Exploration of Engineering Technology, 工程技术探索(14)2023, 5
ISSN:2737-4114(Print) 2705-1242 (Online)

工业控制系统网络安全体系的架构设计

党　正
大唐山西电力工程有限公司 山西 太原 030003

【摘　要】随着信息技术的高速发展和工业互联网的兴起，电力工业控制系统网络安全问题日益凸显。电力工业控制系统作为关键基础设施的一部分，其稳定和安全对于保障国家经济发展和社会运行具有重要意义。然而，由于其开放性和复杂性，在网络攻击和威胁面前，工业控制系统网络安全面临巨大挑战。本文将围绕电力工业控制系统网络安全体系的架构设计展开讨论，希望可以为不同行业和企业提供网络安全建设的参考和指导。同时，也有助于增强工业控制系统网络的抗攻击能力，提高电力工业控制系统的安全性和稳定性，为保障国家经济安全和社会稳定提供有力支撑。

【关键词】电力工业；控制系统；网络安全；架构设计

1 电力工业控制系统受网络攻击的影响

随着信息技术的不断发展，电力系统逐渐向工业控制系统（ICS）转型。工业控制系统是指用于监控和控制各种工业过程的系统，包括电力系统在内。然而，这种转型也使得电力系统变得更加容易受到网络攻击的影响。

首先，网络攻击可能导致电力系统的服务中断。如果黑客成功侵入电力系统的工控网络，他们可以通过修改或破坏控制命令来切断电力供应，进而引发停电事件。这不仅会给用户带来不便，还可能给社会经济活动带来巨大损失。

其次，网络攻击可能危及电力系统的稳定性和安全性。电力系统运行依赖于各种自动化设备和传感器，这些设备通过网络相互连接并与控制中心进行通信。如果黑客能够突破这个网络，他们可能通过恶意指令或篡改数据造成电力系统的混乱。这不仅可能导致电力系统的不稳定运行，还可能引发设备损坏、事故甚至灾难。

另外，网络攻击还可能导致电力系统的信息泄露。电力系统中包含大量的敏感信息，如供电区域布局、用户信息和用电数据等。如果黑客获取了这些信息，他们可能会用于商业竞争、个人利益甚至其他非法目的。

为了应对电力系统工业控制系统的网络攻击，各个国家和组织已经加强了网络安全防护措施。例如，加强网络监控、实施访问控制、加密通信以及进行安全演练等，以提高电力系统的抵御能力。此外，加强安全意识教育，培养员工的网络安全意识，也是保护电力系统免受网络攻击的重要手段。

总之，电力系统工业控制系统受网络攻击的影响不容忽视。要保障电力系统的安全稳定运行，需要加强网络安全措施、提高安全意识，并与各方积极合作，共同应对网络攻击带来的挑战。

2 电力工业控制系统网络安全体系架构设计

2.1 网络分段

网络分段是电力工业控制系统网络安全体系架构设计中非常重要的一环。它的目的是将电力工业控制系统网络根据其功能和安全级别进行合理的划分，划分为不同的网络区域，以保证不同区域之间的隔离和互不干扰。首先，可以将控制网络、监控网络和数据网络等不同类型的网络分开。控制网络主要用于控制和操作电力系统，因此其安全级别要求非常高。监控网络用于对电力系统的运行状态进行实时监控和数据采集，其安全级别相对较高。而数据网络主要用于数据的存储和交换，其安全级别相对较低。其次，在不同的网络区域之间设置网络隔离设备，如防火墙和安全路由器等，来实现网络的隔离和边界保护。这些设备可以限制流量的传输和过滤恶意流量，防止攻击者或未经授权的设备进入关键网络区域。同时，通过网络隔离还可以降低安全漏洞的传播范围，确保系统的整体安全性。此外，在每个网络区域中，还可以通过使用网络隔离设备、访问控制列表（ACL）和虚拟专用网络（VPN）等技术，进一步分隔和保护系统内部的子网和设备。这可以限制不同子系统之间的通信，减少攻击面和风险。

2.2 访问控制

访问控制是电力工业控制系统网络安全的重要组成部分，它通过建立严格的授权机制，只允许授权的用户或设备进行访问，以保护网络免受未经授权的访问和恶意活动的侵害。首先，可以在网络边界上部署防火墙来控制网络流量。防火墙可以根据事先设定的规则，对网络连接进行过滤和监控。只有符合授权条件的用户或设备才能通过防火墙访问网络，而不符合条件的连接则会被阻止或拦截。这样做可以有效防止未经授权的用户或设备进入系统，确保网络的安全性。其次，在网络内

部还可以部署入侵检测系统（IDS）或入侵防御系统（IPS），来监控和检测潜在的威胁。这些安全设备可以实时监测网络流量，识别异常行为和攻击迹象，并采取相应的措施进行阻止和报警。这样可以及时发现并防范攻击，保护系统的安全。此外，还可以使用访问控制列表（ACL）和身份认证等技术，对用户进行身份验证和权限控制。通过为每个用户分配唯一的身份标识符和访问权限，可以确保只有经过验证的用户才能访问关键设备和数据。同时，可以限制不同用户在网络中的操作范围和权限，进一步提高网络的安全性。

2.3 身份验证

身份验证是确保电力工业控制系统网络安全的关键环节，采用强身份验证机制可以有效防止非授权用户访问系统并保证用户的身份真实性。首先，双因素认证是一种常见的强身份验证方式，它要求用户在登录时除了提供账号和密码外，还需要提供第二个因素进行验证，比如指纹、手机短信验证码或硬件令牌。这样一来，即使恶意用户知道了账号和密码，也无法成功登录系统，因为他们无法提供第二个因素。通过采用双因素认证，可以大大提高身份验证的安全性。其次，智能卡也是一种常用的强身份验证方式。智能卡内置了安全芯片和存储器，通过与读卡器的交互，实现对用户身份的认证和存储敏感信息。用户需要将智能卡插入读卡器，并输入配套 PIN 码才能获得授权访问系统。智能卡可以实现高度的安全性和隐私保护，防止非授权用户冒充合法用户进行访问。

3 结束语

综上所述，电力工业控制系统网络安全体系的架构设计是保护电力工业控制系统安全的关键。通过遵循设计原则和采取相应的安全措施，能够有效预防恶意攻击和数据泄露，并保护电力工业控制系统的正常运行。只有通过共同努力，我们才能建立一个安全可靠的工业控制系统网络环境。

【参考文献】

[1]曲家兴,周莹,王希忠,等.工业控制系统无线网络安全体系的研究[J].信息技术,2013(1):4.DOI:10.3969/j.issn.1009-2552.2013.01.010.

[2]詹乃松,乔振亚,Zhan,等.工业控制系统信息安全防护的研究[J].网络空间安全,2017(12):5.DOI:CNKI:SUN:AQJS.0.2017-12-015.

[3]林晓琳,徐东超,朱游龙,等.基于功能安全的轨道车辆网络控制系统设计研究[J].工业控制计算机,2022(005):035.