浅析火电厂工控网络信息安全策略

刘志强
国能亿利能源有限责任公司电厂　内蒙古　鄂尔多斯　014300

摘　要：随着信息化技术在火电厂的深度应用，工控网络已成为保障电力生产、调度、管理高效运行的核心支撑。本文聚焦火电厂工控网络信息安全策略展开分析。首先强调火电厂工控网络信息安全的重要性，其关乎电力供应稳定与生产安全。接着剖析工控网络信息面临物理安全、网络攻击、系统漏洞、应用安全及管理安全等多方面威胁。基于此，从加强物理安全防护、构建网络防护体系、提升系统安全防护能力、保障应用安全以及完善管理策略等多个维度，提出全面且针对性的火电厂工控网络信息安全策略，旨在为火电厂工控网络信息安全保障提供参考。

关键词：火电厂；工控网络信息；安全策略

引言：在电力行业信息化快速发展的当下，火电厂作为重要电力生产单位，其工控网络信息安全至关重要。火电厂工控网络承载着生产控制、运行管理等关键业务数据，一旦遭受破坏或泄露，不仅会影响电厂正常生产运营，导致设备故障、生产中断，还可能引发大面积停电等严重后果，危及社会公共安全与稳定。同时，随着网络技术不断进步，火电厂工控网络面临的安全威胁日益复杂多样。因此，深入探讨火电厂工控网络信息安全策略，提升其安全防护水平，成为保障火电厂安全稳定运行的迫切需求。

1 火电厂工控网络信息安全的重要性

火电厂工控网络信息安全关乎电力生产的稳定与可靠运行。在生产环节，工控网络连接着众多关键控制系统，如锅炉控制、汽轮机调节等，一旦遭受网络攻击或数据泄露，可能导致控制指令异常，引发设备故障、生产停滞，造成巨大的经济损失，甚至引发安全事故，威胁人员生命安全。从电力供应角度看，火电厂是电网的重要电源支撑点。工控网络信息安全问题可能引发发电出力不稳定，影响电网的频率和电压稳定，进而导致大范围停电，给社会生产生活带来严重不便，影响金融、交通、通信等众多行业的正常运转，造成难以估量的社会经济损失。此外，火电厂工控网络还涉及大量企业机密和敏感信息，如生产工艺、设备参数、运营数据等。这些信息一旦泄露，可能被竞争对手利用，损害企业利益，削弱企业在市场中的竞争力。因此，保障火电厂工控网络信息安全，是确保电力生产安全、稳定供应以及企业可持续发展的关键所在[1]。

2 火电厂工控网络信息面临的主要安全威胁

2.1 物理安全威胁

火电厂工控网络物理安全面临诸多潜在威胁。自然环境因素是不可忽视的一点，如地震、洪水、雷击等自然灾害，可能直接破坏机房建筑、网络设备及线路，导致工控网络瘫痪。此外，人为的物理破坏也时有发生，例如不法分子蓄意破坏机房设施、盗窃关键设备，或者因施工操作不当，误挖断网络线缆等。同时，机房的温湿度、灰尘等环境条件若控制不当，也会影响设备的正常运行，加速设备老化，间接威胁工控网络信息安全，影响火电厂的正常生产运营。

2.2 网络攻击威胁

火电厂工控网络面临着多样化的网络攻击威胁。黑客可能利用网络扫描工具，探测工控网络漏洞，进而发起拒绝服务攻击，使工控网络服务器过载，无法正常响应合法请求，导致生产控制系统瘫痪。病毒和木马也是常见威胁，它们可通过网络传播，感染工控网络设备，窃取敏感信息或破坏系统文件。此外，APT 攻击更具隐蔽性和针对性，攻击者长期潜伏在工控网络，窃取关键数据，对火电厂的生产安全和商业机密构成严重威胁。

2.3 系统漏洞威胁

火电厂工控网络中的各类操作系统、数据库管理系统等软件，不可避免地存在安全漏洞。这些漏洞可能源于软件开发过程中的疏忽，或者未及时更新补丁。攻击者一旦发现这些漏洞，便可能利用它们获取系统权限，进而控制工控网络设备，篡改生产数据或破坏系统功能。而且，随着系统复杂性的增加，漏洞的发现和修复难度也在增大。同时，不同系统之间的兼容性问题也可能引发安全漏洞，给火电厂工控网络信息安全带来潜在风险。

2.4 应用安全威胁

火电厂工控网络应用广泛，涵盖生产管理、设备监控等多个领域，但也面临着诸多安全威胁。Web 应用是

常见攻击目标，攻击者可利用 SQL 注入、跨站脚本攻击等手段，窃取用户信息或篡改应用数据。移动应用的普及也带来了新的风险，如恶意应用可能窃取工控网络敏感信息。此外，应用开发过程中的安全编码规范执行不到位，可能导致应用存在安全缺陷，为攻击者提供可乘之机，影响火电厂工控网络应用的正常运行和数据安全。

2.5 管理安全威胁

管理方面的漏洞是火电厂工控网络信息安全的重要威胁源。人员安全意识淡薄是一大问题，员工可能因疏忽泄露账号密码、随意点击不明链接，导致工控网络被入侵。信息安全管理制度不完善，如权限管理混乱，员工可能拥有超出其工作需要的系统权限，增加了信息泄露风险。同时，缺乏有效的安全审计和监督机制，难以及时发现和处理安全事件[2]。

3 火电厂工控网络信息安全策略

3.1 加强物理安全防护

3.1.1 设备与环境安全

为保障设备与环境安全，火电厂应将机房选址在干燥、通风且远离强电磁干扰的区域。机房内配备精密空调，精准调控温湿度，防止设备因环境不适而损坏。安装防静电地板，避免静电对电子设备造成损害。同时，配置不间断电源（UPS），确保在突发停电时设备能持续运行一段时间，防止数据丢失。此外，安装烟雾报警和灭火系统，及时发现并扑灭火灾，全方位保护工控网络设备免受环境因素影响。

3.1.2 设备防盗防毁

在设备防盗防毁方面，火电厂要采取多重防护措施。机房应安装坚固的防盗门和防盗窗，设置门禁系统，只有授权人员凭有效证件或指纹、面部识别等方式才能进入。对重要设备，如服务器、交换机等，使用专用机柜并加锁，防止设备被随意搬动或破坏。在机房内外安装高清监控摄像头，实现24小时实时监控，记录人员活动情况。并且，安排专人定期巡查机房，检查设备状态，及时发现并处理异常情况，确保设备安全。

3.2 构建网络防护体系

3.2.1 防火墙技术

防火墙是火电厂工控网络的第一道安全屏障。它依据预设的安全策略，对进出工控网络的网络流量进行严格审查和控制。通过过滤数据包的源地址、目的地址、端口号等信息，阻止非法访问请求进入工控网络，同时限制工控网络用户对外部不安全网络的随意访问。例如，可禁止工控网络生产控制系统访问外部娱乐网站，防止恶意软件入侵。防火墙还能记录网络访问日志，为安全审计和事件追踪提供依据，有效保障工控网络与外部网络之间的安全隔离。

3.2.2 入侵检测系统

入侵检测系统（IDS）是火电厂工控网络安全的“警卫员”。它实时监测网络流量和系统活动，通过分析网络数据包、系统日志等信息，识别潜在的入侵行为和异常活动。一旦检测到可疑行为，如端口扫描、异常登录等，IDS会立即发出警报，通知安全管理人员及时处理。与防火墙的被动防御不同，IDS 主动监测入侵迹象，能够及时发现未知的攻击手段，为工控网络安全提供更全面的保护，有效降低安全风险。

3.2.3 划分网络安全域

根据火电厂工控网络的业务功能和安全需求，合理划分网络安全域是构建防护体系的重要环节。将不同安全级别的系统和设备划分到不同的安全域中，如将生产控制大区与管理信息大区严格隔离。各安全域之间设置访问控制策略，限制域间的非法访问和数据流动。例如，禁止管理信息大区的普通办公设备直接访问生产控制大区的核心控制系统。

3.2.4 网络流量监控

网络流量监控对于火电厂工控网络安全意义重大。通过对网络流量的实时采集和分析，可以掌握网络的运行状态和使用情况。及时发现异常流量，如流量突增、异常协议通信等，这些可能是网络攻击或设备故障的迹象。例如，若检测到某台设备向外部大量发送数据，可能存在数据泄露风险。网络流量监控还能帮助优化网络带宽分配，确保关键业务的网络性能。

3.3 提升系统安全防护能力

3.3.1 系统漏洞扫描与修复

系统漏洞是火电厂工控网络安全的重大隐患，黑客常利用这些漏洞入侵系统。定期开展系统漏洞扫描工作十分必要，借助专业的漏洞扫描工具，对操作系统、数据库、应用程序等进行全面检测，精准定位存在的安全漏洞。扫描完成后，依据漏洞的严重程度和影响范围，制定详细的修复计划。及时安装官方发布的补丁程序，对无法立即修复的漏洞，采取临时防护措施，如限制访问权限、加强监控等，降低被攻击的风险，保障系统安全稳定运行。

3.3.2 主机安全加固

主机作为火电厂工控网络的关键节点，其安全性直接影响整个网络。主机安全加固从多个方面入手，首先是操作系统加固，关闭不必要的服务和端口，减少攻击面；设置强密码策略，防止密码被破解。其次，对主机

上的应用程序进行安全配置，限制其权限，避免应用程序滥用系统资源或泄露敏感信息。此外，安装主机防火墙和入侵防御软件，实时监测和阻止恶意攻击。通过这些措施，增强主机的安全性和抗攻击能力，为工控网络安全提供坚实保障。

3.3.3 系统日志监控

系统日志记录了系统运行过程中的各种事件和操作信息，是分析系统安全状况的重要依据。建立完善的系统日志监控机制，实时收集和分析主机、网络设备等的日志数据。通过对日志的深度挖掘，及时发现异常行为，如频繁的登录失败、异常的文件访问等，这些可能是攻击者试图入侵的迹象。同时，利用日志进行安全审计，追踪事件的发生过程和责任人。定期对日志进行备份和归档，以便在需要时进行查询和分析，为系统安全防护和故障排查提供有力支持。

3.4 保障应用安全

3.4.1 Web应用安全防护

Web应用是火电厂工控网络与外部交互的重要接口，易成为攻击目标。为保障其安全，首先要进行输入验证，对用户提交的数据进行严格过滤，防止SQL注入、跨站脚本攻击（XSS）等。采用安全的编码规范开发Web应用，避免出现安全漏洞。部署Web应用防火墙（WAF），实时监测和拦截恶意请求。同时，定期对Web应用进行安全评估和渗透测试，及时发现并修复潜在的安全问题。此外，限制Web应用的访问权限，仅允许授权用户访问，降低安全风险。

3.4.2 数据加密与备份

数据是火电厂的核心资产，保障数据安全至关重要。数据加密可防止数据在传输和存储过程中被窃取或篡改。对敏感数据，如生产参数、用户信息等，采用对称加密或非对称加密算法进行加密处理，确保数据的保密性。同时，建立完善的数据备份机制，定期对重要数据进行全量或增量备份，并将备份数据存储在安全的位置，如异地数据中心。制定数据恢复预案，在数据丢失或损坏时能够快速恢复数据，减少对火电厂生产的影响，保障业务的连续性。

3.5 完善管理策略

3.5.1 健全信息安全管理制度

健全的信息安全管理制度是火电厂工控网络安全的基石。要制定涵盖网络安全、系统安全、数据安全等多方面的详细规章制度，明确各岗位在信息安全中的职责与权限。例如，规定网络设备的操作流程、数据访问的审批机制等。同时，建立制度执行监督机制，定期检查制度落实情况，对违规行为进行严肃处理。此外，随着技术发展和业务变化，及时修订和完善制度，确保其适应火电厂工控网络信息安全的新需求，为工控网络安全提供坚实的制度保障。

3.5.2 加强人员培训与管理

人员是火电厂工控网络信息安全的关键因素。加强人员培训，定期组织信息安全知识讲座、技能培训等活动，提高员工的安全意识和防范能力，使其了解常见的安全威胁及应对方法，如如何识别钓鱼邮件、正确设置密码等。同时，严格人员管理，对不同岗位人员分配合理的系统权限，避免权限滥用。实施人员离岗审计，确保其不再接触敏感信息。通过加强人员培训与管理，减少因人为疏忽或恶意行为导致的安全事件，保障工控网络信息安全。

3.5.3 建立应急响应机制

建立应急响应机制是火电厂工控网络应对安全事件的重要保障。制定完善的应急预案，明确在遭遇网络攻击、系统故障等安全事件时的处理流程和责任分工。成立应急响应团队，定期进行应急演练，提高团队的应急处理能力和协同配合能力。同时，储备必要的应急资源，如备用设备、数据备份等。一旦发生安全事件，能够迅速启动应急预案，及时采取措施控制事态发展，减少损失，并尽快恢复工控网络正常运行，确保火电厂生产不受严重影响[3]。

结束语

火电厂工控网络信息安全策略的制定与实施是一项长期且复杂的系统工程，关乎电力生产的安全稳定运行。本文从物理安全、网络防护、系统安全、应用安全以及管理策略等多个层面进行了浅析，各层面相互关联、缺一不可。在未来，随着信息技术的飞速发展和网络攻击手段的不断演变，火电厂工控网络信息安全面临着更为严峻的挑战。因此，需持续关注安全动态，不断优化和完善安全策略，加强技术创新与人才培养，构建全方位、多层次、动态化的信息安全防护体系，为火电厂的可持续发展提供坚实可靠的信息安全保障。

参考文献

[1]刘海波.水电厂电力监控系统安全防护策略浅析[J].四川水力发电,2021（a02）：66-67.

[2]明婧薇.计算机网络信息安全及其防护对策[J].电子技术与软件工程,2021（3）：209-209.

[3]李亚军.火电厂集控运行技术的相关问题分析[J].中国高新技术企业，2021，No.31233：112-114.