

电力监控系统安全防护的风险评估与应对策略

——评《电力监控系统网络安全攻防演练平台建设与应用》

电力监控系统是电力网络的“中枢神经”，随着数字化转型深化，网络攻击、设备漏洞等新型威胁叠加，电力监控系统面临数据泄露、功能失控等风险。开展科学的风险评估与针对性应对，既是筑牢电力安全防线的关键，更是保障经济社会正常运转的必然要求。

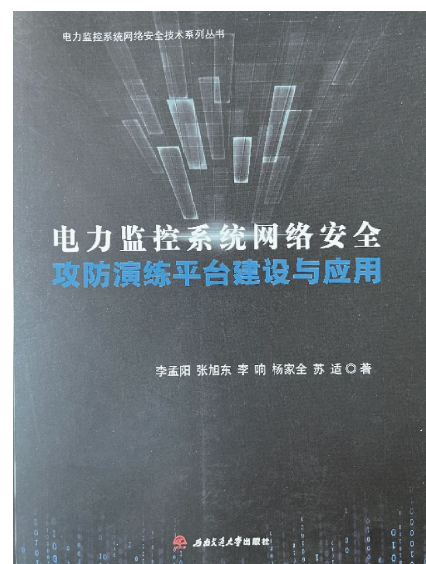
《电力监控系统网络安全攻防演练平台建设与应用》一书以电力监控系统网络安全防护需求为核心，系统构建了全方位攻防演练平台技术体系。就全书内容而言，该书开篇分析国内外网络空间靶场建设概况，指出电力行业因系统复杂度高、设备异构性强、业务连续性要求严苛等特性，靶场建设面临场景构建难、成本控制难、内容运营难3大核心挑战，并提出通过原生网络靶场专用引擎与数字孪生技术实现“虚实结合”仿真的解决方案。在全书技术实现层面，书中详细阐述了多维度平台搭建方法：①基于 Docker 容器技术构建本地化漏洞环境时，采用多安全域划分与两级防火墙数据采集通道设计，解决传统方案隔离性差的问题；②通过模拟虚拟环境——下一代网络仿真平台实现复杂电力网络拓扑复现，支持思科、华为等多厂商设备模拟，满足电力监控系统多协议交互需求；③针对传输控制协议/网际协议栈安全缺陷，重点解析网络层 ARP 欺骗、传输层 SYN Flood、应用层 Modbus 协议攻击等电力系统常见威胁的防御技术；④在恶意代码分析环节，整合 Cuckoo 沙盒动态分析、Sysmon 系统监控、Process Monitor 进程监视器进程追踪及 REMnux 逆向工具包，形成多维度检测体系；⑤渗透测试部分强调 Kali Linux 子系统部署优势，实现与宿主环境无缝衔接，提升测试效率。

作者在书中提出，电力监控系统作为电力生产运行的核心神经中枢，其安全风险评估需基于系统性、动态性及专业性原则，围绕资产识别、威胁分析与脆弱性评估展开多维度研判。从网络架构维度看，系统遵循“安全分区、网络专用、横向隔离、纵向认证”原则划分为生产控制大区（安全Ⅰ、Ⅱ区）与管理信息大区（安全Ⅲ、Ⅳ区），二者间的边界隔离强度直接决定攻击面扩散风险。若网闸配置不当或逻辑隔离策略存在缺陷，攻击者可通过纵向渗透路径突破生产控制区防护，窃取数据采集与监控系统核心控制指令。设备层风险聚焦于可编程逻辑控制器、远程终端单元等工控设备，其固件更新滞后、弱口令配置普遍、协议兼容性缺陷等问题，易成为勒索病毒或高级长期威胁攻击的植入点。风险评估方法需融合定性分析与定量技术：定性层面，依据《电力监控系统安全防护评估指南》（GB/T 35580）通过文档审查、现场勘查识别安全策略缺陷，如权限分配过度、日志审计机制缺失、跨区威胁监测空白；定量层面，采用 Nessus、OpenVAS 等漏洞扫描工具对设备进行 CVE 漏洞匹配，结合渗透测试模拟攻击路径，量化风险等级。

笔者认为，安全风险需构建“技术-管理-人员”三位一体的纵深防御体系，实现从被动防御到主动防御的转型。①技术层面，首先，强化网络分段与边界防护。在Ⅰ/Ⅱ区与Ⅲ/Ⅳ区交界处部署电力专用正向隔离网闸，实施 MAC/IP 绑定、端口安全及协议白名单机制，阻断非法跨区访问；对生产控制区内部，采用工业以太网交换机划分虚拟局域网，限制广播域范围，降低横向渗透风险。其次，提升终端安全韧性。基于国产密码算法加密关键控制指令，对可编程控制器、远动终端设备实施固件签名验证，防止恶意代码注入；针对勒索病毒，采用行为检测技术（如异常进程监控、文件加密行为识别）与沙箱隔离，实现未知威胁的主动防御。②管理层面，首先，建立动态风险评估与闭环整改机制。依据《关键信息基础设施安全保护条例》，制定涵盖资产全生命周期管理、脆弱性评估、事件响应的安全策略，明确各部门安全职责；其次，引入 ISO 27001 信息安全管理体系，每季度开展第三方渗透测试，将漏洞修复率、安全事件处置时效纳入部门关键绩效指标考核，形成“评估-整改-复查”的闭环管理。③人员层面，首先，强化安全意识与能力建设。对运维人员开展工控安全专项培训，涵盖协议分析、漏洞识别、应急处置等内容，并通过注册信息安全专业人员-工业控制系统认证提升专业能力；其次，对第三方人员，实施“最小权限”原则，严格审批访问权限，部署堡垒机实现操作行为全记录与审计，防止内部威胁。

总之，电力监控系统网络安全事关国家能源安全与经济社会稳定，需基于科学风险评估构建主动动态防御体系，并结合智能技术为电力系统提供坚实安全支撑。

（路明/国网辽宁省电力有限公司/副高级工程师）



书名: 电力监控系统网络安全攻防演练平台建设与应用

作者: 李孟阳, 张旭东, 李响, 杨家全, 苏适

出版社: 西南交通大学出版社

ISBN: 9787564384708

出版时间: 2021年12月

定价: 49元