AnaTraf 应用案例 —— 电网工控网络流量分析

Application

随着“工业4.0”、“中国制造2025”等战略的推进，电网工业控制系统正加速向数字化、网络化和智能化转型。智能变电站和配电自动化系统等关键基础设施日益依赖开放的网络环境，采用通用的软硬件和通信协议（如IEC 61850、Modbus TCP等）进行数据交互。然而，传统的电网工控系统多采用物理隔离方式，主要关注系统的功能安全，缺乏对网络信息安全的考虑。因此，构建基于网络流量分析的安全防护体系，提升对电网工控系统的安全监测和防御能力，已成为当前亟需解决的问题。

面临的挑战

资产管理困难

电网工控系统中设备种类繁多，分布广泛，且部分设备老旧，缺乏统一的资产管理机制，难以及时发现和识别非法接入的设备，增加了安全管理的复杂性。

缺乏实时的异常检测机制

现有的安全防护措施多依赖于特征库，难以应对未知攻击和 0 day 漏洞，缺乏对异常行为的实时检测和预警能力，无法及时发现和响应安全事件。

解决方案

为应对上述挑战，AnaTraf 网络流量分析系统在电网工控网络中部署，构建了基于流量分析的安全防护体系，主要包括以下几个方面：

安全无忧的流量采集：在电网工控网络的关键交换机配置端口镜像，将网络流量镜像到 AnaTraf 系统进行分析，采用旁路部署方式，对现有业务系统零扰动，保障电网的正常运行。

资产识别与管理：通过对网络流量的分析，系统能够自动识别网络中的工控设备，提取设备的厂商、IP 地址、MAC 地址等信息，建立资产白名单，实时监测非法设备的接入，提升资产管理的效率和准确性。

工控协议分析：支持对工控协议（如 IEC 61850、Modbus TCP 等）的深度分析，再结合一些策略规则识别流量中的安全风险。

客户价值

保障电网的稳定运行：通过对网络流量的实时监测和异常行为快速响应，保障电网工控系统的稳定运行，避免因安全事件导致的生产中断和经济损失。

支持合规与审计要求：流量分析系统记录所有网络通信行为，提供详尽的数据和报表，支持安全事件的溯源分析和合规审计，满足监管机构的合规要求。

实现资产管理：流量分析系统识别网络中的工控设备，建立完整的资产清单，提升资产管理的效率和准确性，降低因非法设备接入带来的安全风险。