智能电网的安全可控性

刘小雪,曹华阳,朱培栋,胡 罡
(国防科技大学 计算机学院,湖南 长沙 410073)

摘 要:计算机与信息技术在电力系统中的广泛应用提高了电网的自动化、智能化水平,同时也将传统 IT 领域的众多安全隐患引入了电网。智能电网是社会域、信息域、物理域多域交互、渗透形成的大规模新型融合网络,其安全威胁具有多域渗透、跨域攻击的特点。文中描述了智能电网基本安全需求及其与传统 IT 安全需求的不同;分析了智能电网中多域渗透攻击并且对信息-物理安全威胁进行分类;基于分域防护、多域协同、边界防护的思想提出了智能电网多域协同安全防护模型。

关键词:智能电网;多域融合;安全需求;多域渗透攻击;多域协同防护
中图分类号:TP39 **文献标识码**:A **文章编号**:1673-629X(2014)09-0146-05
doi:10.3969/j.issn.1673-629X.2014.09.033

Security and Controllability of Smart Grid

LIU Xiao-xue,CAO Hua-yang,ZHU Pei-dong,HU Gang
(School of Computer,National University of Defense Technology,Changsha 410073,China)

Abstract:Computer and information technologies have been widely applied into the power system to enhance its automation and intelligence level,which brings numerous threats from traditional IT areas to power grid. Smart Grid is a new converged network formed by the interaction and penetration of social domain,information domain and physical domain,and the threats and attacks in Smart Grid can cross domains. In this paper,discuss the primary security requirements of Smart Grid and their differences from traditional IT security. Cross-domain attacks are analyzed and information-physical threats are classified. Based on the thoughts including protection in separating domains,multi-domain cooperation and enhancing protection on boundaries,the multi-domain and cooperative protection model for Smart Grid is proposed.

Key words:Smart Grid;multi-domain fusing;security requirements;multi-domain penetration attacks;multi-domain and cooperative protection

0 引 言

智能电网是当前世界各国普遍关注与研究的热点。关于智能电网的定义有很多,文中参考的是:智能电网是将计算机网络与信息基础设施同现有的电力系统基础设施相结合而形成的自动化、智能化的新型电网。计算机网络与信息技术的广泛使用提高了电网的数字化、自动化水平,但是也不可避免地将计算机网络与信息领域的众多安全隐患引入了电网[1]。近年来,黑客通过网络攻击手段注入电网并最终实现对电力系统及物理设备等基础设施的攻击事件不断出现,由信息域向物理域的渗透攻击是当前智能电网安全面临的重大挑战。据报道,2009 年,曾有黑客向美国电网注入恶意代码并且远程控制其发作,最终导致美国部分地区电网瘫痪[2];2010 年 9 月,一个名为“Stuxnet”的震网病毒攻击全球工业领域,该病毒的攻击目标是监测控制与数据采集系统(SCADA),感染了全球超过 45 000个网络,给各国的电力部门带来了巨大的威胁和破坏。作为国家关键基础设施,电力系统安全关系到国计民生和社会稳定[3];然而电力行业的众多系统与设备在最初设计时并未考虑计算机与网络环境下的安全问题,针对智能电网安全的研究变得迫在眉睫。当前,许多组织与机构在研究开发智能电网的安全需求[4]并致力于安全标准的制定,如北美电力可靠性委员会关键基础设施保护(NERC-CIP)。此外,众多的

收稿日期:2013-11-01 **修回日期**:2014-02-14 **网络出版时间**:2014-07-17
基金项目:国家自然科学基金资助项目(61170285)
作者简介:刘小雪(1990-),女,山东潍坊人,硕士研究生,CCF 会员,研究方向为大规模人机物融合网络的安全可控性;朱培栋,教授,博士生导师,研究方向为移动网络、路由协议和组播技术、社会网络。
网络出版地址:http://www.cnki.net/kcms/detail/61.1450.TP.20140717.1235.060.html

学者及研究团体针对智能电网安全进行了大量研究,并提出了自己的解决方案。文献[5]认为智能电网架构中网络–物理的攻击具有多域、跨域、跨边界的传播特点,并对网络–物理威胁进行分类,提出通过对威胁类型建模实现对跨域信息流和控制流的安全可控性,但未给出具体的解决方案;文献[6]讨论了公钥基础设施(PKI)和可信计算等可用于智能电网的安全技术,并给出了 PKI 和可信计算应用于智能电网的逻辑方案,但是其未考虑智能电网安全与传统 IT 安全的不同之处;文献[7]给出了一种面向智能电网自动化系统的网络安全集成防护机制,但是其并未考虑智能电网多域融合及安全威胁跨域攻击的特点,具有一定的局限性。

文中认为,智能电网是社会网络、信息网络、物理网络交互、渗透而形成的大规模新型融合网络[8-9],其中社会网络由电力公司员工及诸多电网用户(家庭用户、工业用户等)构成,由于当前电能应用的普遍性,智能电网的社会网络几乎涵盖了不同地区、不同层次的所有群体,规模巨大;信息网络则以传统的 IT 技术为核心;物理网络包括全部的电力系统基础设施。这种新型融合网络为新的服务及应用的出现提供了良好的平台,但同时也为攻击者带去了更多的可能。智能电网中社会域、信息域、物理域交互融合的特点使得安全威胁在电网中的跨域传播及影响成为可能,这使得智能电网安全面临更大的挑战。文中将分析智能电网的安全需求与传统 IT 安全的不同之处;讨论智能电网中的多域渗透攻击并对其信息–物理安全威胁进行分类;基于分域防护、多域协同、边界防护的思想,给出了智能电网多域协同安全防护模型。

1　与传统 IT 安全需求的不同

根据美国电力研究协会(Electric Power Research Institute,EPRI)报告[10],智能电网部署的最大挑战是系统的网络及信息安全,这不仅包括故意的攻击,例如,工业间谍、恐怖分子、政治军事组织等采取的由网络域向物理域的恶意渗透,也包括用户错误、设备失败和自然灾害引起的电网基础设施损毁。可见,智能电网面临的安全威胁不仅仅源自信息域,也可能来自社会域和物理域。

当前,传统 IT 领域的安全标准体系与安全技术手段已较为成熟,但对于智能电网来说还远远不够,因为与传统的计算机网络安全相比,智能电网具有不同的安全目标、安全结构、技术基础及性能要求:

(1)智能电网安全的首要目标是保证人的生命财产安全,其次是保护系统的可靠性和电力系统基础设施的安全[7];

(2)电力系统中,处于边缘的终端设备(如 RTU,PLC 等)如果受损通常造成停电事故的发生甚至会进一步影响整个电网的运行;

(3)电力网络中有很多专用的系统和设备,它们基于专有的操作系统和通信协议(如 IEC61850,DNP3.0,ICCP 等);

(4)智能电网中传输的数据大多是时间关键的,对传输带宽、延迟性能要求很高。

因此,在把当前各种 IT 安全手段与技术标准应用于智能电网时,需要考虑智能电网自身的特点。此外,由于智能电网具有多域融合的特性,其安全威胁具有跨域传播的特点,攻击者可针对智能电网进行多域渗透攻击,这是仅靠传统的 IT 安全技术所无法应对的,因此需要分析智能电网中的安全威胁并构建新的智能电网安全防护模型。

2　智能电网中多域渗透攻击

智能电网的发电、输电、变电、配电及用电等各个环节,涵盖了众多的电力设备及 IT 基础设施,运行了各种实现监控、调度等功能的系统及应用,涉及大量工作人员和用户,是一个规模巨大的多域融合网络。社会域、信息域及物理域的融合在提高电网的整体性能及智能化水平的同时,也增加了电网的复杂性和脆弱性,为攻击者提供了更多的潜在入侵路径和攻击点;此外,多域融合使得安全威胁和攻击在智能电网中的跨域传播成为可能[11],这大大增加了威胁及攻击的影响面,使智能电网安全面临巨大的挑战。

2.1　多域渗透攻击模型

智能电网对计算机信息系统严重依赖,信息域的安全隐患给物理域的设备安全带来了巨大威胁,如 2010 年针对 SCADA 系统的“震网”病毒攻击伊朗核电站,实现由信息域向物理域的跨域渗透攻击,而这种病毒也完全可以在智能电网中传播并造成巨大破坏;另一方面,由于安全威胁在多域融合网络中的跨域传播,物理域中的设备故障也会对信息域、社会域带来巨大影响,如众多的由于电力设备的损坏导致的停电事故的发生及给人们生活带来的不便。

如图 1 所示,是智能电网多域渗透攻击模型,其中操作员工、操作层属于智能电网的社会域,控制层及操作系统、网络层属于信息域,硬件/系统层及物理设备、通信链路属于智能电网的物理层[12]。

(1)来自智能电网社会域的攻击可能有来自电网员工的内部攻击或无意的行为,他们可以删除重要数据、发布虚假信息或者制定并执行错误政策,如在用电高峰期恶意调低电价使用户增加电能的消耗,进而加重电力供应危机;而错误政策的制定与执行会带来非

最优化的结果;

(2)来自智能电网信息域的攻击是源于当前 IT 领域的诸多安全问题,包括蠕虫病毒、恶意软件及 DoS/DDoS 攻击等,会导致信息的机密性、完整性、可用性受损进而导致错误、故障的发生;

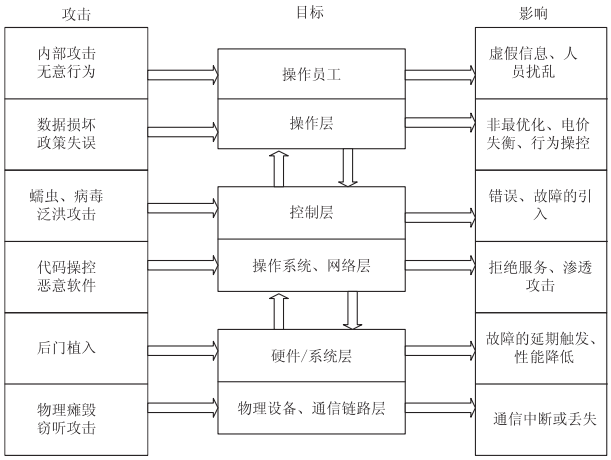

图 1 智能电网多域渗透攻击模型

(3)来自智能电网物理域的攻击包括在电网设备中植入后门、物理手段损坏设备以及对通信链路进行信号窃听。植入的后门可以在敏感时期如战时触发故障使物理设备瘫毁,这将严重影响电网的正常运行,如摧毁某个关键变电设备会导致大面积停电的发生,甚至会严重威胁当地居民的生命财产安全。

由于智能电网社会域、信息域和物理域的相互渗透、融合、交互,智能电网的安全威胁具有多域渗透、跨域攻击的特点,即攻击的发起与最终影响可以处于不同的域。图 2 表示了智能电网的跨域攻击,来自于社会域的间谍或内部员工的攻击会导致信息域中关键数据被泄露、篡改,进而造成物理域中的设备故障;发起于信息域的 DoS/DDoS 攻击能够导致物理域中智能电表、数据服务器或应用服务器的瘫毁;而物理域中多个传感器被毁可能会严重影响信息域中 SCADA 系统的正常运行,电网中的异常不能被及时发现并处理可能导致停电事故的发生,最终影响社会域中人们的正常生活。

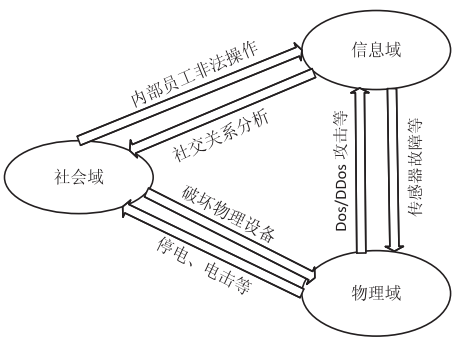

图 2 智能电网跨域攻击描述

此外,社会域中的人可以对物理域中的设备进行恶意或无意的直接物理攻击而导致设备瘫毁;而物理域中的设备故障可能会直接威胁社会域中人们的生命财产安全,如输电线因超负载而引发电击、火灾等。

2.2 信息-物理安全威胁分类

在多域融合的智能电网中,多域渗透、跨域攻击是智能电网安全面临的巨大挑战。下面重点考虑智能电网的信息域和物理域,从安全威胁的产生、传播及感知的角度,对智能电网中安全威胁进行分析和描述,并提出了相应的应对策略。

如图 3 所示,根据安全威胁的产生域和感知域(即影响域)的不同,智能电网中信息-物理安全威胁可分为以下四类[5]:

(1)信息域-信息域威胁(Cyber-Cyber Threat,CCT):产生于信息域,并仅在信息域范围内造成影响,关系到数据的机密性、完整性和可用性及相关应用服务的可靠性,如针对用户隐私信息的窃取及篡改,向用户发布虚假价格数据及向电力公司发送虚假电表数据等。针对此类威胁,传统的安全防护手段和技术均可使用,如加解密机制、身份认证机制及 VPN 等。

(2)信息域-物理域威胁(Cyber-Physical Threat,CPT):产生于信息域,但对智能电网物理域中的设备及物理参数造成影响,这种由信息域向物理域的跨域渗透攻击是近年来智能电网等关键基础设施面临的巨大挑战。例如,通过向信息域中控制系统注入蠕虫病毒或恶意软件实现对物理设施的非法操控甚至造成物理设备的自我瘫毁。针对此类攻击,需要在信息域和物理域分别采取安全防护措施,如在信息域进行入侵检测,采用针对蠕虫病毒及恶意软件的查杀机制。

(3)物理域-物理域威胁(Physical-Physical Threat,PPT):物理域中某些设备的损坏或某些物理条件的改变影响了其他物理设备的正常运行或导致其他物理条件的变化,历史上的大部分停电都是由于物理-物理的交互作用。如攻击者在一个电路中打开大量用电设备以使该电路继电器故障,某区域用户过度用电导致该区域配电网络超负载等。有些 PP 威胁甚至会威胁人们的生命财产安全,如输电线路超负载引发火灾等。针对 PP 威胁,可在物理域进行防护,如使用限制负载的设备或监测设备,也可通过制定相应的规章制度进行规范。

(4)物理域-信息域威胁(Physical-Cyber Threat,PCT):物理域中的设备损坏或物理参数的变化对信息域中相关应用与服务造成影响。如对智能电表进行物理攻击会严重影响自动计量及需求响应功能的实现,损坏关键应用服务器会导致众多控制系统及服务停止运行。针对 PC 威胁,可考虑对重要的物理设备加强物理防护(如安全外罩并上锁)、设置备份及报警装置

(一旦关键物理设备被毁就发出报警信号)。

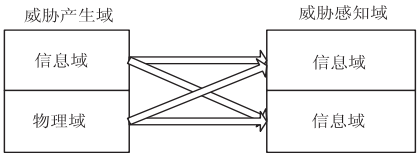

图 3　智能电网信息-物理安全威胁描述模型

上述四类安全威胁并不是相互独立、毫无关联的,而是相互影响甚至牵一发而动全身。图 4 为智能电网中四类信息-物理安全威胁的相互关系:PCT 发生可能会造成 CPT 或 CCT 的发生,而 CPT 的出现有可能会导致 PPT 或 PCT 的出现,进而发生连锁反应。例如,某区域用于数据采集及状态监测的多个传感器被毁,电网超负载异常不能及时反馈给 SCADA 系统,导致该区域输电线、智能电表等多个电网设备因负载过大被毁,进一步影响需求响应及输配电的实现,最终导致停电事故的发生。

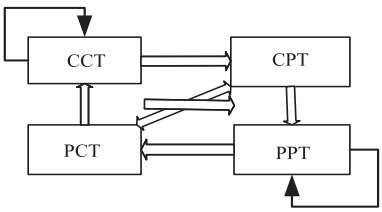

图 4　智能电网信息-物理安全威胁分类关系表示

此外,新的攻击技术层出不穷,如最近引起广泛关注的 APT(Advanced Persistent Threat)攻击,综合了当下先进的网络技术、社会工程学方法,有组织、有特定目标、持续时间长且不易被察觉,其主要目标就是智能电网等国家关键基础设施。

3　智能电网多域协同安全防护

智能电网是大规模的多域融合网络,其安全威胁具有多域渗透和跨域攻击的特点。一方面,攻击者可以综合利用 IT 技术、社会工程学方法及物理手段对智能电网进行全面的分析和漏洞的扫描,进而利用社会域、信息域、物理域任何一个域中的脆弱节点打开攻击的缺口;并且由于安全威胁的跨域传播,攻击能在任何域中造成破坏,例如,攻击者可利用蠕虫病毒对电网信息域的各控制系统进行攻击并致其瘫毁,这会导致物理域中设备损坏及大规模停电事故的发生,进而影响社会域中人们的正常生活甚至引发民众骚乱;因此需要对智能电网进行分域的安全防护。另一方面,仅靠单一域中的安全防护并不能保证智能电网的整体安全,传统的 IT 安全技术和手段仅能面向信息域中的安全事件,而无法应对物理域中恶意损坏设备等物理攻击行为[13],也无法应对社会域中的潜在威胁,如内部员工攻击及结合了社会工程学方法、针对智能电网等国家关键基础设施的 APT 攻击,因此需要对智能电网进行多域协同的安全防护。此外,还要加强域间边界的安全防护,采取强访问控制和身份认证等手段。

基于分域防护、多域协同、边界防护的原则,文中提出了智能电网多域协同安全防护模型,如图 5 所示。该模型将智能电网分为社会域、信息域及物理域三个安全防护域,针对每个安全防护域均采取相应的安全防护策略,并通过域间的交互、渗透、融合实现对智能电网的多域协同防护;此外,强化了域间边界的安全防护,以进一步应对安全威胁的多域渗透和跨域攻击。

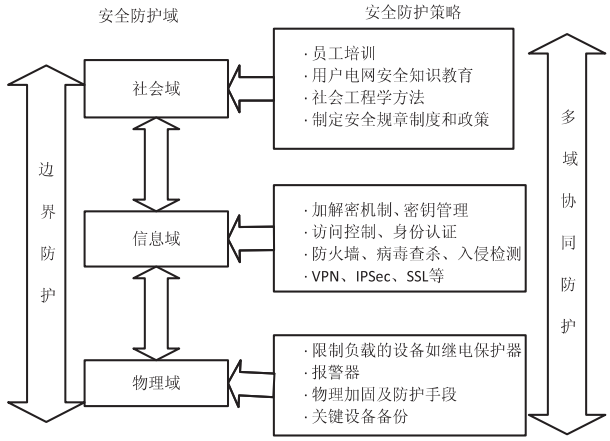

图 5　智能电网多域协同安全防护模型

(1)针对社会域的安全防护策略:包括对员工进行电网安全防护知识和安全操作技能的培训,对用户进行电网安全使用教育,提高人们的安全防护意识;制定安全规章制度和政策法规,增强对电网安全的制度保证;以社会工程学方法反制社会工程学攻击等。

(2)针对信息域的安全防护策略:传统的 IT 安全技术和手段均可用于对智能电网信息域的安全防护,如加解密机制、密钥管理等技术可用于保证数据的机密性、完整性和可用性;访问控制、身份认证及审计可用于保证智能电网中各种业务的正常运行及其安全可控性;IPSec、SSL、TLS 等则可在协议层强化智能电网安全;而防火墙、入侵检测、病毒查杀等技术手段则可实现安全威胁的及时发现并对其传播进行抑制,以使破坏性最小化。

(3)针对物理域的安全防护策略:智能电网中由于覆盖面积广,其有些物理设备所处的地理环境恶劣,风吹日晒、昼夜温差大,因此针对一些关键的电网设备可采用耐腐蚀、抗高温严寒的特殊材料制造;使用限制负载的设备,如继电保护器等;此外还可为关键设备设置备份、进行物理加固、设置报警器等。

(4)多域协同的安全防护:首先,由于智能电网社会域、信息域、物理域之间的相互渗透、融合、交互,针对各个域安全防护策略的配置也应相互配合、相互协作,进而实现对智能电网的多域协同安全防护,如信息

域安全技术的选择要考虑社会域中相应的安全规章制度,并结合物理域中设备的实际物理安全需求及可用的物理安全策略;再者,当一个域中的安全策略改变时,其他域中的安全策略也要进行适当的调整,如社会域中规定要进一步增强智能电表的数据安全及物理安全,那么信息域中针对智能电表就应采用强度更高的加解密算法和访问控制机制,而物理域则可加强对设备的物理安全监察并对关键设备进行重点保护。

此外,要加强社会域、信息域、物理域间信息的共享[14],当某个域检测到安全威胁时,要将当前的安全态势及时告知其他域进而采取相应的安全手段,以在时间和空间上多域协同实现对攻击不同环节的拦截。如某个关键的数据集成设备受到恶意的物理损坏,其上安装的报警器将发出报警信号,接到报警电力维护人员将赶赴现场对其进行维修,而基于该数据集成设备进行数据传送的控制系统或应用服务将启用新的路由进行数据的传输以维持系统的正常运行。

(5)加强域间边界防护:由于智能电网中的安全威胁可实现跨域传播,因此有必要加强对域间边界的防护,以抵御电网中的多域渗透攻击。图 6 是智能电网域间边界防护模型。在社会域与信息域的边界,通过使用强访问控制机制和身份认证算法来加强系统的访问控制和对管理人员的身份认证;在信息域和物理域边界要加强对设备的认证;在社会域与物理域边界可设置物理隔离装置防止人员对设备的直接损坏。

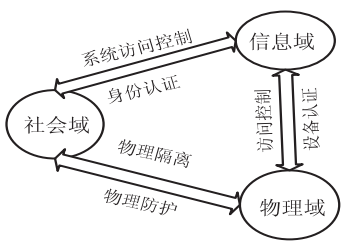

图 6 智能电网域间边界防护模型

此外,在内部可信网络与外部非可信网络之间可设置防火墙、入侵检测系统及进行物理隔离,以抵御来自外部网络的攻击。

4 结束语

计算机与信息技术在电网中的广泛应用使电网的智能化成为可能,但同时也将电力系统置于诸多传统 IT 安全威胁之下。由于智能电网是社会域、信息域、物理域多域交互、融合的结果,其安全威胁具有多域渗透、跨域攻击的特点,这使智能电网的安全可控性面临巨大的挑战。文中讨论了智能电网的基本安全需求与传统 IT 安全需求的不同之处,分析了智能电网中的多域渗透攻击并对其信息-物理安全威胁进行分类,基于分域防护、协同防护、边界防护的原则提出了智能电网多域协同安全防护模型。下一步的工作包括:研究发现多域渗透攻击机理和威胁跨域传播路径,开发多域协同防护技术和安全态势评估机制,提出并实现可行的多域协同安全防护机制。

参考文献:

[1] 曹军威,万宇鑫,涂国煜,等. 智能电网信息系统体系结构研究[J]. 计算机学报,2013,36(1):143-167.

[2] Gorman S. Electricity grid in U. S. penetrated by spies[J/OL]. 2009 - 08 - 08. http://online. wsj. com/article/SB123914805204099085. html.

[3] 关志涛,颜 立,何杰涛,等. 面向智能电网的信息安全技术展望[J]. 陕西电力,2010,38(6):5-8.

[4] NIST. Draft smart grid cyber security strategy and requirements [S/OL]. 2009. http://csrc. nist. gov/publications/drafts/nistir-7628/draft-nistir-7628. pdf.

[5] Neuman C,Tan K. Mediating cyber and physical threat propagation in secure smart grid architecture[C]//Proc of IEEE international conference on smart grid communications. Brussels:IEEE,2011:238-243.

[6] Metke A R,Ekl R L. Security technology for smart grid networks[J]. IEEE Transactions on Smart Grid,2010,1(1):99-107.

[7] Wei Dong,Lu Yan,Jafari M,et al. An integrated security system of protecting smart grid against cyber attacks[C]//Proc of innovative smart grid technologies. Gaithersburg, MD: IEEE,2010:1-7.

[8] 刘 晓,张隆飙,Zhang W J,等. 关键基础设施及其安全管理[J]. 管理科学学报,2009,12(6):107-115.

[9] 梅生伟,王莹莹,陈来军. 从复杂网络视角评述智能电网信息安全研究现状和若干展望[J]. 高电压技术,2011,37(3):672-679.

[10] Report to NIST onsmart grid interoperability standards RoadmapEPRI[R/OL]. 2009 - 06 - 17. http://www. nist. gov/smartgrid/InterimSmartGridRoadmapNISTRestructure. pdf.

[11] 陈来军,梅生伟,陈 颖. 智能电网信息安全及其对电力系统生存性的影响[J]. 控制理论与应用,2012,29(2):240-244.

[12] Yampolskiy M,Horvath P,Koutsoukos X D,et al. Taxonomy for description of cross-domain attacks on CPS[C]//Proceedings of the 2nd ACM international conference on high confidence networked systems. [s. l.]:[s. n.],2013.

[13] Mo Yilin,Kim T H,Brancik K,et al. Cyber-physical security of a smart grid infrastructure[J]. Proceedings of the IEEE,2012,100(1):195-209.

[14] 欧洲网络与信息安全局发布智能电网安全报告[R/OL]. 2013 - 03 - 18. http://www. djbh. net/webdev/web/HomeWebAction. do? p=getXxgg&id=ff8080813cf61c1a013d7b28f1590013.

智能电网的安全可控性

作者： 刘小雪， 曹华阳， 朱培栋， 胡罡， LIU Xiao-xue， CAO Hua-yang， ZHU Pei-dong， HU Gang

作者单位： 国防科技大学 计算机学院,湖南 长沙,410073

刊名： 计算机技术与发展 ISTIC

英文刊名： Computer Technology and Development

年，卷(期)： 2014(9)