DOI：10. 16516/j. gedi. issn2095-8676. 2020. 03. 002

电力系统信息物理网络安全综合分析与风险研究

杨至元✉，张仕鹏，孙浩
（中国能源建设集团广东省电力设计研究院有限公司，广州 510663）

摘要：［**目的**］我国电网将步入“电力-信息-业务”紧密互联的智能电网阶段，信息系统的网络安全和物理系统的工程安全高度耦合，将带来信息物理融合系统（CPS）的综合安全问题。［**方法**］综述了现有的CPS安全分析技术并总结了CPS网络安全风险评估和管理方法，介绍了电力安全防护的总体现状，梳理了CPS网络安全分析方法、风险评估框架、建模思想等，并详细分析了各个模型的优劣特性及发展前景。［**结果**］提出的风险分析框架可以帮助电力企业筛选、识别网络安全事件，探究安全风险事件的相关性和依赖性，探究网络安全分析的潜在方向。［**结论**］有助于电力企业优化资源配置，对网络安全规划人员开展电力基础设施安全风险评估、网络安全应急预案等工作有参考意义。

关键词：电力信息物理融合系统；网络安全分析；网络风险评估；电力系统信息安全；电力系统工程安全
中图分类号：TM73；TP393. 08　　**文献标志码：**A　　**文章编号：**2095-8676(2020)03-0006-17
开放科学(资源服务)二维码：

Integrated Cyber-physical Contingency Analysis and Risk Estimates

YANG Zhiyuan✉, ZHANG Shipeng, SUN Hao
(China Energy Engineering Group Guangdong Electric Power Design Institute Co. , Ltd. , Guangzhou 510663, China)

Abstract: [**Introduction**] China's power grid is now entering the new era of smart grid with the "power-information-business" interconnected stage, where the cybersecurity in the information system and the operational security in the power system are closely coupled, which, however, would cause severe security problem of the cyber-physical system(CPS). [**Method**] This paper surveyed on the cybersecurity issue of CPS and summarizes the corresponding risk estimation and management framework. Then the paper introduced the background and current status of cybersecurity, categorized the state-of-the-art methods, risk estimation framework, modeling insights, etc. This paper also fundamentally investigated both the advantages and disadvantages of each model and evaluated its development potentials. [**Result**] This study would help enterprises to screen and identify cybersecurity events and explore the correlation and dependency within the events, which may help researchers to exploit new interests. [**Conclusion**] This work induces investors to optimize their resources and budget allocations, which would also guide for security engineers to proceed with cyber risk estimates and to prepare contingency plans.

Key words: power cyber-physical system; cyber-based contingency analysis; cyber risk estimate; power system information security; power system engineering stability

随着电力系统信息化建设的不断发展、信息技术与业务的高度融合，电力系统安全威胁也趋于信息化，具有隐蔽性、突发性及不确定性，甚至引起严重级联故障，世界上很多国家和地区都因此类突发性事件遭受巨大损失。电力信息物理融合系统（CPS）作为支撑电力信息化和工业化深度融合的关键技术体系，因其包含大量的量测和控制信息极易成为攻击对象，电力系统安全风险分析由此从以工程故障为主的物理安全分析逐渐转变成同时考虑信息网络和物理系统的综合安全风险分析。

然而，常规的信息安全研究和系统运行研究之间较为割裂，信息安全分析模型重点分析通信网络本身的机密性、完整性和可用性；而传统电力系统工程安全则以“三道防线”系统进行构建，为各种系统故障提供安全稳定的控制措施，确保系统在遭

收稿日期：2020-05-11　　**修回日期：**2020-08-04
基金项目：中国能建广东院科技项目“基于信息物理融合系统的网络安全的电力系统运行风险评估”(EV05391W)

受大扰动的情况下仍能满足正常运行条件。现有的电力监控系统防护体系尽管可以满足当下的要求，但面对具有跨领域专业知识的高级、智能攻击威胁时，仍存在过度依赖边界防护、纵深防御能力不足以及核心控制系统防护强度不够等问题。搭建可行有效的CPS网络安全综合风险分析模型是提升电力监控系统综合防御能力的重要内容。

本文首先介绍网络安全防护的总体现状，重新梳理CPS网络安全的主要分析方法、建模思想以及发展轨迹，详细阐述各个模型的优劣特性及发展前景，为后续的网络安全分析提供研究思路；提出CPS网络安全风险评估框架，重点介绍经济损失风险的金融保险模型，通过列举系统内各个关键信息基础设施的风险指标，识别“高危”风险事件和节点，有助于电网安全规划人员优化资源配置，对电力基础设施安全风险评估、网络安全应急预案等工作的开展有参考意义。

1　电力系统信息物理网络安全事件

1.1　电力信息网络安全事件定义

美国国家标准与技术研究院（NIST）在《智能电网网络安全指南：卷1》[1]中定义了3组电力信息系统安全指标：机密性、完整性及可用性。

机密性：通过保护用户的授权隐私和专有信息的安全传递等方法，保留信息获取和信息公开的授权限制。系统的机密性破坏即信息未经授权的泄露。

完整性：通过保护信息的不可否认性和一致性，防止不当的信息修改和破坏。系统的完整性破坏即信息未经授权的修改和损毁。

可用性：通过有效的手段，确保用户可以及时和可靠地获取信息。系统的可用性破坏即信息的使用或获取被恶意中断。在本文的讨论范围中，破坏系统的可用性实质上是破坏电力通信系统，即影响通信网络的数据传输、加密等安全功能，并带来生产业务系统的安全隐患。

CPS通过集成先进的感知、计算、通信、控制等信息技术和自动控制技术，构建物理空间元素和信息空间元素相互映射、适时交互、高效协同的复杂系统[2]。基于电力CPS的网络攻击会破坏信息网络与物理系统间的耦合关系，造成CPS系统故障或诱导故障在系统中传播，影响信息网络完整性和物理系统有效性。电力CPS网络威胁具有隐蔽性、突发性和不确定性等特点，网络安全运维和监管部门无法提前准备预案，处理网络攻击事件往往比处理特定的传统故障更为复杂[3-4]。电力系统安全风险分析正从以工程故障为主的物理安全分析，变成同时考虑信息网络和物理系统的综合安全风险分析。

本文基于CPS的系统特点并沿用[5]中网络攻击定义：以破坏或降低电力CPS功能为目的，在未经许可情况下对通信系统和控制系统行为（各种保证电力系统正常运行的电力自动化控制组件以及对实时数据进行采集、监测、传输的过程控制组件的工作状态）进行追踪，利用电力信息通信网络存在的漏洞和安全缺陷（如操作系统漏洞／通信协议漏洞／应用软件漏洞等）对系统本身或资源进行攻击，其影响应从信息系统延伸至物理系统。

1.2　电力系统网络安全事件

近年来，针对电力能源系统的网络攻击事件频频发生，持续威胁着电网的电力系统的机密性、完整性和可用性，给系统的运行安全带来巨大挑战：2010年在伊朗爆发“震网”蠕虫病毒攻击、感染了多座核电设施，共影响了约1 000台铀浓缩离心机[6]；同年乌克兰电网遭受攻击，攻击者利用Office软件漏洞电力数据采集和监控系统（SCADA），造成大停电[7]；2019年3月，委内瑞拉古里水电站疑似遭受网络攻击，影响3 000万人正常用电[8]；7月，南非约翰内斯堡City Power电力公司遭遇勒索软件攻击，官方数据库、应用程序、客服网络等服务被劫持[9]；9月，印度库丹库拉姆核电站遭到黑客网络渗透，网络域控服务器被植入远程控制程序[10]；新型的网络攻击，如协同攻击（CCPA），则会将攻击行为隐藏在普通的线路或设备故障中[11]，并结合数据篡改攻击（FDIA）伪造仪表读数或量测值，躲避检测系统，造成电网连锁故障而引发大停电[12-14]。

2015年的乌克兰停电事件被认为是首次由网络攻击导致的电力中断事件，攻击者利用Office漏洞CVE-2014-4114劫持了工作人员办公网络并通过SSH安装后门程序，以方便攻击者对被感染系统的远程控制。黑客通过SCADA系统直接下达断电控制指令，并结合电话拒绝服务攻击，有意的延缓运维进度，造成大面积停电[7]。配置独立专网的总体

防护架构一直被认为是保护电力网络安全的最有效方式，但过度依赖专网和边界防护往往会忽视提升核心控制系统的主动防御能力。2017年，美国塔尔萨大学的研究人员对5个风电场做了渗透测试：攻击者潜入机组内部，通过简单的物理接触，劫持内部控制主机，利用协议漏洞开展攻击。尽管发电机的控制系统与互联网无直接连接，但攻击者通过简单的路由通讯装置，可实现远距离攻击，同时利用控制区的身份验证机制的协议漏洞，恶意扩散攻击范围[15]。

由上述安全事件可知，攻击者在经由信息攻击劫持电力通信网络之后，其最终目的是入侵控制系统，恶意篡改控制信号，影响电网整体运行安全。选择适用的网络安全风险分析方法和评估框架对提高系统的网络安全综合防御能力至关重要。

1.3 电力网络安全风险分析内容和范围

电力能源基础设施的可靠运行在经济发展中起着重要作用，NIST提出了《提高关键信息设施网络安全的框架》的执行标准[16]，确定了5个主要功能模块：识别（Identify）、保护（Protect）、检测（Detect）、反馈（Respond）、恢复（Recover）。其中，识别模块中共包含了资产管理（Asset management）、商业环境（Business environment）、管理监督（Governance）、风险评估（Risk assessment）、风险管理决策支持（Risk management strategy）6个二级功能模块，本文选取风险评估和风险管理决策支持两个功能及其三级模块做重点介绍，如表1所示。

由表1可知，标准中讨论的潜在业务影响不仅包括业务通信系统的失效，还需包括一次系统功能失效影响。本文将基于电力信息物理系统，重点讨论二级功能模块风险评估功能中，风险建模和风险计算两个子功能模块，即确定潜在的业务影响和威胁事件的可能性，以及综合系统漏洞、攻击等网络威胁的整体风险评估方法。

表1 风险评估和风险管理决策功能描述

Tab. 1 The category description of risk assessment and risk management strategy functions

二级功能	三级功能	功能描述
风险评估	安全隐患记录和备份	记录、备份系统资产的安全隐患。
	安全隐患(漏洞)获取	从商业或开源数据库获取最新威胁和漏洞信息。
	威胁识别	识别、记录工控系统内部(外部)威胁。
	风险建模	确定潜在的业务影响和威胁事件的可能性。
	风险计算	根据威胁、漏洞、可能性和影响被用来确定风险。
	结果反馈	基于风险计算结果,确定风险事件等级及优先级。
风险管理决策支持	风险确认	风险计算结果及缓和应急决策由系统管理者确认。
	风险承受	分析能源基础设施的安全风险承受力。
	影响分析	确定风险承受力分析中“脆弱”或“关键”的基础设施或部门。

2 电力系统网络安全总体防护和风险分析框架

2.1 电力监控系统总体防护框架

我国是世界上较早重视电力监控系统信息安全的国家，2004年发布的《电力二次系统安全防护规定》中首次明确了“安全分区、网络专用、横向隔离、纵向认证”原则[17-18]，确定中国电力监控系统安全防护体系。为了应对逐渐升级的信息安全事件和进一步提高电力监控系统安全防护体系的防御能力，电力监管委员会在2012年发布《电力行业信息系统安全等级保护基本要求》，规定电力系统要从“物理安全、网络安全、主机安全、应用安全和数据安全”四个方面提出全面技术要求[19]。国家发改委在2014年印发《电力监控系统安全防护规定》，要求生产控制大区实现网络环境的安全可信并对恶意代码具备免疫能力[20]，强调了电网的主动防御能力。2017年《中华人民共和国网络安全法》正式实施，明确要求运营者需对关键信息基础设施就潜在的安全风险做“定期评估”并“实行重点保护”[21]，确保电力网络风险的安全可控。2019年，中国国家标准化管理委员会发布了《信息安全技术网络安全等级保护基本要求》，对工业控制系统的安全环境和关键信息基础设施提出了更高的安全要求[22]。

近20年来，网络安全相关的国家、行业标准相继推出，完善了电力监控系统安全防护体系的总体框架，细化了防护原则，对防范黑客及恶意代码入侵、集团式攻击以及网络安全相关电力设备事故

或安全事件具有关键作用。电力监控系统的安全防护方案[19]主要包括以下几个方面：

1）安全分区：安全分区是电力监控系统安全防护体系的结构基础。发电、电网等电力能源相关企业的业务通信网络总体应分为生产控制大区和管理信息大区。生产控制大区又分控制区（安全I区）和非控制区（安全II区）。安全I区的业务系统主要包括SCADA、能量管理系统（EMS）等，是电力生产的重要环节，直接实现对电力一次系统的实施监测和调控，也是安全防护的重点与核心。安全II区的业务系统主要包括电能力计量系统等非控制功能的在线系统，同为电力生产的必要环节。管理信息大区是生产控制大区以外的电力企业管理业务系统的集合。

2）网络专用：电力调度数据网是安全I区和II区的专用网络，在专用通道上使用独立的网络设备组网，采用不同的光波长、不同纤芯等方式在物理上实现与外部公共信息网的安全隔离。此外，电力调度数据网还需采取网络路由防护、网络边界防护、网络设备安全配置、数据网络安全分层分区设置等方法，提高调度数据网的安全性。

3）横向隔离：在生产控制大区与管理信息大区之间必须设置电力专用横向单向安全隔离装置，隔离强度应当接近或达到物理隔离标准。按照数据通信的方向，单向隔离装置分为正向型和反向型。正向隔离装置用于生产控制大区向管理信息大区单向数据传输；反向隔离装置用于管理信息大区向生产控制大区单向数据传输。单向数据传输严格禁止E-mail、Web、Telnet等高风险的通信服务。

4）纵向认证：纵向加密认证装置及加密网关用于生产控制大区的广域边界防护，采用认证、加密等技术实现双向身份认证、数据加密和访问控制，保护数据从调度数据网传输至站端生产控制大区的机密性和完整性。

5）电力调度数字证书系统：电力调度数字证书系统是基于公钥技术开发的分布式证书系统，主要应用于生产控制大区，可提供高强度的身份认证功能。电力调度数字证书应满足配置统一的规划数字证书信任体系、统一的数字证书格式、规范的数字接口。

除了上述主要的防护方案以外，电力监控系统总体防护体系还配置高强度的物理安全防护措施、恶意代码检测和主动防御、控制区与非控制区的逻辑隔离、边界入侵检测（IDS）、安全审计等其他常规安全保护措施。然而，现有的电力系统网络安全防护过于依赖边界防护，并未对潜在的网络攻击和入侵渗透开展详细的建模分析，极易忽视来自内部工作人员或是设备供应商的违规操作带来的隐患，造成纵深防御能力不足、核心控制系统防护强度不够等问题。主要体现在以下几个方面[23]：

1）国家对电力系统网络安全管理制度及技术标准尚未完善。涉及网络安全设备和组件的供应商、服务提供商、企业用户的安全责任体系仍需发展，缺少切实可行的安全评估方案和管理标准。

2）电力企业网络安全管理、意识培训仍需要提高，部分运维和安防人员不按防护要求和规定操作执行，存在安全隐患。例如，移动存储使用不规范、远程维护留后门等安全隐患极易被攻击者利用并以此绕过边界防护，直接影响核心控制系统的安全。

3）网络安全主动防御能力不足。现有的电力监控系统网络安全态势感知平台已实现大部分厂站的历史流量、报文、日志的采集，但基于历史数据的智能入侵检测、溯源分析、攻击反制以及主动防御的应用和研究仍在探索阶段。

2.2　电力CPS网络安全综合风险分析框架

网络风险安全评估应贯穿电力系统的网络安全建设、规划、设计、运维等工作中[19]。基于网络态势感知系统的风险值可以准确评估当前电力系统的网络安全状态，有助于运维人员定位可能的潜在威胁，发现系统的安全问题。本文在传统的风险分析基础上新增了系统运行的稳定分析，因为电力系统的通信网络本质是为一次系统的稳定运行服务，通信系统的脆弱性和严重程度的评价标准应基于系统的运行结果[24]。由此，本文在电力监控系统网络安全总体防护原则下[16,19]，提出CPS综合风险分析框架，如图1所示。

基于电力监控系统态势感知采集平台，分析框架通过采集日志和流量信息，运用无监督算法对可疑的恶意流量进行识别和聚类，分析调度数据网的恶意流量特征；采集系统登录信息、关键文件变更信息及磁盘、内存、网口信息等数据，通过特征工

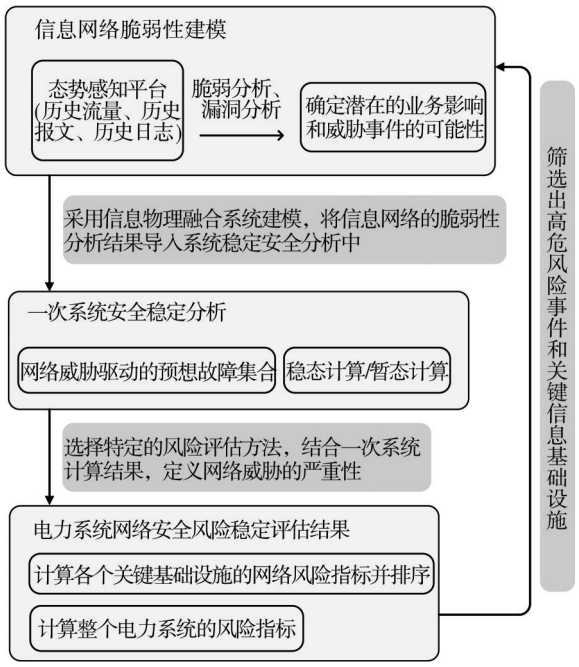


图 1 基于态势感知平台的 CPS 综合风险分析框架

Fig. 1 The framework of CPS risk estimates based on cybersecurity situational awareness platform

程对采集数据进行清洗和降维，运用机器学习算法学习异常主机行为；根据恶意流量信息和异常主机行为的学习结果，以及正反向隔离装置、加密认证装置、防火墙等网络环境安全监控组件的架构特点，基于佩式网理论和马可夫状态转移矩阵求解威胁事件的可能性。

分析框架还将通过 CPS 复合关联关系[25]统一业务系统的通信节点和物理控制节点，获得业务系统失效的运行故障集，得到故障的电气接线图，并结合稳态计算和暂态计算完成网络威胁驱动的系统安全稳定分析。选择特定的风险评估方法，根据威胁事件的可能性和严重性模型，得到系统的综合风险量化方法；基于评估结果，可以列举系统各个关键信息基础设施的风险指标，识别“高危”风险事件和节点。

3 电力系统网络安全分析模型

3.1 电力系统信息网络安全的脆弱性分析

近年来的安全事件显示，攻击者会利用工作人员不规范操作遗留的安全隐患或第三方网络设备的源程序漏洞，绕过系统的边界防护，破坏通信系统的机密性、完整性和可用性，直接影响电力系统的稳定安全。信息网络的安全建模是包括通信网络、节点和设备在内的综合数据建模。国内外学者在电力系统的信息安全方面开展了诸多研究。Liu 等学者基于脆弱性状态图（VSG）描述系统中目标节点到达不安全状态的可能路径，定义状态转移的脆弱度函数，并根据 VSG 的连接方式，提出了多种类型的脆弱度计算模型[26-28]，其中基于 VSG 的串联系统脆弱度计算公式为：

$$1-\sum_{i=1}^{n}\frac{\prod_{j=1,i\neq 1}^{n}\lambda_j e^{-\lambda_j c}}{\prod_{j=1,i\neq 1}^{n}\lambda_j-\lambda_i} \tag{1}$$

式中：c 和 λ_i 分别为第 i 步行为成功时的等效代价和脆弱度因子。根据 λ_i 的影响因素，文献［26］构造了目标层、准则层、指标层和行为层 4 层组织结构，有效地识别出信息系统的脆弱节点。

Tang 分析了信息系统影响电力系统的主要途径，提出复合系统关联矩阵来描述信息-物理复合系统的拓扑结构，并基于通信系统脆弱性指标以及电力通信业务信息交互的脆弱性得到复合系统脆弱性指标及静态脆弱性矩阵[25]。从节点 i 到节点 j 的通道脆弱性指标 C 的计算公式为：

$$C=\varepsilon_{\mathrm{t}}\sum_{k=1}^{n}\left(\frac{v_k}{\sum_{j=1}^{n}v_j}B_{\mathrm{sk}}\right) \tag{2}$$

式中：ε_{t} 为通道传输实际时延与固有时延之比；n 为通道中的业务流通数量；v_k 为第 k 类业务的传输速率；B_{sk} 为第 k 类业务的重要度指标。基于电力-通信复合系统和脆弱性评估标准，文献在通信业务系统中对通信时延、误码、中断等故障建模，可以得到系统的单元集合。相较于文献［26］的脆弱性指标和评估结果，文献［25］重在分析信息系统本身结构的网络安全脆弱性，但复合矩阵的思想也可用在网络攻击建模和严重性程度分析的研究中。

基于图论，文献［29］提出了一个评估电力通信网络信息安全的专家系统。系统搭建了电力通信架构的连通图，通过边和点来表是通讯通道和节点，并定义在攻击环境下的设备可见度和可见度先决条件（visibility preconditions）的四元组（quartet）：

$$q=\{s,m,l,o\} \tag{3}$$

式中：$s\in S$，表示系统中所有的可能发起攻击的攻击主体，可以是一台服务器或服务器机群，由人为攻击驱动的第三方操作系统或变电站或主站内部的控制系统；$o\in O$，表示系统中所有可能的被攻击

对象，依据研究对象选取不同的攻击对象，一般选取电力系统的控制和保护装置；$m \in M$，表示 s 访问 o 的物理通讯先决条件，具体指代攻击者窃听、监听设备 s 与设备 o 的通道，并通过一定的访问手段直接或间接，有限连接至公共网络；$l \in L$，表示逻辑通讯通道，具体指代设备 s 与设备 o 之间实现通讯的必要协议。基于（3），Leon通过最短路径算法对设备的可见度脆弱性进行排序，指出其中包含最长搜索路径或搜索代价最高路径的脆弱性。

文献［29］结合攻击树模型和随机佩式网（Petri net）理论，提出布尔驱动的逻辑马可夫过程（BDMP）来描述网络安全的脆弱性问题，对潜在的供给渠道搭建了复杂的攻击树模型，通过对各个攻击树的结果进行概率描述，各个“树叶”和“分支”的结果可以通过求解马可夫链获得。BDMP方法有良好的软件适用性，通过简单的程序嵌入就能得到有效的输出，有广泛的应用前景。相较于直接对信息系统安全性的量化方法，基于图论的脆弱性建模更加直观，延展性也更好。但上述方法均不能体现信息系统受攻击的状态变化，无法对网络攻击的可能性进行评估。

基于图论和概率方法，Sommestad提出结合贝叶斯理论的影响图（Influence diagram）模型，量化SCADA系统广域网（WANS）的网络安全水平[30-32]。文献利用概率的不确定性描述针对SCADA WANs的广泛攻击，并将运维人员应对攻击的措施一并建模得到防御图（Defense diagram）模型。根据模型中多个评估指标，例如信息加密、数据长度、认证签名、设备密码等，共同计算成功攻击的概率，并提出一般性的防御结论。McQueen等学者提出平均攻击时间（MTTC）T_{pi} 来评估网络攻击的成效和攻击对象的脆弱性[33]。函数 T_{pi} 的定义为攻击者获取攻击对象（系统）的某个安全组件 i 的一定权限 p 所需的时间，所以直接由攻击对象（系统）本身的脆弱性和攻击者的专业程度决定。

MTTC可通过以下3组子随机过程求得：子过程1表示已知系统组件 i 上存在至少一个已知漏洞可以达到权限 p，攻击者可以通过至少一种方法利用漏洞开展攻击；子过程2表示已知系统组件 i 上存在至少一个已知漏洞可以达到权限 p，攻击者无法通过任何方法利用漏洞开展攻击；子过程3表示识别新的漏洞并且利用新的漏洞。子过程3是子过程1和2的并行过程，即攻击者可以等待新的漏洞公布/识别并探测新的漏洞。所以MTTC的定义为：

$$T = t_1 P_1 + t_2\left(1 - P_1\right)(1 - u) + t_3 u(1 - P_1) \quad (4)$$

式中：t_1、t_2 和 t_3 分别为子过程1、2和3的期望值；P_1 为攻击者位于子过程1的概率；u 为子过程2失败的概率。（4）不仅可以量化系统的脆弱性，也可平衡网络安全缓解措施的收益和成本。但由于模型缺少必要的控制参数，在实际的应用中，模型的有效性和灵敏性还需验证。

基于式（4），Zhang和Wang根据SCADA系统特点，将MTTC函数应用到电力CPS的网络攻击模型中[34-37]，并通过贝叶斯网络对攻击路径图进行综合建模，揭示了攻击者的专业能力对MTTC的影响机制，同时得到了更准确的脆弱性指标：

$$\mathrm{MTTC}(c) = \frac{\sum_{v_i \in V} T(v_i) p(v_i \wedge c)}{p(c)} \quad (5)$$

式中：c 为目标攻击的条件达成；v_i 为第 i 个安全隐患；$p(v_i \wedge c)$ 为攻击者成功利用隐患 v_i 达成攻击目标条件；$p(c)$ 为攻击目标条件达成。文献还结合平均维修时间（MTTR）定义了网络攻击的可能性：

$$p_{\mathrm{a}} = \frac{\mathrm{MTTR}}{\mathrm{MTTR} + \mathrm{MTTC}} \quad (6)$$

Wang团队提出结合MTTC与贝叶斯方法的信息系统脆弱性分析模型，提高了前文模型的准确性同时，给出了网络攻击的潜在可能性模型，为后续的风险研究提供了研究理论。除了上述的几种网络安全分析方法以外，本文将介绍以下几种常用的仿真模型和测试平台[38]。

1）高级体系架构（HLA）：HLA是由美国国防部设计的综合协同仿真平台。在HLA框架下，单一或多组仿真软件可用于不同的领域，在网络安全领域，有学者基于HLA，采用OMNeT++和MATLAB设计安全分析与监测平台[39]。

2）SCADASim：该框架基于OMNeT++、MATLAB/Simulink等平台搭建了网络仿真和真实设备联动的综合SCADA仿真系统，将大量智能电表、遥测装置等实物信息整合到仿真软件中，在现实场景中也有广泛应用[40]。

3）国家SCADA测试床（NSTB）：美国能源部于2003年开发了国家SCADA测试床[41]，旨在提供

测试、研究和培训设施，提高控制通信系统的安全性。NSTB的核心能力在于将国家实验室用于测试的最先进操作系统与网络安全专家的研究结合起来，开发、分析、研究能源系统中潜在的重大安全漏洞和威胁。

4）通用网络安全研究仿真器（CORE）：CORE是一个实时网络仿真器，支持将实物硬件和虚拟网络节点组成的混合拓扑模型快速实例化[42]。CORE通过FreeBSD网络堆栈的虚拟化来扩展物理网络，以便实现系统的规划、测试及开发，同时减少了昂贵的硬件部署。CORE的主要特点有延展性、易用性、在TCP/IP网络堆栈上运行程序的潜力，以及信息物理实时交互能力。

工业通信系统的信息安全问题直接影响关键信息基础设施的安全生产工作[43]。本小节回顾了国内外研究学者针对电力信息网络安全问题采用的常规建模方法及常用的仿真测试平台。上述方法在分析网络安全状态、脆弱性以及研究特定网络攻击对信息系统的影响等方面有着良好的适用性，但电力系统的风险评估模型不仅需要考虑信息系统的脆弱性，还需充分考虑智能电网的运行状态、信息基础设施和电力控制系统的耦合性[44]。上述文献在搭建网络安全攻击的概率模型时采用了经典的泊松分布，例如式(4)-式(6)，尽管固定形式的概率分布并不影响上述工作介绍的数学方法和思路，但会严重限制结论的准确性与合理性。

3.2 电力信息物理融合系统的综合安全分析

3.2.1 基于攻击类型的安全建模

基于攻击类型的安全建模研究会给出合理的攻击假设，基于传统电力系统稳定判据，重点研究攻击发生以后对系统运行的影响。

1）拒接服务攻击（DDoS）：DDoS主要目的是使攻击对象的网络和系统资源过度消耗，造成系统无法响应正常的服务和请求，从而暂停或中断整体系统功能[45-46]。在信息物理融合系统的网络安全分析中，DDoS的攻击目标是破坏控制中心与测控等装置之间的通信中断。Liu等学者假设电力量测数据在发送回控制中心的传感回路上遭受DDoS攻击[47]，并对遭受攻击的电力测控系统的开关（刀闸）动作作为建模对象，将DDoS的攻击描述为一次回路的开关（刀闸）动作并给出了攻击状态下的负载频率控制（LFC）分析方程：

$$\dot{\boldsymbol{x}}_i = \boldsymbol{A}_{ii}\boldsymbol{x}_i + \boldsymbol{B}_i\boldsymbol{v}_i + \sum_{i\neq j,j=1}^{N}\boldsymbol{A}_{ij}\boldsymbol{x}_j + \boldsymbol{F}_i\Delta P_{L_i} \quad (7)$$

式中：$\boldsymbol{x}_i$是频率偏移量、发动机机械功率偏移量、误差等参数组成的向量参数；$\boldsymbol{A}_{ii}$为发动机阻尼参数、转动惯量等组成的参数矩阵；$\boldsymbol{B}_i$为调速机参数；ΔP_{L_i}为负载偏移量。于是，模型遭受DDoS攻击则可通过式（7）反映各个参量的变化，进而分析整个系统的负载和频率的动态变化。通过定量的计算可知，在一定的影像范围内，DDoS对系统负载和频率的影响是可控且收敛的。文献［48］进一步讨论了时滞开关攻击（TDS）和LFC对发电系统和自动发电控制（AGC）系统的影响，并细致讨论了严重的TDS会产生剧烈的频率震荡及相关稳定问题。

2）中间人攻击（MIM）：中间人攻击可以将自己伪装成参与会话或通信的某个终端，同时确保自己不被识破。攻击成功的前提是利用系统通信协议的认证漏洞，所以中间人攻击研究大都是以通信协议为主的安全性分析。信息系统的脆弱性分析在上节有详细介绍，本节将重点讨论MIM攻击对电力系统的影响建模。

一般地，针对电力系统的MIM攻击现实中较难实现，因为现有的能量管理系统（EMS）配备有完善的错误数据检测（Bad measurement detection）和拓扑结构检测系统，实时提醒运维工作人员，正在使用的数据是否可疑或网络拓扑结构发生的是否变化。在文献［49］中，Kim假设攻击者可以调整传感器中电气量的测量值、系统断路器的开闭状态，欺骗EMS系统使得拓扑估计值与错误数据一致，从而躲避数据错误检测和拓扑检测系统。这种攻击也称未暴露攻击（Undetectable attack）。Kim提出了一种针对未暴露攻击的拓扑估计方法，并分析电力网架拓扑结构中脆弱的传输线及变压器等设备。文中给出未暴露攻击的定义：

$$\boldsymbol{c} + \boldsymbol{b}(\boldsymbol{c}) \in \mathrm{Col}\left(\overline{\boldsymbol{H}}\right), \forall \boldsymbol{z} \in \mathrm{Col}(\boldsymbol{H}) \quad (8)$$

$$\boldsymbol{b}(\boldsymbol{c}) = \left(\overline{\boldsymbol{H}} - \boldsymbol{H}\right)\boldsymbol{x} = \left(\overline{\boldsymbol{H}} - \boldsymbol{H}\right)(\boldsymbol{H}^T\boldsymbol{H})^{-1}\boldsymbol{H}^T\boldsymbol{c} \quad (9)$$

式中：$\boldsymbol{c}$为网络系统中的各线路上的功率量测值和节点的注入功率值；$\boldsymbol{b}(\boldsymbol{c})$为未暴露攻击对量测值的修改；$\boldsymbol{H}$和$\overline{\boldsymbol{H}}$分别为系统的所有量测值矩阵和受攻击后的矩阵；Col(·)为取矩阵的列空间；$\boldsymbol{x}$为由平

衡节点以外的节点电压相角组成的列向量。（8）表示系统遭受攻击以后的量测值应与系统的两侧矩阵相一致，且只有满足了该条件，攻击才不会暴露。但由于采用稳态潮流计算，导致文献结果过于保守，还需交流模型做后续验证。

3）数据篡改攻击（FDI）：EMS是保证电力系统稳定运行的重要组件，其中电网潮流计算和状态估计是电力系统自动化的核心功能。错误数据检测算法大都基于假设：当偶尔出现错误数据时，该量测值与状态估计结果的差值很大。该假设的前提是自然因素下出现错误量测数据的情况是极少且随机的，但在网络攻击的前提下，攻击者往往具有专业的电力背景知识且极有可能为系统内部的专业人员，了解当前的电力系统参数配置。攻击者通过修改、注入恶意量测数据，绕过错误数据检测模块直接影响状态估计和潮流计算结果，从而影响电力系统的稳定运行[50]。

Liu和Ning团队给出了详细的分析模型。令：

$$z = Hx + e \tag{10}$$

式中：z为量测值；x为系统状态变量；e为各个节点的量测误差；H为满秩矩阵，用来表示z估计x的过程。于是：

$$\hat{x} = (H^T W H)^{-1} H^T W z \tag{11}$$

式中：W为对角矩阵，其元素为两侧误差的方差倒数。又令：$z_a = z + a$，其中z_a为含有篡改数据的量测值，a为篡改数据向量。于是由（11）可得：

$$\hat{x}_{\text{bad}} = (H^T W H)^{-1} H^T W z_a \tag{12}$$

$$\| \hat{x}_{\text{bad}} - \hat{x} \| = \| (H^T W H)^{-1} H^T W a \| \tag{13}$$

Liu和Ning还给出了模型的两个使用假设：a）限制性的接入权限—系统中存在部分量测装置由于物理隔离等手段难以攻陷；b）限制性的攻击成本—从攻击成本的角度，攻击者会尽可能少的攻击系统的测量装置，达到最大得攻击效果。基于模型分析爱模型和假设，文献［50］指出，相较IEEE 14、30节点等小系统，IEEE 300节点的大系统受FDI攻击的影响更明显；特别对于300节点系统，攻击1122个量测装置中的10个即可造成系统的状态估计结果错误并带来严重的运行隐患。

1）信息物理协同攻击（CCPA）：协同攻击基于FDI思想，对信息和物理两方面搭建攻击模型，其核心公式同（10）-（13）类似，但新增了系统的支路功率方程并修改了矩阵H的内容[51]。在3）的基础上，Deng先后给出了物理侧和信息侧的分析模型：

a）物理侧：

$$\hat{x}_{\text{bad}} = \hat{x} + \Delta x + E \Delta H x_{\text{bad}} \tag{14}$$

式中：$E = (H^T W H)^{-1} H^T W$；ΔH为量测变化矩阵。攻击矩阵：

$$A = H \Delta x + \Delta H x_{\text{bad}} \tag{15}$$

b）信息侧：

$$A = -(H \Delta x + \Delta H x_{\text{bad}}) \tag{16}$$

Deng证明，在出现线路故障时，攻击者可以修改量测值以满足状态估计的限制条件，成功欺骗控制中心系统依然处于正常状态。Li等学者在系统遭受CCPA条件下，提出了一种灵敏性参数，用以分析母线节点注入功率对线路潮流的影响，并证明该参数独立于平衡节点且不受节点位置的干扰[52]。此外，文献还论证了系统在遭受物理攻击后，攻击者可采用信息攻击加强对网架结构和负载分布信息的控制以持续欺骗控制中心，进而扩大物理侧的影响。

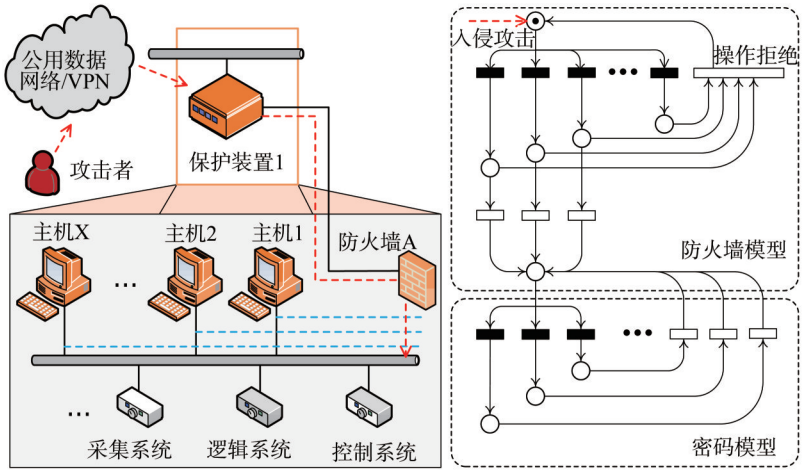
本小节重点介绍了几种典型的网络攻击模型及其分析方法。从系统运行的角度针对不同的攻击类型提出适用的处理方法，有助于提高网络安全的防御能力，但稳定运行的判据较为单一，往往由单个或几个电气量变化，和潮流计算结果给出。

3.2.2　基于广义随机佩式网（GSPN）的安全建模

广义随机佩式网属于离散时间动态系统，主要用来描述计算机的系统模型。但在传统的电力系统故障诊断和控制决策中，佩式网也得到了很好的应用和发展[53-54]。Liu和Ten团队基于攻击树模型和GSPN搭建了入侵检测分析模型，并通过负荷水平评估了变电站CPS环境中潜在的安全隐患，指出变电站中易受攻击的脆弱节点。

图2简单描述了基于网络安全组件的GSPN建模。其中潜在的攻击路径由红色虚线标出：可疑的流量数据包经过伪装，欺骗突破防火墙A，感染控制主机机组得到权限，渗入继电保护装置和开关设备，进而影响电力系统稳定。图2（b）给出了两个GSPN模型，防火墙模型和密码模型。以防火墙模型为例，一个完整的GSPN由四个部分组成：库所，由圆形的空心节点表示；变迁，其中包括瞬时

变迁和时延变迁，分别由图中的黑条和白条表示；有向连接，通过连线箭头表示，用以连接库所和变迁；令牌，为库所中移动的动态对象，通过库所中的黑点表示，用以对入侵攻击的建模。本节将简单介绍基于GSPN的网络攻击影响模型。



(a) 潜在的入侵攻击　　(b) 基于防火墙和密码模型的GSPN建模

图2　基于电力工控系统的GSPN攻击建模

Fig. 2　The framework of GSPN from electric power industrial control system

图3给出了详细的GSPN模型和对应的可达性图。图中，瞬时变迁和延时变迁分别用绿色和灰色箭头标出。假设该模型包含两个防火墙规则并与两个主机系统相连，库所A表示通过攻击者成功侵入防火墙，并可接入主机1的登录界面。库所B表示攻击者成功突破2个主机系统的密码保护。$p^{f}_{1,a}$和$p^{f}_{2,a}$分别表示攻击者突破防火墙规则1和2的概率，即传递概率（Transition probability）。被规则1和2阻止的传递概率记为$p^{f}_{1,b}$和$p^{f}_{2,b}$。$p^{w}_{1,a}$和$p^{w}_{1,b}$分别表示通过密码尝试登录主机系统1的成功和失败的传递概率。

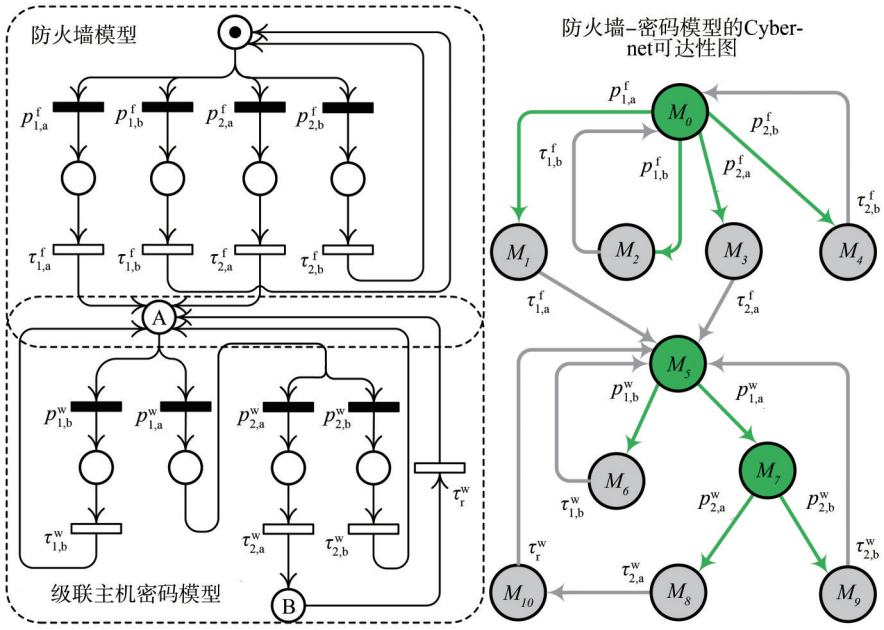


图3　防火墙-密码模型的GSPN和可达性图

Fig. 3　GSPN and the corresponding reachability graph of the firewall-password model

变量 $\tau^{\mathrm{f}}_{1,\mathrm{a}}$，$\tau^{\mathrm{f}}_{1,\mathrm{b}}$，$\tau^{\mathrm{f}}_{2,\mathrm{a}}$，$\tau^{\mathrm{f}}_{2,\mathrm{b}}$，$\tau^{\mathrm{w}}_{1,\mathrm{b}}$，$\tau^{\mathrm{w}}_{2,\mathrm{a}}$，$\tau^{\mathrm{w}}_{2,\mathrm{b}}$ 和 $\tau^{\mathrm{w}}_{\mathrm{r}}$ 为传递率（Transition rate），其中 $\tau^{\mathrm{f}}_{1,\mathrm{a}}$ 和 $\tau^{\mathrm{f}}_{1,\mathrm{b}}$ 分别表示攻击者在突破防火墙规则 1 时，系统对打开和拒绝登录接口 A 的响应时延；$\tau^{\mathrm{w}}_{1,\mathrm{b}}$，$\tau^{\mathrm{w}}_{2,\mathrm{a}}$ 和 $\tau^{\mathrm{w}}_{\mathrm{r}}$ 分别表示，攻击者反复攻击主机 1 的密码保护失败时的响应时延，攻击者成功登录主机 2 的响应时延以及成功登录主机系统 1 和 2 之后实施攻击时主机的响应时延。由可达性图可知，防火墙-双密码模型的 Cyber-net 共有 11 个状态（State），其中根据状态的滞留延时（Sojourn time）特性被标记（Marking）为两类。属于消失类标记（Vanishing marking）的状态有：

$$V = [M_0, M_5, M_7]$$

有形类标记（tangible markings）的状态包括：

$$T = [M_1, M_2, M_3, M_4, M_6, M_8, M_9, M_{10}]$$

图中的绿色和灰色箭头分别表示集合 V 和集合 T 的变迁概率和速率。传递概率矩阵 $\boldsymbol{P}$ 可写为：

$$\boldsymbol{P} = \begin{array}{c} \begin{matrix} M_0 & M_5 & M_7 & M_1 & M_2 & M_3 & M_4 & M_6 & M_8 & M_9 & M_{10} \end{matrix} \\ \begin{pmatrix} 0 & 0 & 0 & p^{\mathrm{f}}_{1,\mathrm{a}} & p^{\mathrm{f}}_{1,\mathrm{b}} & p^{\mathrm{f}}_{2,\mathrm{a}} & p^{\mathrm{f}}_{2,\mathrm{b}} & 0 & 0 & 0 & 0 \\ 0 & 0 & p^{\mathrm{w}}_{1,\mathrm{a}} & 0 & 0 & 0 & 0 & p^{\mathrm{w}}_{1,\mathrm{b}} & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & p^{\mathrm{w}}_{2,\mathrm{a}} & p^{\mathrm{w}}_{2,\mathrm{b}} & 0 \\ 0 & 1.0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1.0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1.0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1.0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1.0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1.0 \\ 0 & 1.0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1.0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix} \end{array}$$

令：

$$\boldsymbol{P} = \begin{pmatrix} \boldsymbol{A}_{3\times 3} & \boldsymbol{B}_{3\times 8} \\ \boldsymbol{C}_{8\times 3} & \boldsymbol{D}_{8\times 8} \end{pmatrix} \tag{17}$$

子阵 $\boldsymbol{A}$，$\boldsymbol{B}$，$\boldsymbol{C}$ 和 $\boldsymbol{D}$ 分别表示状态从 V 标记转移到 V 标记，V 标记转移到 T 标记，T 标记转移到 V 标记和 T 标记转移到 T 标记的转移概率。对于状态 j，定义预期滞留时间（Expected sojourn time）：

$$S_j = \begin{cases} \left(\sum_{k\in V\cup T}[\boldsymbol{C}|\boldsymbol{D}]_{(j,k)}\right)^{-1}, j \in T \\ 0, \qquad\qquad j \in V \end{cases} \tag{18}$$

由公式（11）可知，$[\boldsymbol{C}|\boldsymbol{D}]_{(j,k)}$ 为子阵 $\boldsymbol{C}$ 和 $\boldsymbol{D}$ 拼接以后的矩阵元素 (j,k)。V 标记的状态不存在滞留时间，即为 0。于是：

$$S_j = [\frac{1}{\tau^{\mathrm{f}}_{1,\mathrm{a}}}, \frac{1}{\tau^{\mathrm{f}}_{1,\mathrm{b}}}, \frac{1}{\tau^{\mathrm{f}}_{2,\mathrm{a}}}, \frac{1}{\tau^{\mathrm{f}}_{2,\mathrm{b}}}, \frac{1}{\tau^{\mathrm{w}}_{1,\mathrm{b}}}, \frac{1}{\tau^{\mathrm{w}}_{2,\mathrm{a}}}, \frac{1}{\tau^{\mathrm{w}}_{2,\mathrm{b}}}, \frac{1}{\tau^{\mathrm{w}}_{\mathrm{r}}}](j \in T) \tag{19}$$

对于 $j \in T$，基于传递矩阵的稳态概率 $\tilde{\pi}$ 满足：

$$\begin{cases} \tilde{\pi} \cdot \mathrm{P}' = \tilde{\pi} \\ \sum_{M_j \in T} \tilde{\pi} = 1 \end{cases} \tag{20}$$

其中：

$$\boldsymbol{P}' = \boldsymbol{D} + \boldsymbol{C}(\boldsymbol{I} - \boldsymbol{A})^{-1}\boldsymbol{B} \tag{21}$$

式中：$\boldsymbol{P}'$ 为 (8×8) 阶矩阵；$\boldsymbol{I}$ 为 (3×3) 阶的单位矩阵。本节介绍的稳态概率 $\boldsymbol{\pi}$ 由两部分决定，基于传递矩阵的稳态概率分布 $\tilde{\pi}$ 和对应状态的滞留时间 S_j。

于是有：

$$\pi_{j|j\in T} = \frac{\tilde{\pi}_j S_j}{\sum_{k\in T} \tilde{\pi}_j S_j} \tag{22}$$

影响因子 γ：

$$\gamma = \left(\frac{P_{\mathrm{LOL}}}{P_{\mathrm{Total}}}\right)^{L^*-1} \tag{23}$$

式中：P_{LOL} 和 P_{Total} 分别表示厂站丢失的负荷和总体负荷；L^* 为负荷运行点，表示当负荷升至原有负荷的 L^* 倍时，系统潮流计算结果不收敛。基于（22）和（23）的建模可以量化网络入侵攻击对变电站的影响[55-56]。Yang 在此基础上，继续研究网络攻击对母线差动保护的影响，分析了网络攻击变电站造成的断电故障以及重要保护设备的故障风险级别，基于传统的“*N-k*”思想提出“*S-k*”模型，成功筛选和判别重要的变电站节点[57-59]。

本小节重点阐述了基于 GSPN 概率模型的网络安全影响评估方法。通过求解马可夫状态转移矩阵的稳态概率来定义网络入侵攻击的概率，相较于上节基于 MTTC 的网络攻击概率，基于 GSPN 的入侵

概率能较好体现入侵攻击的状态转移过程并通过反映通信模型脆弱通信节点。但上述分析框架也存在局限性：基于GSPN或贝叶斯网络攻击图的概率模型都是理想模型，尽管采用了合理的假设，但缺少必要的历史和统计数据导致部分概率函数的参数不够准确；模型的检验大都基于系统稳态仿真计算，方法的有效性和灵敏性也缺乏验证。

3.2.3 基于信息物理融合仿真系统的安全建模

相较于上述方法，搭建CPS仿真系统的分析框架可以直接用来验证、测试攻击对系统运行的影响，得到结果也更直观、结论也更为准确性。Morris、Vellaithurai等学者基于RTDS搭建了基于广域测量系统（WAMS）架构的半实物仿真系统，将商业控制设备和量测装置的通讯协议整合到仿真系统的环境中，测试WAMS在不同攻击下的系统响应以及IDS的数据挖掘和路径挖掘结果，指出CPS耦合系统在广域保护系统和预防电力系统级联故障方面的有效性[60-61]。Wu分析了各类可控负荷面临的安全威胁与攻击成本，提出了可控负荷被恶意控制的攻击模型，验证了大规模的可控负荷遭受网络攻击可能造成低电压越限、三相不平衡等安全隐患[62]。Grilo和Cazorla通过搭建电力无线传感器网络的信息通信模型成功识别了关键的基础信息设施[63-64]。Hahn深入讨论了基于纵深防御机制的广域监控、保护、控制（WAMPC）系统的CPS攻击自愈控制思想（ARC），其中CPS网络威胁风险分析和系统的运行风险分析是ARC的关键[65-66]。

尽管基于CPS仿真系统的运行分析框架可以较好的模拟网络攻击对系统的影响，但模型对攻击机理的理论分析深度不够，导致其在处理新型的网络安全问题时不能体现攻击全貌以及潜在影响，无法有针对性提出防御方法。

3.2.4 基于信息物理融合系统的状态控制模型

传统的电力系统稳定研究与信息网络安全研究在理论和方法上一直存在着壁垒，搭建可行有效的CPS耦合模型是研究电力网络安全和风险分析的重要内容[67]。Zhao等学者利用微分代数方程组、有穷自动机、随机过程等数学工具，建立了稳态与动态的分析模型并给出了一般性的研究方法[67]。Guan和Liu团队提出了一种基于控制中心、物理设备、执行器与传感器构成的信息物理融合系统的控制模型，并从时间相关性和空间相关性等维度，将CPS攻击事件抽象为系统的控制流程，揭示了电力CPS网络攻击的控制机制[68]。

以离散时间的线性时不变系统为例，Liu给出了建模标准：

$$\boldsymbol{x}[k+1]=\boldsymbol{A}\boldsymbol{x}[k]+\boldsymbol{B}\boldsymbol{u}[k]+\boldsymbol{w}_x[k] \quad (24)$$

$$\boldsymbol{y}[k]=\boldsymbol{C}\boldsymbol{x}[k]+\boldsymbol{w}_y[k] \quad (25)$$

式中：$\boldsymbol{x}[k]\in\boldsymbol{R}^{n}$与$\boldsymbol{y}[k]\in\boldsymbol{R}^{m}$分别表示系统状态与传感器测量值；$\boldsymbol{u}[k]\in\boldsymbol{R}^{l}$为系统的控制信号输入；$\boldsymbol{A},\boldsymbol{B},\boldsymbol{C}$分别表示系统矩阵、控制矩阵与量测矩阵；$\boldsymbol{w}_x$和$\boldsymbol{w}_y$分别表示过程噪声和量测噪声。基于此，文献假定状态估计器可计算系统状态如下：

$$\hat{\boldsymbol{x}}[k+1]=\boldsymbol{L}_1(\hat{\boldsymbol{X}}[k],\boldsymbol{U}[k],\boldsymbol{Y}[k]) \quad (25)$$

式中：$\hat{\boldsymbol{X}}[k]$为$\boldsymbol{x}[k],k=0,1,\cdots k$组成的状态集合；同理$\boldsymbol{U}[k],\boldsymbol{Y}[k]$也为对应的状态集合。$\boldsymbol{L}_1(\cdot)$为抽象函数。系统的量测值残差为：

$$\hat{\boldsymbol{y}}[k+1]=\boldsymbol{L}_2(\hat{\boldsymbol{X}}[k],\boldsymbol{U}[k],\boldsymbol{Y}[k]) \quad (26)$$

$$\epsilon[k+1]=\boldsymbol{y}[k+1]-\hat{\boldsymbol{y}}[k+1] \quad (27)$$

式中：$\hat{\boldsymbol{y}}[k+1]$为第$[k+1]$时段量测预测值；$\boldsymbol{L}_2(\cdot)$为抽象函数；$\epsilon$是系统量测值残差，异常检测器基于残差额检测各种数据异常或FDI攻击。于是可知：若$-\epsilon_0<\epsilon<\epsilon_0$，则说明未检测到异常，即不存在数据篡改攻击；反之，则说明存在数据异常或篡改攻击。

基于状态分析的电力CPS控制理论不仅适用于传统分析中由于通信时延、中断等故障造成的系统运行影响，还揭示了电力CPS网络攻击对系统运行的控制机制。在发展智能电网、提高智能决策技术等方面具有广阔的应用前景。现有的电力系统分析与控制方法不能适当容纳电力信息系统的模型，这也是阻碍电力信息系统与电力系统深度融合并最终实现智能电网的主要障碍之一，目前仍在探索阶段[67]。

4 电力系统网络安全风险模型

4.1 电力网络安全概率风险评估框架

概率风险分析方法（PRA）最早于上世纪50由NASA提出，用以识别、定位系统工程中存在的潜在事故并估计其可能发生概率及后果，现已应用到航空航天、电力发电、化工和国防等多个领域[69]。Lin给出了电力基础设施网络安全PRA框架，即安

全风险值为安全事件的可能性与严重性乘积。但经典的PRA方法一般用于处理具有大数据库容量的安全问题，因为大量的历史数据可以帮助工程师搭建统计学模型来描述事件的可能性。然而在网络安全风险场景下，成功的网络入侵案例和样本较少，PRA难以直接应用。Lin通过事件树（Event tree）和故障树（Fault tree）搭建网络安全事故发生的具体模型，推导系统失效的根本原因，建立“顶事件”（Top event）演绎过程。在核电站的算例中，Lin定义了发电及机组故障的停工时间为风险事件的严重性，并基于蒙特卡洛法（MC）模拟得到停工时间占总体运行时间的7%，成功估计核电站的停工风险。

4.2　电力信息系统失效的安全风险建模

电力信息系统是由各个调度中心、发电厂、变电站内部各个子业务系统通过紧密且有序的互联网络构成的广域分布的综合系统。电力信息系统本身的安全风险也会对电力系统的工程安全产生重大影响。现有的风险管理标准主要采用的资产-风险-安全措施三元组合的列表归纳法，并没有搭建动态级联的风险管理和分析系统，同时难以量化信息系统的安全风险值[16]。Hu采用事件序列描述与系统安全相关行为的方法设计安全体系设计迹语言（SADTL），用以描述系统的结构、业务、安全策略、可能的攻击事件以及可用的措施等安全元素[70]。文献定义了角色、行为、事件、事件历史、迹和行为模式等12个维度，并将相对安全度定义为系统安全指标，其实质是：当系统采取安全措施后，攻击迹的总数占之前的比例。因此攻击迹的数量可以理解为系统抵御攻击的能力，越多的攻击迹表示该系统越脆弱，反之则越坚固。Hu指出配置广域网防火墙和分区局域网等措施最多可减少85%的攻击迹。

在此[70]基础上，Guo团队分析了变电站自动化系统（SAS）功能失效风险[71]。在t时刻，Guo给出了失效概率计算式：

$$p_{\mathrm{f}}(t)=1-\prod_{i=1}^{n}\left[1-p_{\mathrm{b}_i}(t)\right]\prod_{j=1}^{m}\left[1-p_{\mathrm{c}_j}(t)\right] \tag{28}$$

式中：p_{b_i}和p_{c_j}分别表示逻辑节点和逻辑连接的失效概率；逻辑节点和逻辑连接为SAS中各个通信节点和通信通道；n和m分别表示逻辑节点和逻辑连接的数量。SAS的失效功能价值参数为：

$$V_{\mathrm{f}}=V_{\mathrm{b}_{\max}}+\sum_{i=1}^{n-1}\frac{1}{n}\cdot V_{\mathrm{b}_i}\cdot\left(\frac{9-V_{\mathrm{b}_{\max}}}{9}\right) \tag{29}$$

式中：V_{b_i}为逻辑节点的价值；$V_{\mathrm{b}_{\max}}$为最大的逻辑节点价值；逻辑节点价值由SAS的机密性、完整性、可用性等级确定；常数9表示采用的9标度法。Guo团队基于上述价值和概率模型，对变电站内部署的电流保护、距离保护以及差动保护等设备进行系统分析，依据各个功能风险等级、风险传递权重以及风险残值确定系统的整体风险等级。

4.3　电力经济损失风险的金融保险建模

上述的网络安全风险分析方法均基于信息网络安全模型，在现有的资产管理、审计和二次系统风险模型研究中均有广泛应用[24]。为了更好的节省成本以及把控网络安全风险，国外电力企业和投资方开始重点研究基于经济损失的网络安全风险管理方案。购买电力网络安全金融保险成为除了传统的资产管理和审计、安全防护等措施以外保护电力资产、控制成本、限制事故损失的新型策略[72]。

由第3节的综述可知，CPS综合分析模型通过GSPN搭建的入侵攻击稳态概率模型可以较好地体现信息网络环境和系统运行之间的相关关系[55]。文献［58-59］进一步讨论了电力系统的关键变电站节点及其影响。在此基础上，文献［73］与［74］结合破产概率（Ruin probability），提出了网络安全事件的电力系统保险费用方案。

定义安全事件索赔额度（claim size）x为：

$$x=\mathrm{PL}\cdot H\cdot\gamma \tag{30}$$

式中：PL表示系统遭受网络攻击丢失的负荷（MW）；H表示系统恢复时间（h）；γ表示损失负荷的成本（$/MWh）。于是，破产概率模型可得：

$$\psi(u)=\frac{1-F_u}{1+\theta-f_0}-\frac{1}{1+\theta-f_0}\cdot\sum_{y=1}^{x}f_y\psi(u-y) \tag{31}$$

式中：$F_u=f_0+f_1+\cdots+f_u$，$\theta\epsilon(0,1)$，为自定义参数；选定适当的参数θ，可以通过迭代求解破产概率$\psi(u)$；f_u是在u时刻的离散概率分布。假设当选取合适的参数θ_{f}时，有最佳破产概率，则保险费用I为：

$$I=(1+\theta_{\mathrm{f}})\lambda\mu \tag{32}$$

式中：λ是网络攻击事件的频率期望；μ是索赔额度期望。部分破产概率和保险费用匹配方案如下：

作为一个有效的风险转移工具，金融保险框架

表2 IEEE测试系统的破产概率和保险费用匹配表

Tab. 2 Numerical results of ruin probability and feasible premium policy using IEEE test cases

IEEE 57-节电系统			IEEE 118-节电系统		
时刻(u)	θ	破产概率(ψ)	时刻(u)	θ	破产概率(ψ)
0	0.2	7.934×10^{-1}	0	0.2	7.999×10^{-1}
	0.6	5.614×10^{-1}		0.6	5.713×10^{-1}
	0.8	4.898×10^{-1}		0.8	4.999×10^{-1}
10	0.2	7.621×10^{-2}	10	0.2	4.860×10^{-2}
	0.6	5.033×10^{-3}		0.6	3.431×10^{-4}
	0.8	1.640×10^{-3}		0.8	2.154×10^{-4}
$\theta_f=0.8$		I=\$12,437	$\theta_f=0.8$		I=\$122,472

可以有效避免大规模的资源浪费。搭建电力系统网络安全的金融保险框架是探索网络安全风险管理手段的新方法。当变电站出现网络攻击，如线路中断，投资修建额外的备用线路是一个有效的防御手段，但在处理其他低可能性、高严重性安全事件时，大规模的投资可能不是最优方案。通过引入金融工具能有效刺激企业、设备供应商、保险公司对安全技术、关键节点进行有针对性的保护。

5 结论

电力系统网络安全风险分析研究是包括通信网络、自动控制、电气工程、风险管理等多领域在内交叉、融合的综合性课题[75-78]。它可以帮助电力企业分析、识别造成系统运行隐患的安全初始事件，探究安全事件的相关性，有效判别系统的脆弱节点和攻击手段，提升系统的主动防御能力。本文介绍了网络安全的总体风险分析框架并给出基于系统运行的风险分析定义，回顾了基于信息安全和CPS工程安全的综合安全研究，总结了现有系统风险评估和管理方法。

电力网络威胁大都具有隐蔽性、突发性和不确定性等特点，运维和监管部门无法提前准备安全事件的应急预案，处理网络攻击事件往往比较被动。未来的安全风险分析模型应该从信息安全和工程安全两个方面，分别开展降低安全事件可能性的关键信息节点研究和限制安全事件严重性的关键电气节点研究，综合得到“高危风险”的节点清单，并通过博弈论、强化学习等方法求解网络安全的最优应急决策，全面提高电力系统网络安全的综合防御能力。

提升电力网络安全分析和风险管理技术无论在学术界和工业界都是一项极具挑战的重大任务。随着人工智能技术的发展，现有的网络攻击者往往具有跨领域的专业知识，攻击更为智能，潜伏时间长，防御难度大，对电力系统的影响范围也更广。此外，由于可再生能源系统一般配备有丰富的电力电子元件，大量接入的新能源系统逐渐改变了传统电力能源的分布格局，减小了系统转动惯量，降低了系统稳定裕度。系统的动态不确定性增加了网络安全事件的风险隐患。未来的网络安全风险分析应在在传统的暂态、稳态分析基础上，增加可再生能源、储能设备等新兴电源的安全分析和测试，验证、修正现有的评估方法，完善网络安全分析模型。

参考文献：

[1] National Institute Standards and Technology (NIST). Guidelines for smart grid cyber security: Vol. 1, smart grid cyber security strategy, architecture, and high-level requirements: NISTIR 7628 [S]. U. S. A.: Department of Commerce Gary Locke, Secretary, August 2010.

[2] 中国信息物理系统发展论坛. 信息物理系统白皮书[EB/OL]. (2017-03-01)[2020-08-03]. http://www.cesi.ac.cn/201703/2251.html.
China Cyber-physical System Development Forum. Cyber-Physical System White Paper [EB/OL]. (2017-03-01)[2020-08-03]. httpss://www.innovation4.cn/library/r14012.

[3] 高昆仑,辛耀中,李钊,等. 智能电网调度控制系统安全防护技术及发展[J]. 电力系统自动化,2015,39(1):48-52.
GAO K L, XIN Y Z, LI Z, et al. Development and process of cybersecurity protection architecture for smart grid dispatching and control systems [J]. Automation of Electric Power Systems, 2015, 39(1): 48-52.

[4] United States Government Accountability Office. Critical infrastructure protection: actions needed to address significant cybersecurity risks facing the electric grid. [EB/OL]. (2019-08-26)[2020-08-03]. https://www.gao.gov/products/GAO-19-332.

[5] 汤奕,陈倩,李梦雅,等. 电力信息物理融合系统环境中的网络攻击研究综述[J]. 电力系统自动化,2016,40(17):59-69.
TANG Y, CHEN Q, LI M Y, et al. Overview on cyber-attacks against cyber physical power system [J]. Automation of Electric Power Systems, 2016, 40(17), 59-69.

[6] HOLLOWAY M. Stuxnet worm attack on Iranian nuclear facilities [EB/OL]. (2015-07-16)[2020-08-03]. http://large.stanford.edu/courses/2015/ph241/holloway1/.

[7] Cyber-attack Against Ukrainian Critical Infrastructure. Industrial control systems cyber Emergency response team (ICS-

CERT）[EB/OL]. (2016-02-25)[2020-08-03]. https://www.us-cert. gov/ ics/alerts/IR-ALERT-H-16-056-01.

[8] VAZ R. Venezuela suffers major power outages after alleged cyber attack [EB/OL]. (2019-03-10)[2020-08-03]. https://venezuelanalysis. com/news/14 374.

[9] WRITER S. City power hit by ransomware attack [EB/OL]. (2019-07-25)[2020-08-03]. https://www. itweb. co. za/content/GxwQDq1AnVWqlPVo.

[10] Cyber Security Intelligence. Cyber attack on a nuclear power plant [EB/OL]. (2019-11-08)[2020-08-03]. https://www. cybersecuri tyintelligence. com/blog/cyber-attack-on-a-nuclear-power-plant-4616. html.

[11] DENG R L, 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.

[12] HUG G. GIAMPAPA J A. Vulnerability assessment of ac state estimation with respect to false data injection cyber-attacks [J]. IEEE Transactions on Smart Grid, 2012, 3(3): 1362-1370.

[13] HENDRICKX J M, JOHANSSON H K, JUNGERS R M. Efficient computations of a security index for false data attacks in power networks [J]. IEEE Transactions on Automatic Control, 2014, 59(12): 3194-3208.

[14] TIAN J, TAN R, GUAN X H, et al. Enhanced hidden moving target defense in smart grids [J]. IEEE Transactions on Smart Grid, 2019, 10(2): 2208-2223.

[15] STAGGS J, FERLEMANN D, SHENOI S. Wind farm security: attack surface, targets, scenarios and mitigation [J]. International Journal of Critical Infrastructure Protection, 2017, 17(1): 3-14.

[16] National Institute Standards and Technology (NIST). Framework for improving critical infrastructure cybersecurity: NIST. CSWP. 04162018 [S]. U. S. Department of Commerce: National Institute of Standards and Technology, 2014.

[17] 中华人民共和国国家经济贸易委员会. 电网与电厂计算机监控系统及调度数据网络安全防护规定：中华人民共和国国家经济贸易委员会令第 30 号 [S]. 北京：国家经济贸易委员会, 2003.
State Economic and Trade Commission, PRC. Regulations on security protection of computer monitoring system and dispatching data network of power grid and power plant: order No. 30 of the State Economic and Trade Commission of the People´s Republic of China [S]. Beijing: State Economic and Trade Commission, 2003.

[18] 中国人民共和国国家电力监管委员会. 电力二次系统安全防护规定：监管委员会令第 5 号 [S]. 北京：国家电力监管委员会, 2004.
State Electricity Regulatory Commission, RPC. Safety protection regulations for power secondary systems: order No. 5 of the State Electricity Regulatory Commission [S]. Beijing: State Electricity Regulatory Commission, 2004.

[19] 中国人民共和国国家电力监管委员会. 电力行业信息系统安全等级保护基本要求：电监信息第 62 号 [S]. 北京：国家电力监管委员会, 2012.
State Electricity Regulatory Commission, RPC. Power industry information system security level protection basic requirements: Electricity Supervision Information No. 62 [S]. Beijing: State Electricity Regulatory Commission, 2012.

[20] 中华人民共和国国家发展和改革委员. 电力监控系统安全防护规定：中华人民共和国国家发展和改革委员会令第 14 号 [J]. 北京：国家发改委, 2014.
National Development and Reform Commission (NDRC). Safety protection regulation for power monitoring system: Order No. 14 of the national development and Reform Commission of the People´s Republic of China [J]. Beijing: NDRC, 2014.

[21] 全国人民代表大会常务委员会. 中华人民共和国网络安全法：中华人民共和国主席令第 53 号 [S]. 北京：全国人民代表大会常务委员会, 2017.
Standing Committee of the National People´s Congress. People´s Republic of China cyber security law: order no. 53 of the President of the People´s Republic of China [S]. Beijing: Standing Committee of the National People´s Congress, 2017.

[22] 中国国家标准化管理委员会. 信息安全技术网络安全等级保护基本要求：GB/T 22239—2019 [S]. 北京：国家市场监督管理总局、中国国家标准化管理委员会, 2019.
AdministrationStandardization. Information security technology —baseline for classified protection of cybersecurity: GB/T 22239—2019 [S]. Beijing: State Administration for Market Regulation and Standardization Administration, 2019.

[23] 丁伟, 唐洁瑶, 曹扬, 等. 电网信息物理系统网络安全风险分析与防护对策[J]. 电力信息与通信技术, 2018, 16(9): 33-38.
DING W, TANG J Y, CAO Y, et al. Network security risk analysis and protective countermeasures for power grid cyber physical system [J]. Electric Power Information and Communication Technology, 2018, 16(9): 33-38.

[24] 郭创新, 陆海波, 俞斌, 等. 电力二次系统安全风险评估研究综述 [J]. 电网技术, 2013, 37(1): 112-118.
GUO C X, LU H B, YU B, et al. A survey of research on security risk assessment of secondary system [J]. Power System Technology, 2013, 37(1): 112-118.

[25] 汤奕, 韩啸, 吴英俊, 等. 考虑通信系统影响的电力系统综合脆弱性评估 [J]. 中国电机工程学报, 2015, 35(23): 6066-6074.
TANG Y, HAN X, WU Y J, et al. Electric power system vulnerability assessment considering the influence of communication system [J]. Proceedings of the CSEE, 2015, 35(23): 6066-6074.

[26] 刘念, 张建华, 段斌, 等. 网络环境下变电站自动化通信系统

脆弱性评估[J]. 电力系统自动化,2008,32(8):28-33.
LIU N,ZHANG J H,DUAN B,et al. Vulnerability assessment for communication system of network-based substation automation system [J]. Automatiojkkjttn of Electric Power System, 2008,32(8):28-33.

[27] LIU N,ZHANG J H,ZHANG H,et al. Vulnerability assessment for communication network of substation automation systems to cyber attack [C]// Anon. 2009 IEEE/PES Power Systems Conference and Exposition,Seattle,WA,USA,March 15-18,2009. Seattle:IEEE,2009:1-7.

[28] LIU N,ZHANG J H,ZHANG H,et al. Security assessment for communication networks of power control systems using attack graph and MCDM [J]. IEEE Transactions on Power Delivery, 2010, 25(3):1492-1500.

[29] LEON DC D and ALVES-FOSS J. Modeling complex control systems to identify remotely accessible devices vulnerable to cyber attack [EB/OL]. (2002-11)[2020-08-03] https://www.semanticscholar. org/paper/Modeling-Complex-Control-Systems-to-Identify-to-Leon-Alves-Foss/2195d5c557771c2a05b482a4d020048aab2824fb.

[30] PIETRE-CAMBACEDES L, DEFLESSELLE Y, BOUISSOU M. Security modeling with BDMP:from theory to implementation [C]// Anon. 2011 Conference on Network and Information Systems Security, La Rochelle, France, May 18-21 2011. La Rochelle:IEEE,2011:1-8.

[31] SOMMESTAD T,EKSTEDT M,JOHNSON P. Combining defense graphs and enterprise architecture models for security analysis[C]// Anon. 2008 12th International IEEE Enterprise Distributed Object Computing Conference,Munich,Germany, September 15-19,2008. Munich:IEEE,2008:1-7.

[32] SOMMESTAD T,EKSTEDT M,NORDSTROM L. Modeling security of power communication systems using defense graphs and influence diagrams [J]. IEEE Transactions on Power Delivery,2009, 24(4):1801-1808.

[33] MCQUEEN M. A,BOYER W F,FLYNN M A,et al. Time-to-compromise model for cyber risk reduction estimation. In: Quality of Protection. Advances in Information Security [M]. USA, MA,Boston:Springer,2006.

[34] ZHANG Y C,WANG L F,XIANG Y M,et al. Inclusion of SCADA cyber vulnerability in power system reliability assessment considering optimal resources allocation [J]. IEEE Transactions on Power Systems,2106,31(6):4379-4394.

[35] ZHANG Y C,XIANG Y M,WANG L F. Reliability analysis of power grids with cyber vulnerability in SCADA system [C]// Anon. 2014 IEEE PES General Meeting,National Harbor, MD, USA, July 27-31, 2014. National Harbor: IEEE, 2014:1-5.

[36] ZHANG Y C,WANG L F,XIANG Y M,et al. Power system reliability evaluation with SCADA cybersecurity considerations [J]. IEEE Transactions on Smart Grid,2015,6(4):1707-1721.

[37] ZHANG Y C,WANG L F,XIANG Y M. Power system reliability analysis with intrusion tolerance in SCADA systems [J]. IEEE Transactions on Smart Grid,2016,7(2):669-683.

[38] NAZIR S,PATEL S,PATEL D. Assessing and augmenting SCADA cyber security:A survey of techniques [J]. Computers & Security,70(1):436-454.

[39] HEMINGWAY G,NEEMA H,NINE H,et al. Rapid synthesis of HLA-based heterogeneous simulation:a model-based integration approach [J]. Journal Simulation,88(2):217-232.

[40] QUEIROZ C, MAHMOOD A, TARI Z. SCADASim – a framework for building SCADA simulations [J]. IEEE Transactions on Smart Grid,2(4):589-597.

[41] Office of Electricity,Department of Energy(DOE). I national SCADA test bed [EB/OL]. (2009-09-16) [2020-08-03]. https://www. energy. gov/oe/technology-development/energy-delivery-ystems-cybersecurity/ national-scada-test-bed.

[42] AHRENHOLZ J, DANILOV C, HENDERSON T R, et al. CORE: a real-time network emulator [C]// Anon. MILCOM 2008 - 2008 IEEE Military Communications Conference, San Diego, CA, USA, November 16-19, 2008. San Diego: IEEE, 2009:1-7.

[43] DZUNG D,NAEDELE M,HOFF T P V,et al. Security for Industrial communication systems [J]. Proceedings of the IEEE, 2005,93(6):1152-1177.

[44] SRIDHAR S,HAHN A,GOVINDARASU M. Cyber-physical system security for the electric power grid [J]. Proceedings of the IEEE,2012,100(1):210-224.

[45] 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 T,TIAN J, WANG J Z,et al. Integrated security threats and defense of cyber-physical systems [J]. ACTA Automatica Sinica,2019,45(1):5-24.

[46] CIANCAMERLA E, MINICHINO M, PALMIERI S. Modeling cyber attacks on a critical infrastructure scenario [C]// Anon. IISA 2013, Piraeus, Greece,July 10-12,2013. Piraeus: IEEE ,2013:1-6.

[47] LIU S C,LIU X P P,SADDIK A E. Denial-of-Service (dos) attacks on load frequency control in smart grids [C]// Anon. 2013 IEEE PES Innovative Smart Grid Technologies Conference (ISGT), Washington, DC, USA, February 24-27, 2013. Washington:IEEE,2013:1-6.

[48] SARGOLZAEI A,YEN K,ABDELGHANI M N. Delayed inputs attack on load frequency control in smart grid [C]// Anon. ISGT 2014, Washington, DC, USA, February 19-22, 2014. Washington:IEEE,2014:1-5.

[49] KIM J and TONG L. On topology attack of a smart grid: undetectable attacks and countermeasures [J]. IEEE Journal on Selected Areas in Communications,2013,31(7):1294-1305.

[50] LIU Y, NING P, REITER M K. False data injection attacks against state estimation in electric power grids [J]. ACM Transactions on Information and System Security, 2011, 1(13): 13:1-13:33.

[51] DENG R L, 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.

[52] LI Z Y, SHAHIDEHPOUR M, ALABDULWAHAB A, et al. Bilevel model for analyzing coordinated cyber-physical attacks on power systems [J]. IEEE Transactions on Smart Grid, 2016, 7(5): 2260-2272.

[53] 吴文可，文福拴，薛禹胜，等. 基于多源信息的延时约束加权模糊 Petri 网故障诊断模型 [J]. 电力系统自动化，2013，37(24)：43-53.
WU W K, WEN F S, XUE Y S, et al. A weighted fuzzy petri net based model with time-delay constraints for power system fault diagnosis employing information from multiple sources [J]. Automation of Electric Power Systems, 2013, 37(24): 43-53.

[54] 叶丹丹，吴维敏，苏宏业. 标签Petri网的路径信息在故障诊断中的应用 [J/OL]. 控制与决策. Doi: 10. 13195/j. kzyjc. 2019. 0698.
YE D D, WU W M, SU H Y. Application of path information of labeled petri nets in fault diagnosis [J/OL]. Control and Decision. Doi: 10. 13195/j. kzyjc. 2019. 0698.

[55] TEN C W, LIU C C, MANIMARAN G. Vulnerability assessment of cybersecurity for SCADA systems [J]. IEEE Transactions on Power Systems, 2008, 23(4): 1836-1846.

[56] TEN C W, HONG J H, LIU C C. Anomaly detection for cybersecurity of the substations [J]. IEEE Transactions on Smart Grid, 2011, 2(4): 865-873.

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

[58] TEN C W, GINTER A, BULBUL R. Cyber-based contingency analysis [J]. IEEE Transactions on Power systems, 2016, 31(4): 3040-3050.

[59] YANG Z Y, TEN C W, GINTER A. Extended enumeration of hypothesized substations outages incorporating overload implication [J]. IEEE Transactions on Smart Grid, 2018, 9(6): 6929-6938.

[60] ADHIKARI U, MORRIS T, PAN S Y. WAMS cyber-physical test bed for power system, cybersecurity study, and data mining [J]. IEEE Transactions on Smart Grid, 2017, 8(6): 2744-2753.

[61] SRIVASTAVA A, MORRIS T, ERNSTER T, et al. Modeling cyber-physical vulnerability of the smart grid with incomplete information [J]. IEEE Transactions on Smart Grid, 2013, 4(1): 235-244.

[62] 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 Y B, LI J E, CHEN X, 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.

[63] GRILO A M, CHEN J M, DÍAZ M, et al. An integrated WSAN and SCADA system for monitoring a critical infrastructure [J]. IEEE Transactions on Industrial Informatics, 2014, 10(3): 1755-1764.

[64] CAZORLA L, ALCARAZ C, LOPEZ J. Cyber stealth attacks in critical information infrastructures [J]. IEEE Systems Journal, 2018, 12(2): 1778 - 1792.

[65] ASHOK A, HAHN A, GOVINDARASU M. Cyber-physical security of wide-area monitoring, protection and control in a smart grid environment [J]. Journal of Advanced Research, 2014, 5(1): 481-489.

[66] ASHOK A, GOVINDARASU M, WANG J H, et al. Cyber-physical attack-resilient wide-area monitoring, protection, and control for the power grid [J]. Proceedings of the IEEE, 2017, 105(7): 1389-1407.

[67] 赵俊华，文福拴，薛禹胜，等. 电力信息物理融合系统的建模分析与控制研究框架 [J]. 电力系统自动化，2011，35(16)：1-8.
ZHAO J H, WEN F S, XUE Y S, et al. Modeling analysis and control research framework of cyber physical power systems [J]. Automation of Electric Power Systems, 2011, 35(16): 1-8.

[68] 管晓宏，赵千川，贾庆山，等. 信息物理融合能源系统 [M]. 北京：科学出版社，2016.
GUAN X H, ZHAO Q C, JIA Q S, et al. Cyber-physical energy system [M]. Beijing: Science Press, 2016.

[69] LIN K, HOLBERT K E. PRA for vulnerability assessment of power system infrastructure security [C]// Anon. Proceedings of the 37th Annual North American Power Symposium, Ames, IA, USA, October 25, 2005. Ames: IEEE, 2005: 43-51.

[70] 胡炎，谢小荣，辛耀中. 电力信息系统建模和定量安全评估 [J]. 电力系统自动化，2005，29(10)：30-35.
HU Y, XIE X R, XIN Y Z. Modeling and quantitative security evaluation for electric power information systems [J]. Automation of Electric Power Systems, 2005, 29(10): 30-35.

[71] 郭创新，俞斌，郭嘉，等. 基于IEC 61850的变电站自动化系统安全风险评估 [J]. 中国电机工程学报，2014，34(4)：685-694.
GUO C X, YU B, GUO J, et al. Security risk assessment of the IEC 61850-based substation automation system [J]. Proceedings of the CSEE, 2014, 34(4): 685-694.

[72] MELAND P H, TONDEL I A, SOLHAUG B. Mitigating risk with cyberinsurance [J]. IEEE Security & Privacy, 2015, 13(6): 38-43.

[73] YANG Z Y. Cyber-based contingency analysis and insurance implications of power grid [D]. Houghton: Michigan Technological University, 2018.

[74] YANG Z Y, LIU Y, CAMPBELL M, et al. Premium calculation for insurance businesses based on cyber risks in IP-based power substations [J]. IEEE Access, in press.

[75] MRABET Z E, KAABOUCH N, GHAZI H E, et al. Cyber-security in smart grid: survey and challenges [J]. Computers & Electrical Engineering, 2018, 67(1): 469-482.

[76] HOLM H, FLORES W R, ERICSSON G. Cyber security for a smart grid-what about phishing? [C]// Anon. IEEE PES ISGT Europe 2013, Lyngby, Denmark, October 6-9, 2013. Lyngby: IEEE, 2014: 1-5.

[77] KNAPP E D, SAMANI R. Applied cyber security and the smart grid: implementing security controls into the modern power infrastructure [M]. Amsterdam: Elsevier, Syngress, 2013.

[78] ALOUL F, ALALI A R, ALDALKY R, et al. Smart grid security: threats, vulnerabilities and solutions [J]. International Journal of Smart Grid and Clean Energy, 2012, 1(1): 1-6.

作者简介：

杨至元

杨至元（通信作者）

1993-，男，土家族，湖南怀化人，中国能源建设集团广东省电力设计院博士后，美国密歇根理工大学博士，主要研究方向为电力系统网络安全和风险分析、机器学习、电力系统稳定计算等（e-mail）yangzhiyuan@gedi.com.cn。

（责任编辑　李辉）

基于网络安全风险事件的破产概率建模：(30)–(31)的推导过程

破产概率$\psi(u)$的定义如下：

$$\psi(u) = \Pr\{M > u\} = 1 - F_M(u) \tag{1}$$

式中：u为初始风险储备金；M表示最大损失总额：$M = L_1 + L_2 + \cdots + L_N$；$L_n$为独立同分布（i.i.d.）的单次损失且满足分布模型L，期望$\mu = E[L]$；$\Pr\{A\}$表示事件A发生的概率；$F_X(x) = \Pr\{X < x\}$表示事件X的累积分布函数（CDF）；N表示损失总额超过风险储备金之前，即破产发生之前的索赔次数。在连续时间破产模型中，损失模型满足复合泊松过程且无记忆性，则N服从$q = \psi(0) = 1/(1+\theta)$的几何分布，$\theta$为保险纯费率（premium load）：

$$Pr\{N = n\} = (1-q)q^n, n = 1, 2, \cdots \tag{2}$$

L_n的概率密度函数（PDF）可以写为：

$$f_L(x) = \frac{1 - F_L(x)}{\mu}, x > 0 \tag{3}$$

结合以上三式推导可知损失总额M的CDF为：

$$F_M(u) = \sum_{n=0}^{\infty} \Pr\{\sum_{k=1}^{n+1} L_k \leqslant u\} \Pr\{N = n\} \tag{4}$$

上式还可写为递推形式：

$$\begin{aligned} F_M(u) &= \sum_{n=0}^{\infty} \{\Pr\{\sum_{k=1}^{n+1} L_k \leqslant u\} \cdot \Pr\{N = n\}\} \\ &= \sum_{n=0}^{\infty} \{\Pr\{\sum_{k=1}^{n+1} L_k \leqslant u\} \cdot [(1-q)q^n]\} \end{aligned} \tag{5}$$

需要额外说明的是，分布函数$f_L(x)$是连续的，但为了推导出破产概率的递推计算公式，L_n的分布必须为离散的。由此，选取离散分布$\{f_x: x = 0, 1, 2\cdots\}$来匹配原分布函数$f_L(x)$中对应阶的中心矩（moment），即$f_x = f_L(x)$。综合以上公式，最终的破产概率为：

$$\psi(u) = \frac{1 - (f_0 + f_1 + \cdots f_u)}{1 + \theta - f_0} - \frac{1}{1 + \theta - f_L(0)} [\sum_{y=1}^{x} f_y \psi(u - y)] \tag{6}$$

由上式可知，通过调节保险费率θ可以得到不同的破产概率值，令$\theta = \theta_f$时，可获得合适的破产概率，则基本保费I为：

$$I = (1 + \theta_f) \cdot \mu \cdot \lambda \tag{7}$$

破产概率自上世纪初以来已经得到了广泛应用，其有效性和可行性已经在长期的投资组合评估中得到了验证。作为基础的保险精算函数，破产概率的主要功能是估计索赔总额超过初始风险储备金的概率，进而搭建初步的保险精算框架。

（杨至元）