

电力监控系统二次安全防护策略探讨

孙航飞 铁勇魁 窦中山 王旭宁
许继电气股份有限公司 河南 许昌 461000

摘要：电力系统自动化发展的过程中，对计算机的依赖程度快速增加，电力监控系统开展二次安防的主要目的就是确保电力系统的稳定运行。随着我国电力行业的快速发展，逐渐意识到了电力监控系统对整个电力系统的重要意义，因此制定了相应的电力监控系统和二次安防来对确保电力监控系统的顺利运行。

关键词：电力系统；监控系统；二次安防；防护策略

1 电力监控系统二次系统安防建设的重要性

电力监控系统是电力行业中至关重要的组成部分，负责实时监测和管理电力系统的运行状态。随着信息技术和网络的发展，电力监控系统的重要性越来越突出，但同时也面临着各种安全威胁和风险。因此，实施电力监控系统的二次安防建设具有重要的意义。第一，电力监控系统的二次安防建设可以保障电力系统的稳定运行。电力系统对社会经济发展和人民生活起着至关重要的作用，一旦电力供应中断或异常，就会对社会造成严重的影响。通过实施二次安防建设，可以有效预防和应对网络攻击、电力故障等意外事件，保障电力系统的稳定性和可靠性。第二，电力监控系统的二次安防建设可以保护系统数据的安全性。电力监控系统中的数据是非常敏感和重要的，包含着大量关于电力系统运行的实时数据和敏感信息。如果这些数据泄露或被篡改，将严重影响电力系统的正常运行，并可能导致安全隐患。通过加强网络安全措施、身份认证和数据备份等手段，可以确保系统数据的安全性和完整性。第三，电力监控系统的二次安防建设可以防范网络攻击和黑客入侵。随着网络技术的发展，电力监控系统也面临着日益复杂和多样化的网络攻击威胁。黑客入侵、拒绝服务攻击等都可能对电力系统造成严重破坏。通过增强系统的网络安全措施，建立入侵检测和防火墙等技术机制，可以及时识别和应对各种网络攻击，维护电力系统的安全稳定。第四，电力监控系统的二次安防建设可以提升管理和运维效率。电力监控系统是一个复杂的系统，需要进行频繁的维护和管理。通过实施二次安防建设，可以降低系统的故障率和运维成本，提高系统的可用性和可靠性^[1]。

2 电力监控系统二次安全防护的具体技术手段

2.1 强化网络安全措施

为了加强电力监控系统的二次安全防护，需要采取一系列的具体技术手段，其中之一是强化网络安全措

施。（1）防火墙：在电力监控系统的网络边界处设置防火墙来过滤网络流量，只允许经过授权的数据通过。防火墙可以根据预先设定的规则对网络流量进行审查和过滤，阻止未授权的访问和恶意攻击。可以配置防火墙规则来限制只有特定的IP地址或网络段才能访问系统。

（2）入侵检测系统（IDS）：IDS可以监测和识别电力监控系统中的恶意活动和攻击行为。通过监控网络流量和系统活动，IDS可以检测到不正常的行为，并及时发出警报。还可以与防火墙、日志管理系统等相结合，形成自动化的安全响应机制。（3）虚拟专用网络（VPN）：电力监控系统通常通过远程访问进行操作和管理，为了保护系统的通信安全，可以使用VPN技术建立一个安全的加密隧道来传输数据。VPN能够加密数据、验证双方身份，确保数据传输的机密性、完整性和可靠性。（4）安全协议和加密技术：采用安全协议和加密技术对电力系统的通信进行保护。例如，使用HTTPS来加密Web操作，使用SSH来加密远程终端访问。此外，还可以使用基于PKI（公钥基础设施）的证书来确保通信的安全性。

（5）强化访问控制和身份认证：设置严格的访问控制策略，对用户进行身份认证，并指定合理的授权访问权限。采用多因素身份认证，如硬件令牌、生物特征识别等方法，加强对用户身份的验证。还可以引入单点登录（SSO）机制，集中管理用户的登录和访问控制。

2.2 加强身份认证与访问控制

为了加强电力监控系统的二次安全防护，另一个重要的技术手段是加强身份认证与访问控制。（1）采用多因素身份验证，例如使用用户名和密码的组合，结合硬件令牌、生物特征识别等，以确保用户身份的真实性和可信度。通过引入多层次身份验证机制，可以降低恶意用户冒充合法用户的风险，提高系统的安全性。（2）制定严格的密码策略，要求用户设置强密码，并定期更换密码。密码应包含大小写字母、数字和特殊字符，并要

求长度至少8个字符。此外,禁止使用常见的密码和个人信息作为密码,增加密码的复杂性和难度^[2]。(3)基于用户角色和职责,对用户进行合理分组和授权,并限制用户对系统资源的访问权限。通过细粒度的访问控制和权限管理,可以防止未授权的访问和误操作,提高系统的安全性。(4)建立监控系统,对用户的行为进行实时监控和日志记录。通过定期审计和监控,可以及时发现异常行为和恶意操作,并追踪其来源,为安全决策提供依据。(5)通过单点登录机制,用户只需一次登录即可访问多个相关系统。这种集中管理的身份认证方式可以减少用户需要记忆的密码数量,降低密码泄露的风险,并提供更便利的用户体验。

2.3 实施数据及时备份和紧急恢复计划

为了加强电力监控系统的二次安全防护,另一个重要的技术手段是实施数据及时备份和紧急恢复计划。制定并执行定期的数据备份计划,确保监控系统各项数据的及时备份。备份数据可以存储在离线设备、云端存储或其他安全的媒介中,以保证数据的安全性和可靠性。备份频率可以根据数据增量和重要程度来确定,以确保数据的完整性和可用性。对备份数据进行验证,确保备份的数据是完整且可用的。同时,定期进行紧急恢复测试,测试备份数据的恢复速度和恢复能力,以确保在系统遭受攻击或灾难时能够快速恢复监控系统的功能。制定应急恢复计划,定义在遇到安全事件或灾难情况时的应急响应流程。应急计划应包括联系人列表、紧急事故报告和恢复时间目标等信息,以确保在紧急情况下能够及时响应和恢复系统。采用高可用性配置策略,包括硬件冗余和容错设计。通过配置冗余的硬件设备、负载均衡和故障转移机制等,确保系统在硬件故障或网络中断时能够自动切换和恢复,保障系统的稳定运行。采用数据加密技术,对敏感数据进行加密存储和传输,以保证数据的机密性。

3 电力二次系统安全防护策略

3.1 制定详细的二次安全防护方案

电力二次系统是现代电力系统中不可或缺的组成部分,而其安全性对电力系统的正常运行和供电可靠性至关重要。为此,制定详细的二次安全防护方案非常必要。首先,进行全面的安全评估,了解系统的弱点和威胁,确定潜在的安全风险。基于评估结果,制定安全策略和计划,确保系统安全性能达到预期。将电力二次系统与其他网络隔离开来,建立独立的内部网络。通过配置防火墙、网络隔离设备和访问控制列表,限制外部对系统的访问,减少恶意入侵和攻击的风险。采用多因素

身份认证,如用户名和密码的组合,结合硬件令牌、生物特征识别等技术,确保用户身份真实可信。严格配置访问控制,根据用户角色和职能分配权限,限制用户仅能访问其授权的功能和数据。建立安全审计和监控系统,通过实时监控和记录系统活动和异常事件,及时发现安全漏洞和潜在的攻击活动。定期进行安全审计,确保系统的合规性和安全性。定期检查和更新系统的安全补丁、操作系统和应用程序,修复已知的漏洞^[3]。同时,及时升级硬件设备和安全软件,提高系统的安全性和抗攻击能力。采用数据加密技术,对敏感数据进行加密存储和传输,保证数据的机密性。使用安全传输协议,如SSL/TLS,确保数据在传输过程中的安全性。定期对员工和系统用户进行安全培训,提高他们的安全意识和识别潜在威胁的能力。建立快速响应机制,确保用户能够及时报告任何安全事件或异常。制定灾备和应急响应计划,包括数据备份和紧急恢复策略。定期备份关键数据,存储在离线设备或云端,以便在遭到攻击或灾难时能够快速恢复系统。定期进行安全审查和漏洞扫描,发现和修复系统中的潜在漏洞和安全风险。

3.2 定期开展安全演练和测试

为确保电力二次系统的安全,定期开展安全演练和测试是一种重要的防护策略。通过模拟真实的安全事件和攻击,检验系统的安全性和应急响应能力,可以有效提升系统的抵御能力和灾难恢复能力。制定定期的安全演练计划,涵盖不同类型的安全事件和攻击场景,例如网络入侵、系统瘫痪、数据泄露等。根据实际情况,确定安全演练的频率和内容,确保全面覆盖系统的安全风险。在安全演练中,模拟真实的安全事件和攻击,运用各种手段和工具进行测试。例如,使用渗透测试工具模拟黑客攻击,测试系统的漏洞和脆弱性;模拟社会工程学攻击,测试员工对钓鱼邮件和恶意链接的识别能力等。对每次安全演练的结果进行评估和总结,分析系统在面对安全事件和攻击时的表现和应对能力。发现演练中的问题和不足,并及时进行改进和修复,提升系统的安全性。在安全演练的过程中,加强员工的培训和意识提升。定期组织相关的培训课程和分享会,提升员工对安全事件和攻击的认识和理解,教育他们正确使用系统和应对安全威胁的方法。根据安全演练和测试的结果,制定详细的应急响应计划。明确应急团队的职责和流程,建立紧急联系人列表,确保在面对真实的安全事件时能够迅速响应和采取应对措施。根据安全演练和测试的结果,不断改进系统的安全措施和策略。及时修复发现的安全漏洞和脆弱性,更新和升级安全设备和防护软

件,提升系统的安全性和抵御能力。

3.3 建立全员安全意识和培训体系

只有所有人员都具备良好的安全意识和知识,才能有效防范潜在的安全威胁和攻击。制定全员安全教育和培训计划,包括新员工入职培训、定期安全培训和特定岗位培训。通过不同形式的培训,如在线学习、培训课程、专家讲座等,向员工普及电力二次系统的安全知识和最佳实践。定期组织安全意识活动,如安全月、安全周,宣传电力二次系统的安全重要性,通过海报、宣传栏、内部通讯等方式提醒员工保持警惕和注意安全。制定明确的信息安全政策和准则,明确员工在电力二次系统中的责任和义务。政策和准则应包括密码安全、设备操作规范、数据保护等方面的规定,确保员工了解并遵守相关要求。定期组织实战演练和模拟攻击,将员工置于真实的安全威胁环境中,让其体验攻击事件和应对措施。通过这种方式,使员工能够更好地了解安全威胁,并学会如何应对和处理实际情况。建立安全邮件和提醒机制,向员工发送相关的安全信息,包括最新的安全威胁、常见的安全问题和解决方案等。通过邮件、通知等形式提醒员工保持警觉,及时采取相应的安全措施。为员工提供安全问题报告的渠道,鼓励员工主动汇报发现的安全问题和漏洞。建立相应的奖励机制,鼓励员工有效参与和贡献安全建设。定期对员工的安全操作进行检查和评估,发现潜在的问题和安全隐患,并及时进行纠正和改进^[4]。

3.4 电力监控系统应急预案

应急预案能够明确应急事件发生时的响应措施和流程,保障系统的正常运行和应对突发情况的能力。组建专门的应急响应团队,成员包括系统管理员、网络工程师、安全专家等。明确团队成员的职责和权限,确保在应急事件发生时有人能够迅速响应和采取措施。对可能发生的应急事件进行分类和等级划分,根据事件的紧急和严重程度,制定相应的应急响应措施。例如,对于

网络攻击事件,将其划分为不同等级,从而决定需要采取的应急措施和响应间隔。建立应急预警机制,对异常事件和安全威胁进行实时监测和预警,并迅速通知应急响应团队。预警机制可以使用监控工具、安全事件管理系统等技术手段,确保应急响应团队及时得知事件的发生。制定明确的应急事件处理流程,确定应急处理的步骤和流程。例如,事件发生后的第一时间,通知应急响应团队,启动应急预案。团队成员根据事件类型和等级,采取相应的处置措施,如隔离攻击源地址、封锁攻击流量等。建立与相关单位的紧急联系机制,以便在应急事件发生时能够及时联系并协同应对。例如,与供电局、安全厂商等建立应急协作机制,实时共享信息并共同对应应急事件。建立定期的数据备份和恢复策略,确保关键数据的安全性和可恢复性。定期将重要数据备份到离线设备或云端存储,以便在出现数据丢失或破坏的情况下能够恢复系统的正常运行。组织应急演练活动,模拟不同的应急事件场景,检验应急预案的可行性和有效性。

结束语

总的来说,随着时代的发展,电力监控系统也应该随之而发展,使其能跟上人们需求的脚步。电力监控系统二次防护能更好的提升电力系统的稳定性,所以很有必要进行二次防护,这样才能最大程度地保证电力监控系统的稳定运行。

参考文献

- [1]丁立顺.电力调度自动化二次系统安全防护研究[J].技术与市场,2021,28(10):115-116.
- [2]郭锦煌.电力调度自动化二次系统安全防护分析[J].光源与照明,2021(04):127-128.
- [3]靳帅,李建清.浅谈枕头坝电站电力监控二次安全防护系统建设[J].四川水力发电,2020,39(01):91-94.
- [4]何鲤.电力二次系统网络信息安全防护的设计与实践[J].通信电源技术,2019,36(08):229-230.