工程技术发展
Engineering Technology Development
第 6 卷◆第 4 期◆版本 1.0◆2025 年
文章类型：论文|刊号（ISSN）：2737-4505(P) / 2737-4513(O)

网络安全等级保护在电力行业的实施与改进

刘晋兵
大唐山西电力工程有限公司
DOI:10.12238/etd.v6i4.15447

[摘　要] 在信息技术飞速发展的今天,电力行业网络安全问题受到了越来越严峻的考验。本文对网络安全等级保护概念以及相关法律法规和标准进行了总结,并指出当前电力行业存在安全防护体系不完善、安全意识不强、应急响应能力不高等问题。然后对电力行业网络安全等级保护的实现策略进行了详细论述,主要从等级保护定级、安全防护体系建设、安全管理体系建设和安全运维与监控等方面进行了阐述。最终提出了在技术、管理、应急响应与恢复以及合作与共享这四个方面的改进措施,目的是全方位提升电力行业的网络安全水平,确保电力系统能够稳定运行。
[关键词] 网络安全等级保护；电力行业；安全防护体系；应急响应；安全管理
中图分类号：TU714　文献标识码：A

Implementation and improvement of network security level protection in electric power industry

Jinbing Liu
Datang Shanxi Electric Power Engineering Co., LTD.

[Abstract] In the era of rapid information technology development, the cybersecurity challenges in the power industry have become increasingly severe. This paper summarizes the concept of cybersecurity level protection and relevant laws, regulations, and standards, highlighting issues such as an incomplete security protection system, weak security awareness, and inadequate emergency response capabilities in the current power industry. It provides a detailed discussion on the implementation strategies for cybersecurity level protection in the power industry, focusing on aspects such as level protection classification, security protection system construction, security management system construction, and security operation and maintenance and monitoring. Ultimately, it proposes improvement measures in four areas: technology, management, emergency response and recovery, and cooperation and sharing. The aim is to comprehensively enhance the cybersecurity level of the power industry, ensuring the stable operation of the power system.
[Key words] network security level protection; electric power industry; security protection system; emergency response; safety management

引言

电力行业是我国关键基础设施之一,随着信息化与智能化的快速发展,使得电力网络安全问题越来越重要。在网络攻击手段日益更新的今天,电力系统受到了空前严重的安全威胁。网络安全等级保护作为一套系统性的安全防护方案,为电力产业提供了全方位的安全保障措施。

1 网络安全等级保护概述

1.1网络安全等级保护的概念

网络安全等级保护(简称等级保护)是我国依据网络安全法律法规及标准,对信息系统和网络环境实施的一种分级管理、分级保护措施。它的核心思想是依据不同的网络与信息系统对国家安全,社会秩序和经济利益的重要性来确定对应安全保护等级并采取相应安全防护措施。等级保护制度最初是在《计算机信息系统安全保护条例》中提出的,并在随后发布的《信息安全技术网络安全等级保护基本要求》标准里得到了清晰的界定和具体的操作指导。具体而言,网络安全等级保护是通过划分信息系统的级别,以便针对每一级别的特点,采取相应的安全保护措施,保证信息系统能抵抗外在与内在网络安全威胁、避免数据泄露、系统失效与服务中断的危险,继而保证企业信息安全与社会稳定[1]。对大唐等电力企业来说网络安全等级保护非常重要。在数字化转型背景下,电力行业信息系统规模逐步扩大,所涉及核心数据与基础设施不断增加,网络安全问题更加复杂。

1.2相关法律法规与标准

我国网络安全等级保护相关法律法规及标准体系逐渐完善,

重点法律法规有《中华人民共和国网络安全法》等、《中华人民共和国刑法》和《计算机信息系统安全保护条例》等。另外，有很多行业性的标准及技术规范对于网络安全的等级保护也做了详尽的规定。如《信息安全技术网络安全等级保护基本要求》中明确规定了不同安全等级下信息系统所应满足的基本安全需求；《信息安全技术网络安全等级保护实施指南》为各企业呈现了详细的操作步骤与策略。对于电力行业来说，伴随着国家对于能源安全以及电力系统的高度重视，电力企业所面对的网络安全问题变得更加错综复杂。在法律法规方面，电力企业一定要遵守国家有关网络安全方面的规定，保证信息系统能够满足等级保护的需求，以免受到网络攻击或者数据泄漏等安全事件。

2 电力行业现有网络安全措施的不足

2.1安全防护体系不完善

尽管我国电力行业在网络安全方面逐步加强了投入和建设，但许多电力企业的安全防护体系依然存在不完善的问题。一方面许多电力企业安全防护设施比较落后，没有及时紧跟信息化建设与技术发展。尽管网络安全设施不断投入，但在面对日益复杂的网络攻击和安全威胁时，许多企业的防护体系依然处于应急应付状态，缺乏足够的深度防护层次。另一方面很多企业的安全防护体系建设没有和实际的业务需求相衔接，安全措施出现盲区，无法有效阻止安全漏洞在体系之间扩散。对大唐等电力企业而言，如何根据特定电力业务及信息系统需求，制定个性化安全防护策略是一个亟待解决的课题。

2.2安全意识不足

电力行业从业人员安全意识比较淡薄，特别是部分基层岗位及非技术人员对网络安全认识比较淡薄。部分职工没有充分认识到网络安全所带来的危险，在日常的工作中忽略了安全防护这一根本需求。比如，有些雇员可能随意处理包含敏感信息的文档或忽略系统更新、密码管理及其他基本操作[2]。这种安全意识上的不足使企业在抵御外部网络攻击时常缺乏由内而外的综合防护。另外，受信息化技术发展的影响，许多电力企业网络与信息系统所涉及的技术与设备越来越复杂，安全管理的难度也越来越大，但是整体安全意识并没有获得应有的提高。

2.3应急响应能力不足

在网络安全威胁日益加剧的情况下，应急响应能力已经成为电力行业是否能够有效应对网络安全事件至关重要的因素。但是，很多电力企业这方面建设还明显不够。尽管多数企业都制定了应急响应方案，但是这些方案实际可操作性不强，并且缺乏定期演练与考核，很难对真实网络安全事件起到应有的效果。另外电力行业信息化水平以及技术应用程度越来越高，使得应急响应复杂度越来越高，很多企业在各种复杂情景下都没有对应急处理方案进行充分考虑，致使企业在突发事件下应急响应与恢复能力不强。

3 网络安全等级保护在电力行业的实施

3.1等级保护定级

定级过程需结合电力企业业务性质，数据价值和系统功能多维度因素对各信息系统进行安全风险评估和合理分级[3]。通常情况下电力行业核心业务系统中，数据管理系统和调度控制系统属于等级更高的体系，应采取更严格的安全防护措施。通过等级定级可以使电力企业更准确地对不同级别的系统采取相应的安全防护措施以保证最主要的系统免受威胁并减少安全风险。对大唐等电力企业的定级工作要结合实际开展。应将企业核心系统以及参与电力调度及生产的数据系统划入最高安全等级中，避免外部攻击或者内部安全漏洞造成更大损失。

3.2安全防护体系建设

等级定级工作结束之后，电力企业有必要依据定级结果构建相关安全防护体系。安全防护体系的构建要从几个层次进行，主要从物理安全防护，网络安全防护和数据安全防护几个方面进行。比如对于核心数据与系统的保护，可采用加密，访问控制和防火墙的技术手段；对于网络进行安全防护可以通过配置入侵检测和入侵防御来保证外部攻击不能轻易攻破企业安全防线。电力企业安全防护体系建设要重视多层次，多维度防护策略，以保证各种潜在安全风险得到有效处置。对大唐这样的电力企业来说，构建满足其实际需要的安全防护体系不仅能够促进其安全防护能力的提高，同时也能够对电力生产与管理起到稳定保障作用。

3.3安全管理体系建设

电力企业安全管理体系建设应该包括安全组织架构，流程制度，人员管理和培训教育的综合规划。一是企业有必要建立一个专门网络安全管理部门来对企业全部信息系统进行安全管理；二是要建立安全管理的科学流程与体系，确定各个部门，各个岗位安全职责与权限。三是企业还应该加强对职工网络安全培训工作，增强全员安全意识，保证每个职工能够意识到信息安全的重要性并主动配合落实安全管理措施。电力企业可以通过建设一套完整的安全管理体系来达到对各信息系统进行全面有效地管理，保证各种安全措施的实施和不断完善。

3.4安全运维与监控

电力企业安全运维及监控体系，是确保信息系统能够长期，平稳运行的重点。企业有必要通过配置安全监控设备来实时监控全部关键信息系统并及时发现与应对可能出现的安全问题。另外，经常性地进行安全检查、漏洞扫描等都是保证系统安全性的重要途径。运维团队要加强系统维护与更新工作，保证系统时刻安全可控。对大唐这样的电力企业来说，其安全运维及监控工作要紧密地结合到日常的生产工作中去，保证系统的安全，同时要保证电力生产及管理不会受到损害。

4 网络安全等级保护的改进措施

4.1技术层面

从技术上讲，电力企业应强化信息系统安全防护工作，增强整体技术防御能力。一是企业要积极引入深度包检测，入侵检测及防御，网络流量分析以及数据加密等先进网络安全技术来提高抵御外部攻击能力[4]。特别是对类似大唐这类发电企业来说，

它的控制系统以及调度系统都牵涉到国家电网以及电力供应这类重要领域，如果受到了袭击，不但会影响到企业正常经营，还会造成大面积电力中断，或者公共安全事件。所以建设全面的防护体系非常关键。二是加强信息系统安全漏洞治理，定期进行漏洞扫描、渗透测试等工作，发现系统安全漏洞及时修补。另外在数据存储与传输的过程中要采用加密技术来避免数据的泄露或者篡改。对发电调度系统等关键设备与系统使用多因素身份验证与访问控制机制以保证仅有被授权人能够对关键资源与数据进行访问。加强这些技术手段能够有效地提高电力企业网络安全防护能力和减少由于技术漏洞带来的安全风险。

4.2管理层面

从管理层面上讲，电力企业要构建完整的网络安全管理体系来保证各种安全措施得以落实。第一，要成立网络安全管理专门部门和配备充足专业人员对企业信息系统进行安全管理。该部门既需要对整个企业网络安全防护措施进行整体规划，又需要定期对网络安全管理方案进行评价与更新，以便应对网络安全面临的新威胁。第二，电力企业要制定和严格落实信息安全管理制度、明确各部门、各岗位安全责任、建立健全安全审计机制。对一切信息系统与网络中的安全活动都应加以追踪，记录与审计，以保证问题能够被第一时间检测出来并且解决。第三，强化职工网络安全培训至关重要。通过对职工进行经常性网络安全培训来增强职工安全意识，让职工在平时工作中积极按照安全操作规程办事，杜绝因人为因素造成安全漏洞。对大唐这类企业来说，建立健全管理制度与安全文化不仅可以保障企业信息系统长期安全运营，更重要的是可以在全体员工当中形成网络安全风险联合防范意识，促进企业整体防护水平的提高。

4.3应急响应与恢复

电力企业要针对可能出现的安全事件制定周密的应急响应预案、定期开展应急演练、促进应急响应高效准确。应急预案应覆盖安全事件发现至业务系统恢复的整个过程，并明确责任人及应急措施，以保证遭遇网络攻击或者安全漏洞时能快速反应，减少事件给企业经营带来的冲击。对大唐等大型电力企业来说，如果出现网络安全事件就有可能造成电力调度系统出现中断或者发电厂控制系统出现威胁等，所以它的应急响应既要效率高，又要有较强的恢复能力。企业需保证备份数据完整性与可靠性，并迅速恢复关键业务系统正常工作。

4.4合作与共享

在网络安全变得越来越复杂的大环境中，电力企业同其他产业及机构之间的协作及信息共享变得更加重要。对大唐等电力企业来说，单一企业在面对复杂网络安全威胁方面实力似乎略显单薄，所以跨行业合作变得尤为重要[5]。电力企业要与政府部门，行业协会和网络安全公司等电力企业密切合作，组成安全联盟共同防御。电力企业通过和这些组织进行信息共享能够及时了解到安全威胁的最新情报并快速作出反应。另外，产业之间安全经验与防护技术能够互相借鉴与优化，有利于电力企业安全防护能力的提高。具体而言，电力企业可通过在产业之间搭建安全信息共享平台来及时告知网络安全事件、交流防护经验、提高整体防御水平。同时电力企业也可参与政府及行业组织网络安全研究及标准制定，促进全行业安全防护水平提高。

5 结束语

总之，电力行业网络安全等级保护工作的开展是一项系统工程，必须从技术、管理、应急响应与恢复、合作和共享几个方面来考虑。目前，电力行业虽然在网络安全上取得了一些进步，但是仍然有很多问题急需解决。通过持续完善安全防护体系、提高安全意识、增强应急响应能力、加强业内外协作和信息共享等措施，电力行业能够有效地应对越来越复杂的网络安全威胁。在今后的发展过程中，伴随着科技的进步与标准的不断提高，网络安全等级保护会为电力系统安全平稳运行提供更扎实的保证。要不断关注网络安全领域发展的新动向，探索创新的解决方案，迎接今后可能面临的种种安全挑战，保障电力行业可持续发展。

[参考文献]

[1]王健羽.网络安全等级保护在电力信息系统中的应用[J].网络安全和信息化,2024,(03):129-131.

[2]陈旭壮,朱琳.电力行业网络安全等级保护及关键信息基础设施保护[J].网络安全和信息化,2023,(11):41-43.

[3]能源局关于印发《电力行业网络安全等级保护管理办法》的通知[J].中华人民共和国国务院公报,2023,(06):54-59.

[4]国家能源局印发《电力行业网络安全等级保护管理办法》[J].自动化博览,2023,40(01):3.

[5]曾琼,倪芳.我国信息安全等级保护研究热点——基于Citespace的关键词分析[J].资源信息与工程,2020,35(3):136-139.

作者简介：

刘晋兵(1982--),男,汉族,山西太原人,本科,工程师,从事信息通信技术、网络安全。