可能会导致端口容易受到外部网络的干扰[20]。工业网络协议数量众多，其中大量工业通信协议是私有的、不对外公开的，其安全性无法得到保障，可能会导致非法访问程序进入工业互联网环境中[21]。

3.2 现存缺陷种类多样，对安全防护能力提出挑战

当前我国工业行业使用的重要关键设备和基础软件绝大多数来自国外[15]，同时，基于传统工业的我国工业互联网设备重效率、轻安全，通过牺牲安全性来换取稳定性。出于对产品效率和空间的考量，工控系统和设备的设计人员将有限的计算资源和存储空间大部分用于性能的提高，使得设备无法支持高级复杂的安全防护策略，很难确保系统和设备的安全使用[19]。此外，许多工厂内部没有部署安全保障设施，缺乏针对设备操作者的网络安全意识培训和操作流程的规范[19]。大部分工业互联网相关企业缺少对网络安全风险的认识，导致在发展中忽视安全的影响。业内缺少专业机构、网络安全企业、网络安全产品服务的信息渠道和有效支持，工业企业网络安全风险意识、监测和应急处置等网络安防能力普遍不足[19]。2018 年，工业和信息化部网络安全管理局委托相关专业机构对 20 余家典型工业企业、工业互联网平台企业安全检查评估时就发现了 2 000 多个安全威胁[22]。

3.3 安全责任界定和安全监管难度大

传统的工业系统与攻击者存在着物理隔绝，除非身处工厂内部否则远程的攻击者很难实施攻击。然而，这种封闭的环境逐渐被工业互联网替代，工业互联网将原本独立存在的设备、系统和人员连接在一起的同时，也使得风险不再孤立。工业互联网互联互通的特点使得在面对攻击时系统会更加脆弱，容易形成链式反应，可能会造成严重的后果。工业互联网的安全性遵循木桶原理，风险链上的短板可能会引起整个工业互联网生态的变化[23]。工业互联网业务和数据在系统层、监管层、应用层等多个层级间流转，安全责任主体涉及工业企业、设备供应商、平台运营商等[24]。发生安全事件后，很难确定故障位置，明确责任归属。

4 法律体系建设对策及建议

针对上述工业互联网中存在的安全风险需要加强相关法律、制度和规范方面的建设。

4.1 加强隐私和数据保护

对于隐私及数据保护问题，建议建立工业企业设备分级分类制度，针对敏感工业内容，建立设备审查制度，保障设备使用、生产安全；建议立法规范工业信息数据分级，定义数据安全流向，对工业信息数据的使用划分权限，保障工业信息数据的真实性、保密性、完整性、可追溯性及脱敏后的可共享性；建议增加关键人员审查制度，明确责任主体边界，保障工业隐私和实现数据保护。

4.2 提高安全防护能力建设

建议依照工业生产内容的敏感程度对工业互联网设备安全性设立分级标准，鼓励工业企业提高设备安全性。在安全策略的指导下根据不同安全需求和工作内容层次化管理，做好安全域的划分，定期进行相应攻防测试，提升应急响应能力，最大程度降级安全风险，保障系统安全。加强对核心技术、关键基础设施设备的开发，摆脱技术依赖，搭建我国自主研发的工业互联网体系。

4.3 培养技术型人才增强后备力量

加强工业互联网安全人才培养，增强后备技术力量，对工业互联网安全人才和互联网安全服务公司开展相关认证，为工业互联网提供安全、可信的维护和技术支持。建议规范工控系统操作规范和要求，设立应急响应处置标准，定期对关键人员进行培训检查。依法落实企业主体责任，划分工业互联网安全责任部门，明确各部门责任人，建立网络安全事件报告和问责机制。

4.4 增强对风险的实时监测管控

建议建立测评系统，根据不同平台安全需求建立风险分析框架，对工业生产的全生命周期进行动

态跟踪，找出可能存在的风险点，并提出针对性的保护措施。重点突破风险链上短板，降低风险间互相触发的连锁性，对各个环节进行切片隔离管理，提升整体安全保障能力。经过认证和测评后的平台、人员方可加入相应的工业互联网体系。建议由科研院所主导，协同业内企业及有关部门尽快搭建国家级工业互联网风险动态监测平台，逐步提高工业网络安全公共服务能力，并提供一套可应用于实践的风险处理标准化模板。建议对国内外各类引发安全事件的漏洞隐患总结分析、风险预测，完善我国工业互联网漏洞库等安全基础资源库，提高工业互联网安全性。

4.5 多方管理增强取证能力

建议推进政府协同社会多方主体共同治理，通过政府监管、行业自律、企业管理等方式达到保障工业互联网安全的目的。建议从政府层面强化工业互联网后台留存取证制度建设，对接入工业互联网中的设备、系统和人员进行认证，并对系统的操作日志、流量数据、异常事件和服务器维护情况等关键信息进行全量留存。建议从行业层面加强录音录像证据的采集，便于相关部门在发生涉及违法违规网络安全事件后进行调查取证，明确行为实施者、责任承担者。建议工业企业对重要应用系统和数据库进行定期备份。当受到攻击或操作失误后能够及时恢复系统，并实现对攻击行为、违法行为再现，降低数据丢失可能造成的风险和损失，为之后研究分析漏洞、攻击方式提供途径。

4.6 针对新技术设定标准规范

建议完善工业用户安全机制，强化身份认证管理。依据《中华人民共和国密码法》和信息安全等级保护，强化加密技术在工业互联网中的应用，普及强口令在关键基础设施的落实。针对各类私有工业通信协议进行安全性分析，并建立统一的安全标准，规范工业互联网中应用的协议种类。

5 结论

提高工业互联网中的安全性，要采用技术手段和管理手段相结合的办法。首先是根据发生的安全事件和经验不断完善工业互联网安全框架及相关法律体系建设，从错误中汲取养分，努力减少未来发生危险的可能性，提升工业信息安全技术能力。其次，需要用法律的手段来规范和完善工业互联网中的行为，提高工业互联网从业者的安全意识，使工业互联网中每一环节都能定位到责任人。

2019 年，我国十部门印发了《加强工业互联网安全工作的指导意见》提出了七项主要任务和四项保障措施，明确指出了指导思想、基本原则和总体目标。这份指导意见为之后工业互联网安全的发展指明了方向，但具体落实到实际中的办法还需要人们不断摸索。工业互联网安全相应的法律法规体系建设也有待完善。

参考文献

[1] 工业互联网产业联盟.工业互联网体系架构(版本 1.0)[EB/OL].(2016-09-07).http://www.aii-alliance.org/static/upload/202003/0302_143638_771.pdf.

[2] 李海花.工业互联网加速创新发展分析与展望[J].信息通信技术与政策，2020(10)：6-9.

[3] 余晓晖，刘默，蒋昕昊，等.工业互联网体系架构 2.0[J].计算机集成制造系统，2019，25(12)：2983-2996.

[4] 国家互联网应急中心(CNCERT).2019 年我国互联网网络安全态势[R].2020.

[5] 谭浩俊.树立正确的网络安全观，构建牢固的网络安全网[EB/OL].(2018-04-24).http://www.cac.gov.cn/2018-04/24/c_1122733270.htm.

[6] 工业和信息化部.《工业和信息化部关于工业大数据发展的指导意见》解读[EB/OL].(2020-05-16).http://www.cac.gov.cn/2020-05/16/c_1591178516-877644.htm?from=singlemessage.

[7] 刘廉如，张尼，张忠平.工业互联网安全框架研究[J].邮电设计技术，2019(4)：53-57.

[8] 黄鑫.我国工业互联网已进入大发展时代[EB/OL].(2018-02-07).http://www.cac.gov.cn/2018-02/07/c_1122379945.htm.

[9] 刘晓曼，李艺，吴昊.工业互联网安全架构及未来发展思考[J].保密科学技术，2019(3)：12-19.

[10] 黄泽斌.基于 P2DR 模型的安全解决方案研究[J].科技信息(科学教研)，2007(29)：79-80.

[11] 宁向延，张顺颐.网络安全现状与技术发展[J].南京邮电大学学报(自然科学版)，2012，32(5)：49-58.

[12] 工业互联网产业联盟.工业互联网体系架构 2.0[EB/OL].(2020-04-23).http://www.aii-alliance.org/static/upload/202004/0430_162140_875.pdf.

[13] 袁捷，张峰，于乐.5G+工业互联网安全分析与研究[J].信息通信技术与政策，2020(10)：18-22.

[14] 于成丽.工业互联网安全形势及监管政策浅析[J].

保密科学技术,2020(5):16-19.
[15] 刘冬,程曦,杨帅锋,等.加强我国工业信息安全的思考[J].信息安全与通信保密,2019(8):24-35.
[16] 钟欣.美国总统特朗普签署网络安全行政令[N].人民邮电报,2017-06-05.
[17] 工业和信息化部,国家标准化管理委员会.工业互联网综合标准化体系建设指南[R].2020.
[18] 尚文利.功能安全与信息安全相结合,实现工业系统的两安融合[J].自动化博览,2020,37(2):16-17.
[19] 安成飞,周玉刚.智能制造工业互联网的安全分析与防护[J].自动化博览,2021,38(1):82-85.
[20] 康帝.5G网络中工业互联网安全问题研究[J].电子元器件与信息技术,2020,4(6):22-23.
[21] 谢丰,伊胜伟,高洋.加强工业互联网风险分析与安全测评,保障"新基建"安全[J].中国信息安全,2020(7):36-38.
[22] 科技日报.5G面临风险大考:我国一半以上工控系统带毒运行[EB/OL].(2019-06-24).http://www.xinhuanet.com/ 2019-06/24/c_1124660796.htm.
[23] 赵丽莉,周彤.以CPS为核心的工业互联网安全风险及监管控制[J].北京科技大学学报(社会科学版),2021,37(1):48-55.
[24] 郭宾,雷曜,朱奕辉.浅谈工业互联网安全服务云建设思路[J].中小企业管理与科技(中旬刊),2020(5):128-129.

(收稿日期:2021-03-31)

作者简介:

肖泄栅(2000-),女,本科,主要研究方向:网络信息安全。

洪晟(1981-),男,博士,副教授,主要研究方向:网络信息安全、复杂系统安全运行状态监测与健康管理、复杂系统通用质量"六性"技术。

(上接第57页)

参考文献

[1] 陈晓兵,陈凯,徐震,等.面向工业控制网络的安全监管方案[J].信息网络安全,2016(7):61-70.
[2] 孟瑾,石怀忠,崔建华.基于烟草工控网络安全防护策略与应用[J].网络安全技术与应用,2019(12):158-161.
[3] 唐亮,唐树莺,杨帆.卷烟物流分拣工业控制系统网络安全防护体系设计[C]//中国烟草学会2017年学术年会,2017.
[4] 匡建华.烟草企业网络安全防护体系建设[J].电子技术与软件工程,2017(18):205-206.
[5] 曾瑜,郭金全.工业控制系统信息安全现状分析[J].信息网络安全,2016(9):169-172.
[6] 何巍.基于纵深防御的烟草行业工控安全解决方案[J].电子技术应用,2019,45(3):88-91.
[7] 耿欣.烟草行业工业控制系统安全保障体系研究[J].烟草科技,2017,50(12):99-105.
[8] 李愿军.省级烟草企业网络与信息安全的思考[J].电子技术与软件工程,2017(21):211-212.
[9] 张承亮,宁欣,郭军,等.烟草行业的数据防泄漏[J].电子技术与软件工程,2019(7):194-195.
[10] 朱洪波.烟草行业数据安全管理平台的研究[J].网络安全技术与应用,2019(6):93-95.
[11] 韩晓樱,冯明辉.浅谈福建中烟网络安全体系建设[J].网络安全技术与应用,2019(7):115-116.
[12] 王昱镔,陈思,程楠.工业控制系统信息安全防护研究[J].信息网络安全,2016(9):35-39.
[13] 樊金健,谢一飞.基于安全域划分的网络安全体系设计:保障烟草工业企业安全生产[J].工业技术创新,2019,6(2):59-65.
[14] GB/T 22239-2019 信息安全技术-网络安全等级保护基本要求[S].北京:中国标准出版社,2019.
[15] 陈兴毕,李源,殷耀华,等.基于烟草工控系统网络安全风险评估的研究与应用[J].信息技术与网络安全,2019,38(7):19-26.

(收稿日期:2021-06-25)

作者简介:

张悦(1990-),女,硕士,工程师,主要研究方向:网络安全。

荆琛(1994-),女,硕士,助理工程师,主要研究方向:网络安全。

衣然(1988-),男,硕士,工程师,主要研究方向:网络安全。

版权声明

经作者授权，本论文版权和信息网络传播权归属于《信息技术与网络安全》杂志，凡未经本刊书面同意任何机构、组织和个人不得擅自复印、汇编、翻译和进行信息网络传播。未经本刊书面同意，禁止一切互联网论文资源平台非法上传、收录本论文。

截至目前，本论文已经授权被中国期刊全文数据库（CNKI）、万方数据知识服务平台、中文科技期刊数据库（维普网）、JST 日本科技技术振兴机构数据库等数据库全文收录。

对于违反上述禁止行为并违法使用本论文的机构、组织和个人，本刊将采取一切必要法律行动来维护正当权益。

特此声明！

《信息技术与网络安全》编辑部

中国电子信息产业集团有限公司第六研究所