工业互联网与光伏制造业融合网络安全防护研究

张俊星，鄢宇寒，周继帅

（中电建武汉铁塔有限公司，湖北 武汉 431400）

摘 要 工业互联网与光伏制造业融合，涉及大量的物联网设备和传感器，这些设备和传感器连接到网络，形成一个复杂的系统。网络安全防护研究可以帮助防止对这些设备的未经授权访问和攻击，确保生产设备和数据的安全与保密。本文深入分析光伏制造业与工业互联网融合现状，针对常见的网络安全风险，通过优化安全防护策略，构建安全防护管理体系等方式，融合工业互联网与光伏制造业，旨在对为人们提供行之有效的网络安全防护服务有所裨益。

关键词 工业互联网；光伏制造业；网络安全防护；光伏支架

中图分类号：TP393.08 **文献标志码**：A **文章编号**：2097-3365(2024)09-0025-03

工业互联网与光伏制造业的融合，给光伏制造企业带来了巨大的机遇，同时也带来了网络安全威胁。光伏制造业的信息系统和设备的安全防护面临着越来越严峻的挑战。光伏制造企业面临的网络安全威胁主要包括黑客攻击、恶意软件感染以及数据泄露等问题。为了保障光伏制造业的网络安全，需要重点关注光伏制造业融合网络安全防护问题。该研究旨在针对光伏制造业的特点和需求，深入分析并建立有效的网络安全防护体系。通过采取合理的网络安全措施，保障企业信息系统和设备的安全性和可靠性，确保光伏制造业与工业互联网的融合发展能够顺利进行。

1 光伏制造业与工业互联网融合现状

1.1 产业发展趋势

近年来，光伏制造业在全球范围内迅速发展成为推动绿色能源转型的重要力量，特别是工业互联网技术的引入，为光伏制造业带来了革命性的变革。通过高度的信息化和自动化，生产效率得到极大提升且生产成本逐步降低，光伏产品的市场竞争力不断增强，数据驱动的决策模式逐渐成为企业发展的新常态，实现了从传统制造向智能制造的转变。在此背景下，光伏制造业开始重视研发投入，不断优化产品性能，延伸产业链。光伏组件的转换效率不断提高，应用领域也在不断拓宽，从屋顶发电系统到大型地面电站再到光伏建筑一体化，光伏制造业正逐步实现多元化发展。此外，随着数字化转型的深入，光伏企业开始探索基于互联网的新型商业模式，如云计算、大数据、物联网技术在光伏制造、监控和维护中的应用，这些都大幅提升了光伏制造业的整体效率，提高了经济效益。

1.2 技术融合挑战

尽管工业互联网为光伏制造业带来了巨大的发展机遇，但在技术融合过程中也面临诸多挑战，首要挑战是数据安全和隐私保护问题，在高度网络化的生产环境中，大量敏感数据的产生和流通，使得光伏制造企业面临更高级别的数据保护需求，如何确保数据在传输和存储过程中的安全，防止数据泄露和滥用，成为技术融合中亟待解决的问题。技术标准不统一、设备互联互通性差，也是光伏制造业面临的挑战之一，不同设备和系统之间的兼容性问题影响了信息的流畅交换和资源的高效利用，从而限制了工业互联网技术在光伏制造领域的深度应用[1]。

此外，人才短缺也是制约光伏制造业与工业互联网深度融合的关键因素，随着技术融合的不断深入，对于具有跨学科知识背景的人才需求日益增加，不仅需要掌握光伏技术的专业人才，更需要懂得信息技术、数据分析等领域的复合型人才，以推动光伏制造业的持续创新和发展。光伏制造业与工业互联网的融合，虽然展现出巨大的发展潜力，但在实际操作过程中还面临多方面的挑战。针对这些挑战需要光伏制造业和信息技术行业的共同努力，通过技术创新和制度创新来逐步解决以促进两者的深度融合，共同推动光伏制造业的持续健康发展。

2 网络安全风险分析

2.1 安全威胁识别

在光伏制造业与工业互联网的融合过程中面临着多样化的网络安全威胁，这些威胁源于多个方面，包括恶意软件、网络钓鱼攻击、内部数据泄露以及服务拒绝攻击等。恶意软件通过病毒、蠕虫、木马等形式侵入网络破坏系统正常运行窃取敏感数据；网络钓鱼攻击通过伪装成合法实体诱导员工泄露个人信息；内部数据泄露可能来源于员工的误操作或有意为之，造成重要数据外泄损害企业利益；服务拒绝攻击通过大量非法请求占用网络资源影响企业服务的正常提供[2]。

除了上述直接攻击外，还应关注到间接威胁，如供应链攻击通过攻击企业供应链中的薄弱环节间接影响目标企业的网络安全。此外，随着物联网设备在光伏制造业的广泛应用，设备安全漏洞也成为攻击者利用的新途径，这些设备通常缺乏足够的安全保护措施，成为网络安全的薄弱环节，面对这些复杂多变的网络安全威胁，需要通过持续的监控、定期的安全评估和快速响应机制，有效识别和应对可能的安全威胁并保障企业网络环境的安全稳定。

2.2 风险影响评估

网络安全风险对光伏制造业产生的影响是全方位的，数据泄露或损坏会直接影响企业的运营安全，涉及财务信息、客户数据、研发成果等被泄露，会对企业声誉和经济状况造成重大损害，生产系统的瘫痪或损坏会导致生产停滞，影响供应链的正常运作，进而影响到产品交付时间和产品质量，损害企业的市场竞争力。此外，网络安全事件的处理成本高昂，不仅包括技术解决方案的成本，还包括法律诉讼、客户赔偿等后续成本，长远来看，频繁的网络安全事件会削弱客户和合作伙伴对企业的信任度，影响企业的长期发展[3]。

网络安全风险的影响是多方面的，不仅限于直接的经济损失，还包括企业声誉的损害、客户信任度的下降等，因此，对于光伏制造业而言，加强网络安全防护，建立完善的风险评估和应对机制是确保企业长期稳定发展的必要条件，通过深入分析网络安全风险的可能来源和影响，企业可以更有针对性地采取措施有效减少网络安全事件的发生并保障企业和客户的利益。

3 网络防护技术研究

3.1 防护技术措施

在光伏制造业这一高科技领域中，精心挑选与周到部署网络防护领域的技术措施，对于确保企业信息系统的安全具有至关重要的意义。由于该行业的信息网络安全性不仅直接影响日常生产活动的顺利进行，还涉及商业机密和个人数据的保护，因此，采取切实有效的防护措施显得尤为重要。边界防护作为第一道防线，通过安装最新的防火墙和入侵检测系统有效拦截未经授权的访问尝试，为企业网络提供了强大的安全隔离屏障，而数据加密技术则在数据的传输和存储过程中提供加密保护，确保敏感信息即便在被截获的情况下也无法被解读[4]。

访问控制机制通过限制只有授权用户才能接触到关键系统资源，进一步强化了内部安全管理，同时安全监控系统的实施，通过对网络行为的实时监控能够及时发现异常行为并迅速采取响应措施，从而大幅度降低了潜在安全威胁的风险。此外，定期的安全审计和风险评估也是不可或缺的部分，它们帮助企业持续了解和评估防护措施的有效性，确保随着网络环境和外部威胁的变化，能够及时调整和优化安全策略，这些防护技术措施的整合应用，不仅为光伏制造业提供了坚实的网络安全保障，也促进了企业对于信息技术的信心，使得企业能够更加专注于核心业务的创新与发展，而不必过度担忧网络安全问题，通过持续投资于网络安全技术，光伏制造业能够在保护关键资产和促进产业发展之间找到一个理想的平衡点。

3.2 技术创新与经济效益

技术创新在增强网络防护能力的同时对企业经济效益的正面影响不容忽视，随着新兴技术尤其是人工智能和机器学习技术在安全防护领域的应用，企业得以采用更加智能化的手段进行威胁检测和响应，这些技术能够自学自适应不断优化威胁识别模型，有效提升了识别精准度和响应速度且显著降低了因延迟响应对企业造成的负面影响，自动化的威胁识别和处理机制不仅减少了对人工操作的依赖，降低了错误响应的可能，也大幅提升了企业防护系统的效率[5]。

此外，技术创新通过简化和自动化安全运维流程，有效减轻了对高级安全专业人才的需求，从而显著节约企业的人力资源成本，同时这一系列的技术进步也加强了企业的数据保护能力，增强了客户对企业处理个人和敏感数据能力的信心，有助于构建良好的商业信誉和品牌形象，在竞争激烈的市场环境中，这种信任感成为企业获得竞争优势的关键因素之一。坚实的网络安全基础能够吸引更多的合作伙伴和客户，开辟新的市场机会并促进企业销售增长和市场份额的扩大。

4 网络防护策略与管理

4.1 防护策略制定

在制定网络防护策略时要重点关注对光伏制造业中核心资产的保护，分析历史数据，识别过往攻击案例中的共同点和独特性以形成针对性的防护措施，探

讨不同层面的防护技术，如入侵检测系统、防火墙以及加密技术的综合应用，强调在全面评估网络环境的基础上，依据资产的价值、易受攻击的风险等级以及业务连续性的要求，定制策略[6]。

针对防护策略分析了综合应用多种技术的重要性，例如通过设置多层防护机制构建深度防御体系，在外围网络部署防火墙，内部网络采用入侵检测系统，对敏感数据进行加密处理，确保数据在传输和存储过程中的安全，同时考虑到物联网设备在光伏制造过程中的广泛应用，提出了专门针对这类设备的安全措施，如定期更新固件并采用安全的通信协议等。在策略制定过程中还需要定期审查和更新防护策略以适应新的威胁和技术变化，提倡采用动态安全策略，灵活调整防护措施，确保策略始终保持最新，以有效应对新出现的安全威胁。

4.2 管理体系构建

在构建有效的管理体系以保障网络防护的实施中，强调了跨部门协作机制的重要性，确保了信息安全、生产与运维等关键部门之间的高效沟通与合作，此举旨在形成一个统一的防护前线，其中每个部门都能在网络安全防护中扮演其独特且不可或缺的角色，实践中这种协作体系的建立依托于明确的沟通流程和快速的信息共享机制，确保了在面对网络威胁时能迅速做出反应。专业的安全运维团队的设立是此管理体系中的核心，这个团队不仅负责进行日常的安全检查和风险评估，还需在紧急情况下迅速响应，确保能够有效控制和缓解安全事件的影响，此外，团队成员需定期接受最新的安全培训，以保持其在网络安全防护领域的专业能力和知识的更新[7]。

为了进一步增强全体员工的安全意识，实施全面的安全培训体系显得尤为重要，通过定期安排的培训和模拟演练，每位员工都能够深刻理解防护策略的重要性，并掌握必要的安全操作技能，这不仅能减少因误操作引发的风险，还能使员工在遇到安全事件时能够采取正确的应对措施。借助先进的信息技术和工具，如安全信息和事件管理系统（SIEM），可以显著提升管理体系的效能，这种系统能够对网络活动进行实时监控，自动化地分析安全日志，快速识别并报告异常行为，从而有效地预防潜在的安全威胁，结合定期的安全评估和审计，这一管理体系能确保对策略的持续优化，使其能够适应安全威胁不断演变的特性，确保光伏制造业网络环境的长期安全与稳定。（见表 1）

表 1 光伏制造业网络防护策略与管理体系概览

防护策略类型	技术工具	应用领域	更新频率	预防目标
多层防护机制	防火墙、入侵检测系统	外围与内部网络	定期	阻断非法访问和攻击
数据保护	加密技术	敏感数据传输和存储	按需	保障数据传输和存储安全
物联网设备安全	固件更新、安全通信协议	物联网设备	定期	防止设备被恶意利用
安全培训	安全培训和演练	全体员工	定期	提高安全意识和操作技能
实时监控	安全信息和事件管理系统	网络活动监控	实时	识别并报告异常行为

5 结束语

在工业互联网深度融合光伏制造业的网络安全防护，是确保产业健康发展的关键，通过深入分析网络安全风险，实施有效的技术和管理防护措施，不仅可以保障光伏制造业的信息安全，还能促进产业经济效益的提升。特别是光伏支架等主打产品的创新与应用，更是展现了光伏制造业在新能源领域的核心竞争力。未来，随着技术不断进步和防护措施的持续优化，光伏制造业将迎来更加广阔的发展空间。

参考文献：

[1] 徐辉.5G 时代工业互联网安全问题及对策分析[J].网络安全技术与应用,2024(03):86-87.
[2] 《网络安全和信息》编辑部.工业互联网安全防护探索与实践[J].网络安全和信息化,2024(01):43.
[3] 季凯玉.工业互联网安全技术研究[J].网络安全和信息化 2024(01):44-46.
[4] 刘晓曼,杜霖,于广琛.浅析工业互联网安全评估评价方法[J].保密科学技术,2023(09):43-48.
[5] 彭浩楠,唐明环,查奇文,等.工业互联网商用密码应用研究[J].信息安全研究,2023,09(09):851-858.
[6] 高佳萌,吕途,国玉琳.工业互联网企业信息安全防护能力提升路径研究[J].青岛大学学报(自然科学版),2023,36(04):139-144.
[7] 白宇.基于区块链技术的工业互联网安全防护效果研究[J].自动化应用,2023,64(16):231-234.