基于 SCD 文件的资产测绘及网络安全分析的研究

王琪，张丽霞，魏真艳，徐明，齐国利，邵季飞，董泉，梁向阳
国网河南省电力公司超高压公司，河南 郑州 450000

摘　　要： 随着近年来中国网络建设和信息化建设速度的加快，企业、政府机关等组织的业务和信息化的结合越来越紧密，业务信息化在给组织带来巨大经济和社会效益的同时，也给组织的信息安全和管理带来了严峻的挑战。本文通过基于 SCD 文件的资产测绘及网络安全分析的研究，介绍了影响电力监控网络安全的因素，阐述了变电站自动化运维在电网中的重要意义，并分析了站控层和间隔层设备的网络安全管理的内容与方法，以及为推进基于调控云的电力监控系统网络安全漏洞库建设，完成电力监控系统漏洞信息收集和共享机制的建立，提升安全漏洞整体闭环消缺管控能力提供支撑。

关 键 词： SCD；网络安全；电力监控；安全防护

Research On Asset Mapping And Network Security Analysis Based On SCD File

Wang Qi, Zhang Lixia, Wei Zhenyan, Xu Ming, Qi Guoli, Shao Jifei, Dong Quan, Liang Xiangyang
State Grid Henan Electric Power Company Ultra-High Voltage Company, Henan, Zhengzhou 450000

Abstract: With the acceleration of China's network construction and information construction in recent years, the combination of business and information technology in enterprises, government agencies and other organizations is getting closer and closer. Business information not only brings huge economic and social benefits to the organization, but also brings severe challenges to the organization's information security and management. Through the research of asset mapping and network security analysis based on SCD file, this paper introduces the factors that affect the network security of power monitoring, expounds the significance of substation automation operation and maintenance in the power grid, analyzes the content and methods of network security management of station control layer and interval layer equipment, and promotes the construction of network security vulnerability database of power monitoring system based on regulation cloud. Complete the establishment of the power monitoring system vulnerability information collection and sharing mechanism, and improve the overall closed-loop security vulnerability elimination control ability to provide support.

Keywords: SCD; network security; power monitoring; safety protection

前言

随着智能站的大量投运，站内设备越来越多，不同品牌、不同型号，不同装置各自发挥着作用，目前公司对于变电站端二次设备资产，如站控层设备、特别是间隔层设备的管理比较模糊，无相关识别技术，只是依靠 SCD 文件进行维护，但是在检修等更换工作时不能及时进行更新；同时对于近几年来网络安全技术的发展，智能化程度越高、网络安全风险越大，一旦变电站发生网络安全事件将造成不可估量的后果。

信息安全由于其专业性，组织信息安全管理人员在数量和技能上的缺乏给全网的安全管理带来了很大的难度；而且网络攻击技术更新很快，往往会在短时间内造成巨大的破坏，互联网的传播使黑客技术具有更大的普及性和破坏性，会给组织造成很大的威胁。基于上述原因，通过基于 SCD 文件的资产测绘及网络安全分析的研究，将有效的解决站控及间隔层二次设备维护管理的误操作及网络安全攻击带来的非法外联等安全风险。全面提升站控层及间隔层二次设备的准确识别及网络安全风险管理，降低网络安全攻击的可能性，提高变电站端网络安全防护水平。

一、基于 SCD 文件的资产测绘及网络安全分析平台的研究

变电站设备信息和智能电子设备（IED）以及它们之间的连接关系均保存于智能变电站配置描述文件 SCD 之内，但保存于 SCD 文件内并不能实时感知资产变更情况，无法对资产情况进行可视化展示和统一运维，同时为了加强威胁对抗能力、升维打击高级威胁、健全调查机制、提高安全防护的网络安全建设需求，构建

作者信息：王琪（1991.09-），男，汉族，籍贯：河南商丘，工程师，学历：硕士研究生，主要研究方向：继电保护及电网调度自动化

网络安全智能运维平台和安全风险检测探针组成的网络安全风险系统，在SCD文件的基础上对资产进行统一的梳理，扫描可能存在的漏洞并对站控及间隔层二次设备实时监控[1]。

利用安全风险检测探针对SCD文件内保存的设备信息及Inputs节点属性进行分析，能够确定与之相连的IED设备的同时可对此连接收、发的GOOSE、SV信息及个数进行获取。在此基础上对不同网络段的设备再进行主动探测，盘点资产数据并整理输出至网络安全智能运维平台。

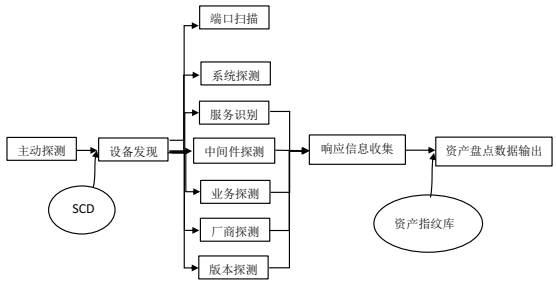

图1 资产盘点流程

二、平台总体架构及功能设计的研究

整体架构由网络安全智能运维平台和安全风险检测探针共同组成，分为数据采集、数据存储、安全分析和业务展示四大层，不同层次对应不同功能模块。探针由资产管理模块、安全检测模块、漏洞验证模块和专项服务模块四大部分组成。主要负责扫描范围内所有资产信息、安全漏洞信息，将采集信息同步到网络安全智能运维平台，也可将网络安全智能运维平台下发的安全策略同步到站内设备。

平台由资产管理、漏洞管理、检测管理、情报管理、安全通报、风险处置、对比分析等业务模块组成。形成安全风险监测、安全运营管理两大体系。实现三个核心管理目标：动态资产核查及异常监控、多维资产脆弱性风险评估、全流程安全风险闭环管理[2]。平台可同时由多台探针做收集数据进行联动，也可进行离线检测后数据导入。

三、网络安全智能运维管控平台核心技术的研究

（1）防火墙全局策略自动化分析及智能管控

网络安全智能运维平台结合装置获取边界防火墙的基本信息，再根据防火墙的基本信息构建对应防火墙的通信策略，获取防火墙的配置信息，策略信息，平台结合其他边界设备信息，综合评估当前防火墙配置是否合理，边界安全状态是否被破坏。

平台通过深度学习引擎对防火墙策略自学习，聚合收敛优化相关策略；同时平台通过装置实时获取防火墙流量数据，结合防火墙策略，分析现网通信状态生成相关策略建议，帮助客户进行决策。平台通过对边界防火墙策略的历史分析和防火墙流量的实时分析，实现了对防火墙的智能管控。

（2）远程安全加固

网络安全智能运维平台通过本体安全检测装置搭建远程加密通道，向目标主机发送加固程序，在平台上输入目标主机账号密码后，平台通过国密加密通道将信息发送至装置，装置解码后访问目标主机，并执行加固操作[3]。

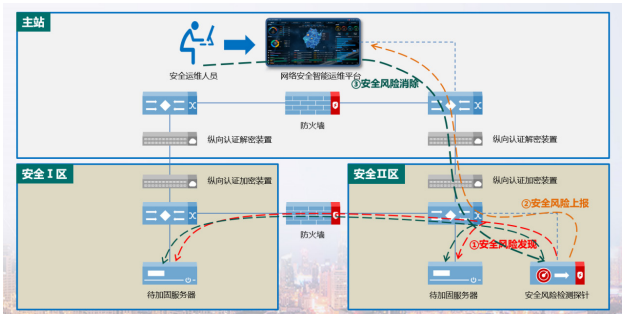

图2 远程安全加固流程示意图

常规状态下由安全风险监测探针实时监测设备情况，发现异常行为后将监测结果通过加密隧道上传至平台，平台根据策略进行分析或提出告警，通过自动化或半自动化的方式完成远程安全加固。

（3）以安全风险为中心的漏洞评估机制

通过站内综合资产全部情报，深度分析资产安全状态，结合资产的物理情况、端口、服务等多维安全情况对漏洞进行全面的风险评估，并提供切实有效的安全决策建议。针对部分高危风险，还可同时通过采用内置的特种漏洞POC，模拟网络中的漏洞环境，将漏洞复现流程代码化，通过模拟攻击技术的手段实现自动化漏洞验证，并通过动态分析技术，分析大量样本进行漏洞自动化验证时所需的方法，根据当前环境进行自动化渗透测试，直观展示脆弱性带来的危害及影响。

（4）多元异构检测引擎融合技术

针对站内可能存在的各类安全风险，单一的检测手段必然无法检出所有的内网威胁，因此利用多元异构检测引擎融合技术来提高网络安全威胁的检出率，同时利用大数据技术进行关联、分析、建模等，通过海量数据深度学习，进而迅速提升安全大数据分析系统在网络中的适应能力。针对安全分析方面，将数据分层过滤、深度挖掘，通过对资产信息、检测结果、边界策略等进行全量的分析后，最后再进行整体评估[3]。针对安全处置方面，将各类风险情报进行整合后，形成整体安全处置方案，提供多种手段进行加固处置。针对安全恢复方面，提供多种手段进行风险复核，通过定期和人工的核查，反复查验网络空间状态，校验网络安全恢复状态。

（5）漏洞全生命周期管理

持续性对电力行业漏洞进行挖掘、跟踪及情报收集工作，并针对涉及漏洞的变电站系统进行专项安全检测，自动对漏洞的真实性进行判断，智能下发安全整改通知单及针对性修复建议，组织安全运营团队进行漏洞修复工作。

对部分高危漏洞提供手工、半自动化、自动化等验证方式[4]。自动化验证结合人工渗透测试的技术和经验，平台自动对漏洞进行验证、判断；手工、半自动化验证平台提供对应的漏洞验证工具以及工具使用方法。

常规情况而言，部分漏洞是确实存在但又确实是无法被利用

的，因此这些漏洞的扫描是无意义的[5]。模拟人工渗透漏洞验证和漏洞知识库集成了大量的 POC、Exploit 等用以验证漏洞能否被利用的代码。同时采用内置的特种漏洞 POC，模拟网络中的漏洞环境 ，将漏洞复现流程代码化，通过模拟攻击技术的手段实现自动化漏洞验证，并通过动态分析技术，分析大量样本进行漏洞自动化验证时所需的方法，根据当前环境进行自动化渗透测试。同时模拟人工渗透漏洞验证和漏洞知识库中还集成了大量漏洞修复建议，以便于输出漏洞修复建议。

（6）基于国密算法 + 电力调度数字证书的安全架构设计

平台和装置采用国密加密算法，在平台侧完成全部传输数据加密，通过电力调度数字证书认证后，通过加密通道将数据发送到装置，再由装置侧进行数据解密，并执行加固操作。平台对于用户键入的账号密码在数据处理过程中不进行任何存储，数据不落盘，用完即销毁，确保数据不泄露。

平台加固包由管理员严格审核，确保加固程序无误后，再由使用人通过平台进行远程加固。加固包除超级管理员外其他任何用户不具有任何修改权限，且使用人在加固前可反复校验加固包状态，防止加固包被恶意篡改和替换。

四、当前部署情况

安全风险检测探针部署在地调、县调和变电站用于识别和校验变电站的安全风险隐患，并上传数据至管控平台；网络安全智能运维平台部署在主站，对数据进行存储和分析，并提供安全可视化展示。同时风险管控平台可对整个系统的不同角色用户进行权限管理。

五、网络安全分析的的重要作用

研究构建了由网络安全智能运维平台和安全风险检测探针组成的网络安全分析系统，增强了变电站的安全监测能力，针对其资产漏洞风险、违规端口、边界配置隐患、设备变更、遭受网络攻击等问题可以做到第一时间的告警和应急处置，从而避免带来更大的损失；同时利用远程加固在平台侧完成策略下发和重大事件的处置响应，当遇到类似永恒之蓝的勒索病毒需要对设备进行漏洞修复等问题时，无需再频繁下站，极大节省了人力物力和财力。

结论

通过基于 SCD 文件的资产测绘及网络安全分析的研究将有效的解决站控及间隔层二次设备维护管理的误操作及网络安全攻击带来的非法外联等安全风险。全面提升站控及间隔层二次设备的准确识别及网络安全风险管理，降低网络安全攻击的可能性，提高变电站端网络安全防护水平以及提高了变电站端站控及间隔层设备的网络安全管理水平，同时对 SCD 文件与通用安全相结合的技术进行了更加深入的研究，为变电站未来的网络安全技术提供更多的选择。

参考文献

[1]徐岩，单肆超．基于 SCD 文件的智能变电站二次回路可视化［J］．电力系统及其自动化学报．2023,35(3).

[2]张衍亮．网络空间测绘与安全评估平台的设计与实现［D］．山东大学，2023.

[3]李扬，寇祎．网络运维管理常见安全隐患分析及防范措施［J］．保密科学技术，2023,(12):11-14.

[4][1]王今，邹纯龙，马海群，等．基于零信任的公共数据平台安全指数构建研究［J］．情报科学，2023,41(08):18-24+36.DOI:10.13833/j.issn.1007-7634.2023.08.003.

[5]张媛．电力配电网自动化系统中网络安全防护有效性探究［J］．山西电力，2020,(05):31-33.