Analisador Automático de Segurança Cibernética para o Setor Elétrico

Lucas H. V. Oliveira[1], **Edmar Candeia Gurjão**[2]

[1]Curso de Engenharia Elétrica – Universidade Federal de Campina Grande (UFCG)
Caixa Postal 10.106 – 58.109-970 – Campina Grande – PB – Brazil

lucashenrique.oliveira@ee.ufcg.edu.br, ecg@dee.ufcg.edu.br

Abstract. *This article simulates the automation of vulnerability analysis and risk assessment in power sector networks, using data from IEDs to extract the communication structure of substations. Based on SCL files, in compliance with IEC 61850, critical assets are mapped and compliance with security standards and OT policies is verified.*

Resumo. *Este artigo simula a automatização da análise de vulnerabilidades e avaliação de riscos em redes do setor elétrico, utilizando dados de IEDs para extrair a estrutura de comunicação de subestações. A partir de arquivos SCL, conforme a norma IEC 61850, mapeiam-se ativos críticos e verifica-se a conformidade com normas e políticas de segurança em ambientes OT.*

1. Introdução

A crescente integração entre Tecnologia da Informação (TI) e Tecnologia Operacional (OT) conectou sistemas industriais antes isolados às redes corporativas e à internet, ampliando sua superfície de ataque. Sistemas OT utilizam hardware e software especializados para monitoramento e controle em tempo real de dispositivos físicos. Apesar de empregarem tecnologias comuns, como servidores e redes, um ataque cibernético a esses sistemas pode ter consequências imediatas e críticas, exigindo atenção especial à segurança.

Essa preocupação se agrava pela presença de equipamentos legados, com atualizações limitadas e ciclos de vida prolongados. Atualizações, quando disponíveis, tendem a ser complexas e custosas. No setor elétrico, bancos de testes e simulação são amplamente usados para detectar falhas, avaliar dispositivos de proteção e testar novas tecnologias. A simulação de redes permite replicar ambientes reais via software, facilitando a análise de segurança em condições controladas.

Este artigo discute métodos de avaliação da segurança cibernética no setor elétrico, com foco na identificação e mitigação de vulnerabilidades em Dispositivos Eletrônicos Inteligentes (IEDs), componentes essenciais da automação em subestações. As avaliações ocorrem por meio de simulações e testes de penetração, visando proteger infraestruturas críticas e garantir a resiliência operacional frente a possíveis ataques cibernéticos.

2. Visão geral IEC 61850

A IEC 61850 é uma norma internacional que padroniza a comunicação entre equipamentos de subestações, independentemente do fabricante. Ela define modelos de da-

dos orientados a objetos, serviços associados e interfaces de comunicação para Dispositivos Eletrônicos Inteligentes (IEDs), promovendo interoperabilidade em Sistemas de Automação de Subestação (SAS) [Silveira 2019], [Ayello and Lopes 2023].

Antes da padronização, cada fabricante adotava soluções próprias, dificultando a integração. Com a IEC 61850, tornou-se possível o intercâmbio de informações entre dispositivos e funções em diferentes níveis da subestação, por meio de redes locais (LAN).

A norma especifica três tipos de serviços críticos de comunicação para proteção e controle.

- **Sampled Values (SV) e Generic Object Oriented Substation Event (GOOSE)**, mapeados diretamente na camada de enlace para alta performance.
- **Generic Substation State Event (GSSE)**, possui seu próprio mapeamento personalizado.

Além disso, define o protocolo Time Sync para sincronização temporal e o Client-Server MMS para gerenciamento dos dispositivos [Konka et al. 2011]. A troca de mensagens segue o modelo publisher/subscriber, onde assinantes recebem eventos como pacotes GOOSE, SV ou GSSE. Dada a criticidade do setor elétrico, avaliações rigorosas de interoperabilidade são essenciais para a adoção segura e eficaz da norma.

3. Substation Configuration Description Language (SCL)

A IEC 61850 define a Substation Configuration Language (SCL), baseada em XML, para padronizar a descrição de dispositivos e parâmetros de comunicação em subestações, garantindo interoperabilidade entre diferentes fabricantes [Adamiak et al. 2009].A SCL organiza os dados em arquivos hierárquicos, sendo os principais:

- **SSD** (System Specification Description): descreve o diagrama unifilar, níveis de tensão e funções lógicas.
- **ICD** (IED Capability Description): detalha as capacidades de um tipo de IED.
- **SCD** (Substation Configuration Description): consolida a configuração completa da subestação, incluindo IEDs e comunicação.
- **CID** (Configured IED Description): representa um subconjunto do SCD, voltado a um IED específico.

Sua estrutura é dividida em três partes principais::

- **Subestação**: define os equipamentos primários e suas funções associadas a nós lógicos.
- **IED**: descreve os dispositivos físicos, dados e pontos de acesso.
- **Comunicação**: especifica as conexões entre IEDs por meio de sub-redes.

Além dessas três partes, um arquivo SCD (Substation Configuration Description) completo inclui uma seção de modelos de tipos de dados, que especifica os dados e atributos utilizados pelos IEDs [Carvalheira and Klien 2019].

Este trabalho utiliza a linguagem SCL para extrair a estrutura de comunicação entre IEDs e mapeá-la em ambientes simulados, como o GNS3. Essa abordagem permite avaliar vulnerabilidades e conformidades de forma automatizada, sem interferência na rede real, promovendo testes de segurança mais amplos e eficazes

4. Graphical Network Simulator 3(GNS3)

Ambientes virtuais reduzem custos e riscos ao permitir testes e ataques cibernéticos sem afetar sistemas reais. O GNS3 é uma ferramenta de código aberto para simulação de redes, capaz de criar desde topologias simples até cenários complexos [GNS3 Team 2025].

O software emula dispositivos reais por meio de máquinas virtuais, oferecendo suporte a equipamentos de diversos fornecedores, como firewalls, IDS, roteadores e contêineres Docker [Emiliano and Antunes 2015], [Alrashide et al. 2022]. Sua compatibilidade com contêineres permite a construção modular e escalável de ambientes de teste, sendo esse um dos principais motivos de sua escolha nesta pesquisa.

5. Metodologia

A avaliação de segurança foi realizada em um ambiente virtual criado no GNS3, escolhido por sua flexibilidade e capacidade de simular topologias realistas com múltiplos dispositivos de rede.

Utilizaram-se arquivos SCL, em formato XML, para obter a estrutura da rede e a comunicação entre IEDs, conforme a norma IEC 61850. Scripts em Python foram desenvolvidos para interpretar esses arquivos e gerar automaticamente a topologia no GNS3, replicando a configuração real de subestações elétricas.

Esse processo automatizado possibilitou a criação ágil do ambiente de simulação, assegurando a veracidade dos testes de segurança sobre a comunicação entre os dispositivos.

5.1. Desenvolvimento

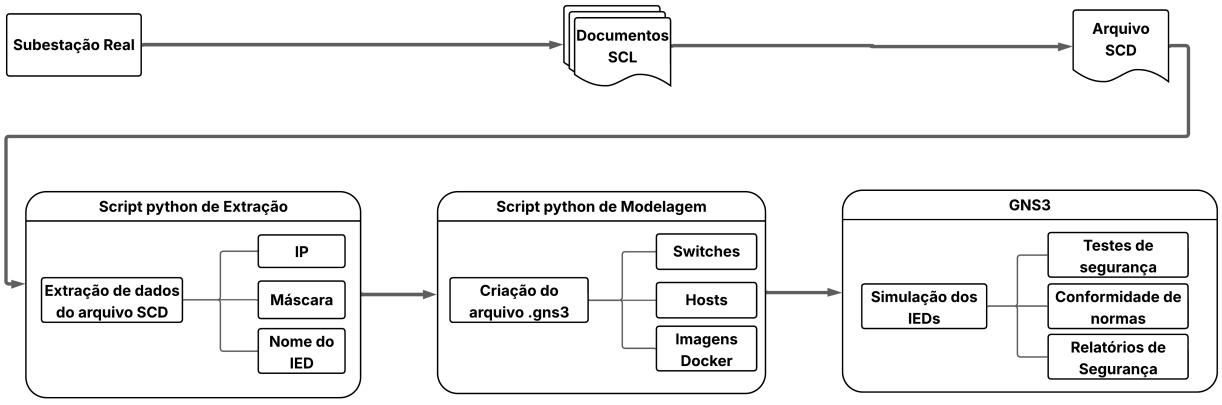

Figure 1. Fluxograma para o mapeamento dos dispositivos da subestação

O modelo de rede no GNS3 foi utilizado para analisar vulnerabilidades em subestações elétricas, com foco na obtenção automatizada da arquitetura da rede para fins de avaliação de segurança cibernética.

A Fig. 1 apresenta o fluxograma do processo, baseado na leitura de arquivos SCL conforme a norma IEC 61850. Utilizou-se especialmente o arquivo SCD, que descreve IEDs com informações como IP, máscara de rede e nome do equipamento.

Um script em Python foi desenvolvido para extrair essas configurações a partir do SCL. Com os dados obtidos, outro script gerou automaticamente o arquivo .gns3, contendo a topologia simulada com os dispositivos configurados. Por fim, a simulação no GNS3 permitiu a realização de testes de segurança, verificação de conformidade normativa e geração de relatórios técnicos.

5.2. Resultados

A criação automatizada da topologia no GNS3, com base em arquivos SCL e scripts em Python, permitiu mapear dinamicamente dispositivos de rede, como switches e IEDs, simulando uma subestação elétrica. A manipulação do arquivo .gns3 (formato JSON) viabilizou a integração com o ambiente virtual de forma eficiente.

A Fig. 2 ilustra a topologia gerada, composta por quatro switches, cinco IEDs (em containers Docker) e o ”Oráculo”, um dispositivo criado via Docker para executar testes de segurança e gerar relatórios automatizados.

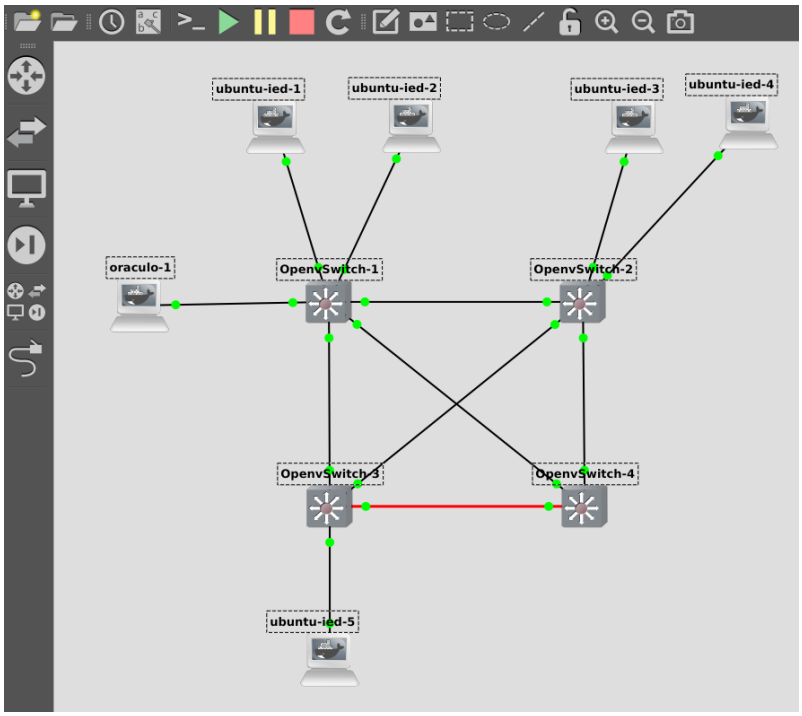

Figure 2. Topologia gerada no ambiente do GNS3

O Oráculo se comunica com os IEDs via modelo cliente-servidor, executando scripts que verificam parâmetros de segurança com base na norma IEC 62443. Foram avaliados critérios como:

Na Fig. 3 é apresentado um relátorio de confomidade de normas de um dos dispositivos IED. Inicialmente utilizou-se a Norma da IEC 62443 como referência de diretrizes para para a segurança cibernética no setor. A norma IEC 62443, é um conjunto de padrões internacionais que se concentram na segurança cibernética de sistemas de controle industrial e automação. Ela foi desenvolvida para garantir proteção de redes, sistemas e dispositivos em ambientes de automação industrial, tais como fábricas, plantas de produção, infraestrutura crítica e instalações de energia [Industrial Cyber 2021].

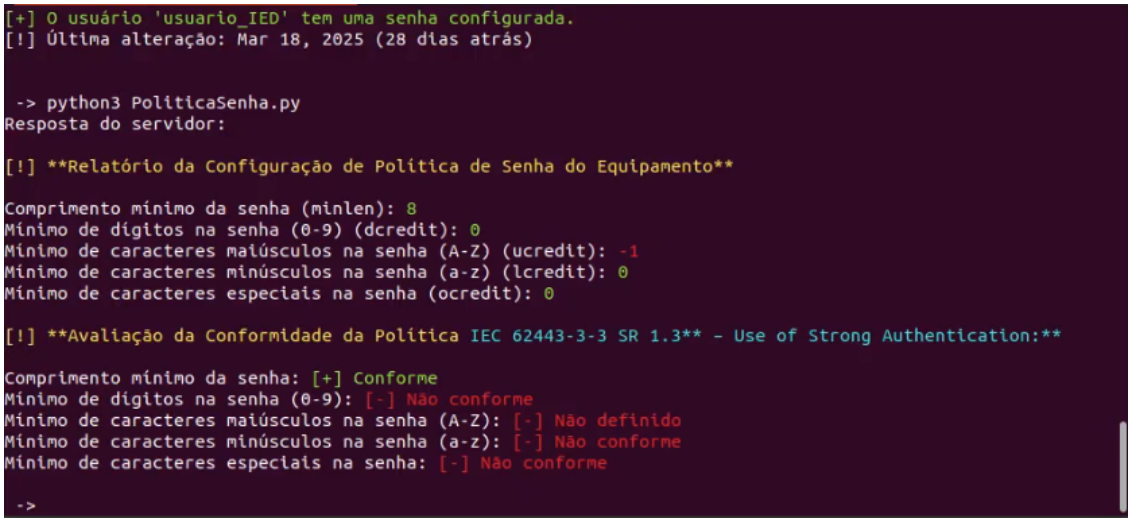

Figure 3. Testes de Conformidades de Normas em políticas de senhas

Inicialmente, foi verificado o periodo de troca de senhas dos dispositivos IED, em referência a norma IEC 62443-3-3 SR 1.7 – ”Password Lifetime Restrictions” na qual define uma troca períodica de senha a cada 90 a 180 dias e evitar o reuso das últimas cinco senhas anteriores [WISE-DeviceOn 2025].

Após isso, foi verificado a políticas de senhas usadas no equipamento IED, de acordo com a diretriz da IEC 62443-3-3 SR 1.3 – ”Use of Strong Authentication” qual verifica a complexidade da senha como o comprimento mínimo de 8 a 14 caracteres, letras maiúsculas e minúsculas, números e caracteres especiais (@, #, $, etc) [WISE-DeviceOn 2025].

6. Conclusão

Este trabalho propôs uma abordagem automatizada para avaliação da segurança cibernética em subestações elétricas, utilizando simulações no GNS3 com base em arquivos SCL da norma IEC 61850. Com o uso de scripts em Python, foi possível mapear e configurar topologias realistas, refletindo redes OT reais.

Foi também desenvolvido o “Oráculo”, um container Docker que realiza testes automatizados de segurança nos IEDs simulados, permitindo identificar vulnerabilidades e gerar relatórios de conformidade. Os resultados demonstraram a eficácia da solução na criação de cenários seguros e flexíveis para testes, destacando o potencial do GNS3, Docker e Python como ferramentas práticas para avaliação de redes críticas.

Como trabalho futuro, sugere-se expandir os testes, incluir novos tipos de ataques e validar a metodologia em ambientes reais, ampliando a aplicabilidade da solução no setor elétrico.

References

Adamiak, M., Baigent, D., and Mackiewicz, R. (2009). Iec 61850 communication networks and systems in substations: An overview for users. *The Protection Control Journal*, pages 61–68.

Alrashide, A., Abdelrahman, M., Kharchouf, I., and Mohammed, O. (2022). Gns3 communication network emulation for substation goose based protection schemes. pages 1–6.

Ayello, M. and Lopes, Y. (2023). Interoperability based on iec 61850 standard: Systematic literature review, certification method proposal, and case study. *Electric Power Systems Research*, 220:109355.

Carvalheira, E. and Klien, A. (2019). How the engineering design process can simplify the testing of automation and control systems. In *2019 72nd Conference for Protective Relay Engineers (CPRE)*, pages 1–7.

Emiliano, R. and Antunes, M. (2015). Automatic network configuration in virtualized environment using gns3. In *2015 10th International Conference on Computer Science Education (ICCSE)*, pages 25–30.

GNS3 Team (2025). Gns3 documentation. Acesso em: 30 abr. 2025.

Industrial Cyber (2021). The essential guide to the iec 62443 industrial cybersecurity standards. Acesso em: 28 abr. 2025.

Konka, J. W., Arthur, C. M., Garcia, F. J., and Atkinson, R. C. (2011). Traffic generation of iec 61850 sampled values. In *2011 IEEE First International Workshop on Smart Grid Modeling and Simulation (SGMS)*, pages 43–48.

Silveira, M. (2019). Iec 61850 network cybersecurity : Mitigating goose message vulnerabilities.

WISE-DeviceOn (2025). Cr-110 authenticator feedback sl4. Acesso em: 28 abr. 2025.