等保 2.0 时代电力监控系统安全防护体系建设研究

李政达,杨　继,姜添元
(中国电子信息产业集团有限公司第六研究所,北京 100083)

摘　要:通过分析电力监控系统现有的典型结构与安全建设需求,针对电力监控系统网络安全的脆弱性和薄弱点,结合等级保护 2.0 体系,提出了一种电力监控系统网络安全防护建设方案。该方案以“一个中心,三重防护”为核心思想,突出安全管理中心建设,明确通信网络、区域边界、计算环境的安全防护建设方法。以某发电企业电力监控系统生产控制区为试点,以等保 2.0 基本要求为衡量标准进行方案应用效果评估,结果表明,通过安全防护体系建设,可有效提升系统安全性。

关键词:电力监控系统;网络安全;一个中心三重防护;等保 2.0
中图分类号:TP399　　**文献标识码**:A　　**DOI**:10.20044/j.csdg.2097-1788.2022.03.008
引用格式:李政达,杨继,姜添元. 等保 2.0 时代电力监控系统安全防护体系建设研究[J].网络安全与数据治理,2022,41(3):48-53,59.

Research on the construction of security protection system of power monitoring system in the era of classified security protection standard 2.0

Li Zhengda, Yang Ji, Jiang Tianyuan
(The 6th Research Institute of China Electronics Corporation, Beijing 100083, China)

Abstract: This paper analyzes the existing typical structure and security construction requirements of power monitoring system. In view of the vulnerability and weakness of the network security of the power monitoring system, combined with the classified security protection standard 2.0 system, a network security protection construction scheme of power monitoring system is proposed. This scheme takes "one center triple protection" as the core idea, highlights the construction of security management center, and defines the construction method of security protection for communication network, regional boundary and computing environment. Taking the production control area of the power monitoring system of a power generation enterprise as a pilot, and taking the basic requirements of classified security protection standard 2.0 as the measurement standard, the application effect of the scheme is evaluated. The results show that through the construction of the security protection system, the system security can be effectively improved.

Key words: power monitoring system; network security; one center triple protection; classified security protection standard 2.0

0 引言

随着我国信息技术安全法律体系建设日趋完善,网络安全等级保护制度同步提出了更全面细致的网络安全保护要求。2017 年 6 月 1 日《中华人民共和国网络安全法》正式实施,网络安全上升到国家战略层面,其中第三十一条明确规定:“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。”2019 年实施的等级保护 2.0 测评体系更加注重全方位的主动防御、动态防御、精准防控和整体防护,明确了工业控制系统的网络安全防护要求[1]。

电力监控系统是以计算机和网络技术为基础,对电力生产和供电过程进行监视控制的业务系统。电力监控系统作为关键信息基础设施,系统的安全运行不仅关系到发电企业的稳定和发展,而且会直接影响公共利益和安全,以及国民经济的健康发

展。电力监控系统与传统信息系统相比,其网络结构更复杂、各层次的组件更多,且大多使用私有协议,这使得电力监控系统的安全保护更加困难。此外,发电企业对网络安全重视不高,缺乏防护手段,人员安全意识薄弱,使电力监控系统面临巨大的安全风险。

近年来,国外电力安全事故频发,例如 2015 年乌克兰因恶意软件破坏发生了大规模停电事件,委内瑞拉近年来因网络攻击发生多次全国范围的大停电。同时勒索事件频繁发生,严重影响了电力监控系统的可用性,巴西电力公司、葡萄牙跨国能源公司、美国电力公司、国内某大型水电厂均曾遭到勒索病毒攻击,导致数据可用性、业务连续性受到威胁,严重影响企业的安全生产。

目前国内的电力监控系统网络安全防护建设均依据 GB/T 36572-2018《电力监控系统网络安全防护导则》,其规定了电力监控系统网络安全防护的基本原则、体系架构、防护技术、应急备用措施和安全管理要求。国家发展改革委员会 2014 年第 14 号令《电力监控系统安全防护规定》对区域划分与隔离、网络通信与认证提出相应的建设要求。国家能源局 2015 年发布的《电力监控系统安全防护方案》对发电、变电、配电、调度四种不同的电力监控系统做出详细的安全防护方案指导。目前针对电力监控系统网络安全建设发布的国标和法规均无安全管理中心的建设要求,也未发布详细的安全计算环境、安全区域边界的建设方案。

1 电力监控系统现状与需求分析

1.1 电力监控系统安全现状

电力监控系统依据现有指导文件进行建设时往往忽略入侵行为检测与阻断、安全漏洞发现与升级、病毒木马网络与主机的协同防御等网络安全基线的建设,因此电力监控系统现有的防护方案在应对黑客发展迅猛的入侵技术时显得捉襟见肘,尤其是面对有组织的高级持续性威胁(Advanced Persistent Threat,APT),其特点主要包括:入侵手段多样化、0day 漏洞信息差、病毒木马隐蔽性不断提高、针对单一系统持续化攻击。因此,电力监控系统亟需更全面、标准化可落地、适度超前的安全建设方案,以应对频发的网络攻击。

本文对河南地区 20 家发电企业的 49 个电力监控系统进行调研得出:使用 2021 年新版算分方法的电力行业等级保护测评项目,安全保护等级为第三级的电力监控系统测评结论九成为“中”,而传统信息系统、云计算系统的测评结论超九成为“良”。在对被调研的电力监控系统进行现场测评时,安全管理中心、安全计算环境、安全区域边界的测评项中存在关键指标不符合的情况,旧的安全体系已经无法满足等保 2.0 测评体系的安全要求。

1.2 电力监控系统现有架构

依据国家能源局发布的《电力监控系统安全防护方案》,电力监控系统安全防护的总体原则为“安全分区、网络专用、横向隔离、纵向认证”[2]。图 1 为现有电力监控系统安全防护总体架构。

(1)安全分区:将电力监控系统分为生产控制大区和信息管理大区,生产控制大区可分为控制区和非控制区。控制区是电力生产的重要环节,直接实现对电力生产的实时监控。

(2)网络专用:纵向数据传输采用专用网络,使用虚拟专用网络(VPN)技术划分实时子网和非实时子网。

(3)横向隔离:在生产大区和信息管理大区之间部署物理隔离装置实现正向、反向隔离。生产大区内部部署带访问控制功能的隔离装置或防火墙实现逻辑隔离。电力监控系统与传统的数字网络均是采用单向隔离装置进行强逻辑隔离。

(4)纵向认证:生产控制大区在不同企业之间的纵向进行数据远程通信时,采用认证加密、访问控制技术措施保证数据交互过程中的保密性和完整性。

1.3 现有架构风险

1.3.1 区域边界与通信网络风险分析

现有电力监控系统的安全防护架构仅限于区域间的安全隔离与纵向通信网络的加密传输,隔离手段使用传统防火墙、单向隔离装置等防护措施,采用白名单方式控制数据进出,使用 VPN、纵向加密认证等技术实现生产大区之间的纵向数据传输与认证,无法实现协议级的高效解析,数据包内包含的攻击载荷无法被及时发现。

而且,现有架构在系统区域边界缺少入侵防范检测与阻断手段,未部署集中的网络流量审计系统,现阶段入侵者通常在数据层面构造攻击负载对系统进行攻击,但是目前大部分电力监控系统使用的安全设备仅能在数据包地址、端口层面进行限制,无法对数据内容的安全性进行检测。

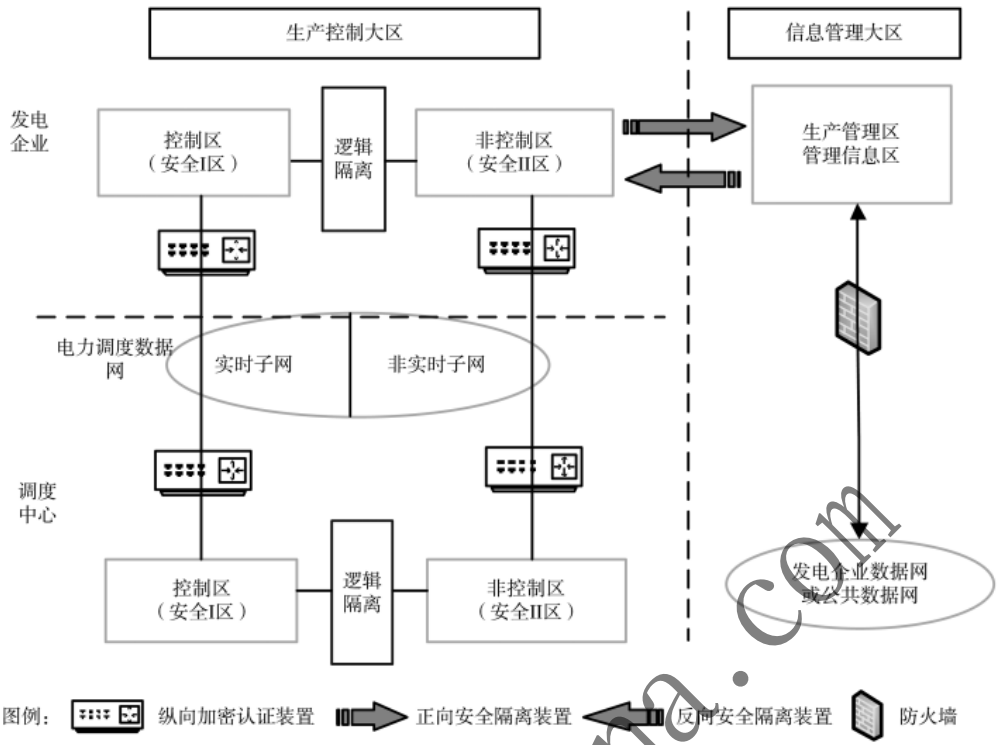

图 1 现有电力监控系统安全防护总体框架示意图

1.3.2 计算环境风险分析

由于工业控制软件普遍较为复杂、兼容性差，导致安装防入侵软件会影响生产过程的连续性与可靠性，大部分电力监控系统只注重可用性，忽略了安全性。即便部分企业对工控终端主机安装了防入侵软件来实现安全防护，但是防入侵软件需要定期升级最新的特征库，电力监控系统在与外界网络隔离的环境下无法保证特征库实时更新[3]。

通过分析国内外的电力安全事故，在边界防护策略设置合理的情况下，对电力监控系统的有效攻击大多以工控终端为突破口，不规范的数据传输方法使系统被植入木马，导致系统失陷。如果安装入侵检测系统则可以很大程度防止此类事件的发生，这样即便单个设备失陷，风险在内网传播时也会很快被发现并阻断。

1.3.3 安全配置风险分析

大多数企业没有建立安全管理中心或未单独划分安全区域，缺乏整体安全系统规划，部署的安全产品之间存在交互壁垒，无法实现网络链路、网络设备和计算设备的集中监测，以及对系统配置、安全配置、审计信息的集中管理与监测。现有的安全设备只能执行单点或单一层面保护，防护体系呈扁平化结构，没有形成统一的安全防护体系，难以做到综合分析和协同防护[4]。

依据等级保护 2.0 标准对电力监控系统进行测评时，安全管理、审计管理、集中管控等控制点出现较多不符合项。根据中关村信息安全测评联盟发布的《网络安全等级保护测评高风险判定指引》，运行监控措施缺失、安全事件发现处置措施缺失被判定为高风险问题，如果测评过程存在上述问题，会导致测评结果不通过[5]。

1.4 安全建设需求

旧的电力监控系统安全建设体系已无法满足当前的安全防护需求，加强电力监控系统的安全防护刻不容缓，对电力监控系统的安全建设需要根据系统特点，设计实际可行的安全防护体系方案[6]。电力生产企业比传统企业更加注重系统的可用性与实时性，所以在进行安全建设时不能影响数据传输的高效和准确[7]。

等级保护 2.0 的安全建设体系有针对性地在工业控制系统扩展中提出了相应的安全防护要求，其“一个中心，三重防护”的防护思想对现有的防护体系更加细化；建立以计算环境安全为基础，以区域边界安全、通信网络安全为保障，以安全管理中心

为核心的信息安全整体保障体系，安全防护与安全监测有机结合，形成“1+1>2”的安全防护模式，构建主动防御体系[8]。

电力生产、调度等相关企业亟需根据等级保护2.0指导文件中的安全建设思路进行系统安全防护升级改造，建设更完善的防护体系，以便通过等级保护、风险评估等合规性的安全测评，保障电力监控系统基础设施持续、稳定、安全运行。

2 安全防护建设

电力监控系统的网络安全防护采用顶层设计结构。在建立横向隔离、纵向认证安全防护体系的基础上，重点在等级保护2.0新增安全防护建设要求上拓展安全防护的新思路，具体体现在构建网络攻击主动发现能力，建立可信安全机制，统筹安全、日志、管理信息有效集成，搭建安全管理制度体系，组建专业的安全管理团队，提升安全防护能力等方面[9]。

2.1 安全架构顶层设计

在现有的系统生产架构上划分出独立的网络区域构建集中管理网。在等级保护2.0体系中提出的安全管理中心概念是为了建立集安全管理、安全监测、安全运维为一体的集中管理平台，为电力监控系统的安全可靠运行安装一个“智能大脑”。目前的安全管理中心实践方案并不是通过单一的设备实现的，而是通过安全监测、日志审计、系统管理等相应的集中管理设备共同建设的，通过设备集合共同实现安全管理中心。

由于电力监控系统网络结构的特殊性，其各大区的数据流向有严格的管控措施，在建立集中管理网时不能打破“安全分区，横向隔离，网络专用”的原则。由于是企业内部建设，故无需继续“纵向认证”，但横向应当与原有区域之间的安全隔离边界保持平行，如图2所示，在原有的系统上层建设集中管理网，集中管理网同样采用横向隔离。

生产控制大区的控制区和非控制区分别部署区域安全管理系统，用于各自区域的安全管理、系统管理、日志收集，并将收集到的设备日志与网络流量发送至集中管理网的信息管理区，通过集中审计设备与安全分析设备，做到对分散在各个设备上的审计数据进行收集汇总和集中分析，并时刻检测网络流量中的特征值和各个设备上报的安全信息，做到全网的实时检测和主动防御。

2.2 区域安全详细设计

如图3所示，生产控制大区安全防护架构是图2整体架构中安全I区的进一步细化设计。该架构图以火力发电企业生产控制大区为例，生产控制区分为操作网和控制网，操作网用于操作员站、历史站等设备的接入，实现DCS生产操作、数据采集和处理、监控画面显示、故障诊断和报警等功能。控制网用于工程师站、DCS服务器等设备的接入，实现对DCS组态上传、下载和修改，并对控制站进行配置。

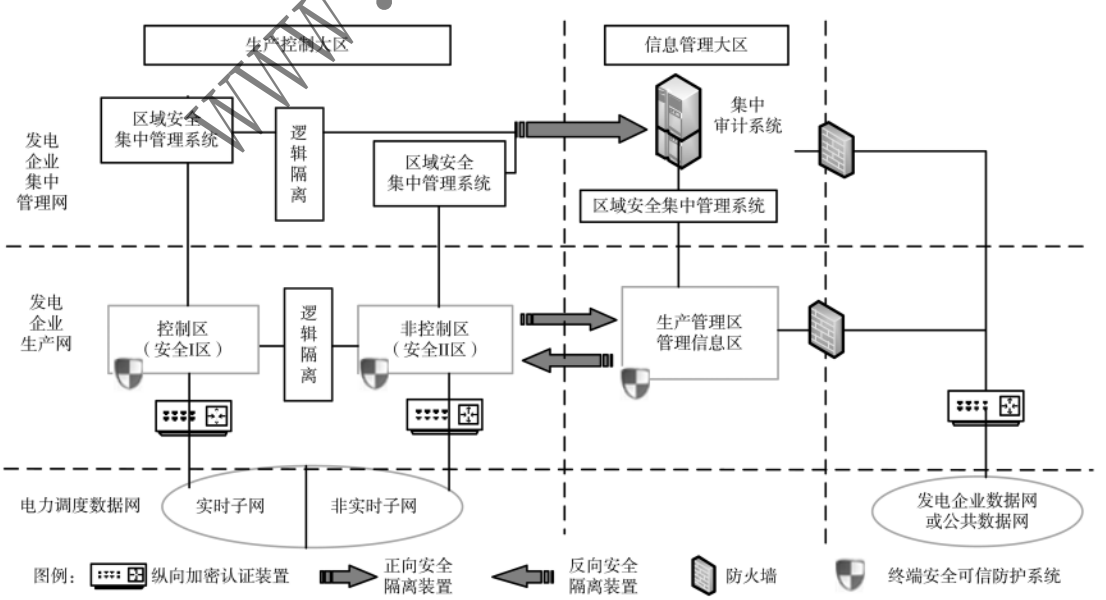

图2 电力监控系统安全防护新思路整体架构

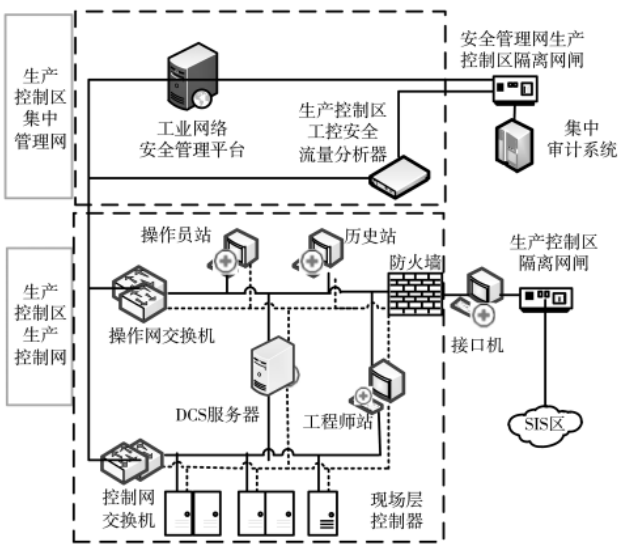

图 3 典型发电企业生产控制大区安全防护架构

2.2.1 典型生产控制区通信网络、区域边界防护

在通信网络方面,采用全流量采集的方法,通过交换机镜像口发送流量数据至工控安全流量分析器,通过 N-gram 算法进行报文切分,然后通过关键词提取算法提取关键词,最后依据提取的关键词进行报文聚类对工控协议报文分类[10],实现对流量的初步过滤,结合单分类器与集成学习训练出二层分类模型,从而对工业控制网络流量进行异常检测[11],消除流量数据中的噪声,防止集中审计系统流量过载。集中审计系统的流量审计模块通过解析工控网络流量、深度分析工控协议与系统内置的协议特征库,实现实时流量监测以及异常活动及时告警。

同时对网络链路、安全设备、网络设备和服务器等的运行状况进行集中监测与日志收集,对日志进行持久化存储,并对安全事件日志进行统计分析。实现在关键网络节点处的检测,防止并限制从外部或内部发起的网络攻击行为,帮助电力生产用户实时掌握网络的运行状况,发现潜在网络流量安全问题。

2.2.2 典型生产控制区安全计算环境防护

在终端的安全管理方面,工业控制系统对可用性和连续性要求较高。当前采用特征值比对黑名单的终端安全防护产品时容易导致工业软件与系统内核的交互和一些操作指令被误判为恶意操作,影响工控系统的高可用性[12]。由于工控主机用途比较单一,运行的软件固定,对外交互数据格式固定,因此使用白名单的终端安全和可信保护系统应运而生。

终端安全可信保护系统部署在每个终端和服务器上,安全可信保护系统由硬件设备层的可信芯片、操作系统层的可信软件基、应用层组成,其中应用层由可信安全管理平台、可信软件库组成[13]。可信安全管理平台统一管理所有接入终端的应用、安全软件和系统环境。可信终端软件是安装在终端操作系统中的安全执行软件,可信软件库为信息系统提供可信软件,受信任的芯片提供了信任的根源,系统架构图如图 4 所示,其中可信安全管理平台和可信软件库为图 3 中工业网络安全管理平台的子模块。

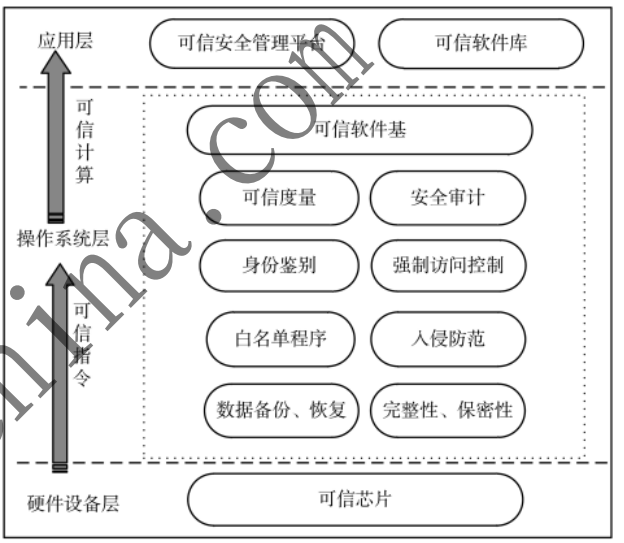

图 4 安全可信计算环境实现思路

可信软件基利用可信芯片的特性,为应用、系统、硬件设备的运行建立可信的安全计算环境,通过可信连接形成可信体系,实现硬件、操作系统、应用系统的融合。由可信芯片提供可信指令,在操作系统层由可信软件基构建安全计算环境,实现操作系统层面的身份鉴别、安全审计、访问控制、入侵防范,在数据层面实现数据的备份、恢复,保证数据的完整性、保密性,同时实现对操作系统的漏洞发现、安全策略配置、恶意代码检测、系统补丁升级等安全相关配置的集中管理[14]。

在应用层通过在可信安全管理平台设置工业控制软件程序及关联程序为白名单,对其进行安全分析和安全规则制定。每一个被设置为可信的软件都有其安全特征值,在软件使用过程中,都会匹配特征值,一旦攻击者利用漏洞进行攻击,可信计算支撑平台会根据软件的安全规则进行拦截,有效弥

补已知、未知安全漏洞未及时修补造成的安全威胁。

2.3 安全制度建设

技术为网络安全防护提供支撑，人员是安全防护的实施者与受益者，电力监控系统运营人员普遍存在重视生产安全，忽视网络安全的情况，网络安全知识欠缺。国家法律法规、行业监管安全防护要求不断提高，发电企业亟需组建具有较高专业性的网络安全运维团队来提供高效的网络安全保障服务，需加强以下管理工作：

(1)制定完善的网络安全制度，包括安全管理制度、安全管理机构、安全管理人员、系统建设管理安全、系统安全运维管理等相关制度体系，使安全运维工作有章可循、有法可依。

(2)实时监控系统警告、预警，制定安全事件报告和处置管理制度，明确不同安全事件的报告、处置和响应流程，规定安全事件的现场处理、事件报告和后期恢复的管理职责等[15]。

(3)做好应急预案框架，明确应急处理流程，定期开展应急预案培训，并进行应急演练，在演练过程中寻找到安全防护体系的短板，通过“发现–验证–修补–再验证”不断迭代的方式提升安全防护能力。

3 应用效果

该方案以河南某发电企业电力监控系统生产控制区为建设试点，在不改变电力生产控制原有软硬件架构，并保证电力监控系统能够正常稳定运行的前提下，该系统在完成安全建设后在等级保护测评、网络安全风险评估中均取得较好的成绩，如表 1 所示，等级保护测评结论由加固前的“差”(60 分以下并存在高等级安全风险)提升为“良”(80 分以上且不含高等级安全风险)，其中不符合测评指标均不是高危风险，中低风险不符合项显著降低。由于主机部署终端安全可信保护系统，加固前渗透测试发现的高风险漏洞均无法再被利用，系统的整体防护水平明显提高。

表 1 系统安全防护建设前后效果比较

测试验证方法	评估指标	加固前	加固后
等保测评	分数/分	59.61	81.32
	高风险数/个	6	0
	中低风险/个	36	13
风险评估	高风险数/个	5	0
	中低风险数/个	25	10
内网渗透测试	高风险漏洞/个	5	0

4 结论

随着电力监控系统的智能化程度逐步提高，其网络安全面临严峻威胁，漏洞挖掘技术的不断成熟，使电力监控系统中的安全漏洞数量明显增多，针对电力监控系统的网络攻击事件层出不穷。

等级保护 2.0 时代电力监控系统的安全防护需要在现有的安全防护基础上，结合等级保护新增安全防护要求项，做好顶层设计，做精底层防护。以“一个中心”为安全建设的核心，以“三重防护”为基本，构建可信主动防御，事后分析、溯源、加固的防御体系，全方位提升电力监控系统网络安全感知能力和防护能力，维持电力企业稳定、安全的电力生产，保障国民经济的发展和人民生活的安定。

参考文献

[1] 张宇翔，陶源.基于等级保护与可信计算构建我国关键信息基础设施保障体系[J].信息安全研究，2017，3(4)：375–381.

[2] 国家能源局.关于印发电力监控系统安全防护总体方案等安全防护方案和评估规范的通知[Z].2015.

[3] 周民军.工控网络现状与安全分析[J].现代工业经济和信息化，2017，7(15)：61–62.

[4] 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.

[5] 中关村信息安全测评联盟.网络安全等级保护测评高风险判定指引[Z].2020.

[6] 王哲峰.电力企业智慧网络安全体系研究与探索[J].网络安全和信息化，2022(3)：113–120.

[7] 胡朝辉，王方立.电力监控系统通信安全技术研究[J].电子技术应用，2017，43(3)：21–24.

[8] 江泽鑫.电力物联网信息安全防护技术研究[J].信息技术与网络安全，2020，39(1)：31–37.

[9] 何占博，王颖，刘军.我国网络安全等级保护现状与 2.0 标准体系研究[J].信息技术与网络安全，2019，38(3)：9–14，19.

[10] 周帅，王绍杰.私有工控协议分类方法研究[J].信息技术与网络安全，2021，40(9)：19–24.

[11] 邵俊杰，董伟，冯志.基于机器学习的工业控制网络异常检测方法[J].信息技术与网络安全，2019，38(6)：17–20，25.

(下转第 59 页)

to detecting highly interactive Twitter communities using tweeting links[J].Web Intelligence and Agent Systems, 2016, 14: 1-15.

[15] FORTUNATO S, HRIC D. Community detection in networks: a user guide[J]. Physics Reports, 2016, 659: 1-44.

[16] KERNIGHAN B W, LIN S. An efficient heuristic procedure for partitioning graphs[J]. Bell System Technical Journal, 1970, 49(2): 291-307.

[17] WHITE S, SMYTH P. A spectral clustering approach to finding communities in graphs[C]//Proceedings of the 2005 SIAM International Conference on Data Mining, 2005: 274-285.

[18] GIRVAN M, NEWMAN M E. Community structure in social and biological networks[J]. Proceedings of the National Academy of Sciences, 2002, 99(12): 7821-7826.

[19] RATTIGAN M J, MAIER M, JENSEN D. Graph clustering with network structure indices[C]//Proceedings of the 24th International Conference on Machine Learning, 2007: 783-790.

[20] NEWMAN M E, GIRVAN M. Finding and evaluating community structure in networks[J]. Physical Review E, 2004, 69(2): 026113.

[21] BLONDEL V D, GUILAUME J L, LAMBOTTE R, et al. Fast unfolding of communities in large networks[J]. Journal of Statistical Mechanics: Theory and Experiment, 2008, 30(2): 155-168.

[22] 李晓红, 孔文文, 马堉垠, 等. 利用词项语义共现和社团划分发现微博热点事件[J]. 计算机应用研究, 2020, 37(5): 1336-1339.

[23] 张继东, 杨杨. 基于用户偏好和信任度的移动社交网络社区聚类模型[J]. 情报杂志, 2018, 37(10): 174-182.

(收稿日期: 2022-06-15)

作者简介:

林国英(1996-), 女, 硕士研究生, 主要研究方向: 信息管理。

汪明艳(1975-), 女, 博士, 教授, 硕士生导师, 主要研究方向: 数据分析、网络舆论治理、电子商务。

(上接第 53 页)

[12] 李实, 万睿, 周帅. 工控系统脆弱性分析研究[J]. 信息技术与网络安全, 2022, 41(3): 26-31.

[13] 黄强, 沈昌祥, 陈幼雷, 等. 基于可信计算的保密和完整性统一安全策略[J]. 计算机工程与应用, 2006(10): 15-18.

[14] 施一明, 高博, 王天林, 等. PLC 可信软件技术研究[J]. 中国仪器仪表, 2022(3): 66-69.

[15] GB/T 22239-2019 信息安全技术网络安全等级保护基本要求[S]. 2019.

(收稿日期: 2022-05-07)

作者简介:

李政达(1994-), 男, 硕士, 主要研究方向: 网络安全、工业互联网安全。

杨继(1992-), 男, 硕士, 主要研究方向: 网络安全、工控信息安全。

姜添元(1996-), 男, 硕士, 主要研究方向: 网络安全、工控信息安全。

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