电力工控网络安全预测

孙 杰[1] 贾壮志[2]
1. 杭州飞钛航空智能装备有限公司 浙江 杭州 311215
2. 浙江大丰实业股份有限公司杭州分公司 浙江 杭州 310000

摘 要：电力工控网络安全面临多重威胁，未来预测技术将向智能化、精准化方向发展。利用人工智能技术提升预测精度，加强对新型威胁的研究，同时推动安全标准化建设，成为关键趋势。通过智能算法分析数据，识别潜在威胁；研究新型攻击手段，提升防御能力；建立安全标准体系，规范各环节操作，确保电力工控网络稳定运行。

关键词：电力；工控网络；安全预测

1 电力工控网络的特点

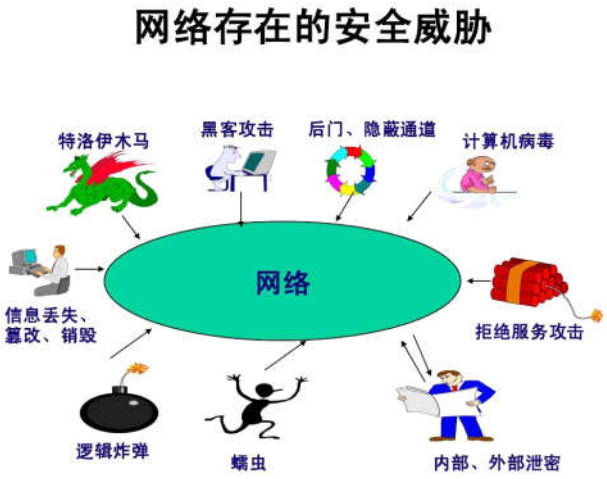
电力工控网络作为工业控制系统中的重要组成部分，具有一系列独特的特点，（1）高实时性：电力工控网络对数据传输的实时性要求极高。在电力系统中，如电网调度、设备监控、故障检测等环节，都需要实时获取和传输数据，以便快速响应并作出相应处理。这种高实时性确保了电力系统的稳定运行和故障的快速恢复。（2）高可靠性：由于电力系统的关键性，电力工控网络必须具备极高的可靠性。网络中的设备、协议和架构都需要经过严格的测试和验证，以确保在极端条件下仍能正常工作。冗余设计、备份机制等也是提高网络可靠性的重要手段。（3）高安全性：电力工控网络面临着复杂的安全威胁，包括黑客攻击、病毒入侵等。电力工控网络在设计时必须充分考虑安全性问题，采用加密技术、访问控制、安全审计等措施来保护网络和数据的安全。（4）环境适应性：电力系统通常部署在复杂多变的环境中，包括恶劣的户外环境、电磁干扰等，电力工控网络需要具备良好的环境适应性，能够抵抗各种不利因素的影响，确保网络的稳定运行[1]。（5）远程监控和管理：电力工控网络支持远程监控和管理功能，使得电力运维人员可以远程监控电力系统的运行状态、诊断故障、调整参数等。这种远程监控和管理能力大大提高了电力运维的效率和便捷性。

2 电力工控网络安全预测的重要性

电力工控网络安全预测的重要性不言而喻，它直接关系到电力系统的稳定运行和国家能源安全。在高度信息化的今天，电力工控系统日益依赖于计算机网络技术来实现远程监控、自动化控制和数据交换，但同时也面临着前所未有的网络安全威胁。电力工控网络安全预测至关重要，它关乎电力系统的平稳运行及国家能源基石的安全。随着信息化深化，电力工控系统高度依赖网络实现智能化操作，却也暴露了前所未有的安全脆弱点。精准预测网络安全威胁，不仅预防潜在损害，还保障电网连续供电，维护社会秩序与经济稳定。因此，强化安全预测能力是保障电力工控安全、护航国家能源战略的关键一环。

3 电力工控网络安全的主要威胁

在探讨电力工控网络安全的议题时，不得不正视其面临的多种复杂且严重的威胁。这些威胁不仅可能直接损害电力系统的正常运行，还可能对国家安全、经济稳定以及民众生活造成深远影响。



网络存在的主要威胁如图所示

3.1 黑客攻击和恶意软件感染

黑客攻击是电力工控网络安全面临的最为直接和严峻的威胁之一。随着网络技术的飞速发展，黑客们的攻击手段也日益复杂多变，他们利用各种技术手段试图渗透进电力工控系统，窃取敏感信息、破坏系统稳定或实施勒索等恶意行为。对于电力工控系统而言，一旦遭受黑客攻击，可能导致控制指令被篡改、关键数据被窃取或系统瘫痪等严重后果，进而影响到电力的稳定供应和

电网的安全运行。恶意软件感染则是黑客攻击的常见手段，恶意软件包括但不限于病毒、蠕虫、特洛伊木马、勒索软件等，它们通过伪装成合法软件、利用系统漏洞或欺骗用户点击恶意链接等方式侵入系统，并在系统中潜伏、传播和破坏。在电力工控系统中，恶意软件可能破坏控制逻辑、篡改参数设置、窃取运行数据，甚至直接控制电力设备，造成不可估量的损失。

3.2 物理和逻辑漏洞的利用

电力工控系统在设计、部署和运维过程中，难免存在各种物理和逻辑漏洞。这些漏洞可能源于系统设计的不完善、硬件设备的缺陷、软件编程的错误、配置管理的疏忽等多个方面。物理漏洞主要涉及系统硬件的安全性问题，如设备的安全防护不足、物理访问控制不严等。攻击者可能通过直接接触硬件设备，如篡改传感器数据、破坏控制线路等方式，对电力工控系统实施攻击。而逻辑漏洞则更多地与软件系统和网络协议相关，如代码中的安全缺陷、协议实现的不当等。攻击者可以利用这些漏洞，通过发送恶意数据包、执行未授权命令等方式，对电力工控系统进行远程攻击。

3.3 供应链安全问题

供应链安全问题是电力工控网络安全中不容忽视的一个方面。在电力工控系统的构建和运维过程中，往往需要采购大量的硬件设备、软件系统和第三方服务。这些供应链环节中的任何一个出现安全问题，都可能对电力工控系统的整体安全造成威胁。供应链安全问题可能表现为多种形式，如供应商恶意植入后门、使用存在安全漏洞的组件、未经充分测试的产品被部署到系统中等。这些问题可能导致电力工控系统被植入隐蔽的恶意代码、控制逻辑被篡改或系统性能下降等后果。更为严重的是，一旦供应链中的某个环节被恶意势力控制，整个电力工控系统就可能面临被全面渗透和攻击的风险。

4 电力工控网络安全预测技术

在电力工控网络领域，安全预测技术扮演着至关重要的角色，它们通过提前识别潜在威胁、评估风险并采取相应的预防措施，为电力系统的稳定运行提供坚实保障。

4.1 安全漏洞扫描和评估技术

安全漏洞扫描和评估技术是电力工控网络安全预测的基础。这些技术通过自动化工具或专业团队对电力工控网络进行全面扫描，以发现可能存在的安全漏洞和弱点。漏洞扫描工具能够模拟黑客攻击行为，对系统的每一个组件进行细致检查，识别出未打补丁的软件、配置错误、弱密码等安全隐患。评估技术则在此基础上，对发现的漏洞进行风险评估，确定其可能造成的危害程度，并为后续的安全加固和修复工作提供指导。安全漏洞扫描和评估技术的优势在于其全面性和及时性，通过定期或不定期的扫描和评估，可以及时发现并修复潜在的安全问题，避免黑客利用这些漏洞对电力工控网络发起攻击。同时这些技术还可以帮助电力企业了解自身安全状况，为制定更为有效的安全策略提供依据[3]。

4.2 入侵检测系统

入侵检测系统是电力工控网络安全预测的重要组成部分。该系统通过实时监控网络流量、系统日志和异常行为等信息，及时发现并响应潜在的入侵行为。入侵检测系统包括基于签名的检测和基于行为的检测两种模式。基于签名的检测通过比对已知的攻击模式和特征来识别入侵行为；而基于行为的检测则通过分析异常行为来发现潜在的威胁。在电力工控网络中，入侵检测系统尤为重要，由于电力工控系统通常具有高度的实时性和复杂性，一旦遭受入侵可能导致严重的后果，通过部署入侵检测系统，可以实现对电力工控网络的全方位监控和防护。当系统检测到潜在的入侵行为时，会立即触发警报并采取相应的防御措施，如阻断攻击源、记录攻击信息等，以确保电力工控网络的安全稳定运行。

4.3 安全事件日志分析技术

安全事件日志分析技术是电力工控网络安全预测的重要手段之一。在电力工控网络中，各种设备和系统都会生成大量的日志信息，这些日志记录了系统的运行状态、用户活动、安全事件等重要信息。通过对这些日志进行深入分析，可以发现潜在的安全威胁和异常行为模式。安全事件日志分析技术通常包括日志收集、预处理、分析和报告等步骤。首先，通过日志收集工具将分散在各个设备和系统中的日志信息集中起来；然后，对收集到的日志进行预处理，去除冗余和噪声数据；接着，利用日志分析工具对预处理后的日志进行深入分析，识别出潜在的安全威胁和异常行为模式；最后，将分析结果以报告的形式呈现出来，为安全管理人员提供决策支持。安全事件日志分析技术的优势在于其强大的数据处理能力和智能分析能力，通过运用先进的算法和模型，可以实现对海量日志数据的快速处理和精准分析，从而发现隐藏在数据背后的安全威胁和异常行为模式。此外，该技术还可以与入侵检测系统等其他安全工具相结合，形成更为完善的安全防护体系，为电力工控网络的安全稳定运行提供有力保障。

4.4 安全态势感知与可视化技术

安全态势感知技术是一种综合性的安全监控方法，它通过对电力工控网络中的各种安全要素进行实时监

测、分析和综合评估，形成对网络整体安全态势的清晰认知。结合可视化技术，可以将安全态势以图形化、直观化的方式呈现出来，帮助安全管理人员快速了解网络的安全状况，并作出及时的决策。这种技术不仅提高了安全管理的效率，还增强了安全管理的科学性和精准性。

4.5 威胁情报共享与协同防御技术

在电力工控网络领域，威胁情报的共享和协同防御是至关重要的。通过建立威胁情报共享平台，电力企业可以实时获取到国内外最新的安全威胁情报和防御经验，及时了解和应对新型的安全威胁。同时，通过与行业内其他企业、安全厂商以及政府监管部门的协同合作，可以形成联防联控的防御机制，共同提升电力工控网络的安全防护能力。在电力工控网络领域，威胁情报共享与协同防御是构建安全防护网的关键。通过建立高效的共享平台，电力企业能够即时掌握国内外安全威胁动态，借鉴先进防御经验，迅速调整策略以应对新挑战。另外，跨企业、跨行业的紧密合作，不仅促进情报的快速流通，还加强技术、资源及策略的协同，构建了覆盖全面的联防联控体系。这种机制有效提升电力工控网络的整体防御水平，保障了电网运行的安全与稳定。

5 未来电力工控网络安全预测发展

5.1 利用人工智能技术提升安全预测精度

在未来，电力企业将深度整合人工智能技术，如机器学习、深度学习等，以构建更高效的网络安全预测系统。通过持续监控和分析网络数据流、设备状态、用户行为等多维度数据，AI模型能够自动识别异常模式，提前预警潜在的安全风险。AI算法还能自我优化，不断提高识别新型威胁的能力，确保预测精度与时俱进，为电力工控网络筑起一道智能化的安全防线。

5.2 加强对新型网络安全威胁的研究

面对不断演进的网络攻击手段，电力企业将加大对新型安全威胁的研究力度，包括但不限于对APT攻击、勒索软件变异、物联网设备漏洞利用等威胁的深入分析。通过建立专门的威胁情报中心，与国内外安全专家保持紧密合作，共享最新威胁信息和防御策略，提升对新兴威胁的响应速度。同时，企业将加大在安全研发方面的投入，开发针对性的防护工具和技术，确保电力工控网络在面对未知威胁时能够迅速应对。

5.3 推动安全标准化建设

为了进一步提升电力工控网络的安全性，未来电力企业将积极投身于安全标准化建设，致力于制定和完善一系列行业安全标准和规范。这些标准将覆盖网络架构设计、设备选型、系统部署、运维管理等多个方面，为电力工控网络的安全运维提供明确指导。通过加强安全培训和教育，提高全体员工的安全意识和操作技能，形成从上至下的安全文化。此外，电力企业还将积极与政府、行业协会等合作，推动安全标准在行业内的广泛应用，共同提升电力工控网络的整体安全水平。

结束语

面对不断演变的网络安全挑战，电力工控网络安全预测技术的发展至关重要。通过技术创新和标准建设，能够更有效地抵御潜在威胁，保障电力系统的安全稳定运行。未来，电力企业需持续投入研发，加强国际合作，共同构建更加安全、可靠的电力工控网络环境，为经济社会的发展提供坚实支撑。

参考文献

[1]汤震宇,曹翔,林青,等.海外电力工控网络安全规范比较及安全方案探讨[J].网络安全技术与应用,2020(2):133-135.

[2]陈斌.电力企业信息网络安全风险分析与管控研究[J]. 百科论坛电子杂志,2020(15):1917.

[3]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.

[4]于洪飞.工业物联网技术的应用及发展[J].由子技术与软件工程,2019(08):20.