水电厂电力监控系统网络安全防护体系建设探析

陈成　陈琳　徐启阳
国网新源集团有限公司富春江水力发电厂

摘　要：水电厂电力监控系统网络安全防护体系的建设对于保障电力系统的安全稳定运行具有重要意义。本文首先介绍了建设网络安全防护体系的目的和方法，然后详细阐述了防护体系的实施与部署过程。本文的研究结论为水电厂电力监控系统网络安全防护体系的建设提供了有益的参考。

关键词：水电厂电力监控系统；网络安全；防护体系
【DOI】10.12252/j.issn.2096-6261.2023.06.118

引言

随着信息技术的发展，水电厂电力监控系统网络安全问题日益突出。为了保障电力系统的安全稳定运行，建设一套完善的网络安全防护体系显得尤为重要。本文旨在探讨水电厂电力监控系统网络安全防护体系的建设，为相关企业和研究人员提供有益的参考。

一、水电厂电力监控系统网络架构与功能

水电厂电力监控系统网络架构主要由三个层次组成：站控管理层、网络通讯层和现场设备层。站控管理层是电力监控系统的管理人员，主要负责人机交互，即通过监控主机实现系统数据的实时显示、处理、存储和传输。这一层是系统的核心，直接影响着监控系统的效率和稳定性。网络通讯层主要负责实现多功能仪表等与站控管理层之间的数据交互，使配电系统管理集中化、信息化、智能化。它通过总线网络，利用通讯协议实现数据的高效传输和交换。这一层的性能对整个监控系统的稳定性和效率起到至关重要的作用[1]。现场设备层主要由智能设备组成，如电力仪表等，通过屏蔽双绞线RS485接口，采用MODBUS通讯协议总线连接接入监控主机进行组网，实现远程控制。这一层是数据采集的终端，负责收集和传输各种电力参数，如电压、电流、频率等。

二、水电厂电力监控系统网络安全风险分析

1.常见的网络安全威胁与攻击手段

在水电厂电力监控系统中，存在各种潜在的网络安全威胁与攻击手段。以下是一些常见的例子：（1）恶意软件：这包括病毒、木马和间谍软件等，在未经授权的情况下侵入系统并窃取敏感信息或破坏系统功能。（2）拒绝服务攻击（DoS）：攻击者通过向目标服务器发送大量请求，使其无法正常响应合法用户的请求，从而使系统不可用。（3）数据篡改：攻击者修改系统中的数据，以达到欺骗用户、破坏设备或影响运营的目的。（4）密码破解：攻击者通过使用暴力破解或其他技术手段获取系统中的密码，进而非法进入系统并执行潜在的恶意活动。（5）社交工程：攻击者通过欺骗、伪装或利用人类的弱点来获取系统中的敏感信息或绕过安全措施[2]。（6）网络钓鱼：攻击者伪造合法机构的通信，并通过诱骗用户点击链接或提供个人信息，从而获取他们的敏感信息。

2.电力监控系统网络脆弱性分析

（1）物理层脆弱性：物理层安全涉及设备硬件、通信线路和网络设施等的安全。由于设备的物理访问和通信线路的暴露，容易受到物理攻击，如破坏、偷窃和电磁泄漏等。（2）网络层脆弱性：网络层安全涉及网络通信协议、路由器、交换机等网络设备的安全。由于网络协议自身可能存在安全漏洞，如TCP/IP协议的安全性问题，以及路由器的配置错误等，都可能导致网络攻击和入侵。（3）应用层脆弱性：应用层安全涉及电力监控系统的各种应用程序和数据库的安全。应用程序可能存在安全漏洞，如缓冲区溢出、注入漏洞等，数据库可能存在安全漏洞，如SQL注入、权限提升等。（4）管理层脆弱性：管理层安全涉及安全管理策略、安全审计和日志管理等。由于管理策略可能存在漏洞，如权限分配不合理、审计日志记录不完善等，可能导致管理上的安全风险[3]。

3.网络安全事件的影响与后果

（1）数据泄漏：电力监控系统涉及大量的敏感数据，如调度计划、设备状态、用户信息等。如果系统存在安全漏洞，可能会导致数据泄漏，对企业的声誉和利益造成损害。（2）系统瘫痪：严重的网络安全事件可能导致电力监控系统瘫痪，无法正常进行电力调度和监控。这可能对水电厂的运营造成严重影响，甚至导致停产和安全事故。（3）恶意操控：攻击者通过入侵电力监控系统，可能对电力设备的运行进行恶意操控，如

非法控制开关设备、篡改调度指令等。这可能导致电力设备的损坏或事故的发生。（4）经济损失：网络安全事件可能导致水电厂遭受经济损失，如设备损坏修复费用、数据泄漏的赔偿费用以及系统瘫痪导致的生产损失等[4]。（5）法律责任：如果网络安全事件涉及用户隐私信息的泄漏，企业可能面临法律责任和监管处罚。这可能对企业的声誉和经营造成严重影响。

三、水电厂电力监控系统网络安全防护体系设计

1.物理安全防护

首先，为了实现物理安全的目标，必须建立合适的访问控制措施。这包括设置适当的门禁系统和进出口通道的监控设备，以确保只有经过授权的人员才能够进入关键区域。此外，使用身份验证技术（如指纹识别、虹膜扫描等）来加强访问控制的安全性，同时记录和审计每个人员的进出情况。其次，应该对关键设备和服务器进行合适的布局和封存。物理设备的位置应该放置在安全的地方，远离可能存在的危险因素，例如火灾或洪水等。此外，服务器室应该配备适当的温度和湿度控制设备，以保证设备的正常运行。为了防止未经授权的物理访问，对服务器室进行严格的限制，只有授权人员才能进入[5]。另外，为了保护关键设备和数据，必须采用适当的安全存储措施。这包括使用防火和防水的设备来保护服务器和存储设备，并定期备份关键数据以应对意外情况。

2.网络层安全防护

首先，建立强大的防火墙来保护水电厂电力监控系统与外部网络之间的连接。防火墙应配置为只允许经过验证的用户和设备访问系统，并且根据需要限制特定IP地址或端口的访问。该防火墙还应具备入侵检测和防御功能，即时识别和拦截潜在的恶意流量，保护系统免受网络攻击。其次，采用虚拟专用网络（VPN）技术加密数据传输。VPN提供了一个安全的通信通道，使得通过公共网络进行的数据传输变得私密和安全。通过使用VPN，可以确保数据在传输过程中的机密性和完整性，防止未经授权的访问和窃听。因此，及时应用这些更新是至关重要的，以减少攻击者利用已知漏洞进行攻击的机会。

3.应用层安全防护

首先，确保所有应用程序和服务都经过严格的安全审计和测试。这包括对代码进行静态和动态分析，识别和纠正潜在的漏洞和弱点。同时，建立安全开发生命周期（SDLC）流程，确保在应用程序开发的每个阶段都进行安全评估和测试。

其次，实施访问控制和身份验证机制，以限制用户对应用程序和服务的访问权限。使用强大的认证方法，如多因素身份验证，可以提高系统的安全性。此外，为敏感操作和数据访问实施细粒度的授权策略，只允许经过授权的用户执行特定的操作或访问特定的数据。另外，加密是保护应用层通信安全的关键技术。通过使用安全套接字层（SSL）或传输层安全性（TLS）协议，可以对数据进行加密和解密处理，确保数据在传输过程中的机密性。特别是对于涉及敏感数据传输的操作，如用户登录、身份验证和数据交换，必须使用加密技术来防止中间人攻击和数据泄漏。

4.管理层安全防护

首先，建立明确的安全策略和规定，以指导组织内部的网络安全实践。这包括确定安全目标、责任分工和工作流程，确保每个成员都了解他们在网络安全方面的职责和义务。此外，安全策略还应考虑法规和合规性要求，确保组织符合相关的法律法规和行业标准。其次，为管理层提供必要的网络安全培训和教育。管理层应该了解网络安全的基本原理和最佳实践，以及当前的威胁和攻击趋势。通过定期的培训和教育活动，可以提高管理层对网络安全风险的认识，并帮助他们做出明智的决策和行动。另外，建立一个专门的网络安全团队或委员会，负责监督和协调组织的网络安全工作。该团队应由具有网络安全专业知识和经验的成员组成，并与管理层保持密切合作。他们的职责包括制定和更新安全策略、评估和管理风险、响应安全事件等。

四、水电厂电力监控系统网络安全防护体系实施与部署

1.实施前的准备工作

（1）需求分析：明确防护体系的建设目标、功能需求和性能要求，为后续的设计和实施提供指导。（2）风险评估：对水电厂电力监控系统的网络安全风险进行全面评估，了解潜在的安全威胁和漏洞，为制定相应的防护策略提供依据。

（3）方案设计：根据需求分析和风险评估的结果，设计出符合水电厂实际情况的网络安全防护体系方案，包括系统架构、设备选型、配置参数等方面。（4）培训与宣传：加强员工对网络安全的认识和意识，培训员工掌握必要的防护技能和应对措施，提高整

个团队的网络安全水平。（5）物资准备：根据设计方案，提前采购所需的设备、软件和材料，确保实施过程中的物资供应。（6）场地准备：为网络安全防护体系的建设提供合适的场地和空间，包括设备安装、线缆布放、监控室等。

2.安全设备的选型与配置

（1）防火墙：选择具有强大性能和良好口碑的防火墙产品，配置相应的安全策略，实现对外来入侵的检测和防御。（2）入侵检测系统（IDS/IPS）：IDS/IPS是用于检测和防御网络入侵的安全设备。在配置IDS/IPS时，需要设置合理的安全规则，并根据实际情况调整报警阈值，避免误报和漏报。（3）防病毒网关：防病毒网关是用于防御网络病毒传播的安全设备。在配置防病毒网关时，需要选择具有最新病毒库和强大过滤功能的网关产品，同时要配置相应的安全策略，实现对外来病毒的防御和过滤。（4）数据加密设备：数据加密设备是用于保护数据传输和存储的安全设备。在配置数据加密设备时，需要选择具有高强度加密算法和良好稳定性的产品，同时要配置相应的加密策略和密钥管理方案，确保数据的机密性和完整性。（5）安全审计系统：安全审计系统是用于记录网络活动和监控系统安全的设备。在配置安全审计系统时，需要选择具有全面监控和智能分析功能的系统，同时要配置相应的审计规则和报警机制，实现对外来威胁的及时发现和处理[6]。

3.安全策略的制定与部署

（1）制定全面的安全策略：安全策略应该覆盖所有可能的安全风险和威胁，包括网络设备、主机、应用、数据等方面。在制定安全策略时，要综合考虑企业的实际情况、业务需求和安全风险，制定出全面、可行的安全策略。（2）明确安全责任和权限：安全策略应该明确各个部门和人员的安全责任和权限，建立完善的安全管理制度。同时，要定期对安全管理制度进行审查和更新，确保其与实际的安全需求相匹配。（3）配置安全设备和工具：根据安全策略，配置相应的安全设备和工具，如防火墙、入侵检测系统、数据加密设备等。在配置过程中，要确保设备和工具的选型、配置和部署符合安全策略的要求，同时要关注设备和工具的更新和维护，确保其正常工作[7]。（4）建立应急响应机制：针对可能出现的网络安全事件，建立应急响应机制，制定相应的应急预案和处理流程。同时，要加强应急演练和培训，提高应急响应的能力和效率。

4.安全监测与审计机制的建立

（1）实时监测：通过部署专业的安全监测设备和工具，对水电厂电力监控系统的网络流量、设备状态、应用运行等进行实时监测。这些设备和工具应具备实时报警和日志记录功能，以便及时发现和处置潜在的安全威胁。（2）安全审计：定期对系统进行全面的安全审计，包括对系统配置、访问控制、数据完整性等方面的检查。通过审计，可以及时发现系统存在的安全隐患和漏洞，并采取相应的措施进行修复和改进。（3）日志分析：建立日志分析机制，对系统产生的各类日志进行定期分析和挖掘。通过对日志的深入分析，可以了解系统的运行情况、发现潜在的安全问题并追溯安全事件。（4）入侵检测与防御：配置专业的入侵检测系统（IDS/IPS），实时监测网络中的异常流量和行为，及时发现并防御网络入侵行为。同时，要定期更新IDS/IPS的规则库，确保其能够防御最新的网络攻击手段。

结束语

通过本文的研究，我们了解了水电厂电力监控系统网络安全防护体系建设的重要性和必要性。在实施与部署过程中，需要综合考虑多种因素。同时，建立完善的安全监测与审计机制也是确保防护体系有效性的关键环节。通过实施这些措施，可以有效提高水电厂电力监控系统的网络安全防护能力，保障电力系统的安全稳定运行。未来，随着技术的不断进步和应用需求的不断提高，水电厂电力监控系统网络安全防护体系的建设仍需不断改进和完善。

参考文献

[1]曾体健.水电厂电力监控系统网络安全防护体系建设探析[J].水电站设计，2022，38（01）：18-19.

[2]赵兴荣.如何提高水电厂电力监控系统网络安全防护水平[J].云南水力发电，2021，37（09）：162-164.

[3]陈亚燕.水电厂信息网络安全防护策略探究[J].网络安全技术与应用，2021，（03）：103-104.

[4]潘峰.水电厂电力监控系统安全防护策略浅析[J].中国新通信，2020，22（17）：149-150.

[5]邓志平.水电厂电力监控系统的安全防护措施研究[J].大众标准化，2020，（10）：182-183.

[6]刘中坚.水电厂电力监控系统安全防护策略研究[J].电子制作，2020，（Z2）：87-88+12.

[7]宗和刚，张朝粤.水电厂网络安全态势感知系统的实现[J].水电站机电技术，2019，42（09）：13-16+70.