 DOI: https://doi.org/10.12349/iser.v6i7.6703

Network security risk assessment and defense of nuclear power plants

Zhengzheng Zhang

Daya Bay Nuclear Power Operation Management Co., Ltd., Shenzhen, Guangdong, 518000, China

Abstract

The widespread application of digital and intelligent technologies in nuclear power plants has increased the reliance on network systems for production control, safety monitoring, and operational management. This paper addresses the cybersecurity issues in nuclear power plants by systematically analyzing risk factors, including external network attacks, internal personnel operations, equipment system vulnerabilities, supply chain risks, and natural disasters. It then establishes risk assessment goals and principles, constructing a comprehensive process that includes asset identification, threat identification, vulnerability identification, risk analysis and assessment, and response monitoring. Furthermore, it proposes cybersecurity defense strategies from three perspectives: technical defense, management defense, and physical environment security.

Keywords

nuclear power plant; network security; risk assessment; defense strategy; risk analysis

核电厂网络安全风险评估与防御

张峥峥

大亚湾核电运营管理有限责任公司，中国 · 广东 深圳 518000

摘　要

数字化、智能化技术在核电厂中的广泛应用，使得核电厂的生产控制、安全监测、运营管理等环节对网络系统的依赖程度日益加深。本论文则针对核电厂网络安全问题，系统地分析了外部网络攻击、内部人员操作、设备系统漏洞、供应链及自然灾害等风险因素。随后通过确立风险评估目标与原则，构建了包含资产识别、威胁识别、脆弱性识别、风险分析评估及应对监控的完整流程，还从技术防御、管理防御和物理环境安全保障三个方面入手提出了网络安全的防御策略。

关键词

核电厂；网络安全；风险评估；防御策略；风险分析

1 引言

核电厂作为关乎国家能源安全与公众生命财产安全的重要基础设施，其网络安全不仅影响自身的安全稳定运行，在遭受了网络攻击或出现安全漏洞时，甚至还可能引发核泄漏等灾难性的后果，最终会对环境和社会造成不可估量的危害。近些年来，全球范围内针对关键基础设施的网络攻击事件频发，核电厂自然也成为了黑客攻击的潜在目标，因此网络安全问题已经成为了核电厂安全管理的重要组成部分。在该情况之下，深入地开展核电厂网络安全风险评估与防御研究，对于保障核电厂的安全稳定运行、维护国家安全和社会稳定都具有重要的现实意义。

【作者简介】张峥峥（1990–），男，中国江苏南通人，本科，工程师，从事通信、网络安全、数字化转型研究。

2 核电厂网络安全风险分析

2.1 外部网络攻击风险

核电厂面临着多种来自外部的网络攻击威胁。黑客便是当中的头号威胁，他们可能会利用网络漏洞对核电厂的控制系统、数据中心等关键的网络设施发起攻击。以分布式拒绝服务（DDoS）攻击为例，黑客通过大量的非法请求可以占用网络带宽和系统资源，进而导致网络瘫痪，使核电厂的监测和控制功能无法正常的运行。此外，恶意软件攻击也是黑客们常见的手段，类似病毒、木马、勒索软件等恶意程序一旦侵入核电厂网络，就可能会窃取敏感数据、篡改控制指令，最终破坏核电厂的正常生产秩序。甚至一些国家或组织出于政治、经济等目的，也可能会对核电厂发动有针对性的高级持续性威胁（APT）攻击，由于这类攻击具有隐蔽性强、持续时间长、攻击手段复杂等特点，所以能够长期的潜伏在核电厂网络中伺机而动，其严重地威胁着核电厂的安全运行[1]。

2.2 内部人员误操作与恶意行为风险

内部人员的行为对于核电厂的网络安全有产生直接的影响。一方面部分员工由于自身网络安全意识淡薄、操作技能不足等原因，极可能会在日常工作中出现误操作，像随意下载不明来源的文件、使用弱密码、未按规定流程操作网络设备等等，从而为网络攻击打开缺口。另一方面则是存在着内部人员恶意行为的风险，个别心怀不轨的员工可能出于利益驱使、报复心理等原因，会选择故意泄露核电厂网络安全信息、篡改系统数据、破坏网络设备，此情况给核电厂的网络安全带来了严重的危害。

2.3 网络设备与系统漏洞风险

现阶段，核电厂内使用的大量网络设备和系统均存在着漏洞风险。其中网络设备如交换机、路由器、防火墙等，在设计、生产和配置的过程中可能存在着安全漏洞，如果这些漏洞被攻击者所利用，就可能导致设备被控制、网络通信被窃听或篡改。不仅如此，核电厂的工业控制系统、管理信息系统等软件系统同样面临着漏洞问题，因软件编程缺陷、未及时更新补丁等因素，使得系统非常容易受到攻击 [2]。

2.4 供应链安全风险

核电厂网络系统的供应链涉及到了众多的环节，从硬件设备的采购、软件系统的开发，再到系统集成和维护，当中的每个环节都可能会存在安全风险。首先是供应商提供的设备和软件旨在，可能存在着未公开的后门或安全缺陷，一旦被植入恶意代码再接入核电厂网络，就会成为极大的安全隐患。其次供应链中的物流运输、存储等环节若管理不善，也可能会导致设备和软件受到物理损坏或者被篡改。最后供应链的稳定性也会影响到核电厂的网络安全，若关键的供应商出现问题，如破产、被恶意收购等，就可能导致核电厂无法及时地获得所需的安全更新和维护服务，进而增加了网络安全风险。

2.5 自然灾害与物理环境风险

地震、洪水、台风、雷击等自然灾害，能够对于核电厂的网络基础设施造成严重的破坏，从而导致网络中断、设备损毁。例如强烈地震可能会使机房建筑倒塌，此时便会损坏服务器、网络交换机等设备；洪水则可能会淹没地下网络设备室，进而造成设备的短路损坏。此外物理环境因素如机房温度过高、湿度过大、电力供应不稳定等，依然也会到影响网络设备的正常运行，直接地降低了设备的使用寿命，也增加了网络故障发生的概率，终将影响到核电厂的网络安全 [3]。

3 核电厂网络安全风险评估体系构建

3.1 风险评估目标与原则

核电厂网络安全风险评估的目标是全面、准确地识别网络系统中存在的安全风险，并且评估风险发生的可能性和潜在影响，为制定有效的风险应对策略提供依据，以此保障核电厂网络系统的安全性、可靠性和稳定性。

实际在风险的评估过程中，相关人员应遵循以下原则：一是系统性原则，即全面地考虑到核电厂网络系统的各个组成部分进行整体评估，当中包括了硬件设备、软件系统、人员操作、物理环境等；二是科学性原则，要求相关人员采用科学且合理的评估方法和技术手段，务必确保评估结果的客观、准确；三是动态性原则，由于核电厂网络系统是不断发展和变化的，加之外部网络安全环境的改变，因此需要定期或不定期地进行风险评估，保障新的风险能够及时地被发现；四是可操作性原则，在该原则下评估的流程和方法应简单易懂、便于实施，评估的结果也应具有实际的指导意义，如此才能够为风险应对提供有效的支持。

3.2 风险评估流程

3.2.1 资产识别

因为资产识别是风险评估的基础，所以相关人员需要对核电厂网络系统中的各类资产进行全面地梳理和分类。而网络资产主要包括硬件资产、软件资产、数据资产以及人员资产。对上述的每类资产均需进行详细地描述，核心在于确定其重要性等级，如核心控制系统服务器、核反应堆运行数据等资产，因其对核电厂的安全运行至关重要，所以应划分为高重要性资产，而一些辅助办公设备和普通数据则可划分为低重要性资产。

3.2.2 威胁识别

威胁识别旨在分析可能会对核电厂网络资产造成损害的潜在因素。结合前文所述的风险分析来看，相关人员应从外部网络攻击、内部人员行为、设备系统漏洞、供应链安全和自然灾害等方面入手，识别出各类威胁源。

3.2.3 脆弱性识别

脆弱性识别是查找核电厂网络系统中存在的安全弱点和漏洞。通过技术检测和人工检查相结合的方式，对网络设备、软件系统、网络配置、安全管理制度等进行全面检查。利用漏洞扫描工具对网络设备和软件系统进行扫描，检测是否存在已知的安全漏洞；对网络配置进行审查，检查是否存在不合理的访问控制策略、未启用的安全功能等问题；对安全管理制度进行评估，查看是否存在制度不完善、执行不到位等情况。例如，发现某网络设备存在未修复的高危漏洞，某软件系统的用户权限分配过于宽松，安全管理制度中缺乏对员工网络安全培训的相关规定等，这些都是网络系统的脆弱性所在。

3.2.4 风险分析与评估

风险分析与评估即根据资产识别、威胁识别和脆弱性识别的结果，确定出风险发生的可能性和潜在影响。通常采用的是定性与定量相结合的方法，对于风险进行综合的评估。其中定性评估是通过专家判断、风险矩阵等方式，对于风险的可能性和影响程度进行主观的评价；定量评估则是利用数学模型和统计方法，对于风险进行量化分析，如计算风险发生的概率和可能造成的经济损失。随后再将风险的可能

性和影响程度通过风险矩阵划分为不同的等级，针对其等级采取相对应的措施。

3.2.5 风险应对与监控

根据风险评估的结果，制定出相应的风险应对策略。一般对于高风险，应优先采取措施将其消除或降低风险，如修复系统漏洞、加强访问控制、增加安全防护设备等；对于中风险则可采取一定的措施进行控制和管理，如制定应急预案、加强员工培训等等；面对低风险仅需进行持续地监控，若风险等级发生变化，再及时地采取相应的应对措施。

3.3 风险评估方法

核电厂网络安全风险评估可采用多种方法进行，目前常见的有德尔菲法、层次分析法（AHP）、故障树分析法（FTA）、模糊综合评价法等等。具体来说：德尔菲法通过专家匿名反馈和多轮调查，能够收集专家的意见，以此对风险进行评估，一般适用于缺乏历史数据和难以量化的风险评估；层次分析法可以将复杂的问题分解为多个层次，再通过建立判断矩阵，确定出各因素的权重，从而对风险进行综合地评估，该方法能够有效地处理多因素、多层次的风险评估问题；故障树分析法则从顶事件出发，经由分析导致顶事件发生的各种可能原因，构建起故障树，进而评估风险发生的概率和影响；而模糊综合评价法利用了模糊数学理论，可以对风险的模糊性和不确定性进行处理，其可更加准确地评估风险。一般实际评估当中，相关人员可根据具体的情况来选择合适的评估方法，也可将多种方法相结合进行评估，如此可提高评估结果的准确性和可靠性。

4 核电厂网络安全防御策略

4.1 技术防御

在技术防御方面，相关人员首先要加强对于网络边界的防护，几部署高性能的防火墙、入侵检测与防御系统（IDS/IPS）、虚拟专用网络（VPN）等设备。此时防火墙可对进出核电厂网络的流量进行过滤和控制，能有效地阻止非法访问和攻击；IDS/IPS 则能实时地监测网络中的异常行为和攻击活动，并及时地对其进行阻断；而 VPN 可以在公共网络上建立安全的专用通道，进而保障远程访问的安全性。同时也应对核电厂网络进行合理的分区和隔离，通过将生产控制网络与管理信息网络分开，并且在不同安全等级的网络之间采用网闸等设备进行物理隔离，来防止网络攻击在不同的网络之间扩散。

4.2 管理防御

一方面应当完善核电厂网络的安全管理制度，制定涵盖了人员管理、设备管理、数据管理、应急响应等多个方面的规章制度。基于此，也应注重加强人员网络安全的培训，务必提高员工的网络安全意识和操作技能，并且定期地组织网络安全演练，进而增强员工应对网络安全事件的能力。同时需要建立严格的人员访问控制机制，以此根据对员工、外包人员等的网络访问权限进行审批和管理，且定期地对人员权限进行审查和更新。

另一方面则需建立健全的网络安全应急响应机制。展开而言：第一要制定详细的应急预案，在其中明确应急响应流程和各部门的职责；第二要定期地对应急预案进行演练和评估，再根据演练的结果对于预案进行修订和完善；第三需加强网络安全事件的监测和预警，即建立安全事件报告制度，一旦发现了网络安全事件，相关人员需及时地向上级部门报告，并迅速地启动应急预案，针对事件采取有效的应对措施，以降低事件而造成的损失。

4.3 物理环境安全保障

核电厂网络设备机房的物理安全防护是至关重要的部分，一般需要设置严格的门禁系统，即采用生物识别技术（如指纹识别、人脸识别等）和智能卡相结合的方式，对于进入机房的人员进行身份验证。同时安装视频监控系统，借此对机房进行 24 小时的实时监控，以确保机房内的设备和人员活动始终处于监控之下。但对于机房的温度、湿度、电力供应等环境参数也应进行实时地监测和控制，并配备不间断电源（UPS）、空调系统等设备，使得网络设备能够一直在适宜的环境中运行。

针对于网络设备的物理保护，则需对重要的设备进行加固和防盗处理，严防设备被盗或被破坏的情况发生。为此要对网络线缆进行规范的铺设和管理，一定要避免线缆被损坏或被非法接入。并且定期地对网络设备要进行巡检和维护，确保能够及时地发现和处理设备故障和安全隐患，确保网络设备的正常运行。另外需要建立异地灾备中心，在此将核电厂的重要数据和关键业务系统进行异地备份，这样在发生自然灾害或重大网络安全事件时，核电厂就能够快速地恢复业务运行。

5 结语

通过对核电厂网络安全风险的全面分析，构建了科学与合理的风险评估体系，并从技术防御、管理防御和物理环境安全保障等多个方面制定了有效的防御策略，最终显著地提升了核电厂的网络安全防护能力。持续地加强网络安全技术研发和创新，使得网络安全管理水平以及人员培训和教育始终跟随时代的脚步，以此为核电厂的安全运行和可持续发展提供坚实的网络安全保障。

参考文献

[1] 王萍.核电厂智能设备的网络安全防护设计[J].自动化仪表,2021,42(S1):314-318.

[2] 程正.智能仪表技术及工业自动化应用发展[J].电子技术与软件工程,2017,(17):137.

[3] 杨景利,刘元,孟庆军,等.核电厂仪控系统安全防护策略研究及应用[J].自动化仪表,2019,40(06):93-97.