

数字化时代仪表电气的信息安全保障研究

李桐 张慧生

陕西延长石油榆林煤化有限公司 陕西 榆林 719000

摘要：数字化时代，仪表电气系统作为工业自动化的核心，其信息安全日益凸显重要性。本研究聚焦于仪表电气信息安全保障策略，探讨风险评估、防护策略、应急响应等关键环节，旨在构建全方位的信息安全体系。通过深入分析技术挑战与管理需求，提出针对性解决方案，为提升数字化环境下仪表电气系统的安全性提供理论支持与实践指导。

关键词：数字化时代；仪表电气；信息安全

1 仪表电气系统中存在的信息安全风险

1.1 黑客攻击对仪表电气系统造成的威胁

在仪表电气系统中，黑客攻击是一个不容忽视的信息安全风险。随着工业自动化和物联网技术的快速发展，仪表电气系统日益成为关键基础设施的一部分，负责监控、控制和优化各种生产流程。黑客通过利用系统漏洞、弱密码、不安全的通信协议等手段，能够渗透进仪表电气系统，进而实施恶意操作。这些攻击可能导致设备异常运行、生产流程中断、甚至引发安全事故，黑客还可能植入恶意软件，如勒索软件，以加密系统数据或关键控制逻辑，要求支付赎金以恢复系统正常运行，给企业带来巨大经济损失和声誉损害。

1.2 数据泄露和系统瘫痪风险

仪表电气系统中存储和传输的数据往往包含企业的敏感信息，如生产数据、客户资料、知识产权等。一旦这些数据发生泄露，不仅可能使企业面临法律诉讼和巨额罚款，还可能导致商业机密被竞争对手获取，进而丧失市场竞争优势。数据泄露的原因可能包括内部人员的不当操作、外部黑客的入侵、以及系统安全防护措施的不足等^[1]。另一方面，系统瘫痪是仪表电气系统面临的另一重大风险。系统瘫痪可能由多种因素引起，包括但不限于软件缺陷、硬件故障、网络中断、恶意攻击等。一旦系统瘫痪，将直接影响生产线的正常运行，导致生产停滞、产品交付延迟，进而对企业造成经济损失和客户信任度下降。在极端情况下，系统瘫痪还可能引发安全事故，对人员和环境造成威胁。

2 数字化时代仪表电气行业的现状分析

在数字化时代的浪潮中，仪表电气行业正经历着前所未有的变革与升级。随着物联网、大数据、云计算、人工智能等先进技术的深度融合与应用，仪表电气系统逐渐从传统的单一监测与控制功能，向智能化、网络

化、集成化方向迈进。当前，仪表电气行业正加速推进数字化转型，通过数字化手段优化产品设计、生产过程、运维服务等各个环节，智能仪表、远程监控、预测性维护等新型解决方案不断涌现，不仅提高生产效率和产品质量，还大幅降低运营成本和维护成本。数字化技术还促进仪表电气系统与企业管理系统的无缝对接，实现生产数据的实时采集、分析与共享，为企业决策提供有力支持。数字化时代也为仪表电气行业带来了新的挑战，信息安全风险日益凸显，黑客攻击、数据泄露等事件频发，对企业的生产运营和信息安全构成了严重威胁，随着技术的不断进步和市场需求的快速变化，企业还需不断投入研发，保持技术领先，以应对日益激烈的市场竞争。

3 仪表电气系统信息安全保障关键技术

3.1 基于云计算的安全存储和备份技术

在仪表电气系统中，数据的完整性和可用性至关重要，而云计算技术以其高可扩展性、灵活性和成本效益，为仪表电气系统的信息安全保障提供了强有力的支持。基于云计算的安全存储和备份技术，是确保数据在数字化时代得以安全保存和快速恢复的关键手段。（1）云计算在安全存储中的应用；云计算平台通过虚拟化技术，将计算资源、存储资源和网络资源封装成一个独立的虚拟环境，专为企业用户提供数据存储服务。在仪表电气系统中，海量的生产数据、监控数据以及管理信息需要被安全地存储起来，以便后续的分析、处理和应用。云计算平台通过提供多层次的安全防护机制，如数据加密、访问控制、审计日志等，确保存储在云端的数据不被未授权访问或篡改。云计算的弹性扩展能力能够满足仪表电气系统随着业务增长而不断增加的数据存储需求。（2）安全备份策略的实施；为了防止数据丢失或损坏带来的风险，基于云计算的安全备份技术显得尤为

重要。企业可以将仪表电气系统的关键数据定期备份到云端，利用云存储的冗余部署和容错机制，确保数据的可靠性和持久性。在灾难恢复场景中，企业可以快速从云端恢复数据，缩短业务中断时间，降低经济损失。云计算平台还提供了灵活的备份策略，如全量备份、增量备份、差异备份等，以满足企业不同的备份需求。（3）数据加密与隐私保护；在数据传输和存储过程中，数据加密是保护数据隐私和安全的重要手段。基于云计算的安全存储和备份技术，通常集成了先进的数据加密技术，如AES（高级加密标准）等，对传输和存储的数据进行加密处理，确保数据在云端的安全性^[2]。

3.2 网络安全监控与实时响应技术

在数字化时代，仪表电气系统面临的网络安全威胁日益复杂多样。为了有效应对这些威胁，网络安全监控与实时响应技术成为了保障仪表电气系统信息安全不可或缺的关键技术。第一、网络安全监控体系的构建；网络安全监控体系是实现对仪表电气系统网络安全态势全面感知和预警的重要基础。通过部署入侵检测系统（IDS）、入侵防御系统（IPS）、安全审计系统等安全设备，以及采用网络安全态势感知平台等先进技术手段，可以实时监测仪表电气系统的网络流量、系统日志、用户行为等关键信息，及时发现并预警潜在的网络安全隐患。第二、实时响应机制的建立；在发现网络安全威胁后，快速响应是减少损失、控制事态发展的关键。基于网络安全监控体系构建的实时响应机制，能够在威胁发生时自动触发预设的应急响应流程，如阻断攻击源、隔离受感染设备、启动数据恢复程序等，以迅速遏制威胁的扩散。实时响应机制还能够将相关信息及时反馈给安全运维团队，以便他们进行进一步的分析和处理。第三、安全情报与威胁分析；为了提升网络安全监控与实时响应的效率和准确性，安全情报与威胁分析技术也至关重要。通过收集和分析来自全球范围内的安全情报信息，如最新的漏洞信息、恶意软件样本、攻击手法等，可以及时发现并应对针对仪表电气系统的定向攻击或零日攻击。对历史攻击事件进行深度分析，挖掘攻击者的行为模式和攻击路径，可以为制定更加有效的安全防护策略提供有力支持。

4 仪表电气信息安全保障体系构建

4.1 风险评估与威胁识别

在构建仪表电气信息安全保障体系的过程中，风险评估与威胁识别是首要且至关重要的环节。这一步骤旨在全面理解系统面临的安全风险，明确潜在威胁及其可能带来的后果，为后续的安全防护策略制定提供科学

依据。风险评估是信息安全管理的基础，它通过对系统资产、威胁、脆弱性和现有安全措施的综合分析，评估系统遭受损害的可能性及其严重程度。在仪表电气系统中，由于涉及大量的敏感数据和关键控制流程，任何安全漏洞都可能引发严重的后果，包括生产中断、数据泄露、财产损失乃至人身安全威胁，定期进行风险评估，及时发现并应对潜在的安全风险，对于确保系统稳定运行、保护企业资产具有重要意义。威胁识别是风险评估的重要组成部分，它要求安全团队运用多种技术手段和情报资源，对可能危害仪表电气系统安全的各种因素进行全面梳理和深入分析。识别企业内部人员可能构成的威胁，如误操作、恶意破坏、内部泄密等。这要求企业建立完善的员工行为规范和监督机制，加强员工安全意识教育。关注来自外部的黑客攻击、病毒传播、恶意软件等威胁，通过收集和分析安全情报、监测网络流量、定期扫描系统漏洞等方式，及时发现并应对外部威胁^[3]。考虑到仪表电气系统可能涉及多个供应商和合作伙伴，供应链中的任何一环出现安全问题都可能影响到整个系统的安全。企业需要对供应链进行严格的安全审查和评估，确保供应链各环节的安全可控。随着技术的不断进步，新技术的应用为仪表电气系统带来了更多的可能性，但同时也带来了新的安全风险。企业在引入新技术时，需要进行充分的风险评估，确保新技术在提升系统性能的同时，不会引入新的安全漏洞。

4.2 安全防护策略制定

在完成风险评估与威胁识别后，接下来需要制定针对性的安全防护策略。安全防护策略是保障仪表电气系统信息安全的关键措施，它涵盖了技术、管理和运营等多个方面。技术防护策略是安全防护体系的核心，它包括几个方面：（1）网络隔离与访问控制：通过划分不同的安全区域、部署防火墙、实施严格的访问控制策略等措施，确保网络边界的安全。（2）数据加密与隐私保护：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性，遵循隐私保护政策，对用户的敏感信息进行脱敏处理或匿名化处理。（3）漏洞管理与补丁更新：建立漏洞管理机制，定期扫描系统漏洞并及时修复，关注软件厂商发布的安全补丁和更新信息，确保系统始终处于最新状态。（4）安全审计与日志管理：部署安全审计系统，记录系统操作、用户行为等关键信息，为安全事件的分析和追溯提供有力支持，加强日志管理，确保日志的完整性和可用性。管理防护策略是技术防护策略的有效补充，建立健全的信息安全管理制度，明确安全责任、管理流程和工作标准。加强员工安全意

识教育和技术培训,提高员工识别和应对安全威胁的能力。对供应商和合作伙伴进行安全审查和评估,确保其在提供服务和产品时符合企业的安全要求。关注国家和行业相关的法律法规、标准和规范,确保企业的信息安全管理符合合规性要求。

4.3 应急预案与响应机制

尽管我们采取了各种安全防护措施来降低安全风险,但完全避免安全事件的发生是不现实的。因此,建立健全的应急预案与响应机制对于迅速应对安全事件、减少损失具有重要意义。应急预案是针对可能发生的安全事件而预先制定的应对方案。它应包括以下内容:

(1)事件分类与分级:明确不同类型和级别的安全事件及其特征和影响范围。(2)应急组织体系:建立应急指挥机构和工作小组,明确各成员单位的职责和协作关系。(3)应急资源准备:提前准备必要的应急资源,包括技术工具、专业团队、备用设备等,确保在应急情况下能够迅速调配和使用。(4)应急响应流程:制定详细的应急响应流程,包括事件发现与报告、初步评估与判断、应急处置措施、事态控制与恢复、后续跟进与总结等步骤,确保应急响应工作有序进行。(5)沟通与通报机制:建立有效的内部沟通和外部通报机制,确保在应急情况下信息能够迅速传递至相关人员和机构,避免信息孤岛和误解。(6)培训与演练:定期组织应急培训和模拟演练,提高员工对应急预案的熟悉度和应急响应能力,确保在真实事件发生时能够迅速、准确地采取行动。应急响应机制是应急预案得以有效执行的关键,它要求企业在面对安全事件时,能够迅速启动应急预案,按照既定的流程进行处置,并及时调整策略以应对事态的发展。一旦发现安全事件,应立即启动应急响应流程,组织相关人员对事件进行初步评估,确定事件的性质、影响范围和严重程度。根据初步评估结果,由应急指挥机构做出决策,明确应急处置的优先级和具体措施,并指挥各工作小组迅速行动。按照应急预案和指挥机构的决策,各工作小组迅速开展应急处置工作,调配必要的应急资源,确保事态得到有效控制。在应急处

置过程中,保持内部和外部的沟通畅通,及时向相关人员和机构通报事件进展情况和处置措施,确保信息的一致性和准确性。通过有效的应急处置措施,努力控制事态的进一步恶化,并尽快恢复系统的正常运行和业务的连续性。在事件得到妥善处理后,组织对事件进行后续跟进和总结,分析事件原因、评估损失、总结经验教训,并提出改进措施,以不断完善应急预案和应急响应机制。

4.4 安全管理制度与培训

在仪表电气信息安全保障体系的构建中,安全管理制度与培训扮演着至关重要的角色。企业需建立一套全面、细致的信息安全管理制,明确安全责任、规范操作流程、强化监督管理,确保信息安全的各项措施得到有效执行,重视员工的安全培训,定期开展信息安全意识教育和技术培训,提高员工对信息安全的认知水平和应对能力。通过安全管理制度的完善和员工培训的加强,能够构建起一道坚固的信息安全防线,有效抵御内外部威胁,保障仪表电气系统的稳定运行和数据资产的安全,还应建立持续改进机制,不断优化安全管理制和培训内容,以适应快速变化的信息安全环境。

结束语

随着数字化进程的加速,仪表电气信息安全保障成为关乎工业安全与发展的重要课题。本研究通过系统分析与实践探索,为仪表电气信息安全保障提供了有效路径。未来,持续的技术创新与管理优化将是保障仪表电气系统安全运行的关键。期待在数字化浪潮中,仪表电气信息安全能够得到更加坚实的守护,为工业智能化发展奠定坚实基础。

参考文献

- [1]李明.张伟.王晓丽.数字化时代仪表电气信息安全防护策略与实践[J].信息安全技术.2023.17(4):45-50.
- [2]赵强.刘慧敏.陈晓东.基于大数据分析的仪表电气信息安全风险评估方法[J].自动化与仪器仪表.2022.36(11):12-16.
- [3]陈静.李华.王刚.数字化仪表电气系统信息安全管理制体系构建[J].中国安全科学学报.2021.31(S1):100-104.