信息科学

电网数字化背景下网络设备端口安全防护研究

吕晓霖 李瑞

（国网天水供电公司 甘肃省天水市 741000）

摘要：网络设备端口安全防护是在电网数字化背景下至关重要的一项研究课题。目前的现状表明，电力专网与外界未能真正实现物理隔离，完全依靠软件进行内外网隔离存在安全隐患，同时“违规外联”问题和运维工作中的误插拔风险也仍未得到有效解决。因此，有必要制定网络设备端口安全防护的实施方案，包括技术方案和应用方案，以解决当前存在的安全问题。实施网络设备端口安全防护具有重要意义，包括实现电力专网与外界的物理隔离、增设在用、空闲网络端口硬件技防手段，以及杜绝“违规外联”和网线误插拔等问题。这些意义的实现将有助于提升电网系统的安全性和稳定性，确保电网数字化运营的顺利进行。

关键词：电网数字化 网络设备端口 安全防护

1 引言

随着电网的数字化进程不断推进，越来越多的设备接入网络，网络设备端口的安全防护问题也日益凸显。网络设备端口作为网络通信的关键节点，承载着大量的数据传输任务。一旦端口被攻击或滥用，可能导致网络服务中断、数据泄露、系统崩溃等严重后果。因此，保护网络设备端口的安全至关重要。网络设备端口安全防护可以通过采取适当的技术手段，继而有效保护网络设备端口的安全。因此，需要针对研究网络的物理安全防护系统，尤其是对端口级安全防护系统的研究则格外重要[1]。

2 网络设备端口安全防护的现状

遵循“安全分区、网络专用、横向隔离、纵向认证”的信息安全防护总体策略，电力专网承载了生产控制大区、管理信息大区的各类业务，生产控制大区与管理信息大区的安全隔离由电力专用单向隔离装置实现，上下级之间调度业务数据的加密和认证保护由电力专用纵向加密认证装置实现。然而，就数字化牵引新型电力系统建立的网络安全防护而言，电力专网目前还存在着以下几个需要解决的问题[2]。

2.1 电力专网与外界未能做到真正意义上的物理隔离

新型电力系统建设，海量终端设备接入，设备分布范围更广、规模更大，网络边缘人防压力大。在电力系统中，电力专网是为了实现电力信息化和数字化而建立的专用通信网络。然而，由于电力专网需要与外界进行数据交换和通信，往往无法做到真正意义上的物理隔离。这就意味着电力专网的网络设备端口仍然面临来自外界的潜在威胁。因此，电力专网不可避免的会有端口暴露人防手段薄弱的位置，让社会工程学入侵有了可乘之机。同时机房，特别是跨专业共用机房，运维外委后人员进出复杂，端口接触式的网络入侵隐患增多，网络安全隐患增大；

2.2 完全依靠软件进行内外网的隔离存在安全隐患

为了保护电力专网的安全，很多电力系统采取了软件隔离的方式，通过配置防火墙和访问控制列表等技术手段来实现内外网的隔离。然而，完全依靠软件进行隔离存在一定的安全隐患。一旦软件出现漏洞或被攻击者攻破，就可能导致内外网的隔离失效，使得网络设备端口暴露在攻击者的威胁之下。因此，现有的网络安全技术防护侧重对于安全数据的分析、网络流量的监控和安全身份认证，偏向于“事中”防护，而“事前”防护手段缺失。同时，现有的入侵检测系统基于对访问行为和特征数据库进行比对，而部署在内网的 IPS/IDS 系统特征库的更新，无法做到及时高效，极易出现系统的漏判，并且完全依靠软件分析，在应对海量数据交互时，也会存在系统误判的隐患。

2.3“违规外联”问题未杜绝

“违规外联”是指未经授权或未经安全审查的情况下，将网络设备端口连接到外部网络。这种行为可能导致未知的安全风险，例如黑客入侵、数据泄露等。尽管有一些安全措施已经被采取，如访问控制列表（ACL）和网络隔离，但仍然存在一些问题。首先，一些员工可能因为方便或无知而绕过这些安全措施，从而导致违规外联。其次，一些恶意人员可能会利用漏洞或社会工程学手段绕过安全措施。

2.4 运维工作存在误插拔风险

运维工作中的误插拔是指在维护或更换网络设备时，由于疏忽或错误操作，错误地插入或拔出设备端口。这种错误可能导致网络中断、数据丢失或设备损坏。另外，一些网络设备的端口设计可能不够人性化，容易导致误操作。为了减少误插拔风险，应加强运维人员的培训和技能提升，确保他们具备足够的专业知识和操作经验。此外，网络设备的端口设计应更加人性化，例如采用颜色标识或形状标识，以帮助运维人

员正确插拔设备。

3 网络设备端口安全防护的实施方案

3.1 技术方案

本研究的总体框架由终端锁、开锁设备和管理软件几个部分组成，主要涉及电磁驱动结构、核心处理单元、开锁模块、通信接口及通信协议、任务管理、设备管理、数据库管理等关键技术，通过授权管理软件–管理设备–终端设备的模型实现网络端口的全方位管控。

详细的实施方案过程如下。其一，网络端口锁上锁解锁结构设计。根据标准 RJ45 水晶头的尺寸，合理设计端口锁内部结构，通过电磁方式驱动端口锁活动机构，实现上锁和解锁的功能。其二，网络端口锁电路设计。设计电磁驱动电路，测试和验证线圈驱动能力，确保可以通过单片机控制端口锁可靠解锁动作，并设计指示灯用于指示设备运行状态。其三，电子钥匙电路设计。设计锂电池充放电管理、网络端口锁驱动、数据存储单元等电路，用于管理和控制网络端口锁解锁。其四，单片机程序设计。根据网络端口锁控制流程，分别涉及网络端口锁和电子钥匙的开锁逻辑程序；通过一定的加密算法，实现开锁权限控制；设计通信接口协议，实现设备管理功能。其五，原型机制作。开模打样，根据网络端口锁和电子钥匙设计模型，对外壳、内部机械部件进行开模打样；电路板打样，调整电路板尺寸和布局，使电路板与外壳模型紧密配合；装配测试，完成模型和电路板打样后，将各部件焊接和组装起来，完成原型机制作，测试各项功能指标是否符合要求[3]。

3.2 应用方案

在完成系统设计和研发后，需要对系统进行试点应用，验证系统方案各方面性能十分满足设计需求。其一，环境搭建。首先是原型软件安装和配置，在服务器上部署原型系统软件，完成数据库、中间件的安装配置。其次是初始化数据生产，利用软件生成初始设备数据。然后是测试设备初始化，由授权软件生成的初始数据对测试设备进行初始化。最后是系统测试，对原型软件系统各功能模块进行联调测试。其二，场景验证。首先是端口上锁场景验证，将网络端口锁部署于需要防护的网络端口上，检查上锁动作是否正常；然后是授权任务生成场景验证，通过授权管理软件生成解锁任务，并将解锁任务导入电子钥匙中；接着是端口解锁场景验证，使用电子钥匙连接到授权任务列表中的网络端口锁上，验证端口锁是否正常开锁；将电子钥匙连接到未授权的网络端口锁上，检查端口锁是否保护不开锁。最后是开锁记录回读验证，通过授权管理软件回读电子钥匙已开锁记录，查看开锁记录是否正常。

4 网络设备端口安全防护的意义

网络设备端口安全防护是保护网络系统免受未经授权的访问和攻击的重要措施。在当今数字化时代，网络设备扮演着连接世界的桥梁，因此保护网络设备的端口安全至关重要。下面将从实现电力专网与外界的物理隔离、增设在用、空闲网络端口硬件技防手段以及杜绝“违规外联”和网线误插拔等多个角度探讨网络设备端口安全防护的意义。

4.1 实现电力专网与外界的物理隔离

网络设备端口安全防护的一个重要意义是实现电力专网与外界的物理隔离。通过对网络设备端口进行安全防护，可以确保电力专网与外界网络之间的隔离，防止未经授权的访问和攻击。这种物理隔离可以有效保护电力专网的安全性和稳定性，防止外界恶意攻击对电力系统造成损害。

4.2 增设在用、空闲网络端口硬件技防手段

网络设备端口安全防护的另一个意义是增设在用、空闲网络端口的硬件技防手段。通过在网络设备端口上安装硬件技术防护措施，如防火墙、入侵检测系统等，可以有效防止未经授权的访问和攻击。这些硬件技术防护手段可以监控和过滤网络流量，识别和阻止潜在的威胁，提高网络设备端口的安全性。

4.3 杜绝“违规外联”和网线误插拔

网络设备端口安全防护的第三个意义是杜绝“违规外联”和网线误插拔。通过对网络设备端口进行安全设置，可以限制外部设备的接入，防止未经授权的外部设备连接到网络设备端口。同时，合理规划和标识网络设备端口，可以避免网线误插拔导致网络中断和安全漏洞的产生。这样可以保证网络设备端口的稳定性和安全性。

总之，网络设备端口安全防护对于保护网络系统的安全性和稳定性具有重要意义。通过实现电力专网与外界的物理隔离、增设在用、空闲网络端口硬件技防手段以及杜绝“违规外联”和网线误插拔等措施，可以有效防止未经授权的访问和攻击，保护机密信息和敏感数据的安全，提高网络的可用性和可靠性。

参考文献：

[1]陈静. 计算机网络故障的处理及网络维护方法探究 [J]. 数字技术与应用, 2023, 41 (07): 30-32.

[2]李三华;杨华. 网络二层故障剖析与排除 [J]. 网络安全和信息化, 2022, (04): 151-153.

[3]李贵华. 端口逻辑环路闸故障 [J]. 网络安全和信息化, 2017, (05): 138-140.

作者简介：吕晓霖 男 1977.8 汉。籍贯：山东省莱州市。职称：副高，学历：本科，研究方向：信息网络。

李瑞 男 1986.6 汉。籍贯：陕西省宝鸡市。职称：副高，学历：本科，研究方向：信息网络。