电力调度自动化网络安全与实现技术

尚浩志
国网浙江省电力有限公司嘉兴供电公司　浙江嘉兴　314000

摘　要：随着信息技术的飞速发展，无线网络通信、多媒体处理等技术水平逐步提升，充分应用智能移动终端的便携性、强大的信息处理能力对复杂庞大的信息业务进行处理，有效降低了人工业务处理的繁琐程度，大大提升了工作效率。基于移动终端的业务处理方法将成为未来信息技术发展的一种必然趋势。

关键词：电力调度；自动化；网络安全

引言：

电网朝着智能化的方向发展就形成了智能电网，智能电网集成了电力、计算机、通信、网络等先进技术，尤其对高速双向通信网络有严重依赖。智能电网的应用使传统的电网更加可靠、安全、经济、高效，可以在无人干预的情况下实现一定程度的自愈、激励和自我防护。但是随着电网规模的不断扩大和电网结构的日益复杂，保障电网的安全、稳定运行更加困难，其中网络安全问题是智能电风系统发展过程中面临的一大挑战，本文将对其进行深入而全面的探讨。

一、智能电网与网络信息安全

智能电网除了要求具有电力电子硬件之外，还要求这些硬件之间建立可靠的联系，信息和数据可以在电网内部自由流动，而这一切都需要网络通信技术作为支撑。由电网中采集到的各种硬件状态信息、用户用电信息、维护检修信息，最终都会通过网络汇聚到特定的信息化平台，例如用于种类业务管理的电网集团ERP、电力营销平台、电力市场交易平台、综合业务平台，以及用于生产管理的安全生产管理系统、运维管理系统、厂级监控信息系统、设计科研平台、能量管理系统等等，这些信息化平台都属于电力系统的内网，共属一个局域网。电网作为重要的国家基础设施，其产生的数据具有特殊的重要性和保密性，因而智能电网的建设就会不可避免地涉及网络安全的问题。电网系统网络安全问题。智能电网系统主要包括发电、配电、输电、供电等生产环节，各环节都需要处理电网信息和用户数据，因此具有较高的网络安全风险。从以往智能电网系统网络安全管理实践来看，智能电网系统面临的安全问题主要包括窃听、重发、信息篡改、拒绝服务、恶意软件等等，实施网络攻击的主体则可能为黑客、网络技术爱好者，甚至是内部员工。在一些案例中，内部人员恶意破坏、越权访问、滥用职权、操作失误、管理不当等是网络安全的主因，内部工作人员可能利用自身的身份便利有意破坏或篡改内部数据，越权使用系统资源，或泄漏账号密码、出卖信息，当然也包括部分工作人员业务不精而出现误操作，对数据造成破坏。来自外部的威胁主要是黑客入侵和病毒攻击，其中黑客攻击是指黑客通过暴力破解账号密码的非法入侵，对系统内部的数据进行破坏或窃取；病毒感染则是通过端口扫描或伪装等方式将病毒文件植入内网，由病毒软件对内网数据进行破坏或加密，最常见的是勒索病毒。

二、电力调度自动化背景下网络安全与实现技术

1.调度核心系统

调度核心系统是建立基于移动平台的电力调度系统的根基所在，提供电网运行调度数据的来源以及辅助平台应用建设的规范和标准，包括了运行管理系统、运行监控系统、数据中心和气象系统等，通过调度核心系统进行停电检修计划、调度指令、图纸信息等实时信息的收发，实现对大电网的电力调度。

2.系统安全控制

在大电网电力调度运行控制的过程中，需要对信息数据进行加密处理，防止信息泄露情况的发生，以保障系统的安全性。而移动通信设备终端所具备的可移动性、高网络开放性、所处环境复杂等基本特点，无法保证信息传输的安全性和保密性。为此，基于《电力监控系统安全防护规定》的基本准则，按照“安全分区、网络专用、横向隔离、纵向认证”的总体策略对移动平台进行设计，从通信、认证、数据3个方面对系统安全进行控制。（1）设备通信。各移动通信设备基于VPN通道在外部公用数据网间进行通信的，采用APN通道形式访问供电局内网与移动通信平台进行通信。通过防火墙等网络

作者简介：尚浩志，1989.12，安徽蚌埠人，汉族，男，研究生，工程师，就职于国网嘉兴供电公司电力调度控制中心自动化专职。研究方向：电力系统调度自动化、智能电网调度控制系统

防护技术以及软硬件系统构建移动通信服务平台的隔离区（Demilitarized Zone，DMZ）和可靠性高、扩展性强、技术先进以及安全性高的调度核心系统数据中心（IDC），实现隔离区与调度核心系统的可控通信。（2）信息认证。对于移动通信设备，其用户密码与动态口令需要通过移动通信服务平台的集中认证系统的认证，才能保证移动智能终端以及访问客户的合法性。对于第三方应用软件，其携带有用户凭证并装设了票据验证插件的业务服务器，因此无需像移动通信设备那样需要输入用户密码，可通过票据认证结果来进行移动通信服务平台的访问，若票据认证通过，则允许访问相关业务数据，否则无法访问相关业务数据。需要说明是，当第三方应用软件需要与调度核心系统进行数据交互时，必须要经过移动通信服务平台转发，且数据信息需要做加密处理。

3.制定可行的处理预案

按照保证电网、设备、人身安全的工作要求，调度人员应根据现阶段电网运行情况，编制事故应急处置预案。从不同等级、不同类型的范畴，进行事故预演，提前做好事故发生后的工作安排和处理步骤。制定出切实可行的处理预案，能够提高调度应急处理水平与效率，为调度人员相关工作的顺利进行指明方向。

4.加强电网调度智能化管理水平

从客观的角度讲，大规模的电网事故通常是基于突发状况下发生的。发生过程中，会出现大量、冗余的电网信息。调度员需要不断甄别、判断各种故障信息，费时费力且容易误导思路。因此，在调度管理系统中引入智能辅助决策功能，帮组调度员进行信息判断，提供故障处理策略，可以大大提高故障处理的时效性。

5.防火墙的设置

智能电网在运营管理过程中，经常需要与外界网络进行数据交换，因此网络层面上必须与外界有互通的端口，这虽然方便了管理，但安全威胁的概率也显著提升。为此，可以采用防火墙进行边界管理。边界防火墙应具备高吞能力，根据内部业务特征、组织机构和部署特点划分不同的安全域，为不同的网络划分清晰的边界。边界防火墙应开启包过滤策略，对网络的相互访问进行精确的控制。防火墙还应支持超高并发访问，用于应对百万包/秒级别的DDoS攻击。对于网络的外部，应采用IPS入侵防御、AV网关防病毒和AS反垃圾邮件三重防护策略，保证外部威胁可以被边界防火墙精确拦截，确保内网安全。

6.数据的安全传输

智能电网系统作为关系国计民生的特殊系统，具备强大的数据采集和数据传输能力，而在数据的传输过程中存在被人非法窃听或篡改的风险。为保证数据的完整性和保密性，需要对数据传输风险进行针对性地防护设计。通过构建一套数据传输安全控制体系可以实现数据的安全管理，体系中主要包括认证机构、注册审核机构、数字证书库、证书作废系统等模块，首先将公钥和个人信息发送给注册机构进行认证，通过后将其发送给认证机构签名并生成数字证书，由服务器端对数字证书进行维护，保证每一次访问都是安全的。为避免明文传输，在数据传输过程中还应采用数据加密算法，但是在加密复杂度和传输速度上要取得合理平衡，防止影响系统的综合性能。

7.提升调度人员事故处理能力

对调度人员做好培训工作。首先，调度员作为电力调度工作中的关键环节，其工作经验以及技术水平会对这项工作整体质量产生直接的影响。所以这就要求调度人员除了要熟知工作流程以及相关规范要求之外，还需要对继电保护和自动装置工作原理与定值有一个全面的认识。应当定期对这些员工进行培训，旨在让他们可以对调度基础知识、继电保护和相关装置的工作原理做到了如指掌，确定相应装置和设备的保护范围和定值。其次，在最近几年里，基于我国电力事业持续发展的趋势下，调度技术也在持续完善与优化，加强新型调度技术的应用十分关键，对提高此项工作整体水平有着积极的作用。企业需要定期或者是不定期开展培训以及教育工作，旨在让调度相关人员均能掌握各种新型的调度技术，从而推动新型调度技术的应用以及创新。不只是这样，还需要对调度工作机制加以完善，构建起各种各样的调度工作机制，持续完善与改进工作流程，旨在让此项工作的规范性上升到一个新的高度。

三、结论

智能电网的发展对网络通信提出了更高的要求，这确实带来了额外的网络安全问题，但通过对技术和管理手段的优化，可以在很大程度上避免这些问题。随着网络技术的进步，人工智能和大数据等先进技术不断在电力系统中得到应用，成为电力网络安全防护领域的重要发展方向。在未来智能电网系统平台的建设过程中，应朝着结构扁平、多层分布、功能可组和布置灵活等方向发展，不仅要考虑当前电网的需求，还要考虑未来电网的发展需求，为智能电网的发展保驾护航。

参考文献：

[1]张加康.电力调度自动化网络运维平台的设计与应用[J].时代农机，2020，47（03）：70-71.

[2]周新.电力调度自动化运行中的网络安全问题处理措施[J].通讯世界，2019，26（12）：224-225.