DOI:10. 3969/j. issn. 1674-1951. 2021. 02. 007

能源工业网络空间安全风险与模型研究

Security risks and models of energy industry's cyberspace

宫月[1],李秋香[1],张心语[2],龚钢军[2],金璐[3]
GONG Yue[1],LI Qiuxiang[1],ZHANG Xinyu[2],GONG Gangjun[2],JIN Lu[3]

(1.公安部第一研究所,北京 100044;2.北京市能源电力信息安全工程技术研究中心(华北电力大学),北京 102206;
3.北京华电云博科技有限公司,北京 102206)

(1.First Research Institute of the Ministry of Public Security of PRC,Beijing 100044,China;2.Beijing Engineering Research Center of Energy Electric Power Information Security(North China Electric Power University),Beijing 102206,China;
3.Beijing Huadian Yunbo Technology Company Limited,Beijing 102206,China)

摘 要:随着能源工业技术体系在开放性、互联互通性和标准化工作等方面的需求越来越强烈,能源工业控制系统物理隔离的传统封闭环境面临着被逐步打破的压力。从关键基础设施和关键信息基础设施的角度,分析了能源工业控制系统的安全定位和不同能源工业体系的安全防护水平的差异性,研究了能源工业网络空间下基于信息物理系统的运营技术(OT)与信息通信技术(ICT)融合控制的安全风险,以及能量流、业务流和信息流深度融合的安全特征,提出了能源工业网络空间安全管理模型,力求实现能源工业网路空间的智能化感知、主动防御和预测性维护,提升能源工业网络空间防护能力。

关键词:能源工业网络空间;工业控制系统;关键信息基础设施;安全防护水平;等级保护 2.0
中图分类号:TM 711;TN 98 **文献标志码**:A **文章编号**:1674-1951(2021)02 - 0040 - 06

Abstract: The increasing demand for an open, interconnective and standardized technical system of energy industry exerts sustained pressure on the traditional physical isolated control system. From the perspective of key infrastructure and critical information infrastructure, the importance of control system security in energy industry and the difference of security protection levels in different energy industrial systems were analyzed. At the same time, security risks on the fusion of operation technology (OT) and information communication technology (ICT) in energy industry cyberspace based on the information physical systems were studied , and the security characteristics of the deep integrations of energy flow, business flow and information flow were described. Finally, a security management model for energy industry cyberspace was proposed to realize its intelligent perception, active defense, predictive maintenance, and improvement of the protection capacity.

Keywords: energy industry cyberspace; industrial control system; critical information infrastructure; security protection level; classified protection 2.0

0 引言

能源工业是指对传统化石能源和可再生清洁能源资源进行开发、加工、输送和利用的能源与动力工业,一般包括电力、石油、天然气和煤炭等类型。能源工业是国民经济的基础和支柱[1],能源的开发与利用是关系到整个国民经济能够持续、稳定和快速发展的关键[2]。目前,以能源互联网和新能源等为代表的第4次能源革命,以高效化、清洁化、低碳化、智能化为目标,促使整个能源工业呈现出高度柔性化、可重构化和社会化的特征,推动着人类文明在资源利用形态、技术方式、管理体制等方面的发展[3]。

目前,我国已成为世界上最大的能源生产国和消费国,并构建了世界上系统规模最大、结构层次最多、复杂程度最高和自动化水平较高的能源工业体系。能源工作的重点已从过去增加产能、保障供应,转向结构调整、技术创新、大力发展新能源、全面提升能源安全保障能力的新阶段。能源生产控制、调度管理和信息管理的基础是由计算机监控系统、通信网络、工业智能化终端和自动化控制系统组成的工业控制系统(ICS)。ICS 主要由数据采集

收稿日期:2020-09-04;**修回日期**:2021-01-04
基金项目:国家重点研发计划项目(2016YFB0901200)

与监视控制（SCADA）系统、分散控制系统（DCS）、可编程逻辑控制器（PLC）、远程测控终端（RTU）等组成，广泛应用于能源领域[4]。

随着能源工业技术体系在开放性、互联互通性和标准化工作等方面的需求越来越强烈，能源工业控制系统物理隔离的传统封闭环境面临着“固守与发展”的矛盾，即在肯定物理隔离有效防护功能的基础上必须增加安全接口[5]。同时，由于传统互联网信息安全问题已经延伸到了工业控制领域[6]，出现了很多专门针对ICS攻击的计算机病毒，致使能源工业系统的安全防护工作形势异常严峻，必须从事前预防、事中控制和事后审计等全方位实现“可控、在控、能控”的管理体系。但工业控制系统的运营技术（OT）与信息技术（IT）系统对信息的机密性、完整性和可用性要求迥然不同[7]，能源工业控制系统及其安全防护体系具有很强的基础性、复杂性和专用性。

由于历史原因和技术制约，我国能源系统核心部位的工控设备和系统仍大量使用国外产品，这些产品和系统在通信协议、内置操作系统和安全防护等方面存在缺陷，致使可远程非法操作以致恶意破坏所控制的生产设施，同时发现并验证了多个人为设置的后门密码等更深层次的安全隐患。在当前国际形势复杂多变，网络安全事件层出不穷的严峻形势下，如果这些漏洞被系统性地恶意利用，将对我国能源工业造成毁灭性打击，严重威胁社会稳定和国家安全。

相对于常规IT系统来说，保证工业生产过程的连续及稳定是能源工业的首要原则，这也带来了生产控制系统更新升级频次低、生产设备老化、生产控制系统与信息安全防护设备间存在代差导致匹配度差等一系列负面影响，而能源工业的行业特征也导致了安全问题多但难以解决的情况。同时，我国的能源工业安全防护水平差异很大，其中，由于电力的特殊性质且其使用范围之广，电力行业的安全防护能力处于能源行业之首；电网企业的安全防护能力要强于发电、售电企业。

总体上，我国能源工业控制系统普遍存在工控设备及工控协议安全性差、工控信息安全产业链发展缓慢、系统主动防御水平低、纯物理隔离防护致使系统互联互通性不足等问题[8-11]。因此，亟须明确能源工业信息安全防护定位，以及能源流、业务流、信息流深度融合下的安全风险，建立能源工业网络空间安全管理模型，并以此为基础研究规范能源工业网络空间发展形态和架构体系，分析能源工业网络空间的预测性、智能化的主动管理模式，提升能源工控系统的安全防护能力。文献[12]从IT领域信息安全管理体系的基本理论和潜在威胁的角度，分析了当前我国工业控制系统存在的威胁，但未结合运营技术与信息通信技术融合（OICT）的新场景；文献[13]提出国内大多数工业控制网络核心设备与网络协议国产可控程度较低；文献[14]阐释了工业控制系统信息安全与传统IT信息安全的区别；文献[15]提出了一种基于工业SCADA系统的网络安全服务框架；文献[16]从技术和管理2个层面提出了相应的安全防护体系；文献[17]从工业控制的角度分析了工业控制系统安全的特殊性，但上述文献均未从关键基础设施和关键信息基础设施的角度分析能源工业控制系统的安全定位，分析能量流、业务流和信息流深度融合的安全特征。

1　能源工业系统简介

1.1　能源工业信息安全防护定位

关键基础设施（CI）是指在国家安全与运转体系中扮演重要角色的系统或设施。2001年，美国颁布的《爱国者法案》对关键基础设施的定义是：“实体或虚拟的系统和资产，重要到如果失效或遭到破坏将会对国家安全、国家经济安全、国家公众健康或安全或这些事项的任何组合造成削弱影响”[18]。法案明确了国家关键基础设施包括：电信、能源、金融服务、海洋、交通领域以及“对维护国防、政府连续性、经济繁荣以及在美生活质量至关重要的网络和物理基础设施服务”。2002年，美国《国土安全法》中将“关键资源”（对政府和经济运作必不可少的公共或私营资源）新增为关键基础设施。经过系列规定，国土安全部将18个经济领域列为关键基础设施。另外，2005年，欧盟和日本分别发布了《保护关键基础设施的欧洲计划》和《关键基础设施信息安全措施行动方案》等系列制度，首次明确了关键基础设施的识别、控制和安全保护的相关标准办法。

目前，我国尚未正式确立国家关键基础设施范畴。2007年，《国务院办公厅关于开展重大基础设施安全隐患排查工作的通知》中将公路、铁路、水运交通设施、大型水利设施、大型煤矿、重要电力设施、石油天然气设施、城市基础设施等9种类别列入了“重大基础设施”。2012年6月，《国务院关于大力推进信息化发展和切实保障信息安全的若干意见》中明确要求：加强核设施、航空航天、先进制造、石油石化、油气管网、电力系统、交通运输、水利枢纽、城市设施等重要领域工业控制系统监管。2015年7月，我国正式实施的《中华人民共和国国家安全法》提出了实现关键基础设施和重要领域信息系统及

数据安全可控的重要战略任务。

能源工业是国家的关键基础设施，必须加强其安全防护，避免其被破坏后对国家政治、经济、军事、文化等方面产生重大不利影响。因此，作为关键基础设施的能源工业，首先体现出 2 个安全防护工作的定位：(1)能源工业是国民经济和社会发展的关键基础设施；(2)能源行业是国家网络安全等级保护的重点行业。

关键基础设施的安全、稳定、连续和可靠运行离不开关键信息基础设施的支撑。目前，我国正在完善“关键信息基础设施(CII)”的分类。2016 年，我国发布的《关键信息基础设施确定指南(试行)》中说明：“关键信息基础设施是指面向公众提供网络信息服务或支撑能源、通信、金融、交通、公用事业等重要行业运行的信息系统或工业控制系统，且这些系统一旦发生网络安全事故，会影响重要行业正常运行，对国家政治、经济、科技、社会、文化、国防、环境以及人民生命财产造成严重损失”。

2017 年，国家互联网信息办公室关于《关键信息基础设施安全保护条例(征求意见稿)》中认为下列单位运行、管理的网络设施和信息系统应当纳入关键信息基础设施保护范围：(1)政府机关和能源、金融、交通、水利、卫生医疗、教育、社保、环境保护、公用事业等行业领域的单位；(2)电信网、广播电视网、互联网等信息网络，以及提供云计算、大数据和其他大型公共信息网络服务的单位；(3)国防科工、大型装备、化工、食品药品等行业领域的科研生产单位；(4)广播电台、电视台、通讯社等新闻单位；(5)其他重点单位。

2017 年 6 月 1 日正式开始实施的《中华人民共和国网络安全法》第 31 条指出：“国家对公共通信和信息服务、能源、交通、水利、金融、公共服务、电子政务等重要行业和领域，以及其他一旦遭到破坏、丧失功能或者数据泄露，可能严重危害国家安全、国计民生、公共利益的关键信息基础设施，在网络安全等级保护制度的基础上，实行重点保护”。从而正式明确了关键信息基础设施的内涵和等级保护制度的法律地位，也进一步强化了能源工业另外 2 个信息安全防护工作的定位：(1)能源工业的重要信息通信系统是国家关键信息基础设施；(2)能源企业是国家网络安全重点保护单位。

1.2 能源工业发展规划

近几年，我国陆续出台了系列重要文件和政策，大力推动能源工业的快速健康发展，也必然加速能源工业控制系统的升级改造和安全防护技术水平的提升。2014 年，国务院印发的《能源发展战略行动计划(2014—2020 年)》中提出了我国应立足国内多元供应，保障能源安全，加快构建以煤、油、气、核、新能源、可再生能源多轮驱动的清洁、高效、安全、可持续的现代能源体系；国家发展改革委、国家能源局在 2016 年先后印发了《能源技术革命创新行动计划(2016—2030 年)》《能源发展“十三五”规划》，对新能源发电、电气设备等领域的高端技术发展做出了明确规划，并提出以“四个革命、一个合作”为能源发展的战略思想，向优化能源系统，推进能源绿色低碳发展，构建智慧能源系统不断努力。2014 年，国家电网有限公司提出了全球能源互联网的建设构想，2019 年正式印发了《推进综合能源服务业务发展 2019—2020 年行动计划》，提出了“三型两网、世界一流”的战略目标。

2 能源工业网络空间安全风险

2.1 网络空间的含义

如今随着信息技术的不断发展，“网络空间”已成为除“海陆空天”之外的国家第五主权空间，足见“网络空间”的关键及重要。2015 年 7 月 1 日，我国正式实施的《中华人民共和国国家安全法》中规定：“国家建设网络与信息安全保障体系，并加强网络管理，防范、制止和依法惩治网络攻击、网络入侵、网络窃密等网络违法犯罪行为，维护国家网络空间主权、安全和发展利益”。《中华人民共和国国家安全法》第 1 次明确了“网络空间主权”的概念，也是我国国家主权在网络空间的体现、延伸和反映。

2.2 OICT 融合发展带来的安全风险及安全需求

伴随着信息化与工业化的深度融合，以及新兴技术在工业领域的应用，能源工业网络空间安全需结合 OICT 展开探讨。国内智慧能源、智慧石油、智慧燃气等公用事业基础设施的智能化建设也日益加快，电力、石油化工、燃气等重要基础设施已逐步成为信息空间与物理空间相互融合的网络空间智能化设施。因此，OICT 使得以往相对封闭的能源工业网络空间的开放性增强，能源工业网络空间开始面临传统信息网络所面临的病毒、入侵攻击、拒绝服务等安全威胁和日益严峻且复杂的安全风险。

工业控制系统安全可分为 3 类，即强调设备和系统能正确执行 OT 的功能安全、基于基础物理设施与环境的物理安全、基于 IT 的传统信息安全。与传统 IT 信息安全不同，所有系统部件的可用性为工业控制系统信息安全需考虑的首要因素，完整性和保密性分别排在第 2，3 位。工业控制系统安全类型及具体要求如图 1 所示。针对工业控制系统开展信息安全工作还应当充分保证系统性能的稳定性、工

作的连续性、系统的可访问性及可操作性。因此，针对工业控制系统安全需要有专用的工业控制系统安全保护技术，以及全生命周期的安全管理。现阶段已开展的风险评估、安全集成、应急处理、灾难备份与恢复、软件安全开发和安全运维服务资质的评价要求是针对通用信息系统的，不能满足工业控制领域开展安全服务认证工作的需求。

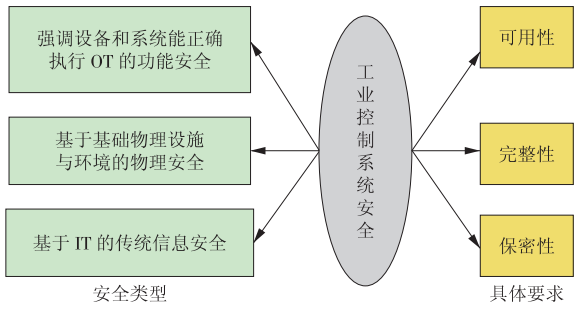

图 1　工业控制系统安全类型及具体要求

Fig. 1　Safety classification and specific requirements of the industrial control system

能源 ICS 有自己鲜明的特征，不能简单地以 IT 思维来研究和改进能源 ICS。但随着基于物联网技术及由信息设备和计算单元耦合而成的信息物理系统（CPS）的研究与应用，能源工业控制系统 OT 与 ICT 的融合势在必行。自动控制系统传统上为基于信号的控制，而 CPS 因其融合了计算、存储等要素，可以理解为“基于信息的控制”，而且 CPS 在实现 ICS 的 OT 与 IT 或 ICT 融合的基础上，也必将实现 IT 向数据技术（DT）的转变。但要求在开展 IT 与 OT 的融合之初，必须对能源工业控制系统的业务类型与安全需求，以及 IT 技术的安全性进行足够充分的研究与验证，避免由于 OT 技术 IT 化带来的安全问题，导致工业控制系统失效或破坏等。

2.3　能源流、业务流和信息流深度融合的安全特征

随着信息化与工业化的深度融合，以及“互联网+”与智慧能源、能源互联网、综合能源服务、“三型两网”等能源发展模式的改变，以及能源工业技术体系在开放性、互联互通性和标准化工作等方面的需求，都促使能源网络结构复杂化、边界模糊化、形态多样化，信息安全风险显著增加[12-16]。同时，随着云计算、大数据、物联网、移动互联、工业互联网、区块链等新技术的不断涌现，以及输配分离、供给侧结构性改革，在新技术和新业务模式的共同推动下，能源电力生产的信息获取方法、存储形态、传输渠道、处理方式和信息安全防护需求均发生明显变化。

在能量流、业务流、信息流的深度耦合下，能源工业体现出了以下几个特征：（1）柔性接入各种分布式、多元能源的包容性；（2）利用各种高新技术自适应广泛接纳多方用户参与的开放性与互动性；（3）以大电网为“主干网”，以微网、能量自治单元为“局域网”，以开放对等的信息-能源一体化架构实现能量流的双向按需传输和动态平衡。

由此可看出，随着新技术的广泛应用及业务的不断扩展，能量流的传输、系统调度信息的准确控制，以及多方用户参与下业务信息数据的复杂性，都使得能源工业面临着安全风险多样性、复杂性、随机性的特征。因此，需要充分考虑能量流、业务流和信息流深度融合的安全特征，结合“能源互联、信息共享、业务互动”的思想，确保能源工业网络空间智能化基础设施的能量流和信息流的对等交换及共享安全，保证整个系统中信息的可用性、完整性、保密性。

3　能源工业网络空间安全管理模型

目前，随着我国《中华人民共和国国家安全法》《工业控制系统信息安全防护指南》《国家网络空间安全战略》《国家网络安全事件应急预案》《中华人民共和国网络安全法》《工业控制系统信息安全事件应急管理工作指南》，以及网络安全等级保护 2.0 系列标准等国家法律法规文件的密集发布，将进一步完善国家网络安全管理制度，助推我国建立更加全面、完善的网络空间战略体系。

保护国家关键信息基础设施安全已成为维护国家网络安全的首要任务。因此，2018 年起，中国电子技术标准化研究院、中国互联网络信息中心、国家信息技术安全研究中心等相关国家标准化研究组织先后起草了关键信息基础设施网络安全保护基本要求、安全检查评估指南、网络安全框架、安全保障指标体系、安全控制要求、安全控制措施等标准体系，围绕认定识别、安全防护、检测评估、监测预警、应急处理 5 个环节，以基本要求为体系基础，提出了关键信息基础设施网络安全工作的基线标准、实施标准、测评标准，以指导各行业网络空间安全工作的切实实施。关键信息基础设施标准体系与网络安全保护流程的作用关系如图 2 所示。

因此，能源工业网络空间安全应在遵循国家法律、法规和标准的基础上，从合规性角度出发，立足能源工业的 4 个信息安全防护工作定位，坚定自主研发和国产化选型发展思路，采用基于 OICT 的 CPS 融合发展技术路线，以业务功能安全为核心，以信息安全为保障，坚持质量管理流程 PDCA，即计划（P）—执行（D）—检查（C）—处理（A）的持续改进机制和全生命周期的管控体系，实现能量流、业务流

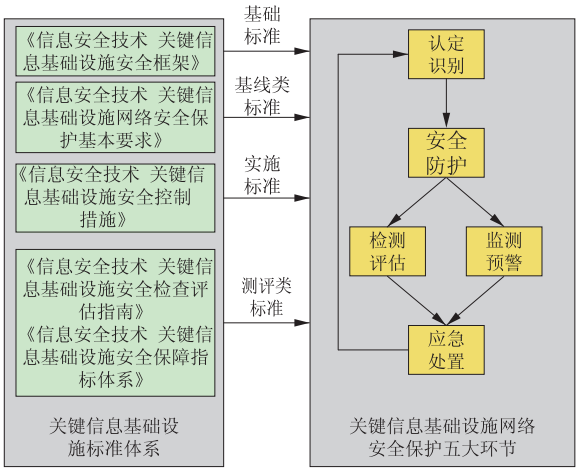

图 2 关键信息基础设施标准体系与网络安全保护流程的作用关系

Fig. 2 Relationship between CII standard system and cyber security protection flow

和信息流的交互和融合控制，方能构建安全、高效和稳固的能源工业网络空间安全管理模型和运行体系，从而确保能源工业控制系统的安全、稳定和连续运行。

4 结束语

我国已成为世界上最大的能源生产国和消费国，并构建了世界上系统规模最大、结构层次最多、复杂程度最高和自动化水平较高的能源工业体系。能源工业网络空间的安全压力巨大，必须在遵循《中华人民共和国网络安全法》、网络安全等级保护 2.0 系列标准的前提下，正确对待能源工业技术体系在开放性、互联互通性和传统物理网络隔离的“固守与发展”的矛盾，紧扣能源网络空间的关键基础设施和关键信息基础设施的分类与安全定位，基于信息物理系统实现能源工业控制系统 OT 与 ICT 的融合控制，从而构建能源工业网络空间安全架构体系，实现能源工业网络空间的智能化感知、主动防御和预测性维护，提升能源工业网络空间的防护能力。

参考文献：

[1]徐锭明. 我国能源工业现状和能源政策[J]. 中国电力，2004，37(9)：1-4.
XU Dingming. Present situation and policy of energy industry in China[J]. Electric Power，2004，37(9)：1-4.

[2]陈琳琳，杨宇，洪辉，等. 中国能源工业空间分布、基地识别与演变特征[J]. 资源科学，2016，38(12)：2256-2268.
CHEN Linlin，YANG Yu，HONG Hui，et al. Spatial distribution，base identification and evolution characteristics of China's energy industry[J]. Resources Science，2016，38(12)：2256-2268.

[3]天工. 中国能源供给革命迫切需要加快发展气体清洁能源[J]. 天然气工业，2015，35(8)：9.
TIAN Gong. China's energy supply revolution urgently needs to accelerate the development of clean gas energy [J]. Natural Gas Industry，2015，35(8)：9.

[4]彭勇，江常青，谢丰，等. 工业控制系统信息安全研究进展[J]. 清华大学学报(自然科学版)，2012，52(10)：1396-1408.
PENG Yong，JIANG Changqing，XIE Feng，et al. Industrial control system cyber security research [J]. Journal of Tsinghua University (Natural Science Edition)，2012，52(10)：1396-1408.

[5]王珂. 基于等级保护 2.0 新标准的工业控制系统安全现状分析[J]. 网络安全技术与应用，2020(10)：134-136.
WANG Ke. Analysis of the current situation of industrial control system security based on the new level protection 2.0 standard [J]. Network Security Technology & Application，2020(10)：134-136.

[6]吴欢. 工业控制环境计算节点安全防护技术研究[D]. 北京：北京工业大学，2016.

[7]王小山，杨安，石志强，等. 工业控制系统信息安全新趋势[J]. 信息网络安全，2015(1)：6-11.
WANG Xiaoshan，YANG An，SHI Zhiqiang，et al. The new trend of industrial control system information security [J]. Netinfo Security，2015(1)：6-11.

[8]郑少波，徐伟，石彬. 工业控制系统安全现状[J]. 网络安全技术与应用，2020(5)：111-113.
ZHENG Shaobo，XU Wei，SHI Bin. Security status of industrial control systems [J]. Network Security Technology & Application，2020(5)：111-113.

[9]杨晟，孙跃，龚钢军，等. 基于能源区块链的综合能源服务研究[J]. 华电技术，2020，42(8)：11-16.
YANG Sheng，SUN Yue，GONG Gangjun，et al. Research on integrated energy services based on energy blockchain [J]. Huadian Technology，2020，42(8)：11-16.

[10]武志军. 综合能源服务下新能源集约化管控评价方法[J]. 华电技术，2019，41(12)：68-71.
WU Zhijun. Evaluation method on new energy intensive management for integrated energy services [J]. Huadian Technology，2019，41(12)：68-71.

[11]韩峰，张衍国，严矫平，等. 综合能源服务业务和合作模式[J]. 华电技术，2019，41(11)：1-4.
HAN Feng，ZHANG Yanguo，YAN Jiaoping，et al. Integrated energy service and cooperation modes [J]. Huadian Technology，2019，41(11)：1-4.

[12]张帅. 工业控制系统安全风险分析[J]. 信息安全与通信保密，2012(3)：15-19.
ZHANG Shuai. Security risk analysis of industrial control system [J]. Information Security and Communications

Privacy,2012(3):15-19.
[13]陈星,贾卓生.工业控制网络的信息安全威胁与脆弱性分析与研究[J].计算机科学,2012,39(S2):188-190.
CHEN Xing, JIA Zhuosheng. Analysis and research on information security threats and vulnerabilities of industrial control networks [J]. Computer Science, 2012, 39 (S2): 188-190.
[14]欧阳劲松,丁露.IEC 62443工控网络与系统信息安全标准综述[J].信息技术与标准化,2012(3):24-27.
OUYANG Jinsong, DING Lu. Overview of IEC 62443 industrial control network and system information security standards [J]. Information Technology & Standardization, 2012(3):24-27.
[15]兰昆,饶志宏,唐林,等.工业SCADA系统网络的安全服务框架研究[J].信息安全与通信保密,2010(3):47-49.
LAN Kun, RAO Zhihong, TANG Lin, et al. Research on the security service framework of industrial SCADA system network [J]. Information Security and Communications Privacy, 2010(3):47-49.
[16]李佳玮,郝悍勇,李宁辉.工业控制系统信息安全防护[J].中国电力,2015,48(10):139-143.
LI Jiawei, HAO Hanyong, LI Ninghui. Information security protection of industrial control systems [J]. China Electric Power, 2015, 48(10):139-143.
[17]魏钦志.工业控制系统安全现状及安全策略分析[J].网络空间安全,2013,4(2):23-26.
WEI Qinzhi. Security status and security strategy analysis of industrial control systems [J]. Cyberspace Security, 2013, 4(2):23-26.
[18]卿斯汉.关键基础设施安全防护[J].信息网络安全,2015(2):1-6.
QING Sihan. Critical infrastructure security protection [J]. Netinfo Security, 2015(2):1-6.

(本文责编:张帆)

作者简介:

宫月(1986—),女,黑龙江齐齐哈尔人,工程师,工学硕士,从事信息安全方面的研究工作(E-mail:50940694@163.com)。

李秋香(1981—),女,吉林长春人,副研究员,工学硕士,从事信息安全方面的研究工作(E-mail:qiuxiangli2008@163.com)。

张心语(1996—),女,山西晋中人,在读硕士研究生,从事能源电力信息安全方面的研究工作(E-mail:zxy7081@126.com)。

龚钢军(1974—),男,河南济源人,副教授,工学博士,从事区块链技术应用、能源电力信息安全等方面的研究工作(E-mail:gong@ncepu.edu.cn)。

****

广　告　索　引