Journal of Project Management
第3卷◆第1期◆版本 1.0◆2022 年
文章类型：论文 刊号（ISSN）：2737-4580(P) / 2737-4599(O)

电力监控系统信息通信网络安全及防护策略

闵 洁
（国网陕西省电力有限公司超高压公司 陕西西安 710065）

10.12238/jpm.v3i1.4554

[摘 要]电力系统运行过程中强化信息通信网络安全防护工作，显著提升电力系统智能化运作水平，提高通信网络安全运行的质量。鉴于此，文中以电力监控系统为着手点，分析实际运行中面临的安全问题，结合实际情况给出提高通信网络安全及防护的策略。

[关键词]电力监控系统；通信网络安全；防护策略

Information and communication network security and protection strategy of electric power monitoring system

Min jie
State Grid Shaanxi Electric Power Co., Ltd. Ultra High voltage Co., Xi'an, Shaanxi Province, 710065

Abstract: In the operation process of the power system, strengthen the security protection work of the information and communication network, significantly improve the intelligent operation level of the power system, and improve the quality of the safe operation of the communication network.In view of this, the power monitoring system as the starting point analyzes the security problems faced in the actual operation, and gives the strategy of improving the communication network security and protection according to the actual situation.

Key words: power monitoring system; communication network security; protection strategy

在日常的工作过程中，使用通信技术虽然顺应了时代发展的需求，并且这一技术也有着较强的开放性，但是在实际的使用过程中还是存在很多不确定的因素。随着时代的进一步发展，电力通信技术在各个领域都产生了较深远的影响。但是，在通信网络的构架中，还是存在一些问题，给一些犯罪分子提供了犯罪的机会。这样不仅会给部分企业带来经济损失，还不利于网络通信行业的可持续发展。因此，加强电力通信信息的安全建设是十分有必要的，这样才能最大限度地发挥电力通信技术的重要价值，并为相关行业提供更多的动力

1、电力监控系统信息通信网络安全现状

1.1 技术应用现状

电力通信网作为与电网同生并存的一张实体网，是电网运行控制的关键基础设施。电力通信网管系统是通信网络的重要组成部分，是保证通信网络高效、可靠和安全运行的重要基础。主要用于对通信传输设备进行配置管理、故障管理、性能管理、维护管理，实现实时监控、故障定位和配置下发等功能。

电力通信网的安全问题一直备受重视，针对相关的安全体系架构及技术已有较为深入的研究，但是针对网络安全问题的研究较少。随着网络安全法的颁布，电力通信网的网络安全问题得到更多的研究，基于大数据、云计算等新技术在电力通信网安全防御体系的应用被逐渐提出。但是针对电力通信网管系统的网络安全问题研究尚是空白。

1.2 技术标准化现状

按照《电力监控系统安全防护总体方案》（国能安全〔2015〕36 号）规定，电力通信网管系统属于电力监控系统，同时属于工业控制系统。电力通信网管系统网络安全方面涉及的相关标准包括有国家、行业、地方、企业标准等类型，通过全国标准信息服务等平台收集标准，截至 2021 年 6 月，我国已发布实施的相关标准共计 22 项，其中国家标准 13 项、行业标准 4 项、地方标准 2 项、企业标准 3 项。在这些标准中有 17 项为 2015 年后发布实施，近年来关于电力通信网管系统网络安全技术标准化水平不断提升。

网络安全等级保护是对信息及其信息载体按照重要性分级别进行保护的标准和要求，是国家信息安全保障的基本制度、基本策略和基本方法。国家于 2008 年颁布《信息安全技术 信息系统安全等级保护基本要求（GB/T22239–2008）》, 2019

第3卷◆第1期◆版本 1.0◆2022 年
文章类型：论文 刊号（ISSN）：2737-4580(P) / 2737-4599(O)

年颁布《信息安全技术 网络安全等级保护基本要求（GB/T22239–2019）》，注重全方位主动防御、动态防御、整体防控和精准防护，实现了对云计算、物联网、移动互联和工业控制信息系统及大数据等保护对象全覆盖。

2、电力监控系统信息通信网络信息安全的主要问题

我国电力通信行业在实际发展过程中存在很多和安全相关的问题，及时解决这些安全问题是十分必要的。做好信息安全工作，可以为后续工作提供更多的便利。在电力通信行业，主要有以下几种信息安全问题。

2.1 信息结构不合理

在电力通信行业，完善的信息结构是重要的基础，可以进一步推进电力通信行业的可持续发展。结合现阶段我国电力通信行业的发展来说，主要通过传输控制协议 / 互联网协议地址（Transmission Con-trol Protocol/Internet Protocol Address，TCP/IP）来实现信息的沟通。但是，需要格外注意的是，在我国电力通信行业中存在信息结构不合理的状况，因此，相关工作人员需要结合通信行业发展的实际情况对信息结构做进一步的调整，并及时地解决其中存在的各种问题，避免出现信息泄露的情况。

2.2 通信软件的信息安全问题

在电力通信行业，除了信息系统的构建工作外，还需要利用通信软件来辅助工作。可以这样说，通信系统和软件是通信工作发展的基本动力。随着我国电力通信行业的稳步发展，在通信行业使用软件的数量和频率得到了进一步提升，这就为我国的电力通信行业注入了活力。但是，其中也增加了很多不稳定因素，致使部分犯罪分子利用通信软件的漏洞入侵到电力信息系统中，这样就给企业带来了不利影响和经济损失。

2.3 工作人员素质较低

在电力通信行业，工作人员的专业素养对于通信工作来说会产生直接的影响。这是因为，工作人员的创新意识对于电力通信行业的实际发展来说有着重要作用。但是，需要注意的一点是，从我国通信行业的运行状况来看，部分工作人员的专业素养不高，这样就导致服务质量达不到标准。

具体情况有以下几种：第一，相关工作人员在日常的工作过程中没有获得专业的学习和培训，致使素质得不到提升；第二，工作人员的流动性较大，一部分工作人员的工作积极性不足，进而无法保障信息安全。

3、电力监控系统信息通信网络的安全防护策略

3.1 相关标准设计与制定

随着我国标准化工作改革的不断深入，标准已成为经济活动和社会发展的技术支撑。标准代表当前最佳实践方法，标准化方法和手段可以提升产业核心竞争力，促进产业向高质量方向发展。当前，围绕电力监控系统及工业控制系统已展开大量标准设计及制定工作，从通用要求上提出了较高标准。但是，电力通信网管系统作为电力监控系统及三级等保系统，其系统架构、设备类型等方面与电力监控系统仍具有较大差异，目前我国的各层级标准均缺少针对电力通信网管系统网络安全防护工作更细化的标准和要求。

后续应在已有标准的基础上，进一步根据电力通信网管系统运行特性，结合实际业务需求，明确总体要求、主要任务和建设步骤，统筹规划设计制定针对电力通信网管系统网络安全防护的技术规范与标准，引领电力通信网管系统向着安全稳定运行的目标发展。

3.2 安全管理原则对策

按照相关标准及法律法规要求，电力通信网管系统应从技术和管理两方面加强对网络安全的防护，防范黑客及恶意代码等对电力通信网管系统和通信设备的攻击侵害，保障电力通信网安全稳定运行。

在安全技术方面，应遵循“安全分区、网络专用、横向隔离、纵向认证”的原则，重点强化网络边界防护，同时加强内部的物理、网络、主机、应用和数据安全，加强对电力通信网管系统配置信息、告警信息等敏感数据的传输保密性和完整性保护。按照相关安全要求，应配备具备入侵检测、恶意代码防范、安全审计、可信验证、传输数据加密等功能的安全防护设备，安全设备应同电力通信网管系统新（改、扩）建工作同步规划、同步建设、同步使用。同时，应建设安全管理中心，作为网络安全统一管理的系统平台，实现统一管理、统一监控、统一审计、综合分析和协同防护，应包括系统管理、审计管理、安全管理和集中管控等功能点。通过安全管理中心，对电力通信网管系统所涉及的主机设备、网络设备、安防设备等进行全方位运行及安全态势感知。

在安全管理方面，应按照“谁主管谁负责，谁运营谁负责”的原则，建立电力通信网管系统的安全管理制度，明确安全管理责任。加强人员管理、权限管理、访问控制管理、安全防护系统的维护管理、常规设备及各系统的维护管理、恶意代码的防护管理、审计管理、数据及系统的备份管理、用户口令密钥

第3卷◆第1期◆版本 1.0◆2022 年
文章类型：论文 刊号（ISSN）：2737-4580(P) / 2737-4599(O)

及数字证书的管理、培训管理等管理制度。同时，应建立健全网络安全联合防护和应急机制，制定应急预案并定期演练，当电力通信网管系统遭到黑客、恶意代码攻击和其他人为破坏时，立即采取紧急联合防护措施，按应急处理预案采取安全应急措施，以防止事件扩大。

3.2 推进信息加密工作

在电力通信工作中，做好信息加密工作是非常重要的。与此同时，信息加密工作也是通信行业实际发展过程中的重要内容。现阶段，尽管技术设备有了很大程度的提高，但是由于管理层面出现了各种问题，致使信息加密工作还是存在一些不足和缺陷。

近年来，随着我国科学技术的飞速发展，信息加密工作得到了不断完善。为了保证信息加密工作的效率，需要做好以下几点：首先，需要将信息加密工作作为电力通信行业的重点工作；其次，相关工作人员要保证管理上的整体性；最后，选择科学、合理的信息加密方法。

3.3 健全网络通信系统

在我国通信信息安全建设的过程中，不断地完善网络通信系统是重点工作。健全网络通信系统需要先加强 IP 地址的保护，这样才能进一步提升信息系统的科学性。不管是对于企业还是普通的家庭来说，工作人员要保证相关参数的选取是科学、合理的。此外，完善通信系统，不仅顺应了时代的发展需求，还符合电力通信行业发展的实际情况，可进一步实现企业综合能力的提升。

为了杜绝恶意攻击事件带来的通信网络安全问题，工作者应提高对通信网络安全防护工作的重视，并基于 GB/T ▮ 20438、GB/T ▮ 21109 这两项电网安全标准，构建出完善的安全防护系统，提升电力系统安全通信水平。在此过程中，工作者可以利用 PON、电力载波 PLC-Io T.无线 e LTE-Io T 等通信技术，结合 IPSec、SSL、VPN、SSH 等安全协议，来构建一个完善的通信网络安全系统，例如：中国国家电网公司 SGCC 构建的“安全分区、网络专用、横向隔离、纵向认证”电力系统信息通信网络安防系统，在该系统中，该公司根据所应用的通信技术类型、通信内容等条件，将整体通信网络划分为四个安全分区，并借助各类安全协议建立的分区防护系统，同时，采用了独立的网络设备进行分区组网，以实现物理层面的防护。在电力系统二次防护机制中，该公司利用 IPSec、SSL 等安全协议，结合防火墙技术，构建了横向边界防护体系，实现了安全防护区域之间的逻辑隔离。并借助认证、访问控制、加密等技术，完成了纵向认证体系的建设，强化了通信网络二次防护效果，形成了一套完整的通信网络防护系统，为电力系统的稳定运行提供了保障。

3.4 提高工作人员素质

我国电力通信行业在实际的发展过程中，对于工作人员的专业素质培养需要重视起来。有效提升工作人员的专业素养是一个长期的工作，需要从以下几个方面进行完善：

首先，需要提高电力通信行业的入职门槛，这样员工的素养就得到了基本保障；其次，做好培训工作，定期或者不定期地对员工进行专业素养和服务质量培训；最后，企业的监管部门要充分发挥监管的作用，这样才能进一步提升工作效率。

4、结语

总之，电力通信网管系统作为电力通信网的重要组成部分，对电网安全有着重大影响。面对当前电力通信网管系统网络安全技术应用与标准化现状，应结合已有标准提出的网络安全防护需求，加快设计、制定具有针对性的各级标准，充分发挥标准化的引领作用，构建完备的电力通信网管系统网络安全防护体系，全面提升防御能力，助力国家“双碳”行动。在我国电力通信行业存在信息安全问题。为了保障我国电力通信行业的可持续发展，需要做好以下几个方面的工作：推进信息加密工作、健全网络通信系统、提高工作人员素质等。此外，还需要做好监管工作，这样才能发挥电力企业的主观能动性。结合我国电力通信行业的实际发展来说，不断地加大科研力度，才能促进行业的健康发展，为电力通信行业注入更多的活力。

参考文献

[1]欧阳宇宏,康文倩,车向北.电力监控系统信息通信网络安全及防护问题研究[J].信息系统工程,2020(12):60-61.

[2]王桂彬.电力系统信息通信网络安全及防护安全探究[J].信息通信,2019(12):168-169.

[3]叶磊,刘立亮,张科健.电力系统信息通信的网络安全及防护研究[J].通讯世界,2019,26(09):319-320.

[4]陈邵权.电力系统信息通信网络安全及防护措施研究[J].数字技术与应用,2019,37(09):188-189.

[5]李勇,李秀芬.电力系统信息通信网络安全及防护研究[J].数码世界,2019(09):36.

[6]李婧源.电力系统信息通信的网络安全及防护研究[J].通讯世界,2019,26(06):186-187.

