电力系统信息通信网络安全及防护分析

任江红
新疆昆仑工程咨询管理集团有限公司　新疆　乌鲁木齐　832000

摘　要：随着信息技术的快速发展，电力系统逐渐实现了自动化和智能化的转型。然而，电力系统的信息通信网络安全问题也日益凸显。信息通信网络是电力系统的神经系统，负责传输和处理关键信息，如实时监测数据、控制命令和故障诊断等。因此，保护电力系统信息通信网络的安全性至关重要。

关键词：电力系统；信息通信网络安全；防护

引言

信息技术的创新发展，可以为电力系统的建设完善提供根本支撑，而且信息技术在电力系统运行中的应用，能有效提高电力能源的生产质量。但是同时，电力系统的网络安全也一直是一个不可规避的问题，它将严重影响电力系统的安全稳定运行。基于此，本篇主要针对当前我国电力系统信息通信网络安全的问题进行分析，并且提出防护措施，希望能够提供一定的参考价值。

1 电力系统信息通信网络的基本特点

电力系统信息通信网络是指为电力系统的运行和管理提供数据传输、通信和控制支持的网络。它在电力系统中起到连接各个子系统、实现数据交换和远程控制的重要作用。以下是电力系统信息通信网络的基本特点：

1.1 高可靠性

电力系统是一个关乎国家经济和人民生活安全的核心基础设施，因此其信息通信网络必须具备高可靠性[1]。这意味着网络应具备充分的冗余设计，能够在设备故障或链路中断等情况下仍能正常运行，并及时恢复服务。

1.2 实时性要求高

电力系统需要对大量的实时数据进行采集、传输和处理，包括电力负荷、发电机状态、线路状态等。因此，电力系统信息通信网络需要提供低延迟的数据传输，以满足电力系统对实时性的要求。

1.3 安全性要求高

电力系统信息通信网络涉及到大量的敏感数据，如发电机运行参数、电力负荷调度等。因此，网络必须具备保密性、完整性和可用性等安全特性，以防止数据泄露、篡改和拒绝服务等安全威胁。

1.4 大容量需求

电力系统中的数据量非常庞大，包括监测数据、调度命令、告警信息等。因此，电力系统信息通信网络需要提供足够的带宽和存储能力，以支持大规模的数据传输和存储需求。

1.5 分布式特点

电力系统的设备和子系统分布在广泛的地理区域内，如发电厂、变电站、配电网等。因此，电力系统信息通信网络需要具备跨地域互联的能力，使各个子系统能够实现远程监控和控制。

1.6 兼容性要求高

电力系统信息通信网络需要与多种不同类型的设备和系统进行交互，如发电机、变电站集控系统、智能电表等[2]。因此，网络需要具备良好的兼容性，能够和各种设备和系统进行无缝集成和互操作。

2 网络安全防护对电力系统信息的作用

2.1 保护数据安全

电力系统信息中包含大量的敏感数据，如发电机、输配电设备状态数据，负荷和电能计量数据等。网络安全防护措施可以确保这些数据在传输和存储过程中不被未经授权的人员访问、窃取或篡改。

2.2 防止信息泄露

电力系统的信息通信网络可能会成为黑客攻击的目标，他们可能试图获取关键信息，如电网拓扑结构、运行策略等。网络安全防护可以防止这些机密信息外泄，保护电力系统的商业秘密和国家安全。

2.3 防范网络攻击

电力系统信息通信网络面临各种网络攻击，如恶意软件、病毒、勒索软件、拒绝服务（DDoS）等。网络安全防护可以通过防火墙、入侵检测和防御系统等技术手段，及时发现和阻止这些攻击，保障电力系统的正常运行。

2.4 提高网络可靠性

电力系统信息通信网络的可靠性对电力系统的运行至关重要。通过采用冗余设计、备份和恢复机制等网络安全防护措施，可以提高网络的可用性和稳定性，减少因网络故障造成的停电和损失。

3 电力系统信息通信网络安全风险

3.1 网络攻击

网络攻击是最常见的电力系统信息通信网络安全威胁之一。黑客可以利用漏洞和弱点，通过恶意软件、病毒、勒索软件等方式入侵电力系统网络，窃取敏感数据或干扰系统的运行。

3.2 身份认证和访问控制漏洞

如果电力系统信息通信网络存在身份认证和访问控制方面的漏洞，未经授权的用户可能获得访问权限并对系统进行篡改、破坏等操作[3]。此外，被盗用的凭证和密码也可能导致未经授权的访问。

3.3 弱密码和默认配置

弱密码和默认配置是电力系统信息通信网络的安全漏洞之一。如果管理员或用户使用容易猜测的密码或者未更改默认配置，黑客可以轻易获得对网络设备和系统的控制权。

3.4 物理安全漏洞

电力系统信息通信网络的物理设备面临物理攻击的风险。攻击者可能对服务器、网络设备或通信线路进行损坏、破坏或拆除，导致系统瘫痪或数据丢失。

3.5 数据泄露和隐私问题

电力系统信息通信网络中包含大量敏感数据，如用户个人信息、电力负荷调度数据等。如果这些数据泄露，将对用户隐私权产生严重影响，并可能被用于非法活动或诈骗行为。

4 电力系统信息通信网络安全防护措施

为了保护电力系统信息通信网络的安全，需要采取一系列的安全防护措施。以下是一些常见的电力系统信息通信网络安全防护措施：

4.1 网络访问控制

1）强化身份认证机制。强化身份认证机制是确保用户身份合法性的关键措施。传统的用户名和密码认证方式已经不再足够安全，因此需要引入多因素身份验证和双重认证等技术来增强身份验证的安全性。下面是一些常见的强化身份认证机制：第一，多因素身份验证。在登录过程中，要求用户提供多种不同类型的身份验证因素，如密码、指纹、动态令牌等。这样可以增加攻击者破解用户身份的难度。第二，双重认证。除了使用用户名和密码进行身份验证外，还要求用户提供其他额外的身份信息，例如通过手机短信验证码或移动应用程序生成的一次性密码（OTP）进行验证。这样即使黑客获得了用户名和密码，也无法轻易登录系统。第三，生物特征识别。利用生物特征（如指纹、虹膜、面部识别等）对用户进行身份认证。生物特征是独一无二的，可以提供更高级别的身份验证。

2）分段网络：分段网络是将电力系统信息通信网络划分为多个子网，并实施严格的网络隔离，以减少攻击面。通过分段网络可以将不同的功能模块或系统隔离开来，使得黑客难以跨越不同的子网进行攻击[4]。下面是一些分段网络的实施策略：第一，逻辑隔离：将电力系统信息通信网络划分为多个逻辑上隔离的区域，每个区域拥有独立的网络设备和IP地址范围。这样即使一个区域受到攻击，也不会对整个系统造成灾难性影响。第二，网络隔离。使用防火墙、路由器等网络设备进行网络隔离，限制不同子网之间的通信。只允许经过授权的用户或系统在不同子网之间进行通信，有效降低了潜在攻击者获取系统控制权的可能性。第三，DMZ设置。在分段网络中设置一个称为“反向代理”或“前置服务器”的特殊区域（DMZ），用于承载外部与内部网络之间的公共服务，如Web服务器、FTP服务器等。通过将公共服务与内部网络隔离开来，可以最大限度地降低外部攻击对整个网络的影响。

4.2 数据加密和传输保护

1）使用强加密算法：强加密算法是保护敏感数据的关键手段，能够防止未经授权的访问者获取敏感信息。加密是将原始数据转换为不可读的密文，只有具有正确密钥的接收方才能解密并还原回原始数据。以下是一些常见的强加密算法：第一，对称加密算法。使用相同的密钥对数据进行加密和解密。常见的对称加密算法有AES（高级加密标准）、DES（数据加密标准）和3DES（三重DES）等，它们在各种应用中都被广泛使用。第二，非对称加密算法。使用一对密钥，即公钥和私钥，来进行加密和解密。公钥可以公开分享给其他人，而私钥则必须保密。常见的非对称加密算法有RSA、DSA和ECC等，它们在数字签名和密钥交换等场景下使用广泛。第三，哈希函数。将任意长度的数据转换为固定长度的哈希值。常见的哈希函数有MD5、SHA-1和SHA-256等，它们被用于验证数据的完整性，例如在数字签名中使用。

2）虚拟专用网络（VPN）：第一，VPN通过建立加密隧道来保护远程访问和数据传输的安全性。它使得用户可以通过公共互联网安全地访问电力系统信息通信网络，并确保数据传输的私密性和机密性。第二，数据加密。VPN使用加密算法对传输的数据进行加密，使得数据在互联网上传输时无法被黑客窃取或篡改。第三，远程访问。用户可以通过VPN连接到电力系统信息通信网络，实现远程访问，并能够像内部员工一样安全地访问

系统资源和数据。第四，匿名性。VPN还可以隐藏用户的真实IP地址，增加用户的匿名性，提高数据传输的安全性和隐私保护。

4.3 恶意软件防护

1）安装防病毒软件和防恶意软件工具：安装有效的防病毒软件和防恶意软件工具是保护电力系统信息通信网络免受恶意软件侵害的重要步骤。这些工具可以实时监测和扫描终端设备上的文件和网络流量，并检测和清除潜在的恶意软件。以下是一些注意事项：第一，及时更新。确保防病毒软件和防恶意软件工具处于最新状态，以获取最新的病毒定义库和恶意软件特征库，能够及时识别和阻止最新的威胁。第二，实时保护[5]。启用实时监控功能，对正在执行的程序、下载的文件和访问的网站进行实时检测，以防止恶意软件感染系统。第三，自动扫描。设置定期自动扫描计划，全面检查系统文件、应用程序和邮件附件等，确保及时发现和清除潜在的恶意软件。

2）策略限制。通过策略限制，对电力系统信息通信网络上的终端设备运行未授权的软件，可以减少恶意软件的风险。以下是一些可行的策略限制措施：第一，应用白名单。定义允许运行的授权应用程序列表，并限制其他未授权的软件执行。这样可以减少未知或潜在恶意软件的风险。第二，权限管理。分配适当的权限给用户，限制其对系统和文件的访问能力。只有经过授权的用户才能进行关键操作，减少恶意软件的传播和危害范围。第三，教育培训。定期开展安全意识教育培训，提高员工对恶意软件的识别和防范能力。员工应知晓不点击可疑链接、打开未知附件等基本安全原则。

4.4 强化物理安全

强化物理安全是电力系统信息通信网络安全的重要措施。以下将详细介绍三个常见的强化物理安全措施：控制访问、监控和报警，以及安全设施。

1）控制访问：控制访问是限制电力系统信息通信网络设备的物理访问权限，确保只有经过授权的人员可以接触和操作这些设备。以下是一些注意事项：第一，门禁系统。安装门禁系统，使用刷卡、指纹识别或其他身份验证方式来限制进入机房、服务器房等关键区域。第二，访客登记。建立访客登记制度，要求访客在进入关键区域之前进行身份核实，并由授权人员进行陪同。第三，安全标识。设置清晰可见的安全标识，包括警示标志、禁止通行标识和安全规定提示等，以增加人员对物理安全的意识和遵守程度。

2）监控和报警：使用安全摄像头、入侵检测和报警系统等物理安全设备，对关键区域进行监控和检测异常行为。以下是一些注意事项：第一，安全摄像头。安装摄像头以监控关键区域，并确保录像数据的备份和存储，以便需要时进行调查和审计。第二，入侵检测系统。部署入侵检测系统来监测任何未经授权的物理入侵行为，例如非法闯入或设备操纵等[6]。第三，报警系统。配置报警装置，如声音警报、短信通知或电子邮件警报，一旦发现异常活动或入侵尝试即时通知相关人员。

3）安全设施。保障机房、服务器房和通信线路等关键设施的安全，可以采取以下措施：第一，防火墙。安装防火墙来限制对网络的未经授权访问，并监测和阻止恶意流量的传输。第二，UPS电源。使用不间断电源（UPS）系统，以提供电力稳定性和冗余备份，确保关键设备在停电或电力故障时能够继续运行。第三，灭火系统。安装自动灭火系统和火灾报警器，及时检测和应对机房内的火灾威胁，减少火灾对设备和数据的损害。

结语

随着科技的不断发展，电力系统信息通信网络的安全形势也在不断演变。人工智能、物联网等新技术带来了新的安全挑战。因此，持续的研究和创新是必须的，以便针对新的威胁采取相应的防护措施。总之，电力系统信息通信网络的安全问题需要得到持续关注和重视。通过采取综合的防护措施和技术手段，我们可以有效地保护电力系统信息通信网络的安全，确保电力系统的稳定运行和供电安全。

参考文献

[1]候正煜.电力系统信息通信的网络安全及防护研究[J].网络安全技术与应用，2020（2）.

[2]丁兆轩.电力系统信息通信的网络安全及防护研究[J].环球市场，2020（10）.

[3]刘群.电力系统信息通信网络安全及防护安全探究[J].建筑工程技术与设计，2020（27）.

[4]赵凝.电力系统信息通信网络的安全防护策略探讨[J].电子元器件与信息技术,2022,6(01):255-256.DOI:10.19772/j.cnki.2096-4455.2022.1.110.

[5]邱思思.电力系统信息通信网络安全及防护分析[J].中国新通信,2022,24(01):18-19.

[6]欧阳宇宏,康文倩,车向北.电力监控系统信息通信网络安全及防护问题研究[J].信息系统工程,2020(12):60-61.