网络安全实战攻防背景下电力系统网络安全体系建设

满翰林，王仲昌，栾　俊，郑林祥，吕　成，陈　伟
（中国长江电力股份有限公司，云南省昆明市，650200）

摘要　随着互联网的普及，电力信息网络已经成为电力系统运行的重要组成部分，作为重要基础设施，它在推动电网生产运营等全流程管理逐步迈入数字化、智能化时代的同时也面临着越来越多的安全威胁。本文提出了构建“识别(Identification)-保护(Protection)-检测(Detection)-响应(Response)”一体化的新型电力系统主动防御模型IPDR，从防御模型、方法技术、防御体系、影响分析四个角度对电力系统网络安全防护体系建设进行了探究，并展望了未来电力信息网络安全防护的发展趋势。

关键词　网络安全；实战攻防；电力系统；IPDR；网络安全体系

中图分类号：TM73　文献标识码：B
文章编号：1008-0899(2025)08-0013-03

随着电力系统向数字化和智能化的转型，信息技术与电力系统的实体设备之间的紧密结合催生了一种新型的电力系统，即信息物理融合系统。这种系统的主要目标是尽可能多地吸纳新能源，依托于一个坚固且智能的电网作为核心枢纽，并通过源网荷储的互动及多种能源的互补机制来实现其功能。该系统具备一系列优点，包括清洁、低碳、安全性、可控性、灵活性、高效率、智能化和开放性。但同时，信息物理的深度融合也引入了安全风险，使得电力系统从封闭的独立系统转变为与外部网络相连的开放系统，从而使得网络安全威胁有可能通过信息与物理的交互影响到电力系统的实体部分，引发运行中断、设备损坏或更严重的后果。

在电力系统不断推进智能化的背景下，确保其安全防护的重要性日益凸显。基于长期的运行经验和对电力系统风险的了解，已经建立了一套包括物理和信息层面防护的体系。然而，由于攻击与防御信息的不平衡、认知逻辑的不足以及与系统可用性需求的冲突，现有的防御体系并不能完全满足新型电力系统的安全防护需求。因此，研究并开发一种基于主动防御的新防御体系变得极为迫切。这种主动防御体系包括拟态防御、信任保护和内在安全等技术，它们具备动态的可靠性、强大的适应性和多维的防御能力，被视为解决新型电力系统安全问题的一种潜在解决方案。这些技术能够协调安全生命周期中的识别、保护、检测和响应等多个环节，以实现新型电力系统的全面主动协同安全防御[1]。

1　电力系统面临的安全问题和挑战

在新型电力系统中，电子通信和计算机技术的应用涉及了众多敏感数据和关键的安全利益。安全问题构成了该系统所面临的一个主要挑战，涉及物联网设备、通信协议和系统业务等多个层面。通过实地调研和对电力系统网络安全的深入研究，可以识别出以下几个主要的安全风险。

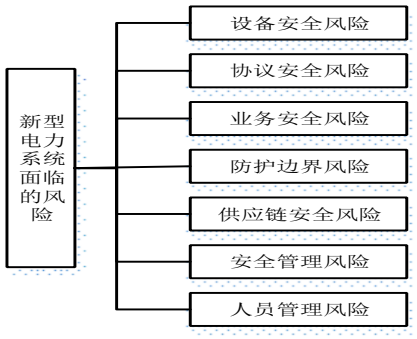

图1　新型电力系统面临的风险

1.1　设备层面的安全风险

基金项目：中国长江电力股份有限公司科研项目(Z542302006)

作者简介：满翰林(1990~)，男，重庆彭水人，本科，工程师，研究方向：网络安全。

电力系统中存在的漏洞往往难以完全避免,这些漏洞可能带来远程攻击和权限滥用等严重威胁,并且这些漏洞的数量还在不断增加。由于电力通信协议的多样性、系统软件更新的滞后性、设备长期使用的现实以及系统补丁兼容性的问题,电力系统的补丁管理变得复杂,难以及时修复关键漏洞。此外,许多电力系统软件的健壮性不足,它们只能在特定版本的操作系统上运行,系统升级可能导致关键设备和软件无法正常工作。

1.2 通信协议的安全风险

在设计电力通信协议时,通常更注重通信的实时性和可靠性,而对安全性的考虑可能不够充分。这包括缺乏强有力的认证和加密措施。特别是无线通信协议,更容易受到第三方的监听和欺骗性攻击。为了确保数据传输的实时性,一些通信协议可能会采用明文传输,这使得数据容易被攻击者截取和篡改。

1.3 业务流程的安全风险

新型电力系统的稳定运行依赖于多个业务系统,包括监控与数据采集系统、生产与调度系统、安全监控与报警系统以及电力市场管理系统等。这些系统各自承担着关键的功能和任务,对这些业务系统的攻击可能导致系统功能丧失,影响电力系统的稳定运行。攻击者可能会利用业务软件的逻辑漏洞和算法缺陷,执行错误数据注入、SQL注入、拒绝服务攻击、对抗样本攻击等,导致业务系统运行出错或功能丧失。

1.4 防护边界的安全风险

网络边界的安全防护高度依赖于管理措施,而实时监控和闭环控制的力度可能不足。现有的技术手段可能只能覆盖到网络边界的防护设备,而无法全面监控系统内部的服务器、工作站和网络设备。此外,对于外部网络访问、外部设备接入、用户登录、人员操作等事件的全面监测也存在不足,这限制了网络安全监控、报警、分析定位、追踪处置、审计溯源、风险核查和协同管控的能力。

1.5 供应链的安全风险

新型电力系统的供应链安全也是一个不可忽视的问题。由于电力系统供应链的复杂性,不可靠的供应商可能为攻击者提供机会。攻击者可能通过在供应链中植入恶意代码或硬件后门等方式发起攻击,从而威胁电力系统的安全。

1.6 安全管理的风险

缺乏分层和分级的安全管理机制可能导致管理难度增加。在电力行业中,由于工作站、服务器和网络设备的数量庞大,需要一个统一的管理平台来进行管理。在电力系统的资产管理、安全策略管理、账户管理、配置管理、日志管理、日常操作等方面,缺乏统一的技术手段和管理方法,也无法对日志、监测和报警数据进行有效的分析和统计。

1.7 人员管理的风险

电力系统的员工可能缺乏必要的网络安全知识,安全防护意识不强,相关的安全技术能力不足,安全技术操作不够熟练。这可能导致外部人员进行无意的、错误的或非法的操作,增加了安全风险。

2 构建新型电力系统主动防御技术体系

本文档针对信息物理融合的电力系统在网络安全方面的挑战和防护需求,提出了一个综合的主动防御框架,即IPDR模型。该模型由四个关键组成部分构成:识别、保护、检测和响应。IPDR框架旨在为电力系统的关键技术,如分布式发电、远距离输电、智能化配电和广泛测量等,提供全面的安全保障。通过识别电力系统中存在的潜在安全风险,建立安全基准和漏洞数据库,进行风险评估和预案制定,该模型利用自动化和智能化的保护机制,探索新的入侵检测技术,确保在系统遭受入侵或出现漏洞时,能够及时进行安全威胁的响应和处理。此外,IPDR模型还包括启动相应的保护措施和防御设备,以实现对电力系统的设备、网络、控制和业务层的全面覆盖,构建起对未知安全威胁的全面防护,如图2所示。

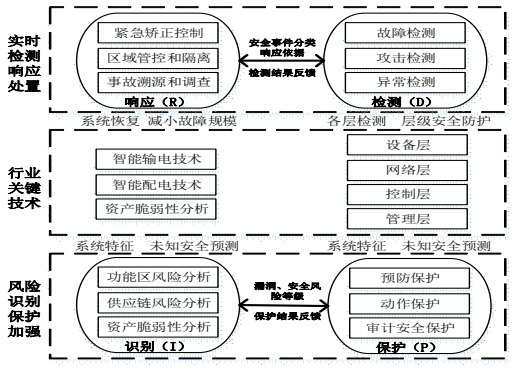

图2 新型电力系统IPDR主动防御模型

在IPDR模型的指导下,电力系统需进行全面的

安全风险评估，以识别潜在的安全威胁和脆弱环节。基于评估结果，制定全面的安全策略，这些策略不仅包含防护措施，也包括检测和响应机制。在电力系统的关键环节部署先进的入侵检测系统，以便实时监控网络活动并及时发现异常行为。同时，应建立一个快速反应团队，以便在检测到安全事件时能够迅速采取行动，减少损害并恢复系统运行。IPDR模型还特别强调了在发生安全事件后恢复阶段的重要性，指出电力系统应具备弹性设计，即使在遭受攻击后也能维持关键功能，并能迅速恢复至完全功能状态。

为了实现动态的安全循环，电力系统的安全策略和措施需要持续更新和改进。这需要一个持续的安全管理流程，通过不断收集和分析安全事件数据，定期进行系统漏洞扫描和安全演练，以提升系统的整体安全性能。IPDR模型为电力系统提供了一个全面的安全防护框架，通过不断的评估、防护、检测、响应和恢复，有效提升了系统的安全防护能力和适应性。随着技术进步和威胁环境的演变，IPDR模型也需要不断进化，以确保电力系统能够应对日益复杂的网络安全挑战[3]。

3　关键技术分析

3.1　基于攻击图的网络脆弱性分析技术

在识别新型电力系统通信网络的安全风险方面，可以采用基于攻击图的网络脆弱性分析技术。该技术通过结合电力系统网络的详细信息和潜在攻击者的行为特征，构建攻击图模型。利用特定的算法来生成可能的攻击路径，并通过设置最大跳数和最低可达概率作为筛选条件，有效控制攻击图的复杂度。在分析阶段，使用生成的攻击图来评估网络节点的重要性、可达性以及对整体网络的影响。

3.2　新型电力系统的攻击行为审计技术

新型电力系统在日常运作中涉及设备间的物联通信和调度人员的决策指令，这会产生大量的系统数据和运行日志。通过分析这些海量日志，可以利用OCSVM算法为每个用户建立行为特征分类器，并对潜在的滥用行为进行预警。这种方法有助于预警个人攻击行为，检测不当的操作指令，识别数据篡改行为，审计操作人员的行为，并制定相应的安全预案。

3.3　人工智能在数据保护中的应用技术

在电力系统中，人工智能的应用可能在模型训练和测试阶段导致数据隐私泄露。这包括在模型参数更新时泄露训练数据信息，以及在测试阶段模型返回查询结果时泄露数据。即使在没有直接遭受攻击的情况下，AI模型的正常运行也可能间接导致数据隐私泄露。

3.4　电力系统连锁故障的动态建模技术

电力系统中复杂的继电保护设备给连锁故障的动态建模带来了挑战。为了应对这些挑战，研究人员开发了一种基于交流潮流模型的级联故障继电保护动态模型。该模型侧重于继电器的建模，并利用交流潮流计算来获得精确的潮流值，以此来确定继电保护动作后的支路状态。模型包括三种类型的继电保护：距离保护、纵联距离保护和累积过负荷保护。纵联距离保护和距离保护是输电线路的主要和备用保护，而累积过负荷保护则代表传输线因过热下垂至植被导致分支关闭。该模型能够基于电网的动态数据和初始扰动，计算级联故障过程中触发事件的影响[4]。

4　结语

随着信息网络安全威胁的日益增加，电力系统的信息网络安全防护变得越来越重要。这是一个长期且复杂的过程，需要采取全面和多层次的防护措施。只有通过不断的技术创新和行业合作，设计适用于新型电力系统的网络安全防护体系架构，攻关关键技术，探索新业务场景下的网络安全防护方案，推进安全防护措施的试点和普及，才能全面提升电力系统的网络安全防护能力，确保系统的安全稳定运行。

参考文献

[1] 唐亚东，刘寅，杨维永.基于等级保护网络安全体系的新型电力系统风险分析与防范[J].网络安全技术与应用.2023(12):130-133.

[2] 张学松，郑嘉璐.电力信息网络安全防护体系建设策略探究[J].网络安全技术与应用.2023(12):104-105.

[3] 徐植，陈俊，张智勇，万俊岭，袁培森.新型电力系统中基于人工免疫和隐马尔可夫的网络安全态势评估[J].华东师范大学学报(自然科学版).2023(05):182-192.

[4] 蒲建发，郭敬东，罗富财，张斌，闫东.面向新型电力系统的光伏电站监控系统网络安全防御体系分析[J].数字技术与应用.2023，41(03):231-233.