电力调度自动化安全防护问题研究

吴雨诗　付登昊　刘　鹏　郑明友　缪林霞
（国网咸宁供电公司，湖北 咸宁 437500）

摘　要　文章首先结合硬件安全问题、通信安全问题、系统安全问题以及应用安全问题四个部分，探讨了电力调度自动化安全防护问题的主要表现。其次，围绕设计因素、技术因素以及管理因素三个方面，分析了电力调度自动化安全防护问题的形成因素。最后，以解决现存问题、淡化风险影响为导向，从完善整体设计、加强技术支持、健全管理体系三个角度入手，提出了电力调度安全防护问题的应对策略。

关键词　电力调度　自动化　安全防护　风险管理
中图分类号：TM73　　**文献标识码**：A　　**文章编号**：1007-0745(2022)11-0022-03

在“互联网 +”的时代背景下，电力工业领域中的电力调度工作逐渐实现了自动化、智能化转型，在很大程度上促成了调度质量与调度效率的提升。但与此同时，更多、更新的安全风险也随之产生，并对电力调度自动化系统的运行管理提出了更高要求。基于此，本文认为有必要对电力调度自动化安全防护的相关问题展开探究讨论，致力于在发现问题、分析问题的前提下，探索出提高系统安全系数、降低风险隐患影响的可行路径。

1 电力调度自动化安全防护问题的主要表现

结合行业经验来看，电力调度自动化安全防护问题的主要表现可分为四类，具体如下：

1.1 硬件安全问题

当硬件设备及其通电、通网线路发生故障时，电力调度自动化系统将面临一定的安全风险，出现运行中断、局部失能等负面运行情况。在实际工作中，常见的硬件故障包括电源故障、通信线路故障、网络设备故障、安防设备故障等。

1.2 通信安全问题

电力调度自动化工作中，系统运行会涉及多种数据信息的传输通信，如实时信息采集、调度指令发送、电力数据存储等。在此背景下，一旦数据信息的通信质量出现损失，发生串口通道中断、通信传输受阻、传输文件被窃取等，既会导致调度主站与各工作终端间的交互反馈出现延迟或中断，也会埋下机密信息外泄的安全隐患。

1.3 系统安全问题

电力调度自动化系统在实际运行中会面临多种网络安全风险，如病毒木马的侵入风险、外部黑客的攻击风险等。同时，若系统本身存在质量问题，也可能出现系统漏洞、程序丢失、运行崩溃等问题，这既会降低电力调度自动化的安全性与稳定性，也会给外部风险源的侵袭创造可乘之机。

1.4 应用安全问题

电力调度自动化软硬件的操作、维护、管理等应用行为具有较强专业性与技术性。在此前提下，若人员缺乏良好的技术素养或应用状态，在工作中出现误操作、越权操作等偏误行为，也会导致电力调度自动化系统的运行安全性大打折扣[1]。

2 电力调度自动化安全防护问题的形成因素

在电力调度自动化系统的运行过程中，其安防问题的产生与风险隐患的形成主要与设计、技术、管理三个方面因素有关。具体来讲：

2.1 设计因素

首先，在系统的结构设计与应用设计时，若未建立科学合理的分级、分区机制，将很容易导致系统安全防护的基础条件薄弱、执行体系模糊。例如，如果系统缺乏安全区与非安全区的有效分化，且未做好各类子系统之间的隔离处理，将直接增加核心性、关键性子系统接触风险源的概率，进而形成相应的安全隐患。其次，若电力调度自动化系统没有专用的工作网络、工作信道作为保障，将会较大程度地暴露在公共网络环境或局域网络环境当中，进而降低黑客、病毒等攻击侵入的难度。最后，若系统为单机运行设计，缺乏备用机、备份库等配置，其一旦发生故障或受到损害，将很容易出现信息丢失、缺损后无法复原的情况。这

样一来，不仅系统运行质量会受到影响，电力企业与电力用户的相关效益也会遭受严重损失。

2.2 技术因素

电力调度自动化系统及配套软硬件并不具备完善的安全保障功能，所以需要额外的安全技术作为支持，如系统防护技术、攻击防御技术、病毒查杀技术、通信保障技术等。对此，若安全技术应用不到位，或安全技术无法满足系统的实际安防需求，也会引发一系列的系统运行与信息安全问题。

2.3 管理因素

在电力调度自动化工作中，管理活动与安全防护质量存在密切关联。所以，若管理制度不健全或管理缺乏执行力，也会导致电力调度自动化系统的安全系数有所降低。例如，如果没有围绕电力调度自动化建立责任制，既会引发相关工作人员在工作认知、安防实践上的模糊性问题，也会埋下相关安全事故问责难、追责难、处理难的隐患。

3 电力调度自动化安全防护问题的应对策略

3.1 完善整体设计，夯实防护基础

确保系统整体设计的科学性、完善性，是降低电力调度自动化安全风险发生概率与影响程度的前提和基础。在基于安全防护目的设计电力调度自动化系统时，要严格落实分层分区、专网专用、横向隔离、纵向保障的基本理念。

“分层分区”即要求自动化系统要基于功能用途、防护等级、控制机制等条件分为多个层次和区域，如安全区与非安全区，控制区与非控制区，生产区、管理区与信息区等。在此基础上，针对各层次、分区实施差异化的安全管控。例如，对于涉及电力调度控制、自动化程序运行、机密信息存储等高安全要求的系统部分，应保证其软硬件在接线、组网等配置上的相对独立性。而对于安全要求较低的系统部分，如常规办公系统、客户服务系统等，则可适当接入公网或局域网，但仍应做好系统防护、安全管理等工作[2]。

“专网专用”即要求电力调度自动化系统在工作运行、传输数据、应用操作时，应有专用的工业网络和数据通道作为支持。如此一来，既有助于提升系统的运行效率，也有助于避免公共网络、公用通道中的风险文件、恶意程序或网络病毒对系统安全构成威胁。

“横向隔离”即要求电力调度自动化系统内部的分区在设计时做到相互隔离，且以生产控制与信息管理两部分的横向隔离最为重要。在此基础上，为了满足系统性、整体性的通信、监控、管理等需求，还应在各分区中进一步设置安全区与接入区，并保证两个子分区之间保有单向隔离、逻辑隔离等隔离设计手段，如访问控制、安全边界等。

“纵向保障”一方面要求电力调度自动化系统中的数据信息在上行、下行传输时，应配有可靠的安全保障机制，如加密传输、分包发送等。另一方面，在设置系统用户的信息查阅、参数设置、业务操作等权限时，也应采取权限分级与识别认证等保障手段，进而从根源上防止越权操作、违规操作等情况发生。

除此之外，为了进一步提高电力调度自动化系统的安全防护水平与风险应对能力，还应做好备份系统、告警系统、云端数据库、实时监视平台等方面的设计配置工作。

3.2 加强技术支持，应用防护工具

在电力调度自动化安全防护实践中，各类技术工具的防护支持也是必不可少的。结合行业经验来看，可增强系统安防能力的技术工具包括但不限于以下几种：

3.2.1 防火墙技术

现阶段，防火墙技术已发展出多种类型，如包过滤型、虚拟代理型、状态检测型等，这些防火墙能为电力调度自动化系统提供不同等级、不同倾向的安全功能支持，达到构筑系统外部防护层的效果。例如，在配置虚拟代理防火墙后，外来数据包或信息文件会停留在虚拟代理服务器中，而不是直接进入系统内部。如此一来，便能避免系统与风险源直接接触，从而实现有效安全防护。再如，在配置状态检测防火墙后，电力调度自动化系统外部会建立一种过滤检测机制，对外来数据包的状态信息进行提取和审核。若防火墙检测引擎判定数据包的传输端口、发送地址、目标地址等信息存在风险或异常，则会对相应数据连接实施阻拦或终止，以免其对系统安全造成危害[3]。

3.2.2 备份恢复技术

当电力调度自动化系统发生软硬件故障或遭到外部攻击时，很可能会发生数据信息丢失、损坏或被篡改的问题，进而对系统运行的安全性、稳定性与连续性造成负面影响。为了应对此类情况，可采取搭建备份服务器、云端备份数据库、远程备份系统等技术手段。在此前提下，一旦风险事件发生，便可依托备份服务器、数据库或系统实现主系统的数据信息恢复处理，从而达到降低风险影响、保证系统安全的目的。此外，

在建立备份机制后，若主系统因信息丢失、文件损坏而崩溃失能，相关备份结构也能及时投用或自动切换到电力调度自动化作业当中。如此一来，便能进一步淡化系统安全风险，防止电力工业的生产管理效益遭受过大损害。

3.2.3 识别认证技术

将该技术应用到电力调度自动化安全防护中，能够针对信息或用户进行识别认证。若判定数据信息安全、用户权限匹配，则可通过相应的传输或访问请求。反之，则不予传输或访问，并触发风险记录、风险告警等机制。通过这样的方式，能够有效降低电力调度自动化系统发生信息安全风险或人为操作风险的发生概率，从而实现安全防护。从目前来看，识别认证技术的研究发展已趋于成熟，并形成了多元化的分支体系，具体包括密码识别、射频识别、面部识别、指纹识别、虹膜识别、声纹识别、数字签名识别等。在开展安全防护实践时，应做好多种识别技术的合理选择与综合运用，以促成电力调度自动化系统安全系数的提升[4]。

3.3 健全管理体系，优化防护机制

在进行电力调度自动化安全防护时，应建立健全安全管理体系，全面优化防护工作机制，并确保各项管理活动具备较强的科学性与执行力。具体来讲：

首先，要做好电力调度自动化系统的硬件与软件管理工作。在硬件方面，应保证计算机、工作站、交换机、路由器、磁盘阵列等各类设备、线路安装合理、配置完整、制式统一，并严格保证设备通电、通网的持续性与可靠性。同时，对于生产控制、信息管理中的重要设备，应全程做到双机热备或多机集群，以确保设备故障不会对电力调度自动化运行产生过大影响。在软件方面，应保证各类模块、程序、系统、平台功能完善、部署健全、状态稳定，不存在带病运行、超负荷运行、高风险运行等异常的运行情况。同时，各软件在运行过程中应保证通信安全、工作协调，以免发生系统运行冲突或外部风险源侵入的问题。在此基础上，需要常态化做好软硬件的检修养护与更换更新。对于软件，可采用杀毒软件查杀防护、防护记录深度分析等手段，并及时对软件、系统进行升级处理。对于硬件，则应做好设备、线路、环境等方面的监管与维护。一旦发现电源、线路、主机等方面的故障问题或风险隐患，应及时通过维修、换件等方式加以解决[5]。

其次，应明确电力调度自动化运行管理与安全管理的制度要求，如“机房温度应保持在 15℃至 28℃的区间内，机房相对湿度应保持在 40%至 75%的区间内。若机房温度过高，系统运行出现异常，应及时进行停机检查与环境温湿度调节”“自动化班组应建立日常运行巡视制度，在规定周期内完成对所有管辖设备的巡视检查，并做好相关工作记录”“进行自动化系统的故障处理或检测调试，不得进行值班人员交接班”等，以便充分发挥管理制度对实践活动的指导和约束作用，从而降低相关系统运行与业务工作风险。

最后，应加强人员方面的安全管理。一方面，要建立严格、专业的组织构建与岗位准入机制，保证自动化工作人员具备良好的专业背景、工作经验、技术资格与履职能力。在此基础上，对电力调度自动化的相关任务、职责进行明确分配，并保证细化到岗、落实到人。例如，在各类系统、软件、硬件投入运行后，要配以专人专岗进行操作、监管与维护。另一方面，要围绕电力调度自动化安全防护做好人员培训、技术交底、工作考核等工作，在积极提升人员自动化素养的基础上，强化人员的安全防护素质，如信息安全意识、风险识别能力、应急处理能力、安全技术应用能力等。只有这样，才能从主体角度保证电力调度自动化安全防护的落实质量，避免各类人为风险的形成与影响。

4 结论

综上所述，电力调度自动化系统在实际的运行过程中，会面临多种类、多源性的安全风险。所以，相关安全防护工作也应做到全面化、精细化。在具体实践中，既要做好电力调度自动化系统软硬件的设计配置与保养维护工作，也要做好防火墙技术、识别认证技术等安全防护技术的科学运用。在此基础上，还应切实加强相关安全管理工作的执行力，并积极提升自动化工作人员的履职素养。如此一来，可有效降低安全风险的发生概率与影响程度，促成电力调度自动化安全水平的提升。

参考文献：

[1] 金贵红 . 浅析电力调度自动化的安全防护问题 [J]. 电子元器件与信息技术 ,2020,04(11):99-100.
[2] 赵自勤 . 电力调度安全风险管理分析 [J]. 中国高新科技 ,2020(17):114-115.
[3] 张敏 . 电力调度自动化网络安全防护系统探究 [J]. 电力设备管理 ,2020(08):111-113.
[4] 杨天丽 . 调度自动化系统及数据网络安全防护技术 [J]. 通讯世界 ,2019,26(12):266-267.
[5] 张振夫 . 电力网络及调度自动化系统的安全防护策略研究 [J]. 中小企业管理与科技 (下旬刊),2019(11):88-89.