网络端口硬件防护在实现电力专网与外界物理隔离的意义

吕晓霖 雷阳

（国网天水供电公司 甘肃省天水市 741000）

摘要：本文讨论了网络端口硬件防护在实现电力专网与外界物理隔离的重要性，然后概述了电力专网与外界物理隔离的现状。接着，文章对现有网络端口硬件防护的几种方法进行了详细介绍，包括使用端口塞和纸张进行封堵，以及 USB 端口的无防护现状。文中也提出了新型网络端口硬件防护的功能，如全方位态势感知及主动防御功能，USB 端口终端防护，以及图形化数字孪生。最后，文章强调了网络端口硬件防护的重要意义，包括提供更安全可靠的网络连接，防止违规外联和一机两用行为，以及主动防御零误判。

关键词：网络端口 硬件防护 电力专网 物理隔离

1 引言

在实现电力专网与外界物理隔离方面，网络端口硬件防护具有重要的意义。首先，电力专网作为关乎国家重要基础设施的网络系统，其安全性和稳定性至关重要。而外界物理隔离则是保障电力专网系统安全的重要手段之一，它可以有效防止外部网络攻击和干扰，确保电力系统运行的可靠性和稳定性。网络端口硬件防护作为实现外界物理隔离的关键技术之一，具有重要意义[1]。

2 电力专网与外界物理隔离的现状

其一，内网物理隔离实际存在安全隐患。独立专网企业往往都是内网专网，通过内网和电信公网的物理隔离来实现内网系统的独立安全运行，而实际内网系统运行时不可避免的会有内网端口暴露在办公室、会议室、楼层弱电井等人防手段薄弱的位置，对内网系统造成一定的网络安全隐患，使内网系统未能做到真正意义上的内外网物理隔离。

其二，机房管控存在漏洞。机房进出虽有出入管控手段，包括视频监控、出入机房登记，甚至包括进出机房全程专人现场监视等，这些手段都是在人防手段框架下对操作流程的规定和约束，并且视频监控只能便于事后溯源，不符合网络系统“以防为主”的运维和安全防护思路，不仅极大增加了运维成本，同时缺乏有效的手段实现人防到技防的转变。

其三，入侵检测系统存在局限性。IDS（入侵检测系统）重在监测，不具备主动防御功能。此外，IPS（入侵防御系统）虽有主动防御功能，但完全依靠软件的感知分析，存在一定的误判风险，且重在网络入侵过程的“事中”防护，缺乏“事前”+“事前”+“事后”的全过程态势感知。因此，纯粹依靠软件防护手段无法规避软件天生的缺陷，包括软件 BUG 及漏洞等，与专网的建设思路相悖。

其四，网络端口操作存在缺陷。在用网线误拔、闲置端口误插、机房布线时造成网线插头松动等，都会造成网络系统不稳定。此外，USB 口通用性及使用性高，接入口无防护措施，在便捷的使用过程中办公人员容易出现手机通过 USB 口充电等“无意识的违规外连”行为或非法拷贝、打印等[2]。

3 现有网络端口硬件防护现状

3.1 用端口塞进行封堵

端口塞进行封堵如下图 1 所示。

图 1 端口塞封堵

其一，开锁工具简单，容易获得或被仿制；封堵端口塞的一个问题是其开锁工具简单，容易获得或被仿制。由于端口塞的设计相对简单，一些人可能会轻易地制作出类似的开锁工具。这就意味着即使使用了端口塞，仍然存在被未经授权的人员打开的风险。为了解决这个问题，可以考虑使用更复杂的端口塞设计，增加开锁的难度，或者采用其他更安全的访问控制措施。

其二，不具备指定开锁功能，钥匙可以打开任一端口塞，不具备精细化管理能力。封堵端口塞并不具备指定开锁功能，钥匙可以打开任一端口塞，缺乏精细化管理能力。这意味着任何一个拥有端口塞的人都可以使用同一把钥匙打开所有的端口塞。这种情况下，无法对不同的用户或者不同的端口进行精确的访问控制。为了解决这个问题，可以考虑使用具备指定开锁功能的端口塞，每个用户或者每个端口都有独立的钥匙，从而实现更精细化的管理。

其三，只能对空闲端口进行封堵，对在用端口却无能为力，只能起到防尘作用。这意味着如果一个端口正在被使用，封堵端口塞将无法阻止未经授权的访问。这对于一些需要保护敏感数据或者系统的场景来说是不够安全的。为了解决这个问题，可以考虑使用其他更高级的访问控制措施，如网络防火墙或者入侵检测系统，以

确保在用端口的安全性。

3.2 用纸张进行封堵

纸张封堵是一种常见的安全措施，主要用于对企业内部人员运维过程中的警示。然而，纸张封堵在防范企业外部人员方面存在一些问题，其安全防护能力相对较弱。首先，纸张封堵主要用于对企业内部人员运维过程中的警示。这种方式通过在设备或系统上贴纸或标签的形式，提醒内部人员在操作过程中要谨慎，遵守相关规定。然而，对于企业外部人员，纸张封堵并不能提供有效的防范措施。外部人员可能无法看到或理解这些警示，从而无法有效地防止未经授权的访问。其次，纸张封堵的安全防护能力相对较弱。纸张封堵主要依赖于人防手段，即依靠人们的警觉性来发现和防止未经授权的访问。然而，人们的警觉性有限，很容易出现疏忽或忽视的情况。这就意味着纸张封堵并不能提供可靠的安全保障。

3.3 USB 端口无防护措施

其一，USB 口通用性高，接入口无防护措施。USB 接口的通用性使得它可以连接各种设备，如电脑、手机、相机等。然而，正是因为其通用性，USB 接口成为了黑客攻击的一个潜在入口。由于 USB 接口的设计并没有考虑到安全性，它很容易受到恶意软件的攻击。黑客可以通过在 USB 设备中植入恶意代码，一旦用户将其插入电脑或其他设备，恶意代码就会被执行，从而导致用户的个人信息泄露、系统被入侵等问题。如下图 3 所示。

其二，手机充电等非恶意行为容易导致“违规外联”。在日常生活中，我们经常需要使用 USB 接口来给手机充电、传输数据等。然而，我们可能没有意识到，当我们将手机连接到公共充电器或其他设备时，我们的手机可能会与这些设备建立起数据连接，从而导致个人信息的泄露。黑客可以通过在公共充电器或其他设备中植入恶意代码，获取用户的个人信息，甚至远程控制用户的手机[3]。

4 新型网络端口硬件防护的功能

随着互联网的快速发展，网络安全问题日益突出。为了保护网络免受各种威胁，新型网络端口硬件防护应运而生。下面将从全方位态势感知及主动防御功能、USB 端口终端防护和图形化数字孪生三个方面，详细介绍新型网络端口硬件防护的功能。

4.1 全方位态势感知及主动防御功能

新型网络端口硬件防护具备全方位态势感知能力，能够实时监测网络流量、识别异常行为和攻击行为。通过对网络流量的深度分析，可以及时发现潜在的威胁，并采取相应的主动防御措施。例如，当检测到大量异常流量时，系统可以自动启动 DDoS 防护机制，阻止攻击者对网络进行洪水攻击。此外，新型网络端口硬件防护还可以对恶意软件进行实时监测和拦截，确保网络安全。

4.2 USB 端口终端防护

USB 端口是计算机与外部设备之间的重要接口，但也是安全隐患的来源。新型网络端口硬件防护通过对 USB 端口进行终端防护，有效防止恶意软件通过 USB 设备传播。它可以对接入的 USB 设备进行实时检测，识别并隔离潜在的威胁。同时，它还可以限制 USB 设备的访问权限，防止未经授权的设备接入系统，从而保护系统的安全。

4.3 图形化数字孪生

新型网络端口硬件防护采用图形化数字孪生技术，将网络端口的实时状态以图形化的方式展示出来。通过数字孪生技术，用户可以清晰地了解网络端口的工作状态、连接情况和安全性。同时，数字孪生还可以对网络端口进行模拟仿真，预测潜在的安全风险，并提供相应的建议和优化方案。这使得网络管理员能够更加直观地管理和维护网络端口的安全。

5 网络端口硬件防护的重要意义

其一，网络连接更加安全可靠。智能网口锁卡扣设计可以有效避免未经允许的端口接触、运维误插拔以及施工布线过程中带来的网线松动，从而使系统网络更加安全可靠，减少了因为端口问题导致的网络故障和安全隐患。

其二，防止违规外联和一机两用行为。硬件防护可以减少人对规章制度主动遵守的依赖，通过技术手段解决“违规外联”及“一机两用”行为，从而提高了网络安全性，减少了未经授权的网络访问和设备共享行为。

其三，主动防御零误判。硬件和 AI 分析的双重判据可以杜绝系统误判性的启动主动防御，防止影响正常的生产经营，构建专网系统网络边界“事前+事中”的主动防御机制，从而有效应对各种网络安全威胁。

总的来说，网络端口硬件防护的重要意义在于提高网络安全性，减少人为因素导致的网络问题，防止未经授权的网络访问和设备共享行为，以及构建主动防御机制，保障网络系统的正常运行和数据安全。

参考文献：

[1]荣世辉;李贵华;赖文鑫. 系统网络端口安全防护[J]. 网络安全和信息化, 2016, (03): 85-86.

[2]翟新彦. 网络端口的安全防护 [J]. 农村电工, 2010, 18 (07): 34.

[3]彭亚发. 基于端口的网络安全控制的实现 [J]. 电脑开发与应用, 2011, 24 (09): 77-78.

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。

雷阳 男 1991.6 汉。籍贯：陕西省渭南市。职称：中级， 学历：本科，研究方向： 信息网络。