电力工控系统攻击威胁分析技术研究

随着信息化和工业化的深度融合以及物联网的快速发展，越来越多的信息技术被应用到工业领域，电力工控系统面临着网络攻击威胁。因此，必须针对电网工控系统的威胁进行有效的监测，才能及时发现可能存在的安全问题。通过对电力工控系统攻击威胁的分析，提出一种基于攻击树的电力工控安全的威胁模型。根据威胁模型，自下向上迭代地计算各个节点的威胁值，从而评估威胁风险等级。威胁值越大，威胁风险等级越高，并且通过电力工控系统中的嗅探实例验证了该方法的实用性。在威胁模型的基础上，设计了电力工控协议威胁识别与监测平台。

张传远　杨夏祎　梁薇　齐永忠／北京中电普华信息技术有限公司

张传远／工程师

关键词／Keywords

电力工控系统·
威胁模型·
风险等级·
威胁监测·

0　引言

近年来，随着电力工控系统采取分区分域和纵深防御策略，通过实施内外网安全隔离、电网生产大区与管理信息大区安全隔离等关键安全防护工程[1]，系统安全防护体系逐渐得到完善。但是，随着工业控制系统和设备中新的漏洞、后门等脆弱性信息的发现和披露，电力工控系统面临更加隐蔽、更加曲折的恶意攻击风险（如APT）。另一方面，由于电网与发电厂工业控制系统安全防护体系及其防护能力的不均衡、不对称，特别是近年来大量光伏发电、风能发电等新能源发电站的接入，使电力工控系统面临越来越复杂的安全威胁[2]，迫切需要在电力工控系统关键节点构建安全威胁监测机制，以保护电力工控系统安全稳定，保证国家重要基础设施安全运行。因此，为解决存在的攻击威胁，开展电力工控系统攻击威胁分析技术的研究，研发了电力工控系统威胁识别与监测平台。

1 电力工控系统攻击威胁分析

1.1　攻击威胁概述

攻击威胁是一种对组织或者资产具有潜在性破坏的可能性因素或事件。无论电力工控系统安全级别有多高，攻击威胁都是客观存在的，它是电力工控系统风险评估的重要因素之一[3-6]。

产生安全威胁的主要因素分为人为因素和环境因素。人为因素有无意和有意之分；而环境因素则是自然界中一些不可抗因素和其他物理因素，如断电、洪灾和火灾等。攻击威胁的作用形式是对电力系统直接或间接的攻击，如非授权的泄密、篡改数据和窃听敏感信息等，在可用性、保密性和完整性等方面造成损害，致使系统瘫痪。通常来讲，攻击威胁总是要利用网络、系统应用或数据的脆弱性才可能对内部有价值的资产造成损害，这里数据的脆弱性是指能被威胁所利用的资产或若干资产的薄弱环节。安全事件及其后果是分析威胁的重要依据。但是有相当一部分攻击威胁发生时，由于未能造成后果，或者没有意识到，而被安全管理人员忽略，这将导致对攻击威胁的认识出现偏差。威胁分析关系如图1所示。

1.2 攻击威胁分类

电力工控系统由设备、系统平台、

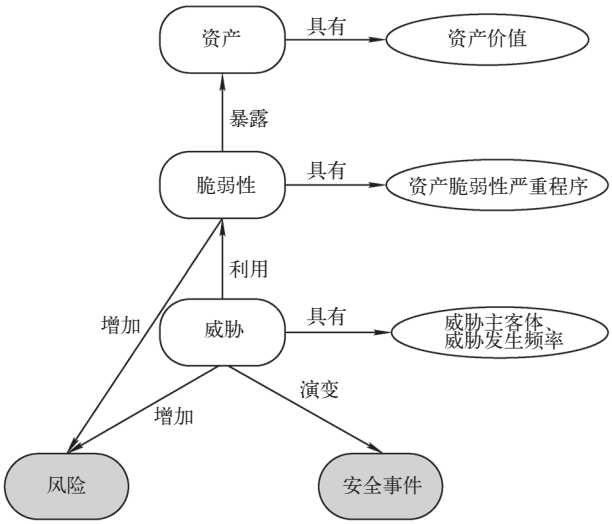

图1 威胁分析关系图

业务系统和网络等要素构成，其每个要素都存在着各种可能被攻击的脆弱性，随着攻击手段的层出不穷，其面临的攻击威胁越来越严重，要想针对每个攻击威胁提出相应的检测方法，需要了解电力工控系统中存在哪些攻击威胁。

1）嗅探[7]。指在网络内部监听、窃取机密数据，冒充合法ID破解通信密钥，造成数据泄密。

2）拒绝服务攻击（DDOS）[8]。借助网络系统或协议的缺陷和配置漏洞进行网络攻击，使网络拥塞、系统资源耗尽或系统应用锁死，常见攻击方式包括SYN Flood、UDP Flood、IP欺骗和Smurf攻击。

3）旁路控制。入侵者针对电网工控系统发送非法控制命令，可修改系统配置、程序和敏感数据，造成网络或系统瘫痪。

4）违规外联。系统内网直接连通互联网或通过其他网络访问互联网，电力工控系统中的设备未经安全防护及策略设置直接连通其他网络，当发生违规外联时，内部网络将面临病毒木马、非授权访问和数据泄密等多种安全威胁。

5）病毒攻击。工控智能设备主要基于Linux系统作为底层操作系统，其可能感染很多种类的Linux木马病毒，主要包括感染ELF格式文件的病毒、脚本病毒、蠕虫病毒、后门程序和其他病毒。

2 基于攻击树的电力工控安全威胁模型

2.1 安全威胁模型

在电力工控系统的攻击过程中，攻击不会以一种方式或者一个步骤得以实现，而是以不同的攻击进程采取不同的攻击方法，且并不是以既定模式展开攻击。本文以攻击树为基础，实现电力工控系统的安全威胁建模。攻击树虽然逻辑结构简单，但其树形结构可以直观准确地描述系统中包含哪些攻击方式和威胁种类，同时攻击树具有很强的扩展性，可以根据逻辑结构按需求增加或删除对系统不足以构成威胁的攻击。

安全威胁建模的思想就是基于攻击树模型，把从系统安全风险中分析出来的安全威胁行为作为树的结构形式建立威胁树，表示威胁行为及其攻击步骤之间的逻辑关系。其中每棵威胁树代表攻击者使用的威胁方法，每条路径代表具体的攻击方式。因此，任何一个网络都会存在一个威胁树集合。一棵基本的威胁树模型包含根节点、叶节点以及中间节点。根节点表示攻击者对系统威胁的最终目标；叶节点表示威胁可能采取的攻击手段；而中间节点则表示攻击者达到最终目标时所采取的中间步骤。其中根节点的各个子树是可选路径，攻击者可采取不同的攻击进程。

传统的攻击树模型[9]包含“与”（AND）节点和“或”（OR）节点。“与”节点表示攻击者需要完成全部子目标，攻击才能继续；否则攻击无效。“或”节点表示攻击者只要达到其中任一子目标，攻击方可继续。而威胁树在此基础上增加了“顺序与”（SAND）节点，表示攻击需要按子目标的顺序进行才可以继续传播。三种威胁树节点关系如图2所示。

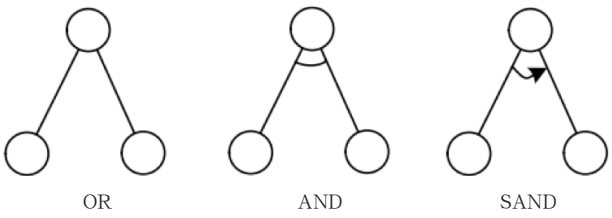

图2 威胁树节点关系

电力工控系统中存在大量对电力公司有价值的信息或资源，是保护的重点对象，威胁则利用资产的脆弱性对资产造成不必要的损失。在电力工控系统的资产识别、设备特征分析与识别中，主要分析变电站综合自动化系统、AGC/AVC和PMU等设备的组成结构、工作原理和工作过程，在此基础上确定各终端的关键性元素，即关键资产（如硬件、软件、系统接口、数据和信息、操作以及它们的用途），也是确定这些终端的安全界限，通过划定安全界限确定需要保护的资产以及易受攻击的过程，同时获取威胁的存在方式以及将要攻击的切入点，从而构造安全威胁建模[10]。构造的具体过程如下。

1）在安全界限处可以推断出存在哪些攻击行为，将电力工控系统的网络安全作为威胁树的根节点，根据各种安全威胁对网络安全的影响，分别从机密性、完整性和可用性三个安全目标出发，依照攻击者可能会使用的攻击手段对系统造成的安全威胁向下逐层扩展。

2）分析了解电力工控系统中存在的安全隐患以及脆弱性，站在攻击者的角度去思考以何种攻击方法攻击最终要达到的目标，列出工控系统中包含的所有威胁、利用其实现攻击的所有可能攻击途径和所要具备的攻击条件。如上述所提到的拒绝服务攻击（DDOS），有“耗尽能源”和“洪泛攻击”两种攻击途径，要达到“耗尽能源”的攻击需要顺序进行两步攻击步骤，首先安装射频装置，其次不断向RFID读写器发送请求，耗尽其读卡器资源，从而达到拒绝服务攻击。其他几种典型的攻击手段以及攻击途径如图3所示。

3）重复步骤1）和步骤2），找出可能针对电力工控系统具有威胁的攻击源，对所有父节点进行扩展，对各个子节点进行细化，直到细化到叶节点。叶节点即为原子节点，是威胁建模的最底层不可再细化的节点，通过威胁评估方法能够对其进行安全评估的节点。由于电力工控系统网络的结构极其复杂，终端设备种类繁多，攻击手段也逐步增多。因此，安全威胁建模会很庞大。

经过上述步骤可构建具有很好扩展性的威胁建模，操作也很方便，若发现一种新的攻击方式，只要在该攻击节点的隶属父节点下加一个代表新攻击方式的子节点即可。威胁建模也具有很好的可重用性，安全人员可以选取威胁建模中的一部分作为新的威胁模型，这样可以简化安全人员的工作。

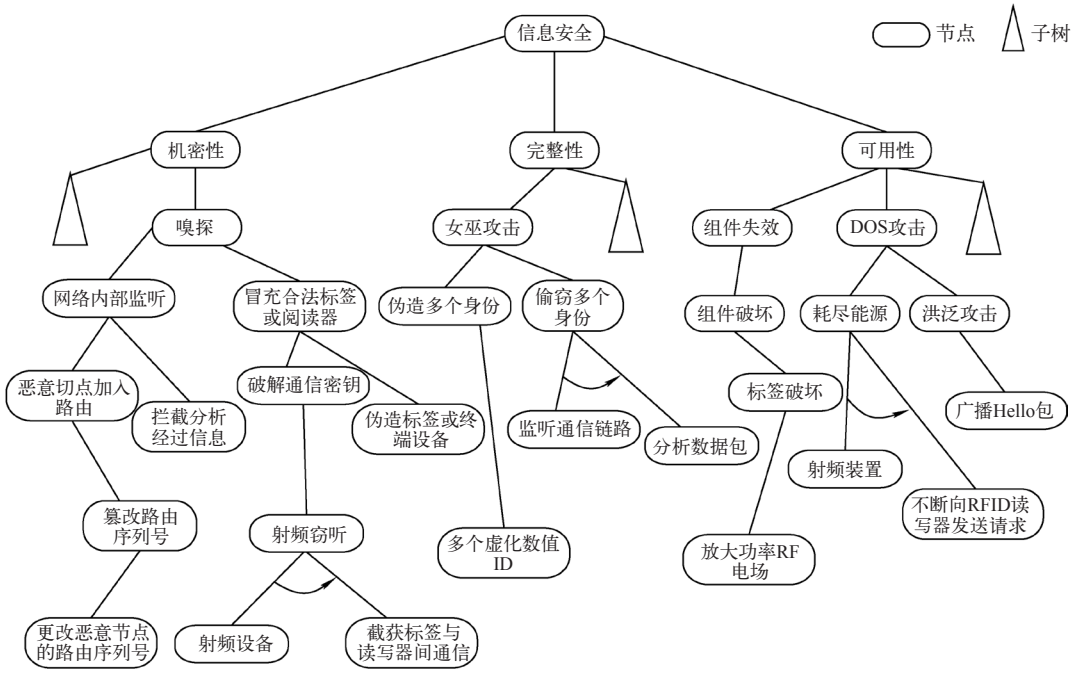

图3 电力工控系统攻击威胁建模

2.2 算法分析

威胁建模建立后，可方便观察电力工控系统中存在的攻击威胁以及其攻击手段和攻击路径，但无法判断攻击威胁的风险值，也就无法确定攻击威胁的风险等级，需要计算攻击威胁风险值[11]。因此，本文提出一种基于威胁攻击路径的威胁评估算法，借助威胁建模，将逻辑结构中每个路径节点看作一个威胁因子[12]，分析各威胁因子可能会被利用到的几率，计算威胁因子的权值，根据威胁因子的权值确定威胁风险值，由此评估威胁攻击能力以及其对电力工控系统造成损失的严重程度确定威胁风险等级等相关信息。

将图3的攻击威胁建模表示为有向树$T=\{V, E, G, c, f, h, g\}$。

其中

$$V=V_e \cup V_m \tag{1}$$

式中，V为树中节点集合；V_e为树中叶子节点集合；V_m为树中非叶子节点集合。

$$E=E_u \cup E_m \tag{2}$$

式中，E为树中弧的集合；E_u为“OR”边；E_m为“AND”边。

$G=\{s, m, n, p\}$表示三个安全威胁类型的集合，其中，m为机密性威胁；n为完整性威胁，p为可用性威胁；s为综合威胁。

$e(i, j)\in E$的权值，当$e\in E_u$时，j为单点集，需要多点共同完成；当$e\in E_m$时，j表示为多点集。

v表示树中某一节点，f为函数计算节点v的安全威胁类型，表示该节点是机密性威胁、完整性威胁、可用性威胁还是综合威胁。节点v是树中叶子节点时，根据节点的安全威胁类型确定其值，计算式为

$$f(v)=\begin{cases} s\ v\in V_m \\ x\in\{m,n,p\}\ v\in V_e \end{cases} x \tag{3}$$

h函数用于计算节点威胁类型的威胁因子，当该节点是机密性威胁、完整性威胁和可用性威胁时，其值用一个常量表示威胁类型的大小；当该节点是综合威胁时，其值为所有子节点值中的最大值，计算式为

$$h[f(v)]=\begin{cases} \alpha\ f(v)=x \\ \max h[f(k)]\ f(v)=s \end{cases} \tag{4}$$

g函数用于评估节点所受的威胁值，其值越大代表该威胁攻击性越大，判断节点是否是叶子节点。计算公式为

$$g(v)=\begin{cases} h(f(v))\ v\ v\text{是叶子的节点} \\ \sum_{(v,j)\cup E_u} E(v,j)[h(f(j))]+g(j)+ \\ \sum_{(v,j)\cup E_n} \Pi_{(v,j)\cup E_n} E(v,j)[h(f(j))+g(j)] \\ v\text{不是叶子的节点} \end{cases} \tag{5}$$

2.3 实例验证

电网工业控制系统安全威胁监测系统是一个综合性的安全风险监控系统，需要和电网边界分析相结合，其中以调控系统与光伏电站工控系统边界为重点，因此必须重视新能源电站工控系统安全风险和电网调控系统安全风险的具体特点。经过上述算法的分析，本文以电力工控系统中基于工控协议的攻击威胁为例[13]，说明具体的威胁建模以及风险评估。计算图3安全威胁建模中的机密性威胁类型，假设每条边的权值为1，α=0.5，根据式（2）～式（4）计算出威胁建模中各节点的威胁值，如图4所示，从而评估各攻击威胁的风险值，威胁风险值越高，威胁也就越大。

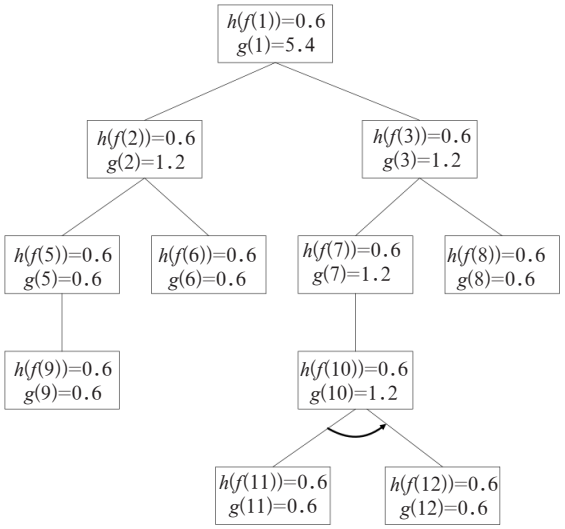

图4 机密性威胁风险值

3 电力工控协议威胁识别与监测

通过对电力工控系统安全威胁的辨识与分析，评估了系统中威胁风险等级，并确定了电力工控系统中安全风险的特点和规律，为研究开发

电力工控系统威胁识别与监测平台提供了技术支持，接下来基于攻击树的安全威胁模型，初步设计了电力工控系统威胁识别与监测平台。

电力工控系统系统由设备、系统平台、业务软件和网络等要素组成，其中每个要素都存在着各种可被攻击的弱点，随着攻击手段的层出不穷，其面临的威胁越来越严重。安全威胁监测主要针对用电采集系统智能终端和配电自动化终端的安全问题进行威胁的监测与分析，系统地分析其所面临的威胁及其存在的脆弱性，评估安全事件一旦发生可能造成的危害程度，并且安全威胁监测需要结合实际的攻击手段来验证安全威胁监测与分析能力。

系统主要面向工业控制系统的控制设备、网络通信流量、I/O状态、DCS工程师站、DCS操作站、网络设备和安全设备等进行数据采集、解析、分析、安全监测及告警。系统基于模块化分层设计原则包括数据采集层、大数据存储层、大数据分析层、监测业务层和数据展现层等层面，提供全方位的异构数据采集能力、大数据存储与分析能力以及进行综合的安全分析及异常攻击告警与管理能力。其中数据采集层针对集散控制系统（DCS）的异构数据源、专有通信协议和组态控制等特点提供工控环网专用采集现场监测装置、设备状态采集代理、I/O状态采集模块、基于Syslog和SNMP的日志与状态采集代理、基于FTP和HTTP/HTTPS的系统配置、关键文件及组态程序采集代理。大数据存储主要针对采集的数据进行解析并格式化，以便于进一步地存储与分析。大数据分析层通过数据预分析构建分类数据库，并基于云数据进行存储，利用大数据分析技术对数据进行抽取、预处理和数据整合提供集散控制系统的控制指令、组态程序等的完整性分析、系统和网络流量的异常分析、攻击的关联分析及系统状态的时序分析等能力。监测业务层提供针对集散控制系统的安全监测核心功能，包括异常流量监测、病毒攻击监测、通信行为监测、总线访问监测、系统负载监测、状态参数监测、控制信号监测、DCS组态监测和DCS数据与操控指令监测等多种安全功能。数据展现层提供统一的可视化的安全态势展现、实时监控、监测告警、溯源分析和统计报表等功能。系统和接口管理提供用户管理、权限控制、配置管理、日志管理、设备管理、监测对象管理及健康自检等管理与配置功能，同时还提供和外部系统的接口管理，包括网管接口、告警推送接口和升级同步接口等。电力工控系统威胁监测体系如图5所示。

电力工控系统威胁识别与监测平台如图6所示。工业网络现场监测装置用于对工业以太网流量的采集与分析，总线现场监测装置用于对典型现场总线上的流量进行采集与分析，控制信号现场监测装置用于对I/O信号线上的信号进行直接地采集与分析，所有采集到的实时数据会被存储到MongoDB数据库集群，供异常监测中央平台分析。

所有监控类设备通过交换机进行连接，分配合理的IP地址保证可以正常通信即可，设备之间的通信会有产品上的VPN服务保证完整性与保密性。

4 结束语

本文对电力工控系统攻击威胁分析的技术研究，主要提出了基于攻击树的安全威胁建模的方法，对威胁监测系统的安全问题展开了整体上的研究，但是由于电力工控系统的智能设备应用十分广泛，种类也较多，再加上以往人们也更关注于后台信息系统的安全性，与电力工控系统智能设备相关的安全体系、标准规范和监测方法还有待完善。而在电力系统中，电力工控系统智能设备的正常安全运行关系到整个电网的安全，因此对信息安全问题展开进一步研究是很有必要的。

参考文献

[1] 徐新国．工控系统信息安全策略探讨[J]．自动化博览，2013(11)：25-25．

[2] 白雪原．工控系统安全威胁及防护应用探讨[J]．中国信息化，2018(5)：48-49．

[3] 于永忱．浅谈网络的攻击源[J]．科技风，

图5　电力工控系统威胁监测体系

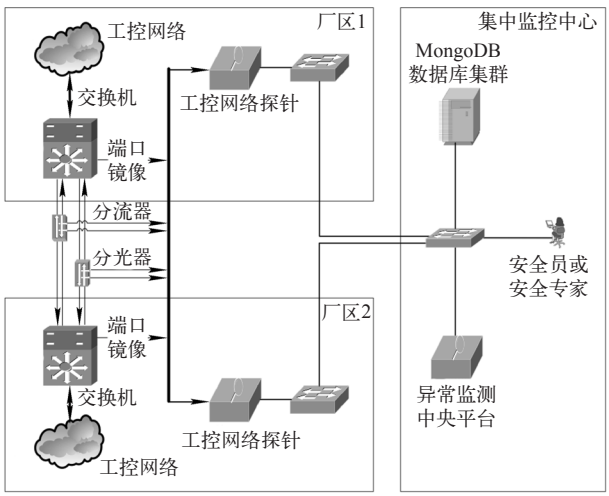

图6　电力工控系统威胁识别与监测平台

2011(13)：7，12.

[4] 闫巧，吴建平，江勇．网络攻击源追踪技术的分类和展望[J]．清华大学学报：自然科学版，2005，45(4)：497-500.

[5] 缪嘉嘉，张瞩熹，贾焰，等．一种基于数据流的网络威胁监控框架[J]．计算机工程与科学，2009(12)：23-26，51.

[6] 卢锦玲，朱永利．基于暂态能量裕度的电力系统脆弱性评估[J]．电工技术学报，2010，25(6)：96-103.

[7] 徐鸿，杨云江．基于嗅探技术的内部网络安全研究[J]．微型机与应用，2011(1)：38-40.

[8] Michael Walfish，Mythili Vutukuru，Hari Balakrishnan，et al．DDoS defense by offense[J]．ACM Transactions on Computer Systems (TOCS)，2010，28 (1)：55-108.

[9] 李奕林，穆灵．电力工控系统安全面临的威胁与对

(下转第107页)

有更高的稳定性。

4 结束语

本文采用的预测方法，是基于不确定性理论的D-S证据理论针对光伏发电受环境、设备因素等不确定因素影响的发电量预测，采用了数据挖掘中的决策树算法，全面综合历史数据，利用Python程序实现算法，得到预测结果。

从预测结果与误差分析来看，所采用的预测方法具有一定的预测准确度，满足NB/T 32011—2013《光伏发电站功率预测系统技术要求》规范要求。

参考文献

[1] 龚莺飞，鲁宗相，乔颖，等．光伏功率预测技术[J]．电力系统自动化，2016，40(4)：140-152

[2] 张玉，张振涛，莫寒．光伏发电的预测综述[J]．制造业自动化，2015，37(11)：27-30．

[3] Heinrich Morf．The stochastic two-state cloud cover model STSCCM [J]．Solar Energy，2011 (85)：985-999．

[4] 王守相，张娜．基于灰色神经网络组合模型的光伏短期出力预测[J]．电力系统自动化，2012，36(19)：37-41．

[5] 姚仲敏，潘飞，沈玉会，等，基于 GA-BP和POS-BP神经网络的光伏电站出力短期预测[J]．电力系统保护与控制，2015，43(20)：83-89．

[6] 周志华．机器学习[M]．北京：清华大学出版社，2016．

[7] Peter harrington machine learing in action [M]．United States of America：Manning Publications，2012．

[8] 杨风暴，王肖霞．D-S证据理论的冲突合成方法[M]．北京：清华大学出版社，2010．

[9] 丛林虎，徐延学，荀凯．基于D-S证据理论的导弹制导控制系统的联合最小二乘支持向量机预测模型[J]．兵工学报，2015，36(8)：1466-1472．

[10] 陈毅波，郑玲，姚建刚．基于粗糙集理论与D-S证据理论改进的多元回归负荷预测方法[J]．电力系统保护与控制，2016，44(6)：62-67．

[11] 吴京秋，孙奇，杨伟，等．基于D-S证据理论的短期负荷预测模型融合[J]．电力自动化设备，2009，29(4)：66-70．

[12] 刘亚南，卫志龙，朱艳，等 基于D-S证据理论的短期风速预测模型[J]．电力自动化设备，2013，33(8)：131-136．

(收稿日期：2018－04－04)EA

(上接第90页)

策[J]．信息安全与通信保密，2014(6)：62-63．

[10] 王继业，孙利民，李晔，等．电力工控系统攻击仿真验证关键技术研究[J]．电力信息与通信技术，2017(6)：9-14．

[11] Baiardi F，Telmon C，Sgandurra D．Hierarchical，model-based risk management of critical infrastructures[J]．Reliability Engineering and System Safety，2009，94(9)：1403-1415．

[12] Esmalifalak M，Ge Shi，Zhu Han，et al．Bad data injection attack and defense in electricity market using game theory study[J]．IEEE Transactions on Smart Grid，2013，4(1)：160-169．

[13] Eom Jung-Ho，Han Young-Ju，Park Seon-Ho．Active cyber attack model for network system's vulnerability assessment[C]．2008 International Conference on Information Science and Security，Seoul，2008．

[14] 王德文，周青．一种电力设备状态监测大数据的分布式联机分析处理方法[J]．中国电机工程学报，2016(19)：5111-5121．

[15] 赵峰，乌大鹏．电力系统高速数据采集系统设计[J]．数字技术与应用，2013(3)：163．

[16] Jia Zhiwei，Wang Lijun，Zhang Jinchuan et al．High efficiency，low power-consumption DFB quantum cascade lasers without lateral regrowth[J]．Nanoscale Research Letters，2017，12(1):281．

(收稿日期：2018－08－14) EA