考虑攻击方身份的电力监控系统网络安全风险分析

单瑞卿[1],盛　阳[1],苏　盛[2],畅广辉[1],李翔硕[1],
薛盖超[1],阮　冲[3],吴　坡[3],张江南[3]

(1.国网河南省电力公司,河南 郑州 450052;2.长沙理工大学电气与信息工程学院,湖南 长沙 410114;
3.国网河南省电力公司电力科学研究院,河南 郑州 450052)

摘　要:信息与物理系统的深度耦合使得网络攻击成为影响电力系统运行可靠性的重要因素。首先,从攻击方视角进行网路安全威胁风险分析,根据攻击者身份推断其可动用的资源,分析想要达成的攻击目的及可能采取的渗透入侵路径和破坏模式,为研制针对性的防护方法提供指导;其次,分析电力行业正在推进的可信计算、等级保护、安全态势感知等防御机制的缺陷,指出软、硬件系统的供应链安全威胁;然后考虑到攻击不同电力监控系统造成的风险水平和危害后果有所差异,从成功攻击可能性和危害后果 2 个维度构建电力系统网络攻击风险矩阵,并指出多目标协同攻击相比于单点攻击将使风险出现跃迁现象;最后,从国家支持型网络攻击可动用的资源和想要达成的攻击目的出法,提出 2 种高危潜在网络攻击破坏模式,并对其攻击实现过程和危害机制进行概要分析。

关　键　词:电力信息物理系统;网络安全;风险分析;无通信协同攻击;国家支持型网络攻击
DOI:10.19781/j.issn.1673-9140.2022.05.001　　**中图分类号**:TM863　　**文章编号**:1673-9140(2022)05-0003-14

Risk analysis of power system cyber security considering identity of malicious adversaries

SHAN Ruiqing[1],SHENG Yang[1],SU Sheng[2],CHANG Guanghui[1],LI Xiangshuo[1],
XUE Gaichao[1],RUAN Chong[3],WU Po[3],ZHANG Jiangnan[3]

(1.State Grid Henan Electric Power Company, Zhengzhou 450052, China;2.School of Electrical & Information Engineering, Changsha University of Science & Technology, Changsha 410114, China;3.Electric Power Research Institute, State Grid Henan Electric Power Company, Zhengzhou 450052, China)

Abstract: The ever-increasing coupling relationship between cyber and physical systems makes cyber-attacks become an important factor affecting the reliability of power system operations. First, this article conducts the analysis of the network security risk from the attacker's perspective, infers the available resources of the attacker based on the identity of the attacker, analyzes the purpose of the attack to be achieved, and infers the possible penetration and intrusion path and damage modes. The guidance can be provided to develop the specific protection methods based on the above

收稿日期:2022-07-20;**修回日期**:2022-09-01
基金项目:国家自然科学基金(51777015);国网河南省电力公司科研项目(SGHADK00DWJS2200211)
通信作者:苏　盛(1975—),男,博士,教授,主要从事电力大数据应用、电力气象灾害分析和电力系统网络安全防护研究;E-mail:eessheng@163.com

analysis. Then this paper analyzes the deficiencies of the trusted computing, hierarchical protection, security situation awareness and other defense mechanisms being implemented in the power industry, and this paper points out the potential supply chain security threats in the security detection of software and hardware systems. Considering the difference of the risk levels and the harmful consequences caused by attacks on different power monitoring systems, the power system risk matrix is constructed from the aspect of the possibility of successful attack and the harmful consequences, and it is pointed out that the multi-target coordinated attack will increase the risk compared to the single-point attack. Finally, from the available resources of the state-supported cyber-attacks and the purpose of the attack, two high-risk potential cyber-attack damage modes are proposed, and the attack realization process and damage mechanism are summarized.

Key words: power system; network security; risk analysis; non-communication cooperation attack; state-sponsored cyberattacks

电力系统是现代社会的关键性基础设施，其安全稳定运行是国家安全、经济高质量发展、社会和谐稳定的重要保障[1-2]。在信息与通信技术深度融合的电力信息物理系统中(cyber physical system，CPS)，信息通信系统异常、大规模不确定对象的网络攻击以及内部人员违规操作引发电网运行控制可靠性降低已成为亟待解决的常态问题[3-4]。从信息侧实施的针对电力 CPS 的恶意网络攻击，可突破两侧防护措施造成信息系统监视功能闭锁和物理系统多点协同破坏失效，极易形成类似严重自然灾害的群发性故障，触发连锁故障大停电[5]。

自 2010 年震网病毒打破物理隔离工控系统不能被突破的思维定势以来，针对电力 CPS 的恶意定向网络攻击受到广泛的关注，国内外学者围绕其网络安全防护开展了大量研究[6-7]。针对具体的攻击形式和电力业务场景，改造和应用认证加密、准入管理、入侵检测和单向网闸等被动安防措施，构建了网络安全纵深防护体系。实际系统中，因真实发生过几次传感器和通信异常等原因导致数据出错而引发的事故，有大量研究集中于错误数据注入攻击的检测和防护[8-9]。传统电网信息安全被动防御依赖于已知安全威胁的统计学行为特征，难以有效检测并阻断全部恶意网络攻击，具有需大量部署防御设备和系统的特点，不但造成防御代价过高，而且影响电力信息物理系统的工作效率[10]。

针对上述被动防御的缺陷，近年来南方电网和国家电网公司相继开始在电力工控终端中应用基于专用芯片和实时工业控制系统的可信计算技术[11]，从系统软硬件底层(电路层、代码层)实现对未知恶意代码的容侵，将电力信息物理系统网络安防推向主动安全防护的新阶段。在此基础上也有研究学者将动态防御思想引入电力安防领域，通过改变系统各种资源配置，可减少攻击面，让攻击方难以发现目标甚至欺骗攻击方实施攻击，从而触发攻击告警[12-13]。动态防御可改变被动防御态势，真正实现对入侵攻击的主动防御。

尽管网络攻击、自然灾害和连锁故障导致大停电都被归结为小概率、高风险事件，但对它们的普遍认知存在显著差异。多年来自然灾害和连锁故障导致的大停电事故反复发生，尽管每次的肇因和发展蔓延过程具有较强的偶然性和随机性，但背后的致灾机理、破坏模式和事故发生概率基本上已为人熟知[14-15]。基于此，有学者将风险评估手段引入电力系统可靠运行与控制研究，根据风险评估结果采取相应的风险处理措施，将风险降低到可接受的水平范围[16]。但相对而言，从已发生的为数不多的利用电力 CPS 特性发动网络攻击造成电网事故的实际案例来看，网络攻击具有高度定制化、智能化特征，其攻击策略可随着目标对象的防护水平快速迭代演化，每次攻击均可能是新的形式，无法准确预测其入侵路径和破坏模式，难以运用风险评估手段对电力系统网络安全风险进行定量分析。

网络安全风险具有客观性，防护体系的短板决定系统应对风险的能力。本文认为，从风险分析的角度出发，准确识别网络安全风险来源和等级，在现有安防体系基础上，找出可能造成系统性风险的潜在安全漏洞，是有效管控网络安全风险的重要基础。由于网络攻防对抗是在一定资源条件下的对抗，攻击者所拥有的资源是决定防护难度的重要因素。特别在目前大国竞争的时代背景下，国家支持

型网络攻击打破了对于攻防双方可用资源的一些基本假设。因此，本文基于攻击方身份分析电力系统不同类型安全威胁的来源及其在攻击目标选择、破坏模式上的特点；然后分析目前正推行建设可信计算、等级保护和安全态势感知技术的缺陷，指出电力监控系统供应链攻击的安全威胁检测是当前需要加速研究的重点问题；最后从国家支持型网络攻击最大化攻击破坏后果角度出发，提出 2 种高危潜在网络攻击模式。

1　考虑攻击方身份的网络安全威胁分析

除风险管理手段外，也有学者运用博弈论进行网络对抗研究，博弈论的基本原则是参与者的博弈策略是否泄露很大程度上决定了对抗结果，但电力 CPS 涉及信息和物理 2 个方面，且部署了较为完备的安防措施，网络安全威胁如果不掌握电力系统的专业知识，大多难以造成重大威胁。从已发生的 2 次乌克兰电网网络安全事故来看，针对电力工控系统的网络攻击明显是在掌握目标对象的先验知识（安防措施和工作流程）的基础上，才能自动匹配通信协议，破坏监控系统可用性，精确导致多座变电站全停[17-18]。因此，实际系统中攻防双方处于敌暗我明、易攻难守的境地。

因网络攻击入侵破坏具有不确定性，准确完整识别风险源成为制定风险防御策略并快速恢复的关键。由于攻击者的身份往往决定了其可调用的资源、目标选择和破坏模式以及想要达成的目的[19-20]，本文从攻击方的视角对电力系统网络安全威胁进行风险分析，根据攻击方身份来推断可动用的资源，分析其想要达成的目的，从而推断出目标选择策略、渗透入侵模式以及攻击破化模式，为研制针对性的检测与防护方法提供指导。

1.1　国家支持型网络攻击

据 2019 年《纽约时报》披露，美国早在 2012 年就在俄罗斯电网中植入可随时发动攻击的恶意软件[21]。大国竞争时代背景下，随着全球网络空间军事化进程持续加速，国家支持的、面向基础设施的网络空间对抗已发展为现实威胁。作为关乎国家安全和国民经济命脉的关键基础设施，电力系统是国家支持型网络攻击定向打击的高价值目标[22-23]。实际系统中，已发生的以电力工业控制系统为目标的 Stuxnet、Black Energy、Industroyer 病毒多具有强烈的国家支持背景和政治目的。

国家支持网络攻击掌握丰富的攻击资源，为达成预设攻击破坏任务，可不计成本地针对目标对象跨领域组织专家量身研制定向攻击恶意软件。作为首个武器化的恶意软件，2010 年突破物理隔离的震网病毒就是典型的国家支持型网络攻击[24]。它基于对伊朗铀浓缩控制系统的先验知识，反复修改控制参数，成功破坏了上千台离心设备[25]。据美国安全公司 Symantec 分析报告指出，Stuxnet 病毒需 5 到 30 名计算机和控制领域专家进行长达 6 个月的研发，其攻击研发成本非一般机构组织或个人所能承担[26]。除具有高度定制化、智能化的特征外，为最大化攻击破坏后果，国家支持型网络攻击还可融合多种攻击手段对多个目标发动协同攻击。如 2015 年 Black Energy 就利用钓鱼邮件入侵、分布式拒绝服务攻击、破坏监控系统可用性等手段造成乌克兰电网 30 座变电站全停[27]。

网络攻防博弈中电网防护水平的提升会倒逼攻击方主动调整渗透入侵和攻击破坏模式。由于工作人员是电力信息物理系统正常运转的重要元素，国家支持型网络攻击可利用社会工程学原理，以内部人员政治立场和经济利益诉求（内部威胁）为攻击实施的突破点[28-29]。实际系统中，内部人员破坏电网稳定运行的案例已有一些报道，如 2019 年委内瑞拉大停电事故中，就发现被攻击的水电站存在被人为破坏的痕迹[30]。2001 年南京银山公司离职工程师就在其生产的变电站故障录波装置中植入可造成录功能闭锁的恶意代码[31]。

需要指出的是，国家支持型网络攻击的攻击手段、要达到的目的以及可能采取的攻击模式明显有别于一般恶意攻击行为。尽管中国电力系统已建立的基于物理隔离的边界安全纵深防御体系和大力推行的基于可信计算技术的防卫体系，使得电力系统在技术和管理上已具备抵御一般性安全威胁和具有有限资源的网络攻击，但并不足以完全应对国家支持型攻击。因此，需要着重考虑如何应对国家支持型网络攻击，并对其防护措施进行强化设计。

1.2　有组织网络攻击

与国家支持型网络攻击不同，有组织网络攻击

可在较丰富网络安全知识和目标系统有限先验知识的支撑下,仅为谋求经济利益而并非政治目的对目标系统进行攻击破坏,如 2021 年 5 月黑客组织 Dark Side 采用勒索软件对美国最大的燃油输送运营商 Colonial Pipeline 营销系统发起攻击,造成 17 个州进入紧急状态[32]。典型的有组织网络攻击场景主要分为以下三类。

1)电力交易市场竞价在半开放网络环境下开展,获取市场参与方的竞价数据可以推测利益相关方的竞价策略,进而谋求竞价中的不对称优势。

2)在比特币等可逃避身份追查的新型支付方式掩护下,以 Wannacry 为代表的勒索软件肆虐全球,先后于 2016 年 1 月和 2019 年 7 月感染破坏以色列和南非电力系统,其中后者攻击约翰内斯堡供电部门的网站和营销系统,使得电费充值和电费结算业务停摆,造成部分用户供电中断[33-34]。

3)除勒索攻击对象外,有组织网络攻击还可通过攻击破坏特定的电力装备,进而在股票市场上买空、卖空相关企业的股票牟利,在 2021 年美国燃油运营商 Colonial Pipeline 被攻击后,纽约交易所原油股票价格大幅上涨 4.3%。此外,在攻击控制目标系统后,也可控制被攻击对象挖矿获取比特币牟利。

可隐匿身份的暗网和基于比特币的利益分享机制,提供了有利于有组织网络攻击犯罪的匿名操作网络环境和利益变现渠道,是有组织网络攻击的温床[35-36]。在暗网的支持下,以牟利为目的的有组织攻击明显地加速了网络安全漏洞利用工具传播使用的速度和范围。随着网络攻击技术的快速迭代和渗透,目前有组织攻击也具有很强的针对特定对象的选择性攻击能力。当他们掌握类似“Wannacry”的高等级网络攻击武器时,有可能在隐匿身份的庇护下选择性攻击电力行业用户,造成攻击破坏后果。

1.3 无特定目标网络攻击与随机失效

因特网中充斥着各类恶意软件,其中绝大部分是不以电力系统为设定攻击目标的病毒软件。中国电力行业高度重视网络安全防护,生产用计算机均只能链接物理隔离的电力系统内网;除使用优盘认证等措施实现访问控制外,还基于白名单机制提高安全屏障;在生产用计算机中强制进行病毒和木马扫描安全防护,足以应对一般性无特定目标的网络攻击行为[37-38]。此外,电力信息物理系统具有复杂的耦合关系,缺乏专业知识的恶意软件即便侵入内网,也只可能采用阻塞通信或格式化系统,造成信息系统失效或者功能闭锁,此时系统退至就地保护阶段,不会直接造成系统误动。由于此类攻击行为会有显著的通信流量异常,容易被已部署的基于流量异常的入侵检测或异常检测系统捕获而暴露,造成的破坏后果相对有限。

除网络攻击外,信息系统的随机失效和异常,包括通信系统异常、安全设备异常和业务设备异常,也会对电力系统造成影响,文献[38]对此进行了详细表述,本文不再赘余。

2 电力系统安全防护机制与缺陷分析

近年来,为强化网络安全防护能力,中国电力行业依据国家发改委、能源局相继出台的 14 号令和 36 号文,新增安全接入区,深化落实边界安全防护;细化等级保护对象,扩大等级保护的覆盖范围;开始在生产控制区部署网络安全态势感知系统,大力推行可信计算技术等主动安全防护措施的工程应用[39-40]。从防护角度来看,中国电力系统现有安防体系已比较完善,但攻击方在目的利益的驱动下总会不断寻找、挖掘和尝试每一个可能的突破点。特别是具有深厚技术能力和专业知识的国家支持型网络攻击发展为现实威胁,使得攻防双方的不平等地位更倾向于攻击方。由于目标对象的脆弱性是攻击者能够达成攻击目标的重要条件,以下结合具体业务场景分析新增安全防护措施的缺陷。

2.1 可信计算

为应对未知安全威胁,中国构筑的基于可信计算技术的防护体系将电力系统网络安防推入主动安防新阶段。大面积应用的国产 D5000 调度系统采用国产的服务器、工作站、网络设备和操作系统,能有效检出和扼杀未经认证的程序或进程[41]。近年来,国家电网和南方电网还联合芯片设计企业和电力设备制造厂商,基于可信计算、加密认证和访问控制等技术研发了微网控制器、充电桩和计量表计等配用电终端芯片,能显著提高终端安全防护能力。作为一种同时实现计算和网络安全防护的计

算机技术，虽可显著提高入侵攻击门槛，但也有其阿喀琉斯之踵，主要表现在以下方面。

1）支撑可信计算的软、硬件系统自身安全漏洞。可信计算通过构建逐级认证和信任的可信链来营造相对可信的网络环境和边界，但难以避免承载其技术实现的软、硬件系统自身的安全威胁[42]。目前可信终端设备制造厂商普遍仅考虑终端的功能性，缺少在芯片和其他固件研制过程中，对底层开发平台、硬件木马、第三方负责的功能模块投毒行为的有效筛查手段。除终端外，配电自动化等系统均基于通用嵌入式系统裁剪优化后进行业务功能的开发，不仅系统本身就存在未知漏洞，还受其补丁或安全软件兼容性问题影响，漏洞将长期存在[43-44]。实际系统中攻击者利用目标系统固件漏洞进行破坏的案例已有一些报道。

2）错误数据注入攻击。目前国内外计算机厂商基于国密算法芯片作为可信计算信任链的初试起点，能较好地解决配电终端传输数据的机密性、完整性和其身份认证[45]，但不能保证接收的数据及通信对象的身份是否可信完整，易受到错误数据注入攻击威胁。电动汽车用户通过无线通信与充电站管理控制系统进行双向数据交换，实现对充电过程的监控与管理，并利用车位部署的智能终端执行用户指令，攻击者可使用合法用户的身份向其注入恶意控制命令或发送大量的充电请求造成充电网点功能闭锁，国家支持型网络攻击还可在突破充电站的防护设施后，直接转而控制大量用户终端，破坏充电汽车的有序充电，影响供电电能质量，破坏配电网的功率平衡。

3）合法认证程序的安全性。可信计算只能保证运行的是通过认证的合法程序，但无法确定其中是否含有恶意代码。基于 0day 漏洞的恶意代码和含有逻辑炸弹的可执行程序，可通过合法程序认证，对目标对象进行渗透破坏。此外可信程序的安全性主要取于认证所用的加密算法安全性[46]，而认证算法安全性取决其数学复杂度。尽管主流的加密算法如 MD5 和 RSA 难以对其进行破解，但对于拥有丰富资源的国家支持型攻击方来说也并非一定无法破解，破解了加密算法也就突破了可信计算的安全防护屏障。如震网病毒就盗取 RealTek 和 JMicron 公司合法产品身份签名，冒充为打印机升级包进行传播扩散[47]。

2.2　等级保护

电力信息系统等保测评机制根据等级保护对象遭到破坏、功能闭锁或数据篡改（包括丢失、泄露、损毁）后对电网整体的侵害程度和受侵害的客体（电网、社会、国家）2 个方面来协同衡量的[48-49]。根据保护等级划分来分配防护资源，以此来确定电力监控系统的相应等级防护措施和防护水平。电力系统中，能量管理系统（energy management system，EMS）对电网的控制运行、决策制定和能量传输起着重要支撑作用，省级 EMS 遭到攻击破坏将严重影响国家安全，对电力行业和公众利益造成特别严重危害。因此，现行规范将其定为第 4 级安全保护等级，要求在统一的安全策略下防护系统能够抵御拥有丰富资源的威胁源发起的恶意攻击、较为严重的自然灾害、以及其他相当程度的威胁所造成的主要资源损害，并能够发现安全漏洞与安全事件，在系统遭到损害后能迅速恢复所有功能。相比于 EMS，220 kV 以上变电站自动化系统（含开关站、换流站、集控站）遭到破坏时危害仅在局部范围内传播，因此现行规范将其定第 3 级安全保护等级，降低了安全防护能力要求。

需要指出的是，这种等级划分评判方法割裂看待电力监控系统遭攻击破坏的后果，没有考虑通过业务流程耦合的风险，存在一定缺陷。如特高压变电站/换流站遭攻击跳闸全停/双极闭锁时，可能造成受端和送端省级电网的大幅动荡，配置的安稳控制预案可能造成大量切机切负荷，危害后果可能达到甚至超过省级 EMS。此外现行等保规范主要针对电力监控系统，尽管最新等保要求中增加对云计算、物联网、移动互联安全的扩展[50]，但新型电力系统和数字化电力系统的发展会引发大量新的业务形态，也会改变脆弱性的来源，需要结合实际业务场景和业务流程展开分析，细化等保粒度，扩大等保对象范围，完善防护资源分配机制，提高应对网络安全风险的能力。

2.3　网络安全态势感知

随着电力市场化改革与能源转型的推进，计量自动化系统支撑的业务功能增加，其遭到攻击破坏

将显著扩大故障异常的影响[51]。为强化其安防水平,国内外电力企业增设终端安全接入区,部署入侵检测系统、防病毒系统和 DB-AUDIT 等安全工具,但各种安全设备数据与威胁检测功能独立,因缺乏协同配合而造成误报、漏报率高,难以检测高级持续性安全威胁。近年来,为了解决上述问题,国家电网公司和南方电网公司开始应用网络安全态势感知技术,在安全接入区、安全Ⅰ区、安全Ⅱ区分别部署感知探针,通过采集提取各区的网络设备、主机设备及其网络设备的安全日志、网络流量、设备配置信息等多源数据,基于建立的安全态势评估指标,从宏观上对电网整体的安全态势进行多元数据融合评估,以此来预测未来运行轨迹和安全趋势预警,为安全管理人员合理有效进行响应提供决策支撑。美国国防高级研究计划局(DARPA)也基于态势感知技术提出了基于攻击检测的故障隔离和系统快速恢复的运行技术,以此提高电力系统的韧性[52]。

现有关于网络安全态势感知的研究主要分为权重估计、概率统计和人工智能等 3 大类。其中,基于权重估计的安全态势评估方法依赖于专家经验进行权重分配,其算法往往简单,难以适应噪声掩盖下高技术手段的攻防对抗需要[53-54];基于大数据人工智能算法如神经网络、聚类分析等[55-56],和基于概率估计的安全态势评估算法,可将不相关的数据进行关联融合和挖掘分析,但其本身依赖于数理统计方法,给出的判断概率性占比大,缺乏机理性的解释,往往带来较高的误报率和漏报率[57-58]。还有研究将基于流量异常检测的入侵检测系统用作网络安全态势感知的输入,来实现对异常行为的有效检测[59],但熟悉目标系统防护措施的国家支持型网络攻击可经过供应链渠道渗透入侵,破坏过程可采用不表现出明显流量异常的无通信方式,此时该方法将呈现高漏报率。因此,未来电力系统网络安全态势感知应结合实际业务场景强化机理性研究基础,着重考虑如何提高对高隐蔽性国家支持型网络攻击的检测成功率。

2.4 供应链安全检测

除利用 0day 漏洞或利用机器学习技术躲过安全威胁检测经厂商运维渠道实施攻击入侵外[60],还可从供应链渠道在设备厂商环节直接植入定向攻击恶意软件。文献[61]强调电力系统安全防护应着重考虑针对基础软硬件系统的供应链攻击。据安全公司 Symantec 数据统计,2019 年全球供应链攻击安全事件增加 78%,而这一趋势还将持续增加[62]。2020 年黑客组织渗透入侵网络安全服务商 SolarWinds,向其网络安全产品注入恶意代码,并通过供应链入侵了其服务的覆盖军工、能源等涉及国家安全的近两万个行业用户[63]。为保障电力系统安全可靠运行,亟待研究应对此类攻击的防护手段。

针对上述问题,2018 年国家能源局发布 36 号文,要求监控设备部署前必须经过代码审计和入网测试,但代码审计只能保证设备厂商自研部分的安全性,缺少对业务功能开发时引入的插件、第三方功能模块的安全管控和有效审查。尽管实际系统中电力监控系统的业务功能开发,均在开源环境下进行,但其安全性主要依赖于社区同行的互相信任,实际上难以杜绝恶意代码的上传,如 2020 年明尼苏达州立大学教授故意向 Linux 内核提交含漏洞的补丁代码来研究测试开源社区的安全性[64]。近年来在电力物联网终端边缘计算 Docker 容器技术官方仓库中也发现植入比特币挖矿恶意软件的镜像程序,相关系统已被下载 2 000 万次[65]。入网测试设置的项目较为简单,主要测试设备是否正常收发数据和报文,是否拒动、误动等。通过设置恶意攻击的启动逻辑即可逃避此类攻击。因此,很难有效检测出在设备供应链环节以逻辑炸弹形式植入的高隐蔽性定向攻击恶意软件。

理论上,不仅各级电力监控系统存在供应链威胁,广泛分布分散的电力终端也可成为供应链攻击的载体。由于系统的复杂性,技术上难以清查从供应链发动的攻击。近年来 DARPA 提出将新一代人工智能技术引入软、硬件系统漏洞挖掘,为后续研究提供了一种选择[66]。由于逻辑炸弹具有特定逻辑触发的特点,作者认为可利用植入逻辑炸弹所要达成的目的来反向设计针对性的检测识别方法。

3 网络攻击的风险分级与风险跃迁

为增强电力信息系统整体安全性,中国电力企

业根据等级保护要求，确定电力工控系统（主要包括电力监控系统和电力信息管理系统两部分）安全等级，并根据等级划分结果差异化分配防御资源、施加防护措施。因此，递减或递增变化的防护水平将导致目标对象被网络攻击突破的可能性呈现递增或递减趋势。反之，掌握不同资源的网络攻击对电网的危害程度也具有显著差异性。为合理刻画上述两种关系，本文采用风险矩阵法，从被成功攻击的可能性和单个系统遭攻击的破坏性后果这两个维度，对网络攻击行为进行风险分级。构建的风险矩阵如图 1 所示。其中横轴表示系统遭攻击的可能性，纵轴表示破坏后果对电网的侵害程度。由于网络攻击具有不确定性、多样性，分类界限不明显，难以准确量化某种具体攻击的破坏后果，文中将成功攻击的可能性、目标对象被突破后对电网造成的攻击破坏后果大致分为 5 个等级，对应的风险划分也相应地分为 5 个级别。

由于省级 EMS（具有 SCADA、AGC、AVC 等控制功能）和安稳控制系统直接向电网提供全方位监视与控制、调度决策、经济运行等重要功能，一旦遭到破坏将严重威胁国家安全，是国家支持型网络攻击破坏的首选目标。因此围绕其部署的防护手段最为周全，被成功攻击的可能性小；中小容量电厂和中低电压等级变电站数量较多且分散分布，在系统 N-1 安全校核原则的约束下，单个厂站遭攻击破坏对整个电网的影响程度有限，配置的防护手段相对简单且不一定能够严格落实，被攻击可能性较大。相比之下，大容量的电厂在电网中承担调峰、调频作用，特高压变电站/换流站及枢纽变电站是现代电网的核心骨干网络，防护水平仅次于 EMS，被攻击的可能性较小。散布于用户侧的电表和充电桩等终端设备数量庞大，单个终端失效几乎不对电网造成影响，分配的防护资源也少，因此遭攻击的可能性大。从数量上来说，实际系统的地市级配电自动化系统处于大容量和小容量厂站的中间位置，因此获得的防护资源处于两者之间的中等水平，即被攻击的可能性为中等层次。

从攻击方角度来看，国家支持型网络攻击为达成最大化攻击破坏后果可采用多种攻击手段对多个目标系统发起协同攻击。相比于对单个目标对象的发起攻击，针对多个目标对象的协同攻击破坏效果更大，在风险矩阵中表现出风险跃迁现象。近年来，国内外学者也开展了关于协同攻击研究。文献[67]证明了多点协同可能造成更大规模的隐秘级联事故，比单点攻击具有更大的自由度；文献[68]研究了多个变电站组合攻击情形下的负荷损失；文献[69]通过实验仿真表明多个变电站比单个变电站遭攻击破坏对电网功率、相角、电压和频率的扰动影响更大。相比于 2016 年 Industroyer 病毒攻击乌克兰电网造成 1 座 220 kV 变电站全停，2015 年 Black Energy 病毒导致 30 座变电站的协同关停的危害风险明显更大。在协同攻击下，即便是危害

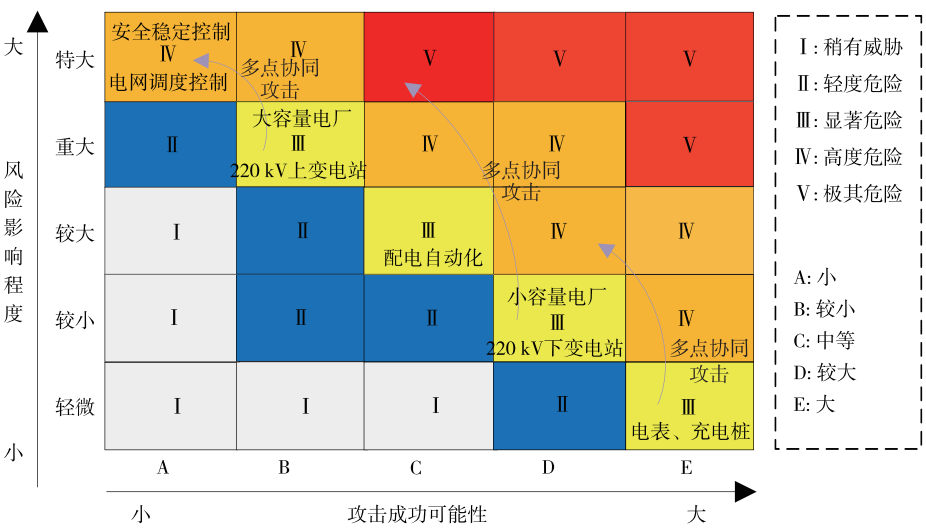

图 1　风险矩阵迁移

Figure 1　Risk matrix and migration of risk level

后果很小的电表终端设备被大规模恶意控制产生的后果叠加也会产生风险跃迁现象，文献[70]就研究了大规模可控终端在三种恶意攻击下对配电网电能质量的影响。

综上所述，强化电力系统网络安防能力，除提高核心节点安防能力外，还应对国家支持型网络攻击借助多点协同攻击实现风险跃迁攻击模式研究针对性的检测与防御方法。

4 高危潜在网络协同攻击模式

作为电能传输的关键基础设施，变电站是电力系统网络攻防对抗的重要场所[71]。由于中国电力系统已部署了较完善的纵深防御体系，加强变电站网络安防应着重考虑国家支持型网络攻击。

针对变电站的恶意软件渗透入侵后可能有多种攻击破坏模式。在不掌握电力系统背景知识的条件下，可采用拒绝服务攻击、格式化或锁定系统等暴力破坏模式，并不会直接触发电网安全事故[72]。调度中心 EMS 错误数据检测机制和业务系统防误设计也可杜绝虚假数据注入攻击造成广域保护系统的误动。从 Stuxnet、BlackEnergy、Industroyer 病毒攻击破坏模式来看，国家支持型网络攻击更多的是获取控制权限后，基于先验知识进行旁路控制[3]。

变电站自动化系统采用变电站描述语言生成不包含电压等级、断路器通信控制地址、网络通信拓扑等参数的变电站配置描述标准化文件[73]。攻击方基于变电站先验知识定向研制恶意软件，可经供应链渠道侵入生产控制区，在获取到控制权限后按规则读取配置文件，解析获取站内所有断路器通信控制信息。然后检测系统运行环境是否满足预设攻击启动逻辑条件，在不满足逻辑条件时，只进行潜伏记录系统运行环境，并不会主动发动攻击；一旦检测到逻辑条件满足时，旁路控制跳开站内全部断路器，造成变电站全停事故。攻击乌克兰电网的 Industroyer 病毒就利用时间逻辑条件，在 2016 年 12 月 17 日 22 点整自动匹配四种通用变电站通信协议跳开一座 220 kV 传输级变电站内全部断路器[74]。

基于逻辑条件发动攻击的恶意代码也称为逻辑炸弹。目前，在工控系统中植入逻辑炸弹的案例已有一些报道。2001 年，南京银山公司的离职工程师在其生产的故障录波装置中植入时间逻辑炸弹，于当年 10 月 1 日 0 点造成全国 147 座变电站录波功能闭锁[75]。随着对攻防对抗的研究不断深入，也有学者开展了在电网频率控制中利用逻辑炸弹进行攻击破坏的研究[76-77]。

对于国家支持型网络攻击而言，渗透入侵变电站并发起旁路控制跳闸攻击只是达成目标的技术手段，最大化攻击破化后果才是最终目标。由于现代互联电网遵循 N-1 安全校核原则，单个变电站退出运行会造成严重的负荷损失，但并不足以为危及整个电网的安全。从攻击方视角来看，模仿 BlackEnergy 攻击破坏模式，同时对多个变电站发动攻击，造成多个变电站同步关停以触发大停电事故，是最大化攻击后果的有效手段。

智能变电站采用单向网闸对生产控制大区和管理大区进行物理隔离。站内配置入侵检测、准入控制和基于流量异常等规则检测网络异常行为。近年来还布设了安全态势感知系统，类似 BlackEnergy 远程遥控跳闸模式难以奏效。尽管可以基于先验知识研制定向攻击恶意软件，在获得断路器控制信息后发起攻击，但若与站外通信进行攻击协同，难以达成攻击目的。因此，为避免提前暴露，我们认为恶意软件可能采用无通信方式进行多个变电站的攻击协同，并有如下两种无通信协同破坏模式。

4.1 无通信时间同步协同攻击

现代电力系统中，为准确记录电网故障时继电保护时序和精确动作时间，调度与变电站已普遍配置基于北斗和 GPS 的电力时间同步装置，并通过 IEEE 1588 协议对厂站内部设备进行统一授时，实现对站内事件序列打印精准的全球同步时间标签[78]。定向研制的恶意软件可将各变电站的同步时间用作无通信的协同机制，潜入变电站后等待系统时钟到达预设时间再跳开站内全部断路器。当攻击方将入侵多个变电站的恶意软件的攻击时间逻辑设置为相同时，将在同一时间按照站内断路器控制流程跳开站内全部断路器，实现多个变电站在

同一时间无通信协同停运，极易触发大停电。其破坏模式示意图如图 2 所示，若侵入 3、4、5 变电站的含时间同步逻辑的恶意软件设定的攻击时间逻辑相同，当系统时钟满足预设攻击时间逻辑时，此 3 个变电站站内全部断路器将被同时跳开，造成 3 个变电站全停并退出运行。

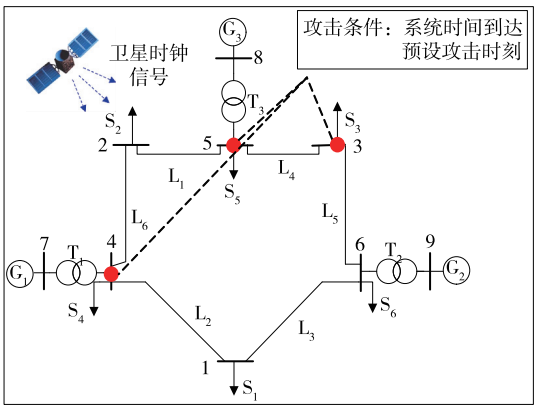

图 2　无通信时间协同攻击

Figure 2　Non-communication time cooperation attack

4.2　无通信扰动同步协同攻击

电网发生故障时，整个电网的频率及故障点附近变电站的母线电压将因受到冲击作用而波动。定向研制的恶意软件也可将故障时的扰动特征（电气量波动）用作无通信协同机制；根据监控主机运行状态实时数据（电压或频率）判定电网运行状态；在检测到变电站母线电气量（电压或频率）数值波动变化达到预设的攻击扰动逻辑时，根据站内断路器控制流程跳开站内全部断路器，造成全停失压事故。

变电站失压全停时也将造成相邻变电站电气量的大幅波动，并将触发其他变电站中的扰动协同攻击恶意软件，从而实现多站点的无通信扰动协同攻击。其攻击破坏模式示意如图 3 所示，以短路故障时低电压作为同步条件，假定入侵 1、2、5、6 号变电站的含扰动同步逻辑的恶意软件设定的电压攻击阈值为 0.8 p.u.。线路 L3 发生短路故障时，其附近变电站母线电压受到冲击而开始跌落，恶意软件检测到母线电压小于 0.8pu 时跳开所在变电站的全部断路器，造成两座变电站全停；在此过程中如将 2 号和 5 号变电站的母线电压拉低到阈值以下，又将触发其中的恶意软件进行跳闸攻击，从而借助扰动同步机制达成对多变电站的无通信攻击协同。

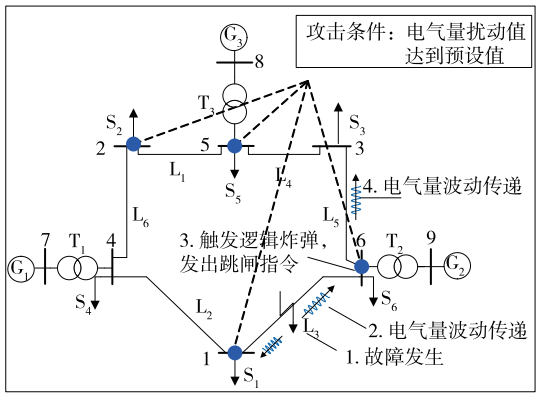

图 3　无通信扰动协同攻击

Figure 3　Non-communication disturbance coordination attack

5　结语

本文将电力系统面临来自不同层面的网络安全威胁按其身份和目的分成三类，分析了现有电力系统网络安全防护缺陷，从国家支持型网络攻击最终目标的角度，提出了 2 种高危害的潜在网络攻击破坏模式。得出如下结论：

1）中国电力系统高度重视网络安全防护，现有安防体系可以应对一般性的网络攻击。但随着网络空间对抗呈现主体国家化、手段武器化，具有丰富资源的国家支持型攻击可通过供应链攻击、0day 漏洞等多种非法手段绕过电力系统现有防护机制展开攻击破坏，电力系统网络安全防护应着重考虑此类攻击。

2）不同的电力监控系统遭攻击后造成的破坏性后果大小有显著差异。对多个目标系统的协同攻击可以造成风险跃迁，显著放大攻击破坏后果。

3）国家支持型攻击可以采用无通信时间同步协同攻击或无通信扰动同步协同攻击躲避安防系统安全检测，通过协同攻击多个厂站造成大停电事故。针对文中提出两种无通信协同攻击方法，作者认为可基于其攻击破坏特性（逻辑炸弹攻击特性）和破除协同机制的角度反向设计针对性的检测方法，提高电力系统应对此类攻击的能力。

参考文献：

[1] 王子骏，刘杨，鲍远义，等.电力系统安全仿真技术：工程

安全、网络安全与信息物理综合安全[J].中国科学:信息科学,2022,52(3):399-429.

WANG Zijun,LIU Yang,BAO Yuanyi,et al.Power system security simulation technologies:engineering safety,network security and cyber-physical integrated security[J].Science in China(Information Sciences),2022,52(3):399-429.

[2] 秦博雅,刘东.电网信息物理系统分析与控制的研究进展与展望[J].中国电机工程学报,2020,40(18):5816-5827.

QIN Boya,LIU Dong.Research progress and prospects of analysis and control of cyber-physical system power grid[J].Proceedings of the CSEE,2020,40(18):5816-5827.

[3] 李田,苏盛,杨洪明,等.电力信息物理系统的攻击行为与安全防护[J].电力系统自动化,2017,41(22):162-167.

LI Tian,SU Sheng,YANG Hongming,et al.Attacks and cyber security defense in cyber-physical power system[J].Automation of Electric Power Systems,2017,41(22):162-167.

[4] DENG R,ZHUANG P,LIANG H.CCPA:Coordinated cyber-physical attacks and countermeasures in smart grid[J].IEEE Transactions on Smart Grid,2017,8(5):2420-2430.

[5] LIAO W,SALINAS S,LI M,et al.Cascading failure attacks in the power system:a stochastic game perspective[J].IEEE Internet of Things Journal,2017,4(6):2247-2259.

[6] CHEN L,YUE D,DOU C X,et al.Study on attack paths of cyber attack in cyber-physical power systems[J].IET Generation Transmission & Distribution,2020,14(12):2352-2360.

[7] ZHANG H,LIU B,WU H.Smart grid cyber-physical attack and defense:a review[J].IEEE Access,2021,9:29641-29659.

[8] MUSLEH A S,CHEN G,DONG Z Y.A survey on the detection algorithms for false data injection attacks in smart grids[J].IEEE Transactions on Smart Grid,2019,11(3):2218-2234.

[9] 王琦,邰伟,汤奕,等.面向电力信息物理系统的虚假数据注入攻击研究综述[J].自动化学报,2019,45(1):72-83.

WANG Qi,TAI Wei,TANG Yi,et al.Summary of research on false data injection attacks for power cyber-physical systems[J].Acta Automatica Sinica,2019,45(1):72-83.

[10] SUN C C,HAHN A,LIU C C.Cyber security of a power grid:state-of-the-art[J].International Journal of Electrical Power & Energy Systems,2018,99:45-56.

[11] 张涛,赵东艳,薛峰,等.电力系统智能终端信息安全防护技术研究框架[J].电力系统自动化,2019,43(19):1-8+67.

ZHANG Tao,ZHAO Dongyan,XUE Feng,et al.Research framework of cyber-security protection technologies for smart terminals in power system[J].Automation of Electric Power Systems,2019,43(19):1-8+67.

[12] MO H,SANSAVINI G.Dynamic defense resource allocation for minimizing unsupplied demand in cyber-physical systems against uncertain attacks[J].IEEE Transactions on Reliability,2017,66(4):1253-1265.

[13] 计丽妍,李存斌,贾雪枫,等.多证据融合下电力信息物理系统风险评估研究[J].智慧电力,2021,49(10):23-29.

JI Liyan,LI Cunbin,JIA Xuefeng,et al.Risk assessment of cyber-physical power system based on multi-evidence fusion[J].Smart Power,2021,49(10):23-29.

[14] YAN J,HU B,XIE K,et al.Data-driven transmission defense planning against extreme weather events[J].IEEE Transactions on Smart Grid,2020,11(3):2257-2270.

[15] 刘天浩,朱元振,孙润稼,等.极端自然灾害下电力信息物理系统韧性增强策略[J].电力系统自动化,2021,45(3):40-48.

LIU Tianhao,ZHU Yuanzhen,SUN Runjia,et al.Resilience-enhanced strategy for cyber-physical power system under extreme natural disasters[J].Automation of Electric Power Systems,2021,45(3):40-48.

[16] LIU X,SHAHIDEHPOUR M,CAO Y,et al.Risk assessment in extreme events considering the reliability of protection systems[J].IEEE Transactions on Smart Grid,2015,6(2):1073-1081.

[17] 郭庆来,辛蜀骏,王剑辉,等.由乌克兰停电事件看信息能源系统综合安全评估[J].电力系统自动化,2016,40(5):145-147.

GUO Qinglai,XIN Shujun,WANG Jianhui,et al.By the Ukrainian blackout incident to see the information energy system integrated security assessment[J].Au-

tomation of Electric Power Systems，2016，40(5)：145-147.

[18] 刘烃，田决，王稼舟，等.信息物理融合系统综合安全威胁与防御研究[J].自动化学报，2019，45(1)：5-24.
LIU Ting，TIAN Jue，WANG Jiazhou，et al. Integrated security threats and defense of cyber-physical systems [J]. Acta Automatica Sinica，2019，45(1)：5-24.

[19] PARKER D B. Fighting computer crime：a new framework for protecting information [M]. John Wiley & Sons，Inc，1998：70-88.

[20] 朱海鹏，赵磊，秦昆，等.基于大数据分析的电力监控网络安全主动防护策略研究[J].电测与仪表，2020，57(21)：133-139.
ZHU Haipeng，ZHAO Lei，QIN Kun，et al. Active protection strategy of power monitoring network security based on big data analysis[J]. Electrical Measurement & Instrumentation，2020，57(21)：133-139.

[21] SANGER D E，PERLROTH N. US escalates online attacks on Russia's power grid[EB/OL]. https://www.nytimes. com/2019/06/15/us/politics/trump-cyber-russia-grid.html，2021-04-26.

[22] SAMAMTHA F，Ravich，FIXLER Annie. The economic dimension of great-power competition and the role of cyber as a key strategic weapon [EB/OL]. https://www. heritage. org/military- strength/topical-essays/the-economic-dimension-great-power-competition-and-the-role，2021-04-26.

[23] BEY M. Great powers in cyberspace：the strategic drivers behind US，Chinese and Russian competition[J]. The Cyber Defense Review，2018，3(3)：31-36.

[24] FARWELL J P，ROHOZINSKI R. Stuxnet and the future of cyber war[J]. Survival，2011，53(1)：23-40.

[25] 谢清玉，张耀坤，李经纬.面向智能电网的电力大数据关键技术应用[J].电网与清洁能源，2021，37(12)：39-46.
XIE Qingyu，ZHANG Yaokun，LI Jingwei. Application of key technologies of power big data in smart grids [J]. Power System and Clean Energy，2021，37(12)：39-46.

[26] FALLIERE N，MURCHU L O，CHIN E. W32. stuxnet dossier[J]. White Paper，Symantec Corp，SecurityResponse，2011，5(6)：29.

[27] LEE R M，ASSANTE M J，CONWAY T. Analysis of the cyber-attack on the Ukrainian power grid [EB/OL]. https://ics. sans. org/media/E-ISAC_SANS_Ukraine_DUC_5.pdf，2016-03-18.

[28] 刘念，余星火，王剑辉，等.泛在物联的配用电优化运行：信息物理社会系统的视角[J].电力系统自动化，2020，44(1)：1-12.
LIU Nian，YU Xinghuo，WANG Jianhui，et al. Optimal operation of Power distribution and consumption system based on ubiquitous internet of things：a cyber-physical-social system perspective[J]. Automation of Electric Power Systems，2020，44(1)：1-12.

[29] XUE Y，YU X. Beyondsmart grid-cyber-physical-social system in energy future[J]. Proceedings of the IEEE，2017，105(12)：2290-2292.

[30] POZZEBON S，BRITTON B. Huge power outage leaves most of Venezuela in darkness[EB/OL]. https://edition.cnn.com/2019/03/08/americas/venezuela-black-out-power-intl /index.html，2021-04-21.

[31] 布雨."逻辑炸弹"炸毁科技功臣[J].中国高新区，2002，9(2)：39-40.
BU Yu. Logic bomb blows up the hero of science and technology [J]. China High-tech Zone，2002，9(2)：39-40.

[32] RUSSON M A. US fuel pipeline hackers 'didn't mean to create problems'[EB/OL]. https://www. bbc. com/news/business-57050690，2021-05-24.

[33] DAVID R B. After ransomware attack，focus turns to backup and prevention services[EB/OL]. https://www. timesofisrael. com/after-ransomware-attack-focus-turns-to-backup-and-prevention-services/，2021-05-24.

[34] AKWEI I. Africa least hit by WannaCry ransomware cyber-attack[EB/OL]. https://www. africanews. com/2017/05/15/africa-least-hit-by-wannacry-ransomware-cyber-attack/，2021-05-24.

[35] WEIMANN G. Terrorist migration to the dark web [J]. Perspectives on Terrorism，2016，10(3)：40-44.

[36] GEHL R W. Power/freedom on the dark web：a digital ethnography of the dark web social network[J]. New Media & Society，2016，18(7)：1219-1235.

[37] 陈武晖，陈文淦，薛安成.面向协同信息攻击的物理电力系统安全风险评估与防御资源分配[J].电网技术，2019，43(7)：2353-2360.
CHEN Wuhui，CHEN Wengan，XUE Ancheng. Physical power system security risk assessment and defense

resource allocation for coordinated information attacks [J]. Power System Technology, 2019, 43(7): 2353-2360.

[38] 苏盛,吴长江,马钧,等.基于攻击方视角的电力 CPS 网络攻击模式分析[J].电网技术,2014,38(11):3115-3120.
SU Sheng, WU Changjiang, MA Jun, et al. Analysis of the attack mode of the electric power CPS network based on the attacker's perspective[J]. Power System Technology, 2014, 38(11): 3115-3120.

[39] 倪伟东,武利会,王俊丰.基于自主安全芯片的配网自动化系统网络安全防护及硬件加速[J].电力科学与技术学报,2020,35(3):166-172.
NI Weidong, WU Lihui, WANG Junfeng. Cybersecurity protection and hardware acceleration of distribution automation system based on autonomous security chip [J]. Journal of Electric Power Science and Technology, 2020, 35(3): 166-172.

[40] 高昆仑,王志皓,安宁钰,等.基于可信计算技术构建电力监测控制系统网络安全免疫系统[J].工程科学与技术,2017,49(2):28-35.
GAO Kunlun, WANG Zhihao, AN Ningyu, et al. Building a network security and immune system for power monitoring and control system based on trusted computing technology[J]. Engineering Science and Technology, 2017, 49(2): 28-35.

[41] 亢超群,李二霞,李玉凌,等.新一代配电主站主动防御架构设计方法[J].电力信息与通信技术,2021,19(3):65-73.
KANG Chaoqun, LI Erxia, LI Yuling, et al. A new generation of active defense architecture design method for distribution master stations[J]. Electric Power Information and Communication Technology, 2021, 19(3): 65-73.

[42] 彭安妮,周威,贾岩,等.物联网操作系统安全研究综述[J].通信学报,2018,39(3):22-34.
PENG Anni, ZHOU Wei, JIA Yan, et al. Survey of the internet of things operating system security[J]. Journal on Communications, 2018, 39(3): 22-34.

[43] 王宇,李俊娥,周亮,等.针对嵌入式终端安全威胁的电力工控系统自愈体系[J].电网技术,2020,44(9):3582-3594.
WANG Yu, LI Jun'e, ZHOU Liang, et al. A self-healing architecture for power industrial control systems against security threats to embedded terminals[J]. Power System Technology, 2020, 44(9): 3582-3594.

[44] 张焕国,韩文报,来学嘉,等.网络空间安全综述[J].中国科学:信息科学,2016,46(2):125-164.
ZHANG Huanguo, HAN Wenbao, LAI Xuejia, et al. Survey on cyberspace security [J]. Science in China(Information Sciences), 2016, 46(2): 125-164.

[45] 苏盛,汪干,刘亮,等.电力物联网终端安全防护研究综述[J].高电压技术,2022,48(2):513-525.
SU Sheng, WANG Gan, LIU Liang, et al. A review of research on terminal security protection for power internet of things[J]. High voltage technology, 2022, 48(2): 513-525.

[46] OPPLIGER R, RYTZ R. Does trusted computing remedy computer security problems[J]. IEEE Security & Privacy, 2005, 3(2): 16-19.

[47] 李志强,苏盛,曾祥君,等.基于虚构诱骗陷阱的电力调度系统针对性攻击主动安全防护[J].电力系统自动化,2016,40(17):106-112.
LI Zhiqiang, SU Sheng, ZENG Xiangjun, et al. Fabricated traps based active cyber security defense against targeted cyber-attack in electric power dispatching systems[J]. Automation of Electric Power Systems, 2016, 40(17): 106-112.

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

[49] GB/T 25070—2019.信息安全技术网络安全等级保护安全设计技术要求[S].

[50] GB/T 22240—2020.信息安全技术网络安全等级保护定级指南[S].

[51] 钱斌,蔡梓文,肖勇,等.基于模糊推理的计量自动化系统网络安全态势感知[J].南方电网技术,2019,13(2):51-58.
QIAN Bin, CAI Ziwen, XIAO Yong, et al. Network security situation awareness of metering automation system based on fuzzy inference[J]. Southern Power Grid Technology, 2019, 13(2): 51-58.

[52] BRAD D W. DARPA's rapid power grid restoration tech goes live[EB/OL]. https://breakingdefense.com/2021/03/darpas-rapid-power-grid-restoration-tech-goes-live/, 2021-05-24.

[53] 刘权莹,李俊娥,倪明,等.电网信息物理系统态势感知:现状与研究构想[J].电力系统自动化,2019,43(19):9-21.

LIU Quanying, LI Jun'e, NI Ming, et al. Situation awareness of grid cyber-physical system: current situation and research ideas[J]. Automation of Electric Power Systems, 2019, 43(19): 9-21.

[54] 陈秀真，郑庆华，管晓宏，等.层次化网络安全威胁态势量化评估方法[J].软件学报，2006，17(4)：885-897.
CHEN Xiuzhen, ZHENG Qinghua, GUAN Xiaohong, et al. Hierarchical network security threat situation quantitative assessment method[J]. Journal of Software, 2006, 17(4): 885-897.

[55] 吴海涛，代尚林，乔中伟，等.基于 RBF-SVM 智能配变终端的网络安全态势评估[J].电力科学与技术学报，2021，36(5)：35-40.
WU Haitao, DAI Shanglin, QIAO Zhongwei, et al. Research on network security situation awareness of intelligent distribution transformer terminal based on RBF-SVM[J]. Journal of Electric Power Science and Technology, 2021, 36(5): 35-40.

[56] 赖积保，王慧强，金爽.基于 Netflow 的网络安全态势感知系统研究[J].计算机应用研究，2007，24(8)：167-172.
LAI Jibao, WANG Huiqiang, JIN Shuang. Research on network security situation awareness system based on Netflow[J]. Computer Application Research, 2007, 24(8): 167-172.

[57] 谢丽霞，王亚超，于巾博.基于神经网络的网络安全态势感知[J].清华大学学报(自然科学版)，2013，53(12)：1750-1760.
XIE Lixia, WANG Yachao, YU Jinbo. Network security situation awareness based on neural network[J]. Journal of Tsinghua University (Natural Science Edition), 2013, 53(12): 1750-1760.

[58] 谢丽霞，王亚超.网络安全态势感知新方法[J].北京邮电大学学报，2014，37(5)：31-35.
XIE Lixia, WANG Yachao. A new method of network security situation awareness[J]. Journal of Beijing University of Posts and Telecommunications, 2014, 37(5): 31-35.

[59] 郝唯杰，杨强，李炜.基于 FARIMA 模型的智能变电站通信流量异常分析[J].电力系统自动化，2019，43(1)：158-167.
HAO Weijie, YANG Qiang, LI Wei. FARIMA model based analysis of communication traffic anomaly in smart substation[J]. Automation of Electric Power Systems, 2019, 43(1): 158-167.

[60] 朱炳铨，郭逸豪，郭创新，等.信息失效威胁下的电力信息物理系统安全评估与防御研究综述[J].电力系统保护与控制，2021，49(1)：178-187.
ZHU Bingquan, GUO Yihao, GUO Chuangxin, et al. A survey of the security assessment and security defense of a cyber physical power system under cyber failure threat[J]. Power System Protection and Control, 2021, 49(1): 178-187.

[61] DUMAN O, GHAFOURI M, KASSOUF M, et al. Modeling supply chain attacks in IEC 61850 substations[C]//2019 IEEE International Conference on Communications, Control, and Computing Technologies for Smart Grids, Beijing, China: IEEE, 2019.

[62] APRIL P. Internet security threat report[R]. Symantec, 2014.

[63] EGGERS S L. The nuclear digital I&C system supply chain cyber-attack surface[R]. Idaho National Lab. (INL), Idaho Falls, ID(United States), 2020.

[64] NICHOLS S V. Greg Kroah-Hartman bans University of Minnesota from Linux development for deliberately buggy patches[EB/OL]. https://www.zdnet.com/article/greg-kroah-hartman-bans-university-of-minnesota-from-linux-development-for-deliberately-buggy-patches/, 2021-04-26.

[65] FIELD Rupert. Attackers found building malicious container images directly on host[EB/OL]. https://www.infoq.com/news/2020/09/Malicious-Container-Images/, 2021-4-26.

[66] MILLER S. DARPA's first bug bounty: Find vulnerabilities in hardware-based security[EB/OL]. https://gcn.com/articles/2020/06/15/darpa-ssith-bug-bounty.aspx, 2021-05-25.

[67] 邓松，蔡清媛，高昆仑，等.基于函数挖掘的能源信息物理系统数据安全风险识别算法[J].中国电力，2021，54(3)：23-30+37.
DENG Song, CAI Qingyuan, GAO Kunlun, et al. Data security risk recognition algorithm for energy cyber physics system based on function mining[J]. Electric Power, 2021, 54(3): 23-30+37.

[68] YANG Z, TEN C W, GINTER A. Extended enumeration of hypothesized substations outages incorporating overload implication[J]. IEEE Transactions on Smart Grid, 2017, 9(6): 6929-6938.

[69] TEN C, YAMASHITA K, YANG Z, et al. Impact assessment of hypothesized cyberattacks on interconnected bulk power systems[J]. IEEE Transactions on Smart Grid, 2018, 9(5): 4405-4425,

[70] 吴亦贝，李俊娥，陈汹，等.大规模可控负荷被恶意控制场景下配电网风险分析[J].电力系统自动化，2018，42(10)：30-37.
WU Yibei, LI Jun'e, CHEN Xiong, et al. Risk analysis of distribution network with large-scale controllable loads with attacks[J]. Automation of Electric Power Systems, 2018, 42(10): 30-37.

[71] 王坤，苏盛，赵奕，等.变电站自动化系统时间同步协同攻击的检测与防护方法[J].电力系统自动化，2021，45(6)：231-239.
WANG Kun, SU Sheng, ZHAO Yi, et al. Detection and protection method for time-synchronized coordinated cyber-attack on substation automation system[J]. Automation of Electric Power Systems, 2021, 45(6): 231-239.

[72] SU S, WANG Y K, LONG Y Y, et al. Cyber attack impact on power system blackout[C]//IET Conference on Reliability of Transmission and Distribution Networks(RTDN 2011), London, UK, 2011.

[73] 胡国，梅德冬.智能变电站采样值报文安全分析与实现[J].中国电机工程学报，2017，37(8)：2215-2222.
HU Guo, MEI Dedong. Safety analysis and implementation of sampled value messages in intelligent substations[J]. Proceedings of the CSEE, 2017, 37(8): 2215-2222.

[74] CHEREPANOV A. Win32/Industroyer: a new threat for industrial control systems[R]. White Paper, ESET, 2017.

[75] 苏盛，刘亮，曹一家，等.基于系统时钟加速的无通信时间同步/扰动同步协同攻击逻辑炸弹检测方法[P].中国，CN110602710A，2019-12-20.

[76] KRISHNA V B, WU Z, AMBARDEKAR V V, et al. Cyberattacks on primary frequency response mechanisms in power grids [J]. Computer, 2018, 51(11): 37-45.

[77] KAMAL K R, SINGH L K, PANDEY B. Security analysis of smart grids: successes and challenges[J]. IEEE Consumer Electronics Magazine, 2019, 8(2): 10-15.

[78] 刘世涛，杨凯，伍弘，等.基于多维信息特征映射的电网风险区段路径匹配模型研究[J].高压电器，2020，56(9)：87-93.
LIU Shitao, YANG Kai, WU Hong, et al. Research on path matching model of power grid risk section based on multidimensional information feature mapping[J]. High Voltage Apparatus, 2020, 56(9): 87-93.