电气自动化系统网络安全风险评估与防护机制研究

师　睿
中铝宁夏银星发电有限责任公司　宁夏　银川　750001

摘　要：本文旨在系统性地分析电气自动化系统所面临的网络安全风险，构建适用于该领域的风险评估模型，并在此基础上提出一套多层次、纵深防御的综合防护机制。文章首先梳理了电气自动化系统的典型架构与安全脆弱点，继而深入剖析了当前主流的网络攻击手段及其潜在影响；随后，结合IEC62443等国际标准，设计了一套融合资产识别、威胁建模、脆弱性分析与风险量化计算的风险评估框架；最后，从物理层、网络层、主机层、应用层及管理策略五个维度，提出了涵盖边界防护、访问控制、入侵检测、安全审计、应急响应等在内的综合防护体系。研究表明，唯有通过科学的风险评估与系统化的安全防护机制协同作用，才能有效保障电气自动化系统的安全稳定运行，支撑国家关键信息基础设施的安全战略。

关键词：电气自动化系统；网络安全；风险评估；防护机制；IEC62443；纵深防御

引言

电气自动化系统广泛应用于电力、石油化工、轨道交通、智能制造等国家关键基础设施领域，负责对生产过程进行监测、控制与优化。传统上，这些系统多采用封闭的专用网络（如现场总线），与外部互联网物理隔离，其安全性主要依赖于“隐匿即安全”（SecuritythroughObscurity）的理念。然而，随着信息技术（IT）与运营技术（OT）的深度融合，以及云计算、大数据、物联网（IIoT）等新技术的引入，电气自动化系统正经历一场深刻的网络化变革。这种变革打破了原有的物理隔离壁垒，使得OT网络暴露于更广阔的网络空间中。近年来，针对工业控制系统的网络攻击事件频发，电气自动化系统一旦被攻破，不仅会造成巨大的经济损失，更可能引发严重的社会公共安全危机乃至国家安全威胁。因此，对电气自动化系统进行科学、全面的网络安全风险评估，并构建行之有效的防护机制，已成为保障国家关键信息基础设施安全的当务之急。

1 电气自动化系统安全脆弱性分析

电气自动化系统安全脆弱性源于独特技术特性与历史发展路径。协议层面，大量工业协议如Modbus/TCP、DNP3设计时未考虑安全，缺认证、授权和加密机制，易遭解析、篡改与重放攻击。设备方面，PLC、HMI、SCADA服务器等核心设备操作系统和应用软件有已知或未知漏洞，厂商因顾虑生产连续性补丁更新滞后，设备长期处于风险中。默认配置与弱口令问题突出，许多设备出厂预设通用登录凭证且未及时修改，为攻击者提供入口。IT/OT网络融合使OT网络边界模糊，传统IT安全策略难直接套用，OT侧又缺有效防护[1]。OT运维人员工程背景深厚但网络安全知识有限，易成社会工程学攻击目标。此外，OT网络普遍缺安全监控与审计能力，攻击行为难被及时发现追溯。

2 网络安全风险评估模型构建

针对上述脆弱性，本文借鉴IEC62443系列标准的核心思想，构建一个四阶段的动态风险评估模型。

2.1 资产识别与分类

风险评估的逻辑起点是对保护对象的清晰界定。在电气自动化系统中，资产不仅包括有形的硬件设备，如PLC、交换机和服务器，也涵盖无形的软件系统、组态数据、工艺参数以及承载这些信息的通信链路。全面的资产识别要求对系统进行地毯式清查，形成一份详尽的资产清单。在此基础上，必须依据资产在生产流程中的角色、失效后对业务连续性的影响程度以及所处理数据的敏感度，对其进行科学的分类与分级。例如，负责核心工艺控制的主控PLC和存储历史运行数据的SCADA服务器，因其一旦受损将直接导致生产线停摆或关键数据泄露，应被归类为高关键性资产；而普通的温度传感器或非核心区域的操作员工作站，则可视为一般资产。这种精细化的资产画像，是后续精准评估威胁与脆弱性、合理分配安全资源的前提。

2.2 威胁建模

在明确资产之后，需要系统性地思考“谁会攻击我们”以及“他们会如何攻击”。威胁建模是一个结构化的过程，旨在识别潜在的威胁源及其可能采取的攻击向量。在电气自动化系统的语境下，威胁源呈现出多元化特征。外部攻击者，如国家级黑客组织或有组织的犯罪团伙，通常具备强大的技术能力和资源，倾向于发起高

隐蔽性、高破坏性的定向攻击，其目标可能是窃取工业秘密或瘫痪关键基础设施。内部威胁则源于组织内部，可能是因不满而蓄意破坏的员工，或是被外部势力收买的内鬼，他们利用合法的身份和权限，能够绕过许多外围防御。供应链攻击作为一种新兴且极具隐蔽性的威胁，通过在软硬件的生产、分发环节植入后门，使得攻击在系统部署之初就已埋下伏笔。此外，非恶意的意外事故，如工程师的误操作或自然灾害引发的设备故障，同样会对系统安全构成实质性威胁。通过运用STRIDE等成熟的威胁分类框架，可以将这些抽象的威胁场景具体化，为后续的脆弱性分析提供明确的靶向。

2.3 脆弱性分析

脆弱性分析是连接威胁与资产的关键桥梁，其核心任务是找出系统中可能被威胁源利用的弱点。这一过程不能仅依赖于理论推演，而必须结合主动探测与被动核查。一方面，可以借助Nessus、OpenVAS等自动化漏洞扫描工具，对网络中的开放端口、运行服务及已知的CVE漏洞进行高效筛查，快速定位显性风险[2]。另一方面，对于工业协议特有的逻辑漏洞或深层次的配置缺陷，则需要经验丰富的安全专家进行手动渗透测试，模拟真实攻击者的行为模式，对系统进行深度的压力测试。同时，对设备的安全配置基线进行严格核查也至关重要，确保诸如默认口令、冗余服务等低级错误已被消除。这种多维度、动静结合的脆弱性分析方法，能够全面揭示系统的真实安全状况，避免评估结果流于表面。

2.4 风险量化与评估

风险量化是将定性的安全问题转化为可度量、可比较的数值，从而为决策提供客观依据。本文采用风险值（R）等于威胁可能性（L）与业务影响（I）乘积的基本模型。其中，威胁可能性需综合考虑威胁源的动机、能力和攻击路径的可达性；业务影响则必须超越传统的信息安全三要素（CIA），将其置于工业生产的具体场景中进行考量。具体而言，业务影响应从四个维度展开：一是安全性，即攻击是否可能导致人身伤亡或重大环境污染；二是可用性，即攻击是否会造成生产线长时间中断，带来巨大经济损失；三是完整性，即攻击是否能篡改控制指令或工艺参数，导致产品质量不合格甚至设备损毁；四是保密性，即攻击是否会导致核心工艺配方、客户数据等敏感信息泄露。通过对这些维度进行加权评分，最终得出每个风险项的综合风险值，并据此划分高、中、低风险等级，为后续防护措施的优先级排序和资源投入提供清晰的路线图。

3 综合防护机制设计

基于风险评估的结果，本文提出一个“纵深防御”（Defense-in-Depth）理念下的五层综合防护体系。

3.1 物理与环境安全层

任何网络安全体系都必须建立在坚实的物理安全基础之上。对于电气自动化系统而言，确保只有经过授权的人员才能物理接触核心控制设备是第一道也是不可逾越的防线。这意味着需要对控制室、机房、配电柜等关键物理区域实施严格的门禁控制，辅以全天候的视频监控和入侵报警系统，形成有效的威慑与追溯能力。同时，物理环境本身的安全同样重要，必须部署完善的环境监控系统，对温湿度、烟雾、水浸、供电稳定性等关键指标进行实时监测，以预防火灾、水灾或断电等意外事件对设备造成的物理损害[3]。此外，对于退役或报废的设备，必须执行严格的数据销毁流程，通过专业的数据擦除工具或物理粉碎手段，彻底清除其存储介质上的所有敏感信息，防止数据通过二手市场或垃圾回收渠道泄露。

3.2 网络边界与通信安全层

清晰的网络边界是实现有效隔离与管控的前提。面对IT/OT融合带来的边界模糊化挑战，必须重新定义并强化网络分区策略。应将整个自动化网络按照功能和安全等级划分为多个独立的安全域，例如严格隔离的OT控制域、用于数据汇聚的监控域以及与外部交互的DMZ隔离区。在各安全域之间，部署具备深度包检测（DPI）能力的工业防火墙是至关重要的。这类防火墙不仅能识别常规的IP/端口信息，更能深度解析Modbus、DNP3、IEC61850等工业协议的内容，基于白名单策略精确控制哪些设备可以在何时发送何种类型的指令，从而从根本上阻断非法的横向移动和恶意指令注入[4]。对于必须跨越边界的通信，特别是远程维护通道，必须强制启用VPN或TLS/SSL等强加密技术，确保数据在传输过程中的机密性与完整性。长远来看，应积极推动OPCUAoverTLS等新一代安全工业协议的应用，从通信协议栈的底层筑牢安全根基。

3.3 主机与设备安全层

网络中的每一台主机和设备都是潜在的攻击入口，因此必须对其进行全方位的安全加固。首要任务是推行统一的安全基线配置策略，关闭所有非必要的网络服务和端口，修改所有默认账户的用户名和密码，并设置符合复杂度要求的强密码策略及账户锁定机制。在此基础上，必须建立一套适应OT环境特殊性的漏洞与补丁管理流程。该流程强调在不影响生产连续性的前提下，通过搭建离线测试环境对补丁进行充分验证后，再择机进行

滚动更新，以平衡安全与稳定的需求。对于工程师站、HMI、SCADA服务器等关键主机，应部署轻量级的主机入侵防御系统（HIPS），持续监控文件系统、关键进程和系统注册表的完整性，一旦发现异常变更立即告警。未来，随着技术的发展，为PLC、IED等嵌入式设备引入基于数字证书的身份认证机制，将成为防止非法设备接入网络的有效手段。

3.4 应用与数据安全层

上层应用和核心数据是攻击者的终极目标，其防护策略应围绕最小权限原则展开。系统必须为不同角色的用户（如普通操作员、高级工程师、系统管理员）精确分配其完成工作所必需的最小操作权限，杜绝权限滥用。对于所有涉及远程访问或特权操作的场景，必须强制实施双因素认证（2FA），大幅提升账户被盗用的难度。在应用开发层面，无论是采购的商业软件还是自主开发的定制化系统，都应遵循安全开发生命周期（SDL）的理念，在需求、设计、编码、测试等各个环节融入安全考量，主动防范SQL注入、跨站脚本（XSS）等常见Web应用漏洞。此外，数据是系统的血液，必须建立完善的数据备份与灾难恢复机制。关键的组态文件、历史数据库和系统镜像应定期进行离线备份，并将备份介质存放在安全的异地位置。同时，必须制定详尽且可操作的灾难恢复预案，并通过定期演练来检验其有效性，确保在遭遇勒索软件等极端攻击后能够快速恢复业务。

3.5 安全管理与运营层

再先进的技术防护措施，若缺乏健全的管理体系支撑，也终将形同虚设。因此，必须将安全管理与技术防护置于同等重要的地位。首先，应制定一套覆盖全面、责任清晰的网络安全管理制度、操作规程和应急预案，并通过培训和考核确保每一位员工都理解并遵守。其次，持续的安全意识教育是抵御社会工程学攻击的关键。应定期组织针对OT和IT人员的专项培训，通过案例分析、模拟钓鱼等方式，不断提升全员的安全素养和警惕性。在技术运营层面，部署工业网络流量分析（NTA）和安全信息与事件管理（SIEM）系统，对全网的日志和流量进行7×24小时的集中监控与关联分析，是实现主动防御的核心。通过建立基于正常业务行为的基线模型，可以有效识别出偏离常态的异常活动，实现对攻击的早期预警。最后，必须组建一支专业的网络安全应急响应团队（CSIRT），明确从事件发现、上报、分析、遏制、根除到恢复的标准化流程，并通过定期的红蓝对抗演练，不断检验和优化整个防护体系的实战能力。

4 结语

电气自动化系统网络安全是复杂系统工程，单一技术或产品难彻底解决。本文构建闭环风险评估模型，设计覆盖五层面的纵深防御机制，为关键基础设施提供系统性保障。未来研究方向多元关键：借助AI驱动主动防御，构建精准异常检测和攻击预测模型，实现从被动到主动的转变；探索零信任架构在OT环境的应用；推动内生安全与可信计算，在核心设备集成可信模块；持续完善相关标准，形成统一行业安全基线和测评认证体系。

参考文献

[1]徐馨怡.电气工程自动化控制系统的网络安全防护策略[C]//《中国建筑金属结构》杂志社有限公司.2024新质生产力视域下智慧建筑与经济发展论坛论文集（五）.盘锦城建设计院有限公司;,2024:89-90.

[2]袁任智.电力系统及其自动化技术安全控制问题研究[J].城市建筑空间,2024,31(S2):410-411.

[3]吴沁,杨靖.基于电气工程的通信网络物理层安全强化研究[J].中国宽带,2024,20(08):88-90.

[4]钱小波.电气工程在智能电网中的应用与发展[C]//中国智慧工程研究会.2024智慧施工与规划设计学术交流会论文集.杭州凯达电力建设有限公司;,2024:209-211.