电力系统调度自动化系统信息安全防护技术研究

沈晓敏 张 恒
内蒙古电力（集团）有限责任公司阿拉善供电分公司，内蒙古 阿拉善 017010

[摘要]电力调度自动化系统是电网运行管控的核心，信息安全直接影响电力系统安全可靠。电网智能化、数字化升级进程加快的同时网络安全面临攻击的风险越来越大。文章对调度自动化系统的信息安全状况进行了研究，详细介绍了网络安全防护、数据加密及传输安全保障、身份认证和访问控制、非法入侵检测与防卫、信息安全审核及记录保存等方面的技术措施以及相应的应用与发展建议。研究发现，建立立体化多层次的信息安全防护体系才能更好保障电力调度自动化系统的安全性。

[关键词]电力调度自动化；信息安全；防护技术；网络安全；数据加密
DOI：10.33142/aem.v8i3.19437 中图分类号：TM734 文献标识码：A

Research on Information Security Protection Technology for Power System Dispatching Automation System

SHEN Xiaomin, ZHANG Heng
Alxa Power Supply Branch of Inner Mongolia Power (Group) Co., Ltd. , Alxa, Inner Mongolia, 017010, China

Abstract: The power dispatch automation system is the core of power grid operation and control, and information security directly affects the safety and reliability of the power system. As the process of intelligent and digital upgrading of the power grid accelerates, the risk of network security attacks is increasing. The article studies the information security status of scheduling automation systems, and provides a detailed introduction to technical measures such as network security protection, data encryption and transmission security, identity authentication and access control, illegal intrusion detection and defense, information security auditing and record keeping, as well as corresponding application and development suggestions. Research has found that establishing a three-dimensional and multi-level information security protection system is necessary to better ensure the security of the power dispatch automation system.

Keywords: power dispatch automation; information security; protective technology; network security; data encryption

引言

电力调度自动化系统完成对发电、输电、变电、配电等各方面的实时监视以及调度控制任务，是目前电网的安全可靠运行的重要保障。随着信息化与电力行业的不断融合，调度自动化系统的网络化、智能化程度不断提升，但是系统的网络暴露面也相应的增大，导致信息安全问题愈加突出。根据国际能源署（IEA）的统计，最近五年全球对于重要信息设施进行的网络攻击提升了 300%以上，而电力网作为国民经济的基础，在众多行业中成为黑客的主要目标之一。2015 年乌国电网遭受网络攻击致使大规模断电、2019 年委国大范围断电事故的发生说明了电力调度自动化系统的信息安全问题已经成为国家安全的重要课题。2025 年 1 月 1 日起施行的新版《电力监控系统安全防护规定》明确规定电力监控系统安全管理必须严格执行国家网络安全等级保护、关键信息基础设施安全保护等相关制度，在新的形势下深入研究电力调度自动化系统信息安全防护技术有着重大的理论及现实意义。

1 信息安全在调度自动化中的重要性

电力调度自动化系统的网络安全关系到电网的安全以及用户的用电安全。系统中包含了电网实时监视、AGC 自动发电控制、AVC 自动电压控制及调度检修计划等诸多重要子业务，如果遭到黑客入侵，则会使得调度命令被篡改、重要信息被窃取或是系统的崩溃，最后造成大面积断电、毁损等严重灾难。据 CISA、ENISA 等权威机构在 2023 年发布的公开数据显示：整个能源行业全年公开披露的漏洞有 4500 个，其中有 42%属于严重的漏洞，工控漏洞占比更是高达 35%，而其中的 68%的工控关键漏洞都直接影响到了电力设备的安全。在法律上，《中华人民共和国网络安全法》、《电力监管条例》以及《关键信息基础设施安全保护条例》等法律规章都对电力监控系统安全

防护做出了规定，《电力调度数据网运行管理规程》还提出了相关的安全管理要求，保障信息安全已经成为电力调度自动化的建设及运行的重要任务之一。再者，基于新型电力系统的建设，新能源的大规模并网、源网荷储之间的实时互动使调度自动化系统的边界也在逐步扩大，从而使得信息安全方面存在的隐患更加突出。所以做好信息安全防护既是迫在眉睫的技术问题也是维护国家安全和社会公共利益的重要保障。

2 电力系统调度自动化系统信息安全现状分析

目前电力建设自动化系统面临的安全风险很大。一方面来自外部的威胁，网络攻击有花样百出、有组织、有针对性的特点。2025 年波兰电网遭受网络攻击，黑客利用针对防火墙之类的边缘系统的漏洞，侵入到几十个分散式发电站的网络保护，控制远程终端装置的通讯装置使其不能工作，在互联网上传播信息传播数据擦除仪差点造成大范围断电事故；2023 年全球电力系统遭受勒索软件攻击数量同比增长 35%，中小规模配电公司以及新能源供应商遭受攻击比例达到 60%以上，每一次事件的平均赎金猛增至 570 万美元。从系统的角度来看，调度自动化系统长期存在的一些漏洞修补延迟现象特别严重，漏洞修复的周期也在不断的加长，传统的系统需要 98d，而工业控制器突破到了 150d，从而造成了长时间的渗透窗口。黑客主要用供应链，勒索病毒和 APT 三种方式入侵，历史上遗留下来的老漏洞和弱密码，初始设置等低级安全措施仍旧被反复地使用[1]。在技术体系方面，《电力监控系统安全防护规定》自 2014 年颁布以来为电力行业的网络安全防护提供指引，但是随着构建新型电力系统过程中出现了许多新的业务类型和服务模式以及运行机制，现有的安全防护机制急需进一步加强和完善。新型电力系统的接入主体更加多元化、边缘分布更加分散、交互形式更加多样化等特点加大了对信息安全保护的复杂性，削弱了防护体系的安全水平。

3 电力系统调度自动化系统信息安全防护关键技术

3.1 网络安全防护技术

网络安全防护技术是调度自动化系统信息安全的第一道防线，其主要任务就是利用网络隔离、边界防护以及访问控制等方式切断外来入侵途径。电力调度自动化系统根据“安全分区、网络专用、横向隔离、纵向认证”的思路，把防护对象按照安全等级分成生产和管理两个大的区域，其中生产控制区应采用电力监控专网，在专有通道中使用专门的网络设备组网，从底层完全隔绝与运营者的其他信息网和其他公共信息网之间的联系。生产控制大区与其管理信息大区、安全接入大区连接点应采取电力专用横向单向安全隔离装置；安全Ⅰ区与安全Ⅱ区之间应当采取具备访问控制功能的设备、防火墙或者相应功能的逻辑隔离措施；防火墙技术是在系统边界上部署，按照预先设定的安全策略对流向不同网络的数据流进行检测和分析从而阻止来自 IP 地址、端口和协议类型等方面的非法访问行为的发生，虚拟专用网技术是在公共网络之上构建起来的加密通道来保证远距离控制系统的安全性。电力企业一般会使用专用网络安全产品加通用防火墙相结合的方式，在保证实时性的前提下达到较好的安全保护效果。

3.2 数据加密与传输安全技术

数据加密及传输安全保障技术是为了保证调度自动化系统的数据存储以及传输过程中具有保密性，完整性，不可抵赖性。调度自动化系统传送的数据主要有遥测、遥控、保护定值等重要信息，若遭到泄密或者破坏，则会对电网的安全造成严重影响。电力调度单位应该根据电力调度管理体制来构建起由数字证书等手段形成的分部式电力调度认证体系，在生产控制大区开展相关的重要业务时需要运用到应用层端到端加密认证方式。国家密码算法在我国的电力系统应用越来越多了。研发支持国密 IP 安全协议虚拟专用网络，国密 NESP 封装与网络地址转换穿越协议，国密 SM1、SM2、SM3、SM4 算法以及电力调度数字证书、零信任接入认证、数据防篡改等一系列的数据安全性通信模块，已经成为电力行业的数据的安全传输的发展趋势。通过使用国产化的加密算法 SM2 和 SM3 进行构建的安全性的通信系统，并配合 SM4 的对称性的加密方式，能够达到传输过程中的保密性完性以及不可抵赖的效果[2]。另外，国际电工委员会 62351 标准采用安全套接字层协议进行加密，认证、数字签名及证书管理等一系列操作来保证通讯协议的安全性，给制造报文规范、面向通用对象的变电站事件、分布式网络协议等电力通信协议提供安全保障措施。

3.3 身份认证与访问控制技术

身份鉴别及访问控制技术是最有效的阻止非法进入以及无权访问的方法。身份鉴别的方法是通过检测用户的身份是否可靠来确定只允许授权合法的用户进行对该系统的访问，常用的识别有固定的密码、动态令牌、数字证书、指纹、虹膜以及人脸识别等多种类型。在具体应用时，调度自动化系统一般为双因子验证，即同时结合使用了数字证书认证和动态令牌的方式大大提高验证力度。而访问控制技术则是依据用户的个人身份及权限级别对于需要

访问系统的请求做出精确管理，其灵活易拓展的特点使其成为了配电自动化系统主要使用的访问控制策略类型之一。零信任架构以“绝不信任，持续验证”的理念为基础，配合采用基于身份的动态访问控制技术来为电力监控系统建立起粒度精确、智能化的保护机制，在电力移动互联网环境下，传统访问控制方式已经无法处理大规模移动终端以及大量异质化的访问要求，运用零信任模式使移动互联网架构由网络集中式转为目标导向式，可以很好地解决新业务模式下的安全问题。

3.4 入侵检测与防御技术

入侵检测与防护技术是进行积极安全防范的重要手段。入侵检测系统通过对实时监控网络流量及主机活动来发现可疑攻击行为并将它们及时报警，入侵防护系统是在此基础上进行拦截攻击流量。电力调度自动化系统入侵检测所面临的挑战在于：工控协议和普通网络协议相差甚远，传统的基于特征匹配的方式很难做到有效的匹配，而且调度系统的时效性非常强，检测系统要在最短的时间内做出判断和反应。分布式入侵检测系统把规则库嵌入到入侵检测系统里去，对变电站局域网 DNP3 流量进行动态监测，即时探测入侵和非法活动，利用分发式的方案完成从分散在各地变电站到调度中心的大范围异动集中监视[3]。过程感知型入侵检测技术为适应现代 SCADA 系统的实际运行条件而专门设计开发，在电网模型基础上增加场站之间的关联，同时纳入潮流计算，可以定位到单一监视手段无法识别出的隐蔽性强、关联性高的联合攻击事件。对于入侵防护方面来说，利用伪造欺骗陷井的主动安全防范策略，在伪造通道上设置欺骗陷井，让恶意代码进行攻击伪造的关键部件，一旦陷阱受到攻击就切换成备用调度系统终结恶意入侵行为，可发挥最后屏障的作用，具有十分重要的实用意义。

3.5 安全审计与日志管理技术

日志管理和安全审计技术是事后追查及合规检查的有效手段。日志和安全审计技术通过全面获取系统的运行日志、操作日志、安全报警等信息并加以集中存储，进行智能化解析，形成可以追责、可追溯的安全体系。电力调度自动化系统包含 SCADA、DCS 以及 EMS 等不同的设备，其日志包括 SNMP Trap，二进制协议等多种类型，其中日志审计系统利用开发出支持 1000+解析规则的日志审计系统来实现对不同协议的日志进行统一采集及规范化转换。聚铭综合日志管理系统实现了从“采集-存储-分析-追踪”的完整日志生命周期管理能力，在系统中收集来自网络设备、安全设备、服务器以及 SCADA、EMS 等重要业务系统所生成的大规模日志信息，支持每日 TB 级别的日志处理量。安全审计系统借助智能化分析引擎对日志数据进行梳理和挖掘，可以实时识别出存在的违规行为或安全风险；电力行业系统日志安全审计不仅是对日志文件进行简单的备份保护，还建立了一个完整的日志的可追溯、可验证的安全体系，涵盖电力生产、调度、营销系统等各类系统中产生的操作日志的采集、存储、分析与报警等一系列过程。

表 1 电力调度自动化系统主要信息安全防护技术对比

技术类别	主要功能	防护对象	典型技术/设备	优势	局限性
网络安全防护技术	隔离非法网络访问	调度数据网边界	电力专用隔离装置、防火墙、VPN	边界清晰，成熟度高	无法防御内部威胁
数据加密与传输安全技术	保障数据机密性与完整性	遥控指令、遥测数据	SM2/SM4 国密算法、TLS、数字签名	防止篡改与窃听	增加时延与计算开销
身份认证与访问控制技术	验证用户/设备身份	调度工作站、运维终端	多因素认证、RBAC、零信任	实现最小权限原则	证书管理复杂
入侵检测与防御技术	发现并阻断攻击行为	网络流量、主机日志	IDS/IPS、工控异常检测	主动防御	误报率较高
安全审计与日志管理技术	事后追溯与合规检查	操作记录、系统日志	审计平台	便于取证与分析	无法实时阻断攻击

4 信息安全防护技术应用与优化策略

信息安全防护技术的应用效果要兼顾技术匹配性、系统及时性和管理可行性等几个方面的要求，在具体使用上就要针对调度自动化系统自身的结构特点以及安全要求来选择合适的防护手段并加以融合。比如在网络边界部署电力专用隔离设备以及防火墙，在生产控制区安装入侵检测系统及安全审查系统，在数据传输管道使用国密算法加密防护等。电力调度中心研发调度数据安全防护平台，使用“加密传输＋权限控制＋行为审计”的三位一体防护模式保障调度数据采集、传送、保存的安全性；对调度系统的工作人员进行分层权限管理，系统自动生成员工的操作命令执行路径，形成可追溯的操作记录，避免因误操作或者恶意操作造成的调度事故。“优化”的措施是应该做到由被动防御到主动免疫的转换。新标准指出“安全免疫”、“态势感知”的防护理念，运用主动免疫、智能检测、即时追查等功能强大的新型设备提升防护水平，增强防护立体化与动态性的特征。

5 结语

电网调度自动化的信息安全保护是一个有组织的过程及一个持续的过程。本文基于信息安全的价值性，对目前电网调度自动化的面临的威胁问题进行了分析，对网络安全保护、信息加密、身份认证、入侵监测、安全审查等核心技术做了系统的介绍，在此基础上结合实例介绍了防护技术的应用情况以及优化方案，研究发现建立“多层次防御，主动免疫”的信息安全保护体系，达到由边缘防护到自主安全的转变来提高电力调度自动化系统的网络安全。未来随着人工智能、量子通信以及零信任架构等新的技术的发展，电力调度自动化系统信息安全保护也将会朝着智能、自动和自适应的方向不断发展，在新型电力系统的大背景下，针对电源结构、电网形态、业务模式、技术基础发生的重要改变，电力监控系统的安全防护也要在继续遵循“安全分区、网络专用、横向隔离、纵向认证”的基础上，不断学习新的思路、策略和技术，在变化中寻求机遇，不断增强自身的防护水平。

[参考文献]

[1]海云桥,王书行.电力调度自动化的应用与优化分析[J].光源与照明,2021(5):125-126.

[2]李强,刘洋.信息时代电力系统调度自动化发展方向探讨[J].决策探索(中),2019(7):71.

[3]杨鹏.信息背景下电力系统调度自动化发展方向分析[J].电脑迷,2017(10):168.

作者简介：沈晓敏（1983.12—），毕业院校：华北电力大学，学历：工程硕士，所学专业：电气工程，当前就职单位：内蒙古电力(集团)有限责任公司阿拉善供电分公司，职务：调度管理处技术室主任，所在职务的年限：10 年，职称级别：高级工程师。