发电厂电力监控系统网络安全关键技术研究

宋新锋

（四川新华智合科技有限责任公司 四川成都 610000）

摘要：随着发电厂的不断快速发展，发电厂电力监控系统常因各种干扰因素而导致网络安全问题的频发，阻碍系统的正常运行，使其无法满足电力各项活动的需求。对此发电厂需要从多技术手段的角度出发构建发电厂电力监控安全防护系统，完善防护措施，有效降低各种风险，确保发电厂日常工作的顺利进行。对此本文主要浅谈发电厂电力监控系统网络安全关键技术的研究，先阐述了发电厂电力监控系统网络安全现状，后提出主要关键的技术。

关键词：发电厂；电力监控系统；网络安全；关键技术

Research on key technology of power monitoring system

Xinfeng Song

Sichuan Xinhua Zhihe Technology Co., LTD. Chengdu，Sichuan，610000

Abstract: With the rapid development of power plants, the power monitoring system of power plants often leads to frequent network security problems due to various interference factors, hindering the normal operation of the system, so that it cannot meet the needs of various power activities. In this regard, the power plant needs to build the power monitoring and safety protection system from the perspective of multiple technical means, improve the protective measures, effectively reduce various risks, and ensure the smooth progress of the daily work of the power plant. This paper mainly discusses the research of the key technology of network security of power monitoring system in power plant, first expounds the current situation of network security of power monitoring system in power plant, and then puts forward the main key technologies.

Key words: power plant; power monitoring system; network security; key technology

引言：

当前发电厂电力监控系统的运行外部环境更加复杂，因网络本身具有开放性和共享性的特点，导致其常会出现网络安全问题，因此必须提高发电厂对电力监控系统安全防护的重视程度。在电力监控系统运行的过程中要重点围绕电力监控系统和网络安全防护核心要素进行科学设计和开展网络安全防护工作，确保系统能够安全、高效率的运行。另外还需要加强监测和分析，有效解决病毒入侵和信息泄露等问题，最终满足发电厂电力监控系统的安全运行和发展需求。

一、发电厂电力监控系统概述

发电厂电力监控系统是指为了保证发电厂电力设备稳定运行、保障电力安全稳定运行而建立的一个集成化的监控系统。其目的是通过对发电厂各项运行数据的实时采集、处理和分析，对发电厂的电力设备、电力运行状态进行实时监控和管理，实现对电力生产过程的全面掌控，保障电力生产的安全、稳定和高效运行[1]。

发电厂电力监控系统通常包括以下组成部分：

（1）数据采集子系统：主要负责对电力设备的运行数据进行采集、处理和传输，包括各种传感器、数据采集终端、数据通信设备等。

（2）数据处理子系统：主要负责对采集的数据进行处理、存储和管理，包括数据处理服务器、数据库、数据挖掘和分析软件等。

（3）监控显示子系统：主要负责对处理后的数据进行可视化显示和报警，包括监控显示终端、报警系统、人机界面等。

（4）通信子系统：主要负责系统内部各个子系统之间的通信，包括局域网、广域网、互联网等。

发电厂电力监控系统的安全稳定运行可以提高电力设备的使用效率，减少能源浪费，降低企业的生产成本，具有重要的经济和社会意义。

二、发电厂电力监控系统网络安全现状

随着信息技术的不断发展和应用，发电厂电力监控系统的网络安全问题日益突出。当前，发电厂电力监控系统所面临的网络安全威胁主要包括以下几个方面：

（1）黑客攻击：黑客攻击是指攻击者通过网络渗透和攻击技术，进入发电厂电力监控系统内部，窃取敏感信息、破坏系统、篡改数据等，从而导致发电厂电力设备的异常运行和电网的不稳定运行。

（2）病毒感染：病毒感染是指发电厂电力监控系统受到病毒攻击，从而导致系统运行异常或瘫痪。病毒可能通过网络传播、移动设备或U盘等方式传入系统。

（3）内部员工失误或恶意操作：发电厂电力监控系统内部员工失误或恶意操作也可能导致系统的安全问题。员工可能误操作、泄露敏感信息或者恶意篡改数据，从而影响发电厂电力设备的正常运行和电网的安全稳定。

针对以上的安全威胁，发电厂电力监控系统的网络安全现状存在以下几个问题：

（1）安全策略不完备：许多发电厂电力监控系统存在安全策略不完备的问题。缺乏安全管理和监控措施，难以识别和防范潜在的安全威胁。

（2）系统安全漏洞：由于发电厂电力监控系统存在软件和硬件等方面的漏洞，黑客攻击者可以利用这些漏洞进行攻击，导致系统瘫痪或者数据泄露。

（3）信息共享不足：当前，发电厂电力监控系统之间存在着信息共享不足的问题。发电厂之间无法实现数据的共享和信息的交流，导致难以及时发现和防范安全威胁[2]。

三、发电厂电力监控系统网络安全关键技术

为了加强发电厂电力监控系统的网络安全防护，需要采用一系列的关键技术来保护系统的安全。以下是一些关键技术的介绍。

（一）访问控制技术

访问控制技术是通过对系统用户进行身份验证和授权管理，来控制用户对系统的访问权限。通常，访问控制技术包括认证、授权和审计三个部分。认证指的是验证用户身份的过程，授权是指确定用户是否有权访问特定资源的过程，审计则是监控和记录用户对资源的访问行为，以便后续进行审计和调查[3]。

（1）身份验证

身份认证是指验证用户身份的过程，以确认用户是否具有访问系统的权利。常见的身份认证方式包括口令认证、智能卡认证、生物特征识别等。

（2）授权

授权访问是指对用户身份进行认证后，对其进行授权管理，限制用户对系统中某些资源或功能的访问。授权管理通常通过访问控制列表（ACL）或角色授权等方式实现。

（3）安全审计

安全审计是指记录系统中所有用户的操作记录和行为信息，以便进行后续的审计分析。通过安全审计可以及时发现和解决用户违规操作、

异常访问等安全事件。

（二）加密技术

加密技术是指利用一定的算法和密钥，将明文转换为密文，从而保证数据在传输或存储过程中不被非法获取和篡改的技术手段。在发电厂电力监控系统中，加密技术可以用来保护敏感信息，防止机密数据被泄露，确保信息的完整性和保密性。加密技术可以根据加密方式、密钥管理和密钥分发等不同方面进行分类。根据加密方式的不同，加密技术可以分为对称加密和非对称加密两种。

（1）对称加密

对称加密是指加密和解密使用同一密钥的加密方式，也称为共享密钥加密。对称加密算法的主要特点是加解密速度快、加密效率高，但密钥分发和管理相对较为困难。常用的对称加密算法有 DES、AES 等。

（2）非对称加密

非对称加密是指加密和解密使用不同密钥的加密方式，也称为公钥加密。公钥用于加密，私钥用于解密。非对称加密算法的主要特点是安全性高，密钥管理方便，但加解密速度相对较慢。常用的非对称加密算法有 RSA、ECC 等。

（三）安全审计技术

安全审计技术是指对发电厂电力监控系统中的安全事件、安全状态和安全配置等信息进行收集、分析和审计的技术手段。安全审计技术可以帮助发电厂及时发现安全问题和风险，及时进行安全补丁升级、安全策略调整等操作，从而提升电力监控系统的安全性和可靠性。

（1）安全日志收集

安全日志是指电力监控系统中记录安全事件、安全状态和安全配置等信息的文件或记录。安全日志收集是指收集并存储这些安全日志信息的过程。通过对安全日志的收集和存储，可以追踪和分析发电厂电力监控系统中的安全事件和异常行为，及时发现和解决安全问题。

（2）安全事件分析

安全事件分析是指对电力监控系统中的安全事件进行收集、分析和识别的过程。通过安全事件分析，可以确定安全事件的来源、性质、影响等信息，从而进行安全应急响应和安全事件处理。

（3）安全状态检测

安全状态检测是指对发电厂电力监控系统中的安全状态进行实时监测和检测的过程。通过对安全状态的检测，可以及时发现电力监控系统中的安全漏洞和风险，进行及时的修复和升级操作，从而保证电力监控系统的安全性和可靠性。安全状态检测可以采用自动化工具进行检测，也可以采用人工审查的方式进行。

在实际应用中，安全审计技术可以配合其他安全技术进行使用，如 IDS/IPS 技术、漏洞扫描技术、弱口令扫描技术等，从而更好地提升电力监控系统的安全性和可靠性。

（四）漏洞扫描技术

漏洞扫描技术是一种主动式安全技术，用于检测系统或应用程序中可能存在的漏洞。发电厂电力监控系统中的漏洞扫描技术可以帮助识别网络或应用程序中存在的安全漏洞，以便及时进行修补，从而提高系统的安全性。

漏洞扫描技术通常通过对系统或应用程序的网络端口进行扫描，并对常见漏洞、已知漏洞和零日漏洞等进行检测。

在发电厂电力监控系统中，漏洞扫描技术需要具备以下特点：

（1）准确性：扫描技术需要准确地检测出系统中存在的漏洞，并给出详细的报告。

（2）可扩展性：系统中可能存在多种不同类型的设备和应用程序，扫描技术需要具备可扩展性，以适应不同的环境。

（3）实时性：随着系统的更新和漏洞的不断出现，扫描技术需要实时更新并检测最新的漏洞。

（4）高效性：扫描技术需要在不影响系统正常运行的情况下，快速地扫描并检测出漏洞。

（五）网络隔离技术

网络隔离技术是指通过技术手段将不同网络之间进行物理隔离或逻辑隔离，以达到保障网络安全的目的。在发电厂电力监控系统中，网络隔离技术可以帮助实现网络安全和信息安全的隔离，提高系统的安全性[5]。

在发电厂电力监控系统中，通常会存在多个网络，如监控网络、数据网络、办公网络等，这些网络需要进行隔离以保障其安全性。网络隔离技术可以通过以下方式实现：

（1）物理隔离：即通过物理手段，如使用独立的交换机、路由器、防火墙等设备，将不同网络进行物理隔离，避免数据在物理层面上相互干扰。

（2）逻辑隔离：即通过虚拟化技术或软件隔离等技术手段，将不同网络进行逻辑隔离，实现虚拟网络之间的安全隔离。

（3）授权访问：即通过授权和认证机制，限制用户访问不同网络的权限，避免未经授权的用户访问网络。

网络隔离技术的实现需要考虑以下因素：

（1）安全需求：根据不同网络的安全需求，选择合适的隔离方案。

（2）设备选型：选择合适的交换机、路由器、防火墙等设备，以实现网络隔离。

（3）管理与维护：对隔离网络进行管理和维护，及时更新设备和软件，以保障网络的安全性。

（六）备份与恢复技术

备份与恢复技术是指通过对系统和数据进行备份，以及在发生故障时进行恢复，保障系统和数据的可用性和完整性的技术手段。在发电厂电力监控系统中，备份与恢复技术可以帮助实现系统的可靠性和稳定性，以及应对系统出现异常时的应急处理能力。

在发电厂电力监控系统中，备份与恢复技术通常需要考虑以下因素：

（1）数据备份：针对不同类型的数据，选择不同的备份策略和方法，如全量备份、增量备份、差异备份等。

（2）备份频率：根据系统的使用频率和数据更新速度，设置合适的备份频率，以保证备份数据的及时性和完整性。

（3）备份存储：选择合适的备份存储设备，如硬盘、磁带等，以确保备份数据的安全和可靠性。

（4）恢复速度：根据系统的恢复需求和数据量，选择合适的恢复策略和方法，以确保系统的快速恢复。

（5）备份验证：对备份数据进行验证和测试，以确保备份数据的可用性和完整性。

备份与恢复技术也是应对系统异常情况的重要手段，可以帮助系统快速恢复并降低故障对系统造成的影响。

四、结束语

因为发电厂本身的电力监控系统的特点和运行调整、网络环境的特点导致在系统运行中常常会出现网络安全问题，且安全问题日益严重。安全问题是国家和电厂行业关注的重点，对于发电厂而言需要根据国家电力监控系统安全防护规定要求和能源局提出的方案、相关辅助设施配套方案等进行管理，遵循安全分区、网络专用、横向隔离、纵向认证、综合防护的原则，做好区域防护管理，并制定科学的防护措施和安全管理制度，有效提高系统运行的安全防护能力和水平。

参考文献：

[1]张露,钱波安,陆习良.发电厂电力监控系统网络安全关键技术研究[J].云南水力发电,2022,38(S1):95-96+100.

[2]安江.信息安全防护技主在电力监控系统中的应用[J].数字技术与应用,2022,40(07):218-220.DOI:10.19695/j.cnki.cn12-1369.2022.07.69.

[3]田海波,何萍,张易牧.发电厂计算机监控系统及其信息安全防护监理实践[J].设备监理,2022(01):23-27.DOI:10.19919/j.issn.2095-2465.2022.02.006.

[4]艾远高,谢秋华,黄家志,杨云.电力监控系统安全防护与监测预警平台建设[J].水电站机电技术,2021,44(10):33-36.DOI:10.13599/j.cnki.11-5130.2021.10.011.

[5]张俊岭.水电站电力监控系统信息化建设探讨[J].新型工业化,2021,11(04):194-195.DOI:10.19335/j.cnki.2095-6649.2021.4.073.