

有效提高电力监控系统中二次安防的防护策略

郑玮 邵旭

国家电网陕西省电力公司榆林供电公司

摘要: 电力监控系统,特别是其中的二次安防部分,作为确保电网稳定运行的技术支柱,其安全性问题一直是业界关注的焦点。随着技术的进步和网络环境的复杂化,传统的防护手段已难以完全应对日益增长的安全威胁。鉴于此,本研究通过详细梳理现有防护措施的不足,深入探讨了提升电力监控系统二次安防防护能力的新策略。研究围绕系统安全性的多个方面,包括但不限于外部网络攻击防护、内部安全漏洞修补、操作人员的安全意识提升等,提出了一系列具体的改进措施。这些措施在理论上的创新性和实践中的可操作性,共同为电力系统的安全稳定运行提供了有力支撑。本研究的成果预计将对电力监控系统的安全管理实践产生积极影响,为后续相关领域的研究提供了新的视角和方法论。

关键词: 电力监控系统; 二次安防; 防护策略; 系统安全

【DOI】10.12252/j.issn.2096-6261.2022.10.068

一、引言

在现代社会,电力系统作为基础设施的核心,其稳定与否直接影响着国民经济和社会生活的各个方面。随着信息技术的融入和电网智能化水平的提高,电力监控系统扮演着越来越重要的角色。尤其是系统中的二次安防部分,它既负责数据的采集和传输,还涉及对整个电网运行状态的监控和控制。因此,任何对二次安防系统的威胁都可能造成不可预测的后果。面对网络攻击手法的不断革新和内部安全隐患的存在,如何有效提升二次安防的防护能力成了亟须解决的问题。本研究旨在通过对现状的深入分析,探索出一套切实可行的策略,旨在弥补现有防护措施的不足,从而为电力系统的安全运行提供更为坚实的保障。通过广泛的文献回顾与实际情况的结合考察,本文将展开对该问题的系统研究。

二、问题分析

1. 安全问题细分

在电力系统的运行维护中,二次安防系统扮演着至关重要的角色,它的稳定性和安全性直接关联到整个电网的正常运作。但这一系统面临的安全威胁日益增多,变得复杂多变,其中外部网络攻击、系统内部的安全漏洞以及人为操作失误构成了三大主要的风险源,每一种风险都可能在一定程度上威胁到电力系统的安全和稳定性。

第一,外部网络攻击的问题日益突出。随着互联网技术的发展,电力监控系统越来越多地依赖网络进行数据传输和远程控制,这就为网络攻击者提供了可乘之机。通过病毒感染、钓鱼攻击、拒绝服务攻击等手段,攻击者可以破坏电力监控系统的数据处理和传输功能,严重时甚至能够使整个系统瘫痪。这类攻击既对电力供应造成中断,还可能对电网安全产生长远的影响。

第二,系统内部的安全漏洞也是不可忽视的风险。

由于系统设计不当、软件缺陷或配置错误等原因,电力监控系统可能存在多种安全漏洞。这些漏洞成为攻击者潜在的入侵点,一旦被利用,攻击者便能控制或干扰电力监控的正常运作。随着电力系统越来越多地采用新技术和设备,未知的安全漏洞可能随之而来,给电力系统的安全防护带来更大的挑战。

第三,人为操作失误同样是导致安全事件发生的重要因素。电力监控系统的操作复杂,需要操作人员具备高度的专业知识和严格遵守操作规程。但在实际操作过程中,由于培训不足、疏忽大意或误操作等人为因素,可能会导致系统发生故障或数据丢失,从而影响到电力系统的稳定运行。这类人为因素导致的风险在一定程度上是可以预防和控制的,但需要系统的培训和规范的管理。

2. 风险实例分析

外部网络攻击的典型案例包括通过网络渗透获取电网控制系统的访问权限,攻击者可能利用这种权限修改控制指令,造成电力供应中断或是电网设备损坏。这类攻击既影响电力供应的稳定性,还可能对公共安全造成威胁。

关于系统内部的安全漏洞,一个实际的例子是软件的缺陷允许未经授权的用户绕过身份验证,访问系统控制界面。这种情况下,攻击者可以修改系统设置或是操作数据,导致错误的电力调度指令被下达。

人为操作失误的案例则更为多样,从简单的密码泄漏到复杂的操作规程未遵守,任何一个小小的疏忽都可能导致严重的后果。例如,操作人员因为忽略了某个警报信号,可能会导致重要的安全设备失效,进而引发电力系统的部分甚至全面瘫痪。

3. 风险影响

外部网络攻击、系统内部安全漏洞以及人为操作失

误这三大主要风险，每一种都有可能导导致电力系统运行的临时或长期中断，从而对电网的稳定供电造成严峻挑战。这些安全隐患并不是孤立的，它们之间存在潜在的相互作用和影响，使得整个电力系统面临更加复杂和严重的安全挑战。

外部网络攻击通过互联网等渠道发起，目的在于破坏电力监控系统的正常运作。这类攻击既能够干扰数据传输，更有可能使整个监控系统瘫痪，导致电力供应中断。在电力系统越来越依赖网络技术的今天，外部网络攻击成了一个不可忽视的安全威胁。

而系统内部的安全漏洞，包括软件缺陷、配置错误等，为不法分子提供了侵入系统的途径。一旦被利用，可能导致电力设施遭到破坏，影响到电力系统的物理安全和运营安全。系统内部的安全管理和技术维护，成为确保电力系统稳定运行的关键因素。

人为操作失误，尤其是在高压工作环境下，更容易发生，其后果往往不容小觑。操作人员的一次疏忽或误操作，可能会引发电力系统的安全事故，甚至导致严重的供电中断和经济损失。因此，提高操作人员的安全意识和专业技能，是防止人为操作失误的重要措施。

这些风险因素之间的相互作用，使得电力系统的安全问题更加复杂。例如，系统内部的一个安全漏洞可能被外部攻击者发现并利用，同时，在系统受到攻击或其他紧急情况下，人为操作失误的风险也显著增加。这种情况下，单一的安全漏洞就可能引发一系列连锁反应，给电力系统的稳定运行带来严重挑战。

三、防护策略

1. 深化防御体系构建

电力监控系统作为国家重要基础设施的一部分，其安全性对于保障国民经济和社会生活的稳定运行至关重要。面对这种形势，单一的防御手段已经远远不能满足对电力监控系统安全防护的需求。因此，采取多层次、多维度的深度防御体系构建策略，显得尤为重要和必要。

深度防御体系的构建是一个全方位、多角度的安全防护策略。它从外部网络边界的防护入手，涵盖了从入侵检测、防火墙部署到入侵防御系统的设置，确保了外部威胁无法轻易穿透系统的第一道防线。而在体系的内部，针对数据处理和传输过程的安全防护，通过加密技术和安全协议的应用，保证数据在传输和处理过程中的安全性和完整性。

深度防御体系还特别强调物理安全和信息安全的结合。物理安全措施，如对电力监控中心的实体安全进行保护，确保关键设备和系统不会受到物理损害或人为破坏，同时，信息安全措施则通过软件和硬件的结合使

用，对系统进行实时监控和管理，以便及时发现并处理安全威胁。

在这一体系中，每一层的防御都设计有针对性，能够在不同程度上拦截和防范潜在的威胁。即便是在外部防护层面遭到破坏或突破，体系内部的其他防护措施仍然能够发挥作用，为系统提供额外的安全保障。这种层层设防的策略，有效提升了电力监控系统对抗外部攻击和内部威胁的能力。

通过这样全面而深入的防护体系构建，电力监控系统的安全性得到了显著提升。既如此，这种深度防御体系还具有很强的灵活性和扩展性，能够根据安全威胁的变化和技术的发展进行相应的调整和优化。这样的安全防护策略，为电力监控系统带来了更为全面和坚固的保护，确保了电力系统的稳定运行，为社会经济的持续发展提供了坚实的安全保障。

2. 定期安全评估与漏洞修补

在电力监控系统的运行过程中，安全漏洞无疑是构成潜在威胁的一个重要因素。这些漏洞可能来源于软件缺陷、系统配置不当或是技术更新滞后等多种因素。如果不被及时发现和修补，就有可能被不法分子利用，对电力系统造成严重的损害。因此，定期进行系统的安全评估和漏洞修补工作，对于保障电力监控系统的安全运行至关重要。

安全评估是一个全面审查和评估系统安全状况的过程。通过这一过程，专业的安全团队能够深入分析系统的安全配置，识别存在的安全风险，并评估潜在威胁的严重程度。这一过程既涵盖了软件层面的检查，如对操作系统、应用程序的安全漏洞进行扫描，同时也包括了硬件和网络配置的审查，确保系统从多个层面上都能抵御外部的攻击和内部的误操作。

在发现安全漏洞之后，及时采取修补措施是保证系统安全的关键一步。这些措施可能包括更新软件到最新版本、修改系统配置以增强安全性、甚至更换存在严重安全隐患的硬件设备。对于特别复杂或难以立即修复的漏洞，还需要制定临时的应对措施，以减少潜在的安全风险，直到找到根本的解决方案。

持续的安全评估和漏洞管理过程，能够确保电力监控系统能够适应不断变化的安全威胁环境。随着新的漏洞不断被发现，以及攻击手段的不断进化，只有通过定期的评估和及时的修补，才能有效地保护系统免受攻击。这一过程还有助于提升系统管理员和运维人员的安全意识，使他们在日常工作中更加注重安全问题，从而进一步增强电力监控系统的安全性。

3. 提升人员安全意识与技能培训

在维护电力监控系统的安全中，除了技术手段的不

断革新和防护体系的深化之外，人的因素同样扮演着至关重要的角色。实际上，不少安全事故的发生，都可以追溯到人为操作的失误或是安全意识的不足。因此，在安全防护策略的制定中，提升操作人员的安全意识和技能培训显得尤为重要，它直接关系到电力监控系统能否稳健运行，以及在遭遇安全威胁时能否做出正确的响应。

定期进行安全培训和演练，是提升操作人员安全意识和技能的有效手段。通过这些培训和演练，既可以让操作人员了解到最新的安全威胁情况和防护技术，还能使他们熟悉日常操作中的安全规范和紧急情况下的应对措施。这种系统性的知识传递和技能训练，能够有效提高员工对安全威胁的识别能力和处理能力，从而在面对安全事件时，能够迅速、准确地做出反应，最大限度地减少可能的损失。

加强安全管理和建立严格的操作规程及审计机制，对于减少人为操作失误也至关重要。严格的操作规程既为操作人员提供了明确的工作指南，确保了操作的标准化和规范化，还有助于新员工快速熟悉工作环境和工作要求。同时，通过实施有效的审计机制，可以对操作过程进行监督和记录，一旦发生安全事件，便于追踪原因和责任人，及时采取纠正措施，防止类似事件再次发生。

在提升操作人员安全意识和技能培训的过程中，还需注重培训内容的实用性和前瞻性。随着网络安全威胁的不断演化和更新，培训内容也应跟上时代的步伐，包括最新的安全防护技术、安全政策法规更新等，确保操作人员能够掌握前沿的安全知识，有效应对新型安全挑战。

4. 制定与实施应急预案

在维护电力监控系统安全运行的过程中，面对不断升级的网络攻击，仅仅依赖日常的安全防护措施已不足以应对所有潜在的威胁。因此，制定一套详细的应急预案，并通过定期演练来确保其实施效果，变得尤为关键。这一过程既能够提升系统在紧急情况下的响应速度和处理能力，还能有效地降低因安全事件带来的潜在损失。

应急预案的内容应全面覆盖安全事件响应的各个环节，包括但不限于事件的初步识别、评估、响应、恢复以及事后分析和总结。其中，事件响应流程是预案中的核心，它指导操作人员在确认安全事件发生后，如何快速有效地采取措施，比如立即隔离受影响的系统部分，通知相关人员，启动备份系统等。通讯协议则确保在整个响应过程中，信息能够及时、准确地传递给所有

相关方，包括内部团队成员和外部支持单位。资源调度则涉及人员、技术和物理资源的有效分配，确保在应对安全事件时，能够有序地进行，不会因资源紧张而影响处理效率。

通过定期的演练，可以确保应急预案的有效性和可行性。演练既能帮助检测预案中可能存在的漏洞和不足，还能提升团队成员面对实际安全事件时的应急处理能力。在演练过程中，模拟各种可能的安全事件场景，让参与人员在尽可能接近真实情况的环境中，练习应对措施的实施，这种高压下的实战训练，对于提高团队的协作能力和应急反应速度非常有效。

演练过程中的每一次行动和决策，都应该被详细记录和评估。通过事后分析，组织者可以总结经验、发现问题，并根据这些反馈对预案进行调整和完善。这样循环往复的过程，能够不断增强电力监控系统面对各类安全挑战时的整体抵御能力。

四、结论

通过对电力监控系统中二次安防现状的深入分析及针对性防护策略的探讨，本研究提出了一系列旨在提升系统安全性的措施。这些措施覆盖了从技术到管理，从防御到应对的多个层面，既有助于防范当前已知的安全威胁，更为潜在风险提供了预防机制。研究表明，通过综合运用这些策略，能够有效提高电力监控系统的整体防护能力，为确保电网的稳定运行提供了强有力的支持。未来，随着技术的进一步发展和安全威胁的不断演变，对二次安防系统的防护策略也需要不断地更新和完善。本研究的成果预计将对电力行业的安全管理实践产生积极的影响，同时也为相关领域的研究工作提供了宝贵的参考和启示。在后续的工作中，本研究团队将继续深入探讨和优化这些策略，以期达到更高的安全防护标准，为电力系统的稳健运行奠定更加坚实的基础。

参考文献

- [1]姚宁. 浅析智能电网调度控制系统安全防护技术及发展[J]. 探索科学, 2019, 0(2): 40-40.
- [2]孙雁斌, 王子强, 周永灿. 一种智能型电网调度倒闸操作即时通信系统设计[J]. 自动化与仪器仪表, 2019(1): 99-102.
- [3]孙竞善. 浅析智能电网调度控制系统安全防护技术及发展[J]. 华东科技(学术版), 2015, 0(12): 295-295.
- [4]刘伟浩, 张伟, 马俊. RTU在电力系统安全监测中的应用[J]. 电气技术, 2015, 16(12): 176-178.
- [5]姜莉, 易辉. 电力系统信息通信网络安全及防护研究[J]. 电子技术与软件工程, 2016(2): 220-220.