工程与管理科学
Engineering and Management Science
第 7 卷◆第 6 期◆版本 1.0◆2025 年
文章类型：论文|刊号（ISSN）：2705-0637(P) / 2705-0645(O)

电力配电网自动化系统网络安全风险及防护策略研究

马俊杰
南京南自数安技术有限公司　江苏南京　211106

DOI:10.12238/ems.v7i6.13856

［摘　要］随着我国经济的飞速发展和社会的不断进步，电力能源在各个领域的应用愈发广泛，已经成为支撑国家发展和人民生活的重要基础。电力配电网作为电力系统的关键组成部分，承担着将电能从输电网或发电设施分配到各类用户的重要任务，其运行的稳定性和可靠性直接关系到社会的正常运转和人民的生活质量。

［关键词］电力配电网；自动化系统；网络安全；防护策略

前言：

近年来，随着信息技术和自动化技术的快速发展，电力配电网自动化系统得到了广泛的应用和推广。通过将先进的通信技术、计算机技术、自动控制技术与电力系统相结合，电力配电网自动化系统实现了对配电网运行状态的实时监测、故障快速定位与隔离、负荷优化分配等功能，大大提高了配电网的运行效率和供电可靠性。例如，在发生故障时，自动化系统能够迅速检测到故障点并隔离故障区域，同时恢复非故障区域的供电，减少停电时间和范围，降低对用户的影响。

一、配网自动化技术应用的优势

（一）配网自动化系统的重要性

在电力系统运行过程中，由于传统建设标准的一些限制，配网设备的运行状态难以被全面掌握。例如变电站和线路设备的实时数据，电力部门可能无法及时获取，这就导致了故障排查和维护工作容易出现延迟。这种滞后性不仅会影响设备的安全性，还可能降低供电的稳定性，最终影响用户的用电体验。为了解决这些问题，必须推进配网自动化技术应用。

（二）建立配网自动化系统提高了电力部门工作效率

通过部署自动化系统，电力部门的工作效率得到了显著提升。这种系统能够持续监控各个线路的负载情况，根据预测数据优化资源配置。例如在夏季用电高峰时段，系统可以自动调整电力分配，避免某些设备因为过载而发生故障。这种方式不仅提高了供电网络的灵活性，也增强了应对突发情况的能力。

二、配网自动化网络安全防护技术

（一）建立 Nginx+Zabbix 的框架结构管理

在网络安全方面，采用 Nginx 配合 Zabbix 的架构管理模式，能够有效提升防护能力。这种框架结构不仅可以实现实时监控，还能对异常流量进行及时预警，为配网系统的稳定运行提供多重保障（如图 1 所示）。通过软件层面的优化配置，让电力调度指令传输和数据采集过程变得更加安全可靠，避免遭受外部攻击或非法入侵的风险。在配置层面，Nginx 反向代理以及访问控制模块的配置，也就是通过设置反向代理服务器来隐藏实际服务器的 IP 地址，同时实现针对异常流量的访问控制功能，例如可以有效缓解 CC 攻击这类网络攻击行为。对于数据库层面的保护，主要采用数据库同步挂载与网络文件系统（NFS）备份相结合的方式。例如通过设置定时同步任务，让主从数据库之间保持数据一致性，再配合 NFS 实现远程文件备份。这种双管齐下的策略可以在遇到服务器故障时，通过负载均衡设备快速切换服务节点，最大程度上避免数据丢失风险。在分布式系统架构中，Nginx 反向代理的重要作用还体现在虚拟 IP 映射方面。当某个后端服务节点出现故障时，这个反向代理机制能够自动切换到备用节点，这样就可以保证服务持续可用，也就是达到了高可用性的设计目标。与此同时，Zabbix 监控系统的部署，给整个架构装上了实时流量监控的"眼睛"，运维人员通过看监控数据就能掌握系统运行状态。再配合部署云锁、安全狗这样的防护软件，加上定期用 X-SCAN、Super-Scan 这些工具进行漏洞扫描，为服务器和网站提供全面的安全防护。

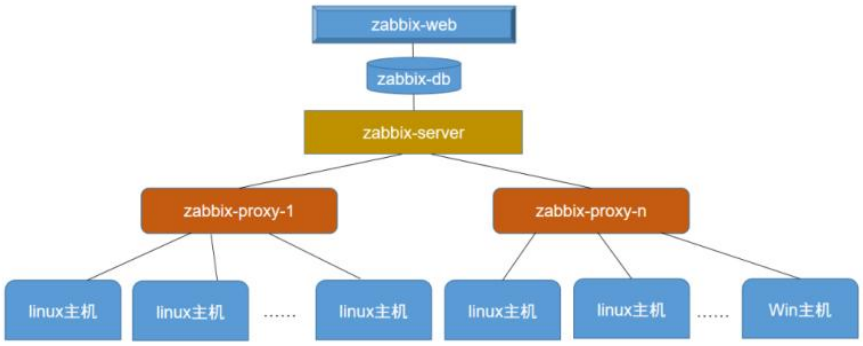

图 1　Nginx 配合 Zabbix 的架构管理模式

（二）建立以防火墙为核心的安全网络体系

整个安全体系的核心是以防火墙为基础构建多层防护网络。这种架构设计不仅能够阻挡外部攻击，还可以对内部流量进行细粒度管控，实现全方位安全保障。例如在网站数据出现异常时，基于 NFS 的远程挂载机制可以让数据库快速恢复，就像给系统准备了备用的"急救包"。通过将反向代理配置、实时监控看板和安全防护设备这三个层面的措施有机整合，最终形成既能抵御大流量攻击，又能防范小规模数据窃取的综合防护体系。防火墙作为网络安全的基础设施，主要承担着物理隔离与访问控制的双重防护功能。值得关注的是，这类设备虽然被认为是网络防护的首道屏障，但在实际应用中仍然存在明显短板。例如存在"只防外部不防内部"的固有认知偏差——也就是默认内部网络是绝对安全的，但统计数据显示超过 80%的攻击行为其实来自内部网络。因此在电力配网这类关键系统中，更推荐使用分布式防火墙方案。分布式防火墙体系主要包含三个组成部分：网络防火墙（也就是

传统防火墙）、安装在终端设备上的主机防火墙，以及进行统一协调的中心管理平台。其中主机防火墙特别针对内部攻击设计，能够对桌面电脑和移动设备提供持续防护。其核心运作原理是通过中心平台将安全策略分发到各个节点，同时将各处产生的日志数据汇总到管理中心进行分析处理。在实际部署时，防火墙还能与入侵检测系统形成联动机制。例如 BlackICE 防护软件和"冰之眼"这类产品，当入侵检测系统（intrusiondetectionsystem）发现可疑行为时，就会通知防火墙在访问控制列表（accesscontrollist）里动态添加拦截规则，从而阻断攻击者的渗透路径。防火墙这种防护装置可以配合反病毒软件共同工作，例如将它们部署在开放系统互联模型（就是常说的 OSI 模型）的数据链路层与网络层中间的位置。这样做的好处是从最开始传输的时候就能对 IP 数据包进行拦截处理。另外还可以和身份认证系统、操作记录审计系统这些配套使用，这样整个配电网络系统的安全性就能得到比较全面的保障。

（三）提升网络物理防护措施

在网络系统防护层面，需要重点加强设备端的实体化防护。在原有架构里新增一个数据缓冲隔离区，通过这个中间层实现公共网络与核心系统的物理隔离。例如可以在数据传输过程中部署具有报文校验功能的网关设备，这种设备能对传输指令进行数字签名，相当于给每个操作指令都贴上防伪标签。这里要注意的是应该使用双因子认证机制，也就是在登录系统时既要输入固定账号密码，还需要配合动态验证码或者生物识别手段——例如现在智能手机常用的刷脸认证、指纹验证这些方式。特别需要注意的是不同品牌设备之间的兼容性问题，有些老旧终端可能不支持新型加密协议，这时候就需要在网关处做协议转换处理。通过这样的多重防护设计，既能防止外部攻击者通过破解单一密码入侵系统，又可以避免某个设备被控制后引发连锁反应影响整个配电网运行的情况发生。

（四）串联加密认证设备

由于配电网中存在大量终端设备，这些终端数据传输的方式各不相同，扩展起来也不太方便。针对这种情况，可以考虑在通信线路中加装专门的安全认证装置。就是，在配电系统里那些使用不同通信协议、来自不同厂家的终端设备之间，通过这个加密认证设备来实现安全防护。特别是在电力物联网需要实现更多自动控制功能的情况下，在感知层的配电设备和网络系统之间加入这类安全装置，可以更好地满足多种通信方式下的电力自动化需求。例如当遇到需要同时处理传统配电终端和新型智能电表数据的情况时，这种设备就能有效保障供电系统的安全运行。

三、电力配电网自动化系统网络安全风险及防护策略

（一）合规制定管理制度

针对电力公司内部存在的某些工作人员责任心不强、遇到问题推诿的情况，电力调度自动化网络需要通过强化管理制度来保障稳定运行。目前这类系统已经在开展规范整改工作并取得阶段性成效，例如要求每个操作环节都要记录具体经办人，这样出问题时候就能直接找到责任人。这种方法可以促使管理人员更主动地履行岗位职责，进而提升整个电力公司的管理效率水平。另外在管理边界划分方面，需要特别关注不同岗位之间的责任重叠问题。通过明确不同部门之间——例如网络设备维护和用户权限审核这两个工作——的具体管理范围，既能避免出现管理盲区，也能防止多个部门重复管同一件事造成的资源浪费。这种权责划分方式对于保障自动化网络的安全运行具有基础性作用，例如去年某地电力公司就出现过由于权限管理混乱导致系统误操作的情况。

（二）提升技术维度的完备性

在新一代信息技术快速迭代的背景下，信息系统都开始往云端模式迁移，逐渐替代过去那种依赖本地服务器的传统部署方式。例如工业生产场景中，当物联网设备与数字化基础架构越绑越紧，加上信息传递渠道变得越来越复杂，网络攻击的手段也跟着花样翻新。企业业务系统从分散式转向集中式管理的过程中，对数据安全的要求自然就水涨船高。需要逐步构建起完整的云端数据中心防护体系，实现各个控制模块的平滑对接，也就是让安全防护机制能够和云平台自身的运行环境紧密配合。从业务实施角度看，应该建立基于大数据分析技术的风险预警模型，例如针对电力调度系统或者在线支付平台这类关键业务场景，部署全天候的异常状态监测，这样既能提升处理突发事件的效率，又能增强应对复杂安全问题的实际能力。

（三）加强计算环境的安全建设

在保障工业系统稳定运行的过程中，安全防护这个事需要从多个维度来考虑。例如怎么防止病毒入侵、及时发现异常操作、堵住系统漏洞这些比较常见的问题，还有对外接设备的管理、操作记录的保存这些容易被忽视的细节。我们这次要讨论的主要是针对工业控制场景中比较常见的那些控制器设备，也就是生产车间里大量使用的那种可编程逻辑控制器（PLC），怎么给它们打造一套可靠的安全方案。实际应用中发现，采用白名单机制效果比较明显。例如给软件程序建立白名单制度，也就是经过严格审核的软件才能运行，同时配合完整性校验手段，只要发现程序被改动过就马上切断运行。对于 U 盘、移动硬盘这些外接存储设备，可以通过实时监控 USB 接口状态来管理，例如只允许登记过的设备接入，而且所有插拔操作都会生成带时间戳的详细记录。现在工业控制系统应用范围越来越广，像电力输送网络、石油管道这些关键基础设施都在用，但安全隐患反而变得更多。特别要注意的是系统漏洞这个问题，很多黑客就是利用这些漏洞进行破坏。但现有的漏洞扫描设备很多只能检查硬件参数，对软件层面的隐患往往检测不出来。所以建议在重要工业设施里部署专门的漏洞扫描系统，这种系统最好能同时检查硬件配置和软件版本。例如扫描的时候不仅要看控制器固件版本是不是最新的，还要检测程序代码里有没有藏着隐患。对于扫描出来的问题，要能给出具体的修复建议，例如某个漏洞需要更新补丁，或者是调整某个端口的访问权限。

四、结束语

电力系统建设中应用配电网自动化非常必要，以此能够保证供电的连续性、质量，这就需要做好对供电情况的监督、管理工作。通过电力系统监控、配电运行管理、配电网电能监测、数据监测、收集信息等多种路径，合理运用配电网自动化系统，加强电力系统建设，更好地为人们提供电能，并且满足人们的用电需求，符合市场经济的发展与建设需要。

[参考文献]

[1]姜奥.配电网系统中的自动化技术应用[J].电子技术，2023，52（09）：100-101.

[2]陶金，周哲民，蒋娴.自动化技术在配电网系统中的应用[J].集成电路应用，2023，40（10）：60-61.

[3]海瑛.电力配电网自动化系统中网络安全防护有效性探究[J].电工技术，2024，（S2）：311-313.

[4]王德玉.电力配电网自动化系统网络安全风险及防护策略[J].城市建设理论研究（电子版），2024，（15）：1-3.

[5]严康，陆艺丹，覃芳璐，等.配电网用户侧异构电力物联设备网络风险量化评估[J].电力系统保护与控制，2023，51（11）：64-76.

[6]国涛，赵学智，封保占，等.电力配电网自动化系统网络安全风险及防护策略[J].网络安全技术与应用，2023，（06）：124-125.

作者简介：马俊杰（1991.2），男，汉，江苏南京，本科，研究方向：网络安全。