浅谈电力监控系统网络安全防护技术研究

高　翔　梁宗裕

国网中卫供电公司 宁夏 中卫 755000

【摘　要】：随着社会经济的发展和进步，互联网的发展速度加快，网络信息技术受到重视，各种类型的网络监控系统出现，各式各样的任务也应运而生，电力行业也不例外。该网络监控系统应用于电力行业，可以提高发电网络监控系统的整体水平，真正提高工作效率，减轻人员负担。然而，网络监控系统仍存在诸多安全隐患，网络安全成为电子监控系统运行中最难、最重要的一点。本文详细分析了电力监控系统运行的安全要求，电力监控系统中出现的各种安全漏洞，并提出了一些有效的保护策略，加强能源监控系统的网络安全，希望给相关从业人员可以提供一些参考和帮助。

【关键词】：电力监控系统；网络安全；防护技术

Research on Network Security Protection Technology of Power Monitoring System

Xiang Gao, Zongyu Liang

State Grid Zhongwei Electric Power Supply Company Ningxia Zhongwei 755000

Abstract: With the development and progress of social economy, the speed of Internet development is accelerated, network information technology has been paid attention to, various types of network monitoring systems appear, a variety of tasks have emerged, the power industry is no exception. The application of the network monitoring system in the power industry can improve the overall level of the power generation network monitoring system, truly improve the work efficiency, and reduce the burden of personnel. However, there are still many security risks in the network monitoring system, and network security has become the most difficult and important point in the operation of electronic monitoring system. This paper analyzes the security requirements of the power monitoring system in detail, and the various security loopholes in the power monitoring system, and puts forward some effective protection strategies to strengthen the network security of the energy monitoring system, hoping to provide some reference and help for relevant practitioners.

Keywords: Power monitoring system; Network security; Protection technology

作为电力控制系统的组成部分，计算机控制系统在电气系统的安全运行中发挥着重要作用。在当前形势下，我国的电力监管体系存在诸多不足。在应用过程中，移动设备硬盘上病毒的存在会导致对网络安全系统的破坏，影响其正常运行和强大的网络监控系统的使用。因此，需要注意电力监控系统的网络安全。

1 电力监控过程中网络防护具体要求

目前的电力控制系统并没有完全发挥其作用。这主要是由于系统故障仍然较多，网络安全威胁较多，电力监控系统效率低下。为了保护网络安全系统，只有制定有效的安全措施，有效管理各种信息，减少网络安全隐患，才会达到安全网络防护的目的。网络安全是信息时代不可避免的问题，也是能源行业面临的挑战。制定和执行网络安全法律将把网络安全提升到一个更高的水平，通过强大的监控系统有效地支持网络安全保护。保护现代监控系统的安全必须符合某些原则要求。在真正安全网络保护的过程中，建立该领域的安全管理和安全意识非常重要。创建专用通道也很重要。对于网外连接，在两个网络系统之间设置一道屏障，实现真正的分离。它还共享安全更新、各种软件的及时更新、网络安全、可靠的监控系统和网络安全。管理、预防和控制有助于快速消除网络安全威胁，降低网络安全风险。尤其是电力监控系统的安全，应该从三个方面入手。除了主机安全外，还需要加强网络管理，提高信息传输的安全性和可靠性。还必须将内部网络与外部网络分开。从另一方面来说，也就是保护系统的边界。

2 电力监控系统网络安全防护存在的问题

2.1 技术管理问题

一个电力监控系统的网络安全防护技术存在的问题主要是区域之间的并行连接和分区错误的问题。

2.1.1 跨区并联操作问题

对于大面积的生产控制和管理区间，通常为批次对象安装单独的保护装置。在一些非生产控制区域或一般信息控制区域，基本的防火墙控制有助于提供有效的逻辑隔离。一般来说，数据信息传输过程，例如将数据信息从低安全性系统传输到高安全性系统的过程，执行信息传输和传输数据的反向分离，受海关行动的约束。但由于员工对电力系统相关网络安全防护意识不足，在电力监控系统网络安全防护实施过程中，存在监控系统跨区域并行运行，威胁系统的安全[1]。

2.1.2 分区错误问题

电力系统的保护具有复杂性、组织性和多样性的特点。因

此，在电力系统被隔离时，往往会出现分段故障的问题，从而难以确定系统的保护等级，增加了保护系统的成本。一般来说，当系统的特点和重要性不同时，应根据实际情况对系统的安全部分进行分离，以增加安全防护的重要性，满足不同安全级别的实际需求。但是，在保护电力监控系统网络安全的过程中，特别是在系统安装之初，由于人员重视不够，出现了分段错误，影响了对电力监控系统保护的有效性，网络的安全保护性。

2.2 运行管理问题

从电力公司的经营运作来看，存在以下问题。

2.2.1 密码口令泄露

电力系统运维人员必须使用密码登录操作系统。如果密码泄露，就会失去电力系统的安全能力，极大地影响系统操作的安全性和稳定性。

2.2.2 台账管理与实际情况不符

如果由于系统管理问题导致系统出现异常或故障，很难立即确定故障原因，也无法对设备的风险进行管理。

2.2.3 网络安全防护工作实施效率低

首先，多个密码和密码被泄露，因为大多数执行相关任务的操作员经常使用遥控器来执行多项任务，而无需更改易系统提供的密码，这会引发严重的安全隐患。一个强大可靠的电力监控系统在运行过程中需要大量的员工。如果没有强有力的监督，密码很容易泄露。其次，许多强大的网络系统仍然存在系统性风险。例如，由于真实的硬件和金融系统没有正确连接，因此秘密外泄，管控力度不行，职责不到位，导致出现网络安全问题[2]。

2.2.4 其他制度体系问题

电力系统的可靠运行应限于适当的标准化制度体系。但是，部分能源企业法规不完善，如机房接入系统、备份系统等，系统操作存在一定的安全隐患。

3 优化电力监控系统网络安全防护技术

3.1 提升电力系统技术人员综合素质

电力系统技术人员的综合素质直接影响系统网络保护的有效性。电力企业要加强技术人员培训，不断提高专业技术技能，为业务发展奠定基础。在电力系统技术人员的培训过程中，电力公司首先要充分调动有利因素，为员工创造适应环境，使他们能够得到良好的培训，提供适当的激励措施，提高自我效能，鼓励和持续改进，取得工作后的最大效果。然后，加强电力系统网络安全防护技术的形成，深入了解网络安全防护知识，增强网络安全防护意识，电力行业网络安全防护技术的实施和管理，确保了整体的管理系统的效率。随着现代信息技术的飞速发展，强大的监控系统新的网络安全技术不断更新，电力系统专业人员需要创造终身学习的理念，不断获得新的知识和技能。更新知识并满足工作不断变化的需求，将网络安全防护技术应用于电力监控系统时，技术人员应根据实际业务情况为企业系统安装定制的网络安全防护平台，以提高电力系统网络的安全。

3.2 应用数据传输加密技术，加强电力系统网络安全性

在当前形势下，数据加密是防止各种信息数据及相关资料泄露到电力系统中的一种非常有效的方法。通信加密利用加密密钥和加密算法来保护电力系统信息，将敏感信息转化为无意义或不可理解的符号，起到保护电力监控系统安全的作用。

加密由三个元素组成：明文、密文和密钥。事实上，数据加密技术的使用需要发送信息的一方使用密钥传输密文，然后员工通过操作强大的跟踪系统对信息负责。密钥也分为私有和公共。虽然相关技术要求有所不同，但应适用于电力监控系统的网络安全保护功能[3]。

应选择经过认证的垂直加密设备，尤其是在国家电力监控系统中。垂直加密和认证设备配置数据网络系统，增强网络的安全元素，应用独特唯一的密文，提高数据库的安全性、稳定性和完整性，不影响用户的网络设置。一般来说，在网络安全领域，应该选择垂直加密方式，使用合适的工具将明文转换为密文，保证数据传输的安全。垂直加密技术包括多种技术，其中 RSA 算法在国内外得到广泛应用。目前国家的用电监控系统需要选择国密算法。强大的电力监控系统的各个方面都进行了加密，以确保信息不会被犯罪分子窃取。而且，就算是被偷了，也没有人知道是什么。

垂直加密技术的主要用途是将设备重置为出厂重置模式并在出厂重置期间安装密钥。无论资源规划水平如何，都应采用垂直保密的方式，尽可能避免电力监控系统运行过程中的信息泄露问题。

3.3 威胁驱动的安全防护能力

目前，功能和能量控制系统的器件具有分布广泛的特点。面对屡屡发生的大规模高级攻击，以前安全围栏的思路难以有效保护电力监控系统的安全，而现在威胁驱动的网络安全模式解决了这个问题。美国洛克希德马丁公司于 2019 年防范在线威胁的建议方式提出这种做法，这种方式可以更好地将安全威胁检测和安全防护与闪电般的监控系统相结合，提高网络安全防护的价值和有效性。面向威胁的电力监控系统的安全防护功能通常由五个模块组成：外网威胁检测系统、内网威胁监控系统、纵向安全系统垂直安全、全横向安全系统和通用安全系统数据的集成。其中外网威胁检测系统和内网威胁监测系统分别设置了检测互联网安全威胁和设备/现场设备漏洞的动态和三维功能。纵向安全综合安全系统和横向安全综合安全系统在访问控制和数据安全方面开发安全功能，横向和纵向安全等数据交换和集成平台实施基于攻击威胁优化的综合安全措施。基于

横向划分的合作交流，目前，该模型已在多家企业实施，测试结果表明该网络安全模型有效提升了网络管理和安全功能[4]。

3.4 应用恶意代码防范技术，加强电力系统网络安全性

顾名思义，恶意软件是犯罪分子用来侵入网络安全系统以监视信息的计算机程序。当电力监控系统被该恶意代码攻击时，数据规划系统的整个网络被破坏，影响其正常运行并暴露相关信息。如今，恶意软件的数量越来越多，包括木马、硬件后门和病毒。因此，需要加强防范措施，落实防范恶意代码的方法，加强电力系统的网络安全。

首先，捕获恶意软件的技术层出不穷。目前，使用网络杀毒盘是一种非常有效的保护手段。在强大的监控系统的各个方面，都可以使用 U 盘杀毒来进行防范，有效防止恶意病毒的运行。将杀毒软件放入 U 盘，连接电脑。杀毒软件可以起到杀毒的作用，相关功能使用简单方便，过程本身也不太复杂。下一步是开发强大的反病毒网关。它是一种网络安全防护技术，可以提高电力监控系统的网络安全性。防病毒网关具有许多功能，包括恶意电子邮件拦截、网络病毒检测和删除、数据安全扫描和调查等。网关本身是一个强大的监控系统网络的一个非常重要的部分。提高网络安全需要加强防范技术，完善网关的安全功能，屏蔽和过滤各种数据，有效隔离病毒。

3.5 对勒索病毒的防范

勒索软件是攻击者用来通过窃取资产和资源来启动勒索软件的恶意软件。勒索软件防护是电力监控安全新背景下需要特别关注的事情之一。需要做到以下几点：首先，对电力监控系统中的数据资产进行分类和管理，然后为重要的数据和系统创建备份机制。第二，密码设置应尽可能复杂并定期更改。第三，电力监控系统资产定期进行风险评估。第四，定期进行杀毒处理。第五，定期关闭不必要的门。第六，发展强大的认证授权机制。此外，恢复电力监控系统中的关键系统和数据需要预先建立的第三方、安全和信任的信息系统服务提供商列表，这些服务提供商满足适用的管理要求[5]。

3.6 强化入侵检测技术，加强电力系统网络安全性

入侵检测技术目前仅指对监控系统中的各种敏感信息和数据进行定期扫描和检查的技术。通过分析研究，可以发现电气系统是否存在问题。与防火墙一样，这是提高网络安全性的有效方法。入侵检测技术有两种：主机检测和网络检测。入侵检测技术可以帮助明确主机流量监控系统的具体状态，判断信息数据是否入侵。另外，判断网络安全状态的相关技术也比较简单方便，可以通过点击连接、检查等链接来检查网络安全状态。盗窃检测技术与其他安全检测技术不同，它与预防性保护技术有关。入侵检测系统采用成熟的入侵检测技术构建，根据各种入侵行为的实际特征和对策设计，实时监控网络安全运行。当网络安全受到威胁时，最响亮的警报就会响起。

3.7 建立防火墙，加强网络身份认证的力度

防火墙不仅可以及时保护网络信息，防止潜在威胁，防止内部信息泄露和病毒侵入，还可以执行扫描和检测功能，防止违反网络安全的非法活动。防火墙分为三种类型，每种都有各自的优缺点。在构建防火墙时，需要详细研究这些具体问题。提高电力监控系统的网络安全性，需要根据实际情况搭建防火墙，保护重要的逻辑数据。越来越多的人因为无法从互联网上获取它们的真实信息而从事违法犯罪活动，加强网上实名认证，阻止他们的在互联网上的犯罪行为。确保每个用户都有一个真实的身份，并确保每个人的身份没有被泄露。

3.8 安全加固要落到实处

为确保可靠运行，电力监控系统还必须采取安全措施，提高系统自动检测安全威胁的能力。必须检测到系统故障才能正常工作，大大提高了系统对隐藏网络的保护。为了增强现代监控系统的安全性使用两种模式的组合。加强系统，以及专门的技术资源。操作过程中，系统自动修复。限制访问并禁用远程控制，密码设置应该易于使用。密码必须在一定时间内更改。如果由业务往来，必须有固定端口接口，未使用的端口必须关闭。优化完善电力监控系统病毒检测功能，在中心须建立病毒库，定期更新防病毒系统[6]。

4 结语

电力监控系统是保障电力系统安全可靠运行的重要组成部分。在对电力系统可靠性要求越来越高的背景下，加强供电监控系统的网络安全势在必行。因此，电力企业应根据实际情况，提高电网保护技术的高效利用，加快建设与自身发展相适应的保护平台。电气系统整体安全稳定运行，保证供电可靠性。

参考文献：

[1] 王辉煌.浅谈电力监控系统网络安全防护问题[J].电子世界,2020(04):202.
[2] 杨芸懿.电力监控系统网络安全防护技术研究[J].电子元器件与信息技术,2020,4(02):124-125.
[3] 李勇.电力监控系统网络安全防护探讨[J].网络安全技术与应用,2020(09):121-122.
[4] 杨浩,陈宝靖,李燕.电力监控系统网络安全防护技术应用研究[J].电子世界,2021(01):128-129.
[5] 李秉裕.试论电力监控系统网络安全防护[J].网络安全技术与应用,2021(09):123-124.
[6] 郑秀佳.安全防护技术在电力监控系统的应用研究[D].广东工业大学,2019.