石化行业工控系统网络安全防护体系建设探析

霍朝宾，武　蕊
（华北计算机系统工程研究所，北京 100083）

摘　要：随着工业互联网的不断发展，石化行业工业控制系统网络安全风险逐渐突出。在“十四五”信息化和工业化深度融合发展的大背景下，工控系统作为国家关键信息基础设施重点保护对象，快速提升其安全防护能力尤为重要。以近年工控系统网络安全事件为出发点，立足国家网络安全法律法规以及等级保护政策标准体系，梳理了石化行业工控系统网络安全防护建设思路，提出了一套石化行业工控系统网络安全防护体系。

关键词：工控系统；网络安全；防护体系；等级保护；自主安全
中图分类号：TP393　　文献标识码：A　　DOI：10.20044/j.csdg.2097-1788.2022.02.009
引用格式：霍朝宾，武蕊. 石化行业工控系统网络安全防护体系建设探析[J]. 网络安全与数据治理，2022，41(2)：55-60.

Analysis on the construction of network security protection system of industrial control system in petrochemical industry

Huo Chaobin, Wu Rui
(National Computer System Engineering Research Institute of China, Beijing 100083, China)

Abstract: The cybersecurity risks of industrial control systems in the petrochemical industry have gradually become prominent with the continuous development of the Industrial Internet. In the context of the in-depth integration of informatization and industrialization in the "14th Five-Year Plan", industrial control systems, as the key protection objects of national key information infrastructure, are particularly important to rapidly improve their security protection capabilities. Taking the industrial control system network security incidents in recent years as the starting point, based on the national network security laws and regulations as well as the hierarchical protection policy standard system, the idea of the network security protection construction of the industrial control system in the petrochemical industry is sorted out, and a set of network security protection system for the industrial control system in the petrochemical industry is proposed.

Key words: industrial control system; cyber security; protection system; grade protection; autonomous and secure

0 引言

工业互联网安全与工业控制系统（以下简称工控系统）安全密切相关，随着工业互联网的应用领域日益广泛，相关安全事件连年频发。工控系统作为石化行业网络安全建设的重要分支，需要不断提升其安全防护体系建设能力，实时构建弹性防御体系，避免、转移、降低系统面临的风险，从而切实保障工控系统网络安全。

1 研究背景

近年来，全球石化行业网络安全事件频发。2020年5月，台湾两大炼油厂分别于两天内遭受不同程度的黑客勒索，该勒索软件攻击系统服务器，使计算机和IT系统强制关闭，给各加油站造成一定程度上的混乱[1]。2021年5月，美国燃油管道运营商Colonial Pipeline遭黑客勒索软件攻击，攻击者以挟持关键基础设施为目的，切断了美国东部地区油气输送主动脉，导致全美进入国家紧急状态，严重影响国家的正常运作能力[2]。同年7月，石油巨头沙特阿美遭盗窃1 TB专有数据，多处炼油厂的重要数据遭受泄露风险[2]。一系列安全事件的发生使我国石化行业网络安全防护建设压力倍增。

当下中国进入“十四五”全面深化改革新时期。

2021 年 3 月 5 日,十三届全国人大四次会议公布《国民经济和社会发展第十四个五年规划和 2035 年远景目标纲要》,提出要加强重要网络和信息系统安全保障,要提升网络安全威胁发现、监测预警、应急指挥、攻击溯源能力,同时还要建立健全关键信息基础设施保护体系,提升安全防护和维护政治安全能力[3]。自 2021 年 9 月 1 日起施行的《关键信息基础设施安全保护条例》指出,国家对关键信息基础设施实行重点保护,采取措施,监测、防御、处置来源于境内外的网络安全风险和威胁,保护关键信息基础设施免受攻击、侵入、干扰和破坏[4]。与此同时,石化行业工业互联网应用进程正不断推进深入,在过去已建立的两网连接中,将进一步响应“十四五”信息化和工业化深度融合发展规划,加快推进工业控制网络与企业网或互联网之间互联互通。但随着国家网络安全相关政策的相继出台,以及当下石化行业工控系统网络安全防护建设所面临的紧迫形势,工业互联网为工控系统带来巨大创造力和生产力的同时,也会引入更加复杂、严峻的安全问题。因此当务之急就是规划并建设一套安全高效的网络安全防护体系。

2 石化行业工控系统网络安全防护现状

如今石化行业工控系统网络安全防护体系建设面临多重机遇和挑战,建立围绕安全服务、安全技术的全方位防护体系,最终实现石化行业工控产品自主安全显得尤为关键。通过对石化行业部分企业工控系统调研发现,现阶段网络安全问题主要集中在以下三个方面。

2.1 安全服务保障不完善

通过调研石化行业不同工艺流程下的多家单位,发现大多企业都未建立一套完善的安全服务体系,安全服务保障工作相对缺失。

安全服务体系包含安全咨询服务、安全检测服务、风险评估服务、渗透测试服务、安全培训服务、安全运维服务、安全集成服务等。安全服务体系建设是为提高石化行业工控系统网络安全防护能力,保障工控系统每个工艺流程在规划、集成、建设、实施、运维等各方面达到网络安全需求,通过安全专家提供完整的安全咨询或解决方案,帮助客户应对来自网络安全领域的各种挑战[5]。

以安全检测服务中等级保护服务为例:测评机构为被测系统责任单位提供安全服务,在定级阶段,网络运营者主要使用 GB/T22240 和相应的行业或企业标准来划分定级对象和确定安全保护等级;在安全建设阶段,网络运营者主要使用 GB/T22239-2019、GB/T25070-2019 和相应的行业或企业标准来进行规划设计和建设工作,科学合理地选择和部署必要的安全措施[6];在等级测评阶段,测评机构主要依据 GB/T28448-2019、GB/T28449-2018 和相应的行业或企业标准来规范和指导等级测评工作。针对石化行业工控系统实施等级保护工作,首要任务应摸清下属企业工控系统网络安全防护现状,理清安全防护需求,针对企业摸底情况,为被摸底企业出具工控系统网络边界安全防护整改方案和措施建议,针对工控系统网络安全等级保护需求,形成工控系统定级指导意见和工控系统定级指南,用于指导企业工控系统定级备案工作,并定期依照国家有关规定开展网络安全测评,针对测评问题进行安全建设整改,并全程接受有关部门监督检查[7]。

随着信息技术的快速提升,石化行业工控系统网络安全防护已不再局限于狭义的信息系统,而是逐渐扩展到云计算、大数据、物联网、移动互联等各类新技术。面对石化行业逐步向工业互联网生态转型的现实情况,未来对工控系统的安全服务需求也将逐步提升[8]。

2.2 安全技术支撑不全面

石化行业作为能源行业重要组成部分,一度使其成为黑客攻击的重要目标。石化行业工控系统因其部署相对封闭、单一,致使针对石化行业工控系统的信息安全事件具有目标明确、隐蔽性强、破坏严重等特点。通过调研走访石化行业相关单位发现,石化行业工控系统在工控设备使用时,针对工控设备自身的安全技术支撑不全面,主要表现在通信协议安全性较弱、工控设备存在安全漏洞较多两方面,由此二者带来的信息系统安全隐患很难被传统的信息安全防护技术所发现。

石化行业工控设备通信协议安全性较为薄弱,以 SCADA 系统为例,其现场设备层和过程控制层主要使用现场总线协议和工业以太网协议。现场总线协议在设计时大多没有考虑安全因素,缺少认证、授权和加密机制,数据与控制系统以明文方式传递,因此数据可以很容易地被攻击者捕获和解析。

石化行业工控设备存在较多安全漏洞，传统设备渐渐被智能化设备取代，致使工控设备遭受到更多的攻击，攻击的形式也越来越多样化[9]，其中，最常见的攻击方式就是利用工控系统的漏洞。根据 CNVD（国家信息安全漏洞共享平台）的漏洞数据，2011~2021 年（其中 2021 年漏洞数量统计截止时间为 2021 年 5 月）工控漏洞走势如图 1 所示。从图中可以看出，自 2016 年始，针对工业控制系统安全问题的关注度日益提升，工控漏洞数量整体上呈现逐年上升的趋势。

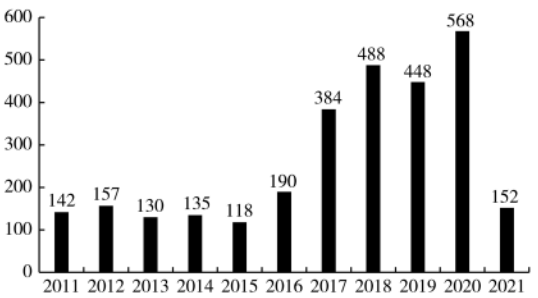

图 1　2011~2021 年工控漏洞趋势图

石化行业的生产离不开工控设备的支持，工控漏洞的发展趋势也侧面反映了石化行业工控设备安全风险形势日益严峻。

石化行业工控设备通信协议的脆弱性和工控设备安全漏洞的威胁性广泛存在，是整个行业网络安全防护技术措施缺失、技术支撑不全面的表现，从而也增加了黑客从网络中各个维度对网络进行攻击的可能性[10]。如果不采取有效的安全技术防护手段进行遏制，不仅会危害石化行业工控系统网络安全，还会危及社会秩序、公共利益以及国家安全，造成一定的国民经济损失，严重可能演化成网络武器，通过战略情报采集、渗透潜伏、精准打击等方式，直接破坏工业互联网核心基础设施。

2.3 核心技术产品受制于人

通过调研石化行业某单位工控相关生产业务，主要包括石油的开采、存储、炼化、输送等环节，发现涉及控制系统的厂商主要有霍尼韦尔、西门子、艾默生、和利时、罗克韦尔等常见品牌。我国石化行业工控设备大多仍严重依赖国外产品，其中超过 90%的PLC 为国外品牌[11]。图 2 统计了石化行业应用广泛的几大工控设备品牌的市场占有率，大众主流品牌在石化行业工控领域占据大多数份额，如西门子占 32%、艾默生占 15%、霍尼韦尔占 12%。

同时，在石化行业工控系统边界防护上也涌现了众多品牌，但在实际应用上国外设备仍占据主导地位[12]。图 3 统计了石化行业工控系统应用广泛的几大边界设备市场占有率，其中 Tofino 工业防火墙使用率达 51%、思科工业防火墙占据 23%。品牌多样化也导致了石化行业工控系统遭受攻击的形式也越来越多样化。

当下我国石化行业工控领域核心技术产品对国外依赖严重，表 1 统计了目前我国石化行业工控领域信息系统核心技术产品使用情况。从表中可以看出，从核心处理器、操作系统、服务器、网络设备到编程编译工具，大都依赖国外品牌。但是近年来“微软黑屏门”“微软操作系统停更”等安全事件的发生，显然已为我国加快发展自主安全产品，实现国产化替代按下加速键。

3 石化行业工控系统网络安全防护体系建设

2017 年，国家发布《中华人民共和国网络安全法》，明确要求实施信息安全等级保护制度[13]。2019

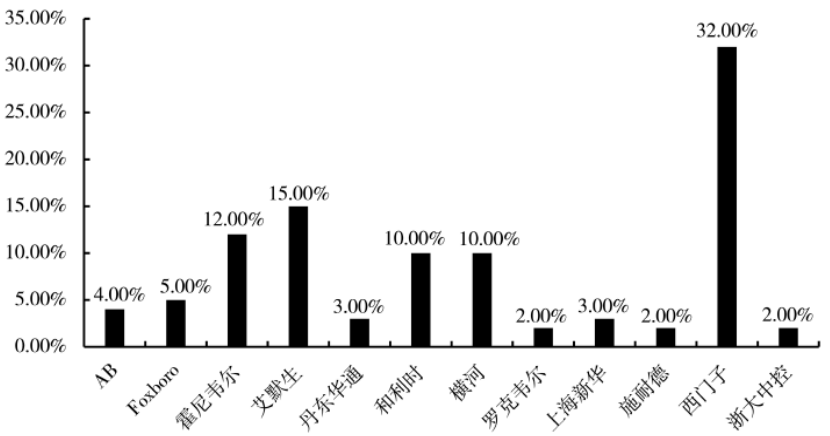

图 2　石化行业工控系统品牌统计

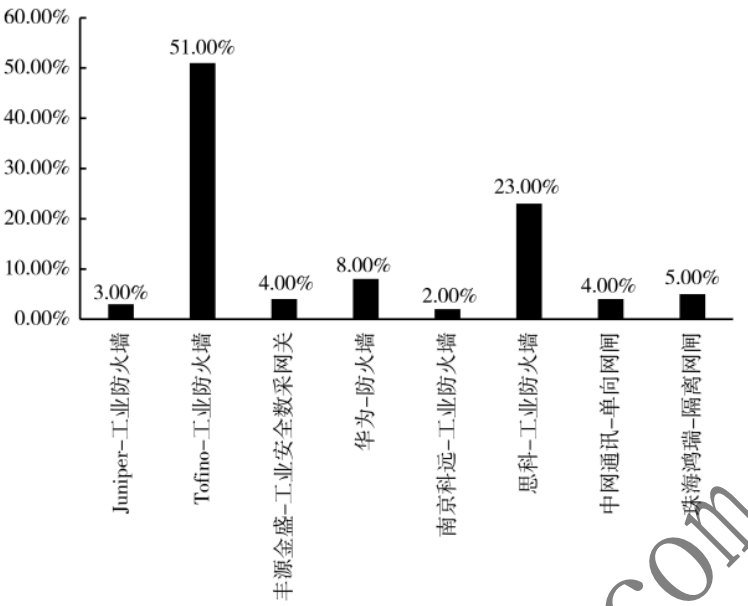

图 3 石化行业边界防护设备使用统计

表 1 石化行业信息系统核心技术产品使用品牌统计

核心技术产品	品牌	核心技术产品	品牌
核心处理器	Intel、ARM、infineon	服务器	IBM、惠普、DELL
嵌入式操作系统	WindowsCE、ecos、VxWorks	工业计算机	IBM、惠普、DELL、西门子
桌面操作系统	Windows、MacOS	网络设备	CISCO、瞻博
数据库	SQL Server、ORACLE、MySQL	DCS、PLC、MC、RTU	施耐德、罗克韦尔
编程编译工具	CoDeSys、infoream	工业软件	西门子、罗克韦尔
现场总线	PROFI NET、EtherCAT、ControlNet	HMI	MITSUBISHI ELECTRIC、OMRON
传感技术	Endress+Hauser、HACH	变频器伺服	ABB、Panasonic

年,基于网络体系新的形势和发展需求,公安部发布了网络安全等级保护 2.0 国家标准,在等保 1.0 的基础上更大程度完善了保护对象的范围,将大数据、云计算、工控全面纳入保护范围,采用“一个中心,三重防护”的理念,强调将安全检测、应急处理、事件追溯等措施落实,总体上从安全物理环境、安全通信网络、安全区域边界、安全计算环境、安全管理中心、安全管理制度等十个层面提出了更高的技术和管理要求[14-15]。

石化行业工控系统在以网络安全法律法规政策体系、等级保护政策标准体系为防护依托的基础上,亟需搭建一套完整的以安全服务为保障、安全技术为支撑、自主安全产品为导向的网络安全防护体系,切实减少网络安全对企业带来的损失。为此本文提出一套石化行业工控系统网络安全防护体系构建框架,如图 4 所示。

安全服务体系是以 GB/T22239 网络安全等级保护基本要求、GB/T20984 信息安全风险评估规范等为理论依据,在安全咨询基本服务的基础上,通过对石化行业工控系统定期进行安全检测、风险评估、渗透测试,动态跟进并发掘系统弱点,对于暴露出的漏洞和弱点通过安全运维和应急处理服务对症下药。在整个安全服务体系建设后期,通过安全培训服务强化系统关联人员的网络安全防护意识、提升安全防护技能。

安全技术体系是以 GB/T25070 网络安全等级保护安全设计技术要求等为理论依据,在完善安全区域边界上采取安全分区、网络专用、单向隔离的技术措施构筑系统安全防护屏障。一方面主要以边界防护产品为依托,通过在系统中部署入侵防御、准入控制、集中管控、工控审计溯源等设备对运行环境中主机安全层面、应用安全层面、终端管理层面以及针对云大物移新技术的互联互通实现安全监测运维;另一方面通过搭建安全预警感知平台,对

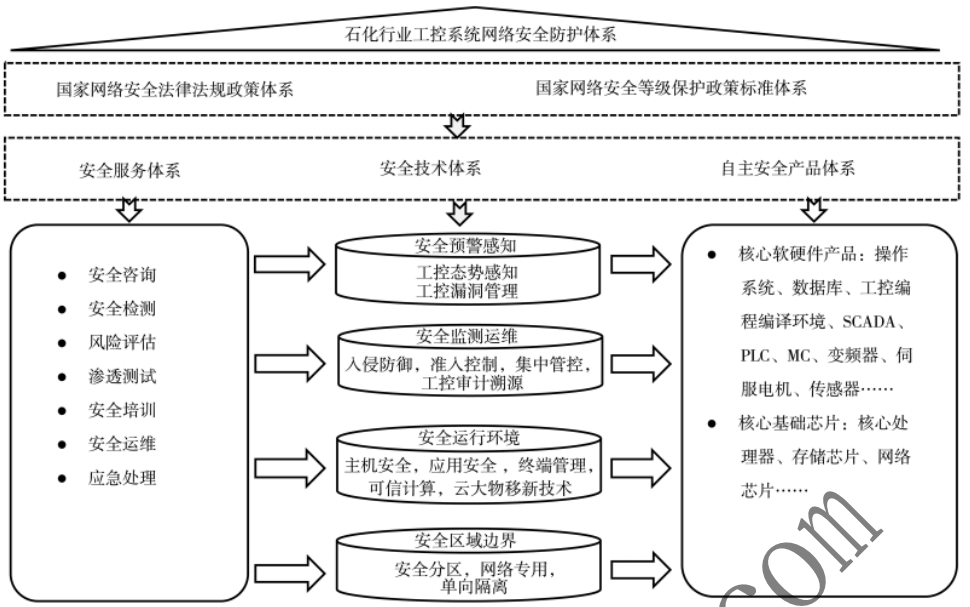

图 4 石化行业工控系统网络安全防护体系

工控系统安全漏洞、工控系统安全态势进行感知分析。

以工业控制系统安全防护指南等为理论依据，自主安全产品体系在结合安全服务体系、安全技术体系做框架支撑的同时，依靠产品自身研发设计，全面掌握产品核心技术，实现石化行业工控系统核心软硬件产品，诸如操作系统、数据库、SCADA、PLC、伺服电机、传感器；核心基础芯片，诸如核心处理器、存储芯片、网络芯片的自主研发、生产、升级、维护的全程可控。

基于石化行业工控系统网络安全防护体系，以安全服务体系、安全技术体系、自主安全产品体系三位一体，打造一套试验案例应用于石化行业某单位工控系统建设，具体落实措施案例如图 5 所示。

图 5 所示实施案例依据 ISO/IEC 62264－1：2013 的层次结构模型，给出石化行业工控系统的层次结构模型，其中石化行业工控系统主要涉及生产管理层、过程监控层、现场控制层和现场设备层，即管理信息大区和生产控制大区。安全服务体系贯穿整个系统全生命周期，包含安全咨询、安全检测、风险评估、渗透测试、安全运维、应急处理以及安全培训七部分；安全技术体系贯穿整个层次结构，实现层和层、域和域之间的隔离防护，从而达到安全分区、网络专用、单项隔离的目的；自主安全产品体系贯穿生产控制大区，从操作系统到控制器再到现场设备加大设备国产化力度，从而实现自主安全的目标。

石化行业工控系统网络安全防护体系以国家网络安全法律法规政策体系、国家网络安全等级保护政策标准体系为扣合点，通过搭建安全服务体系保障网络安全、安全技术体系支撑网络安全，以实现石化行业工控系统内部核心关键设备自主安全、整体工控网络可控为最终导向。

4 结论

工业控制系统作为石化行业的神经中枢，一旦受到破坏，其后果不仅仅局限于经济损失，还会直接影响国民日常生活甚至造成人员伤亡，乃至影响社会稳定。只有构建安全的石化行业网络安全防护体系，通过政策法规约束，安全管理服务保障，安全技术措施支撑，才能有效抵御外界攻击，消除内部潜在威胁，实现石化行业工控系统网络安全防护目标。

参考文献

[1] 东北大学，谛听网络安全团队.2020 年工业控制网络安全态势白皮书[Z].2021.
[2] 东北大学，谛听网络安全团队.2021 年工业控制网络安全态势白皮书[Z].2022.
[3] 新华社.国民经济和社会发展第十四个五年规划和 2035 年远景目标纲要[Z].2021.
[4] 国务院.关键信息基础设施安全保护条例[Z].2021.
[5] 王晔，陈丽娟，衣然.等保 2.0 时代城市轨道交通信号系统网络安全防护新思路[J].信息技术与网络安全，2020，39(3)：1－5.
[6] 孟庆军.如何提升石油化工企业网络安全管理现状[J].中国信息化，2017(7)：74－76.

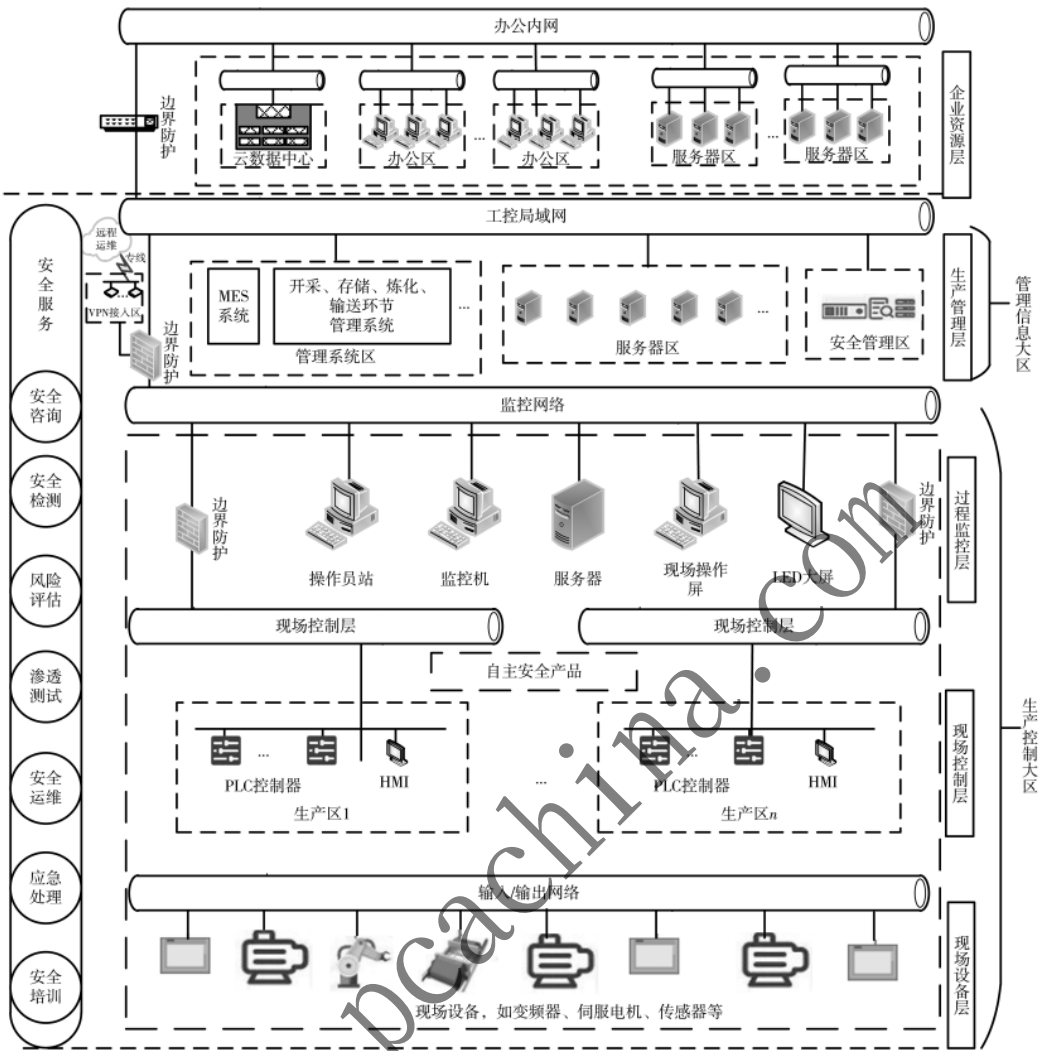

图5 石化行业工控系统网络安全防护体系实施案例

[7] 朱杰.浅析石油化工集成自动化系统网络安全策略[J].中国石油和化工标准与质量,2022,42(1):78-79.

[8] 王子洋,何文.大型石化控制系统替换升级过程中网络安全防护策略设计[J].自动化与仪表,2021,36(9):34-39.

[9] 王泽政.构建内外一体、纵深防御的多层次工业互联网安全监测保障体系[J].新型工业化,2021,11(10):160-163.

[10] 段少敏.蒋白桦:石油化工行业在智能制造领域的探索与实践[J].智能制造,2022(1):21-23.

[11] 甄涛.石化工控信息网络安全区域识别与防护[J].软件导刊,2016,15(9):151-153.

[12] 刘远.石油化工行业网络安全运营的探索与思考[J].中国信息安全,2019(8):68-70.

[13] 于慧超,白文海.石油石化行业自动化和信息化集成网络安全[J].中国石油和化工标准与质量,2019,39(24):96-97.

[14] 孙天宁,邹春明,严益鑫.工业控制系统信息安全防护分析[J].自动化博览,2021,38(1):57-61.

[15] 郭启全.深化国家信息安全等级保护制度全力保卫国家关键信息基础设施安全[J].网络安全技术与应用,2016(9):1.

(收稿日期:2022-05-07)

作者简介:

霍朝宾(1983-),男,硕士,高级工程师,主要研究方向:工控信息安全。

武蕊(1994-),通信作者,女,硕士,助理工程师,主要研究方向:工控信息安全。E-mail:lee64579@163.com。

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