电力安全生产中的信息化技术应用

旦增欧珠　张官佳
国网西藏电力科学研究院

摘　要：近年来，随着网络通讯技术的迅速发展，我国的信息化程度也在逐步提高，同时也在不断地改善着电网的运行状况。电力企业应以其自身的特点为基础，利用计算机网络技术，构建一个完整的企业安全管理信息系统。通过对这些数据的有效集成，可以为企业提供更科学、更有效的数据，从而更好地服务于电力企业的生产实践。通过对电力企业的安全生产管理技术进行持续改进，可以降低事故的发生概率，提升电力企业的发电效率，进而提升其核心竞争能力。

关键词：电力安全；生产安全；信息化技术
【DOI】10.12252/j.issn.2096-627X.2022.05.205

引言

在电力工业中，发电企业的安全运行和生产过程中的信息化监控是至关重要的。通过信息技术的运用，可以提高电力生产的安全性和效率，降低设备的故障率，减少事故的发生。因此，研究电力发电企业安全生产全过程信息化监控方法具有重要的现实意义。电力发电企业的安全生产不仅关系到企业的经济效益，还关系到广大人民群众的生命财产安全和社会稳定。电力设备的故障和事故往往会给企业和用户带来重大的经济损失和安全隐患。因此，电力发电企业的安全生产是至关重要的。为全面落实并推进此项工作，电力发电企业在开展了大量研究后，明确了信息化监控在电力发电企业安全生产中应用的重要意义。利用信息技术可以对发电生产过程进行模拟和优化，提高生产效率和能源利用率，降低生产成本，同时也可以对生产过程中的数据进行实时采集和分析，发现和解决问题。总之，信息化可以对发电企业的安全管理提供有力的支持。

一、电力企业信息化安全管理中存在的问题和原因

1.电力企业生产过程中存在的问题和原因

在电力工业的发展过程中，它已经形成了一套完善的、稳定的责任管理体系和需求，尤其是近年来，市场经济的飞速发展，更是促使了社会对电力企业的生产工艺提出了更高的要求。然而，在科技进步、用电需求不断增长的今天，电力企业在生产工艺上也出现了许多新的问题与挑战。首先，在电力生产流程中，由于信息化管理的孤立性，已成为制约其高效运行的最大因素，因此，在电力生产流程中，各环节间的信息交互是确保全流程顺利运行的关键。当前，许多发电企业的生产系统之间往往存在着信息互联不畅的现象，形成了“孤岛效应”，对整个电网的运行效率与安全性造成了极大的威胁，已成为制约我国电网安全运行的重要因素。其次，电网本身的安全性能无法有效地与生产流程相适应，导致整个生产装置的控制性能下降。它的控制体系不能合理、科学地管理和处置各个生产环节，从而导致了许多生产环节的延迟和延迟。在生产过程中，由于不完美的控制系统，导致了许多生产环节都发生了问题，如果其中一个环节出了问题，那么整个生产流程就会陷入瘫痪，从而导致严重的生产事故。

2.电力生产过程中安全问题的原因分析

要想更好的处理电力生产中所遇到的问题，就必须要找出问题的根源，并将其与信息科技相融合，从而对今后的电力公司发展起到一定的促进作用。首先，随着信息化水平的提高，电力行业对信息化的依赖越来越强，在一定程度上也会严重地影响到员工的工作心态，尤其是在自动化的控制流程下，许多技术人员往往忽视了日常的生产检验，极易引起重大安全事故。其次，信息时代的生产工艺要求有专门的工程师对其进行适时的维修与维修，许多电力制造企业受传统的生产工艺的制约，许多在生产工艺上的员工的整体素质都比较差，无法科学地对现代化的资讯科技进行管控。

二、电力安全生产中的网络信息化技术

1.入侵检测技术

入侵检测技术是指通过对网络流量和系统运行进行监控和分析，它能够及时地发现并告警网络中的非授权或异常情况。通过基于反向管理的入侵检测技术，在各变电站等信息站点实时和非实时交换机上部署综合威胁探针用于采集涉网侧业务系统日志及流量，通过联动安全管理平台实现涉网侧的全流量采集、分析及溯源。在监控侧部署大数据分析平台，利用大数据平台强大的大数据分析能力及各类机器学习算法，结合攻击链模型快

速定位涉网侧的安全风险并汇总各场站安全分析结果以及进行综合分析、研判和展示，实现电力信息网络场站涉网侧的全局安全态势可视化。

2.虚拟专用网络技术

电力信息网络物理网架支撑主要随电网主网同步规范、同步建设、同步投入使用，OPGW复用光缆随输电线路敷设的同时，电力信息网络在放射状辐射，虽然电网主网覆盖范围广，但是仍然有例如市区或偏远地区的信息站点未覆盖光缆资源，考虑到投入产出比，通常电力企业采用虚拟专用网络技术（VPN）实现各站点的网络互通，具有现实意义[1]。虚拟专用网络技术本身已具备数据加密和认证的属性，具备一定的安全性，但是在实际使用中，仍然需要加强管理，网络访问授权采取最小化原则，加强设备运行健康监测，实时对设备相关操作系统、各类特征库版本进行更新。如果访问的业务或资源安全级别比较高，为了提升安全性，还需额外购置VPN防护设备或服务。

3.防火墙技术

防火墙技术是指通过对网络流量进行过滤和控制，保障电力信息网络的合法访问。采用网络防火墙、主机防火墙、应用程序防火墙等技术手段，实现对网络流量的过滤和控制。相较传统防火墙，电力信息网络投入智慧防火墙可实现复杂危险源的防御和快速处置，结合互联网强大的威胁情报信息，将极大提升电网网络安全风险管控能力和处置效率[2]。值得注意的是，随着电力企业向“两地三中心”网络架构和信息系统云化发展战略的深化，传统网络架构与云化混合网络下的防火墙安全策略统一运维问题将日渐显著，垃圾策略不断堆积，人工处理难度大，一旦操作失误，会给业务访问及网络使用授权带来安全隐患，进而招致网络攻击，威胁电网安全运行，因此，在安全策略管理和运维方面，构建面向全网的集中可视化管理和自动化运维平台具有很大的必要性。

4.恶意软件检测和清除及安全漏洞管理技术

恶意软件检测和清除是最常见的一种网络安全技术，用于检测和清除计算机上的恶意软件。应用门槛最低，也是网络安全防护中的首要防线，常用的恶意软件检测工具包括杀毒软件、反间谍软件、反恶意软件等，可以检测和清除恶意软件，例如病毒、木马、蠕虫、间谍软件等。恶意软件检测和清除技术通过实时扫描、定期扫描、自动更新病毒库等方式提高安全性。安全漏洞管理技术则可以及时修复终端设备上的漏洞和安全缺陷，以防止攻击者利用漏洞进行攻击，它通过自动更新、手动更新等方式提高安全性[3]。通过建设内外网准入控制平台，确保防病毒软件和安全防护类软件的百分百安装率，并将安装防病毒软件作为网络入网的准入条件，设置防病毒特征库自动更新策略，在用户无感知的情况下，实现终端防病毒能力提升。此外，由于互联网暴露资产是不法分子最重要的攻击方向和目标，因此需要对资产进行全面梳理，摸清家底才能做好防守工作，企业遭受网络攻击，很多情况下是由于未知资产防护不到位引起的，需要通过技术手段结合管理手段，对电力信息网络中的资产信息进行全面梳理，在网盘、Github、Ozone等工具或网站，使用关键词查询和人工搜索对互联网暴露面资产进行收敛。借助使用资产发现设备和扫描设备，实现各类设备漏洞发现和漏洞修复验证[4]。最后，等级保护测评是安全漏洞管理的重要手段，通过第三方检测机构开展电力信息网络及信息系统等保测评，从安全管理、技术管理、边界安全防护等多方面排查治理安全隐患，建设纵深网络安全防护体系。

5.数据备份和恢复定期备份和测试

数据恢复程序是确保备份和恢复策略有效性的关键步骤。加强电力信息网络数据安全防护，首先是强化数据安全管理，采取全备份、按需备份等方式实现重要数据的备份，定期有规律地开展重要数据备份，同时要保障存储数据的安全性，主要是环境安全，存储介质放置于温度、湿度、磁场等环境因素均符合要求的场所并指定专人负责，做好数据分类，在发生系统故障时，第一时间定位备份数据源并开展数据恢复工作。其次是建设数据中心级的异地灾备中心，从通信距离及管理可行性角度考虑异地灾备中心位置，采取三副本备份方式，实现重要信息系统，如营销数据的自动数据备份及数据恢复。此外，电力信息网络安全应考虑建设两地三中心应用级容灾备份，实现重要业务，如营销缴费，企业经营管理的应用服务安全，在发生不可抗力因素时，保障供电服务的连续性、稳定性[5]。最后，随着大型能源企业的云化改造推进，在建设企业私有云的同时，还应提前谋划云安全事宜，构建异构云和云备份安全，打造企业坚强云应用服务。

三、加强电力安全生产管理信息化管控的措施

1.加强电力企业内部交流

第一，企业的发展离不开企业内部的信息交流，企业精神的战略性传达、企业文化的宣传指导等，这些都需要快速地传递出去；而信息技术则能很好的适应这

一需求，加快企业内部的信息传递速度，提高工作效率[6]。第二，信息化的应用为企业经营开辟了一条新的途径，既可以对员工进行科学的工作分配，又可以推动企业文化的形成。信息化科技虽然可以提升企业的核心竞争力，但也要求企业不断地进行变革，进行知识储备的革新，对系统设施进行更新，如果只是遵循旧的规则，就不能跟上市场的变化，不能跟上市场的节奏。

2.巩固信息系统网络安全

要根据企业的实际情况和未来发展的实际需要，充分发挥它在网络、资源、信息等方面的优势，加强企业内部信息安全管控平台的建设，提高全体员工对互联网安全的认识。在技术上，还需要不断地加强对信息安全的控制。要保证资料存储和分发的安全性，并要有完善的网络体系。

3.提高电力企业职工对信息化管理的关注水平

尽管我国电力企业的网络建设一直在进行，但仍有很多电力企业对这一工作的重视程度不高，对相关从业人员的技术需求也不高，这就导致了信息管控工作不能充分发挥自己的作用。要预防这种情况，就必须根据实际情况，全面考虑自己的实际需求，明确信息控制人员的职责，并且定期进行相关的技术培训，提升员工的职业水平，评估员工的业务能力，对不合格的员工予以解聘。此外，要加强对信息技术人员的思想认识，明确其权利与责任；指导他们在工作中总结和分析自己的实际经验，不断地提升自己的能力，逐步完善信息化管理平台。

4.结合企业实际制定科学的信息化管理模式

不同的电力公司所面对的现实问题是不一样的，所以在进行信息化管理的时候，要根据自己的实际情况，制定一套科学、稳定、合理的信息化控制方式，并根据各个部门的工作特征来进行设计，确保生产流程的无故障、无延迟和协调化。总之，在电力安全生产流程中，要结合具体的问题，对各个生产环节进行科学的设计，保证整个生产过程的稳定与安全。

5.加强信息化监控

1）安全生产全过程监控布置

为了适应电力企业全流程的安全监测需要，在设计方案之前，应按照企业的生产设备数量、规格和覆盖范围来确定监测范围。在这一过程中，引入了现场总线技术，将电网企业的厂级管理体系与企业的安全生产现象联系起来，生产操作设备，机械设备。采用现场总线技术中的开发型网络连接模型，实现了现场通讯协议方式的设置，保证了设备在接入后仍能与监测终端保持良好的通讯状态。根据技术要求，现场布置宽带基带，设计设备在低速率总线状态下的通讯速率为30Kbps至35Kbps，高速总线状态下设备的通讯速率为2.5Mbps，1Mbps。在确定了基本参数之后，对监测装置的数量，总线的长度，监测通讯的响应时间进行了设计。根据以上方法，在完成了监测参数的设计之后，对电力生产企业的安全生产全过程监测装置进行调试和试运行，保证监测工作符合要求，并且在设备之间能够维持较好的通信状态，对发电企业的安全生产进行全程监测和部署。

2）企业安全生产信息追溯

为了保证整个监测过程的信息化，首先要对企业的安全生产信息进行编码，并对其进行编码，从而可以追踪到整个安全生产流程中存在的不安全信息和隐患。信息部门还应对系统自动记录的生产信息进行管理，对历年的产品数据进行汇总，放入专门的文件存储系统中，避免占用过多的内存，从而影响到系统的运行。通过对这些数据的分类、总结，可以实现标识信息的溯源。

结束语

随着社会、经济、科技的飞速发展，在市场经济环境下，电力公司面对着越来越多的挑战与竞争。因此，要想得到更好的发展，就必须采用信息化的管理方式和生产技术。在提高生产效率与安全性的前提下，强化对生产数据与信息的保护，进而提高公司的整体竞争力。

参考文献

[1]李旭峰.电力安全信息化管理中常见的问题及应对措施探讨[J].数字通信世界，2022，（10）：188-190.

[2]张胜男，刘晓.基于信息化系统的电力企业安全风险管控问题研究[J].企业改革与管理，2021，（21）：10-11.

[3]罗莎莎.信息化技术在电力安全管理工作中的应用研究[J].中国新通信，2021，23（21）：145-146.

[4]王均.云安全终端在电力信息化管理中的应用[J].集成电路应用，2021，38（10）：118-119.

[5]索吉鑫，李文娟，韩宝卿，杨生婧，马忠梅.安全技术在电力信息化建设中的应用研究[J].电子元器件与信息技术，2021，5（06）：40-41.

[6]迟克寒.探析电力系统信息化安全技术的解决方案[J].数字技术与应用，2021，39（05）：193-195.