ANÁLISE DA INTEROPERABILIDADE DE IEDs INSTALADOS EM SUBESTAÇÕES ELÉTRICAS DE ESTAÇÕES DE TRATAMENTO DE ÁGUA SEGUINDO REQUISITOS DA NORMA IEC 61850

Marcio Pereira da Silva (Universidade Federal do ABC) E-mail: marcio.eng.bsb@gmail.com
Thales Sousa (Universidade Federal do ABC) E-mail: thales.sousa@ufabc.edu.br

Resumo: Um dos insumos mais importantes para a indústria do saneamento é a energia elétrica utilizada nas Estações de Tratamento de Água (ETA) e Estações de Tratamento de Esgoto (ETE). O consumo de energia é bastante grande na indústria de saneamento e o atendimento muitas vezes é feito em potência elevada, necessitando, por vezes, da construção de subestações de energia elétrica de grande porte em níveis de tensão de 34,5 ou 138kV. Em geral, em subestações elétricas mais antigas a concepção do sistema de comando, controle e proteção é convencional, com o uso de relés eletromecânicos que utilizam fiação de cobre para os esquemas de intertravamento e lógicas de proteção. Por outro lado, em subestações mais recentes, os dispositivos de proteção já são eletrônicos, com maior dependência de elementos de rede, como, switches, fibra ótica, rede Ethernet, entre outros. Com isso é necessário o uso de protocolos de comunicação e esquemas mais modernos de comando, controle e proteção descritos e normatizados pela Norma IEC 61850, uma vez que a mesma adota protocolos de comunicação padronizados e delimita os requisitos mínimos de hardware para os dispositivos utilizados em subestações elétricas. Nesse sentido, o presente trabalho apresenta uma análise qualitativa da arquitetura de rede que inclui o estudo sobre os dados obtidos de uma subestação da Companhia de Saneamento Ambiental do Distrito Federal (CAESB) com a verificação de pontos de vulnerabilidade em segurança de dados (*Cyber Security*), desempenho da rede de dados e validação de requisitos previstos na Norma 61850.

Palavras-chave: Cyber Security, IEC 61680, Interoperabilidade, Protocolos de Comunicação.

ANALYSIS OF IEDs INTEROPERABILITY INSTALLED IN ELECTRICAL SUBSTATIONS OF WATER TREATMENT PLANTS CONSIDERING THE IEC 61850 STANDARD REQUIREMENTS

Abstract: One of the most important inputs for the sanitation industry is the electrical energy used in Water Treatment Plants (WTP) and Sewage Treatment Plants (STP). Energy consumption is quite large in the sanitation industry and these plants are often supplied with high power, sometimes requiring the construction of large energy substations at voltage levels of 34.5 or 138kV. In general, in older electrical substations the design of the command, control and protection system is conventional with the use of electromechanical relays using copper wiring for interlocking schemes and protection logic. On the other hand, in more recent substations, protection devices are already electronic, with greater dependence on network elements, such as switches, fiber optics, Ethernet networks, among others. Therefore, it is necessary to use communication protocols and more modern command, control and protection schemes described and standardized in the IEC 61850 Standard adopting standardized communication protocols and defines the minimum hardware requirements for devices used in electrical substations. In this sense, the present work presents a qualitative analysis of the network architecture that includes the study of data obtained from a substation of the Environmental Sanitation Company of the Federal District (CAESB) with the verification of points of vulnerability in data security (Cyber Security), performance of the data network and validation of the requirements set out in Standard 61850.

Keywords: Cyber Security, Communication Protocols, IEC 61680, Interoperability.

1. Introdução

Nos últimos anos, a busca pelo avanço das tecnologias, da eficiência dos processos envolvidos e da confiabilidade do fornecimento de energia tem trazido uma grande mudança nos padrões construtivos de subestações de energia elétrica. As subestações estão cada vez mais digitalizadas e automatizadas, dependendo da necessidade da intervenção humana, com a substituição dos equipamentos eletromecânicos e da infraestrutura de fiação de cobre por dispositivos eletrônicos inteligentes (IED) e comunicação via fibra ótica.

Nesse sentido, de maneira a otimizar, simplificar, aumentar o desempenho e a confiabilidade de redes de subestações, a Norma internacional IEC 61850 torna-se imprescindível, uma vez que adota protocolos de comunicação padronizados e delimita os requisitos mínimos de hardware para os dispositivos utilizados em subestações elétricas.

A aplicação da norma possibilita ganhos substanciais na automatização e digitalização das subestações, com a diminuição do tráfego analógico por meio de fios e cabos de energia e o aumento do tráfego digital por meio de cabos de rede e cabos de fibra óptica.

Uma das premissas da norma é a utilização de IEDs para fazer todo o processamento da proteção, comando e controle. Isto cria uma quantidade elevada de informações que trafegam pelos níveis de processo, bay e estação. Os equipamentos, então, têm a necessidade de padronização de protocolos de comunicação para garantir a interoperabilidade completa entre os diversos equipamentos, não importando o fabricante e sistemas empregados (PEREIRA et al., 2008), (LACERDA, 2008).

Os protocolos da Norma IEC 61850: GOOSE (Generic Object Oriented Substation Event), SV (Sampled Variables) e MMS (Manufacturing Message Specification) objetivam tornar a comunicação transparente, eficiente, robusta e confiável para diferentes equipamentos de diferentes fabricantes e sistemas que compõem o Sistema de Automação da Subestação (SAS), utilizando padrões abertos e não proprietários, reduzindo os custos de projeto, engenharia, comissionamento, monitoramento, diagnóstico e manutenção e gerenciamento em geral.

Os diversos fabricantes de IEDs afirmam que seus dispositivos atendem aos requisitos das normas, mas ainda há alguns problemas, sejam eles, de comunicação ou desempenho. As renovações de ativos da subestação também podem ocasionar problemas de interoperabilidade com os equipamentos já existentes, tornando-se um fator que dificulta esta renovação.

Assim, o presente trabalho propôs a realização de uma análise qualitativa de uma subestação da Companhia de Saneamento Ambiental do Distrito Federal (CAESB) com a verificação do desempenho da rede de dados, a validação de requisitos previstos na Norma 61850 e a verificação de pontos de vulnerabilidade em segurança de dados.

2. Desenvolvimento

A automação de uma subestação de energia elétrica significa, de uma forma geral, monitorar e controlar as grandezas elétricas envolvidas no processo de transmissão e distribuição de energia: tensões, correntes, potências ativas, reativas e posições aberta/fechada de seccionadoras e disjuntores. Várias gerações de tecnologias convivem hoje em dia dentro das subestações, sendo que cada uma resolve uma determinada necessidade e foram agregadas às instalações, criando o que se convencionou chamar de

"ilhas de dados" dentro da subestação (SEL, 2010).

Essas "ilhas de dados" têm formato próprio, com a propriedade em cada desenvolvedor da tecnologia e dos equipamentos utilizados. É verificado que até hoje existe uma separação entre as soluções de proteção, sendo totalmente independentes das demais, principalmente pela característica própria envolvendo a segurança operacional da instalação.

Para a supervisão, controle e monitoramento surgiram diversos protocolos de comunicação. Em se tratando de protocolos abertos, os mais conhecidos são o Modbus, DNP3 e IEC 60870-5-101. Essa variedade de protocolos dificulta e encarece os projetos de ampliações de subestações e novas implantações, pois não há interoperabilidade entre os equipamentos dos diversos fabricantes. Diante disso, surge a importância da utilização da Norma IEC 61850, que propõe uma arquitetura de comunicação única entre os dispositivos independente do fabricante e da função exercida na subestação.

2.1.Norma IEC 61850

Com os avanços da eletrônica e das redes de computadores, verificou-se que haveria um grande ganho na automação de subestações se estas tecnologias fossem a ela incorporadas. Assim, foi adotada a tecnologia TCP/IP, onde todos os conceitos oriundos das redes de computadores comerciais, como endereços IP, endereços MAC, LAN, WAN, roteamento, frames e datagramas passaram a fazer parte do universo da automação e proteção de subestações, de forma total e completa. O transporte das informações entre dois dispositivos passou então a ser encapsulado em TCP/IP, padrão da internet mundial, confiável e já testado em todo mundo há mais de 20 anos (SEL, 2010).

Com a tecnologia TCP/IP consagrada, a norma IEC 61850 tem foco na modelagem/arquitetura dos dispositivos de automação das subestações, possuindo níveis de comunicação (processos, *bay* e estação) onde se localizam os protocolos com funções bem definidas (Figura 1).

As soluções mais atuais de automação de subestações são baseadas em redes Ethernet. Os IEDs (relés de proteção, multimedidores, unidades de aquisição e controle etc.) são entidades da rede. Todos possuem endereços MAC, IP e estão conectados aos *switches*, roteadores e servidores.

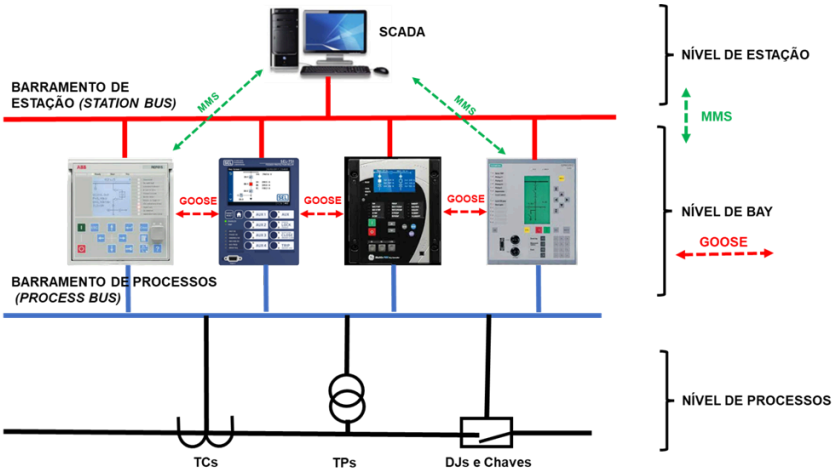

Figura 1 - Exemplo dos Níveis da Norma e dos seus Protocolos.
Fonte: próprio autor.

2.2. Subestação

A Subestação da CAESB considerada no desenvolvimento do presente trabalho foi projetada Figura 2, que mostra uma imagem aérea da subestação mais moderna da CAESB, localizada em Valparaiso-GO. É uma subestação rebaixadora 138/13,8kV com potência instalada 2 x 15/20 MVA, arranjo de barra simples no setor de alta (138kV) e em barra simples no setor de baixa (13,8kV) que é abrigada.

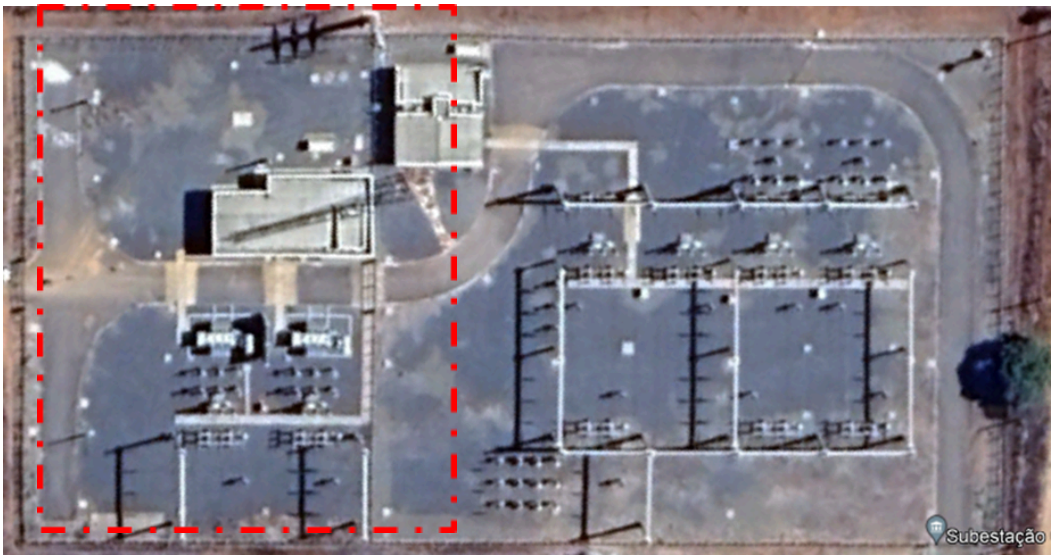

Figura 2 - Subestação da CAESB, destacado lado esquerdo.
Fonte: imagem *Google Earth*.

A experiência da CAESB com a Norma 61850 é incipiente sendo implementada pela primeira vez na SE que alimenta o complexo Corumbá e é basicamente com a implementação do protocolo GOOSE entre os IEDs e o SMS na comunicação vertical.

Os funcionários da empresa estão em formação para conseguir dar a devida manutenção nesta subestação quebrando paradigmas com a adoção de ferramentas não convencionais, baseada em análise de dados, análise de desempenho de redes etc.

2.3.Sistema SCADA (Supervisory Control and Data Acquisition)

Um SAS é composto por relés de proteção, controladores, redes de comunicação, concentradores para facilitar a integração com o sistema de supervisão e aquisição de dados (SCADA), registradores de perturbação, medidores, unidades de medição sincronizada de fasores, estações de engenharia local e remota e uma IHM (Interface Humano Máquina) local (ALBUQUERQUE, 2009).

O SCADA é um componente de *software* do SAS e seu principal objetivo é refletir o estado atual da subestação através de diagramas unifilares, tabelas apresentando grandezas elétricas aquisitadas dos componentes do SAS. Todas as informações apresentadas neste sistema têm por finalidade disponibilizar informações para a adequada tomada de decisões pelos vários *stakeholders* que interagem com o sistema, seja o SCADA local ou o SCADA remoto (Figura 3).

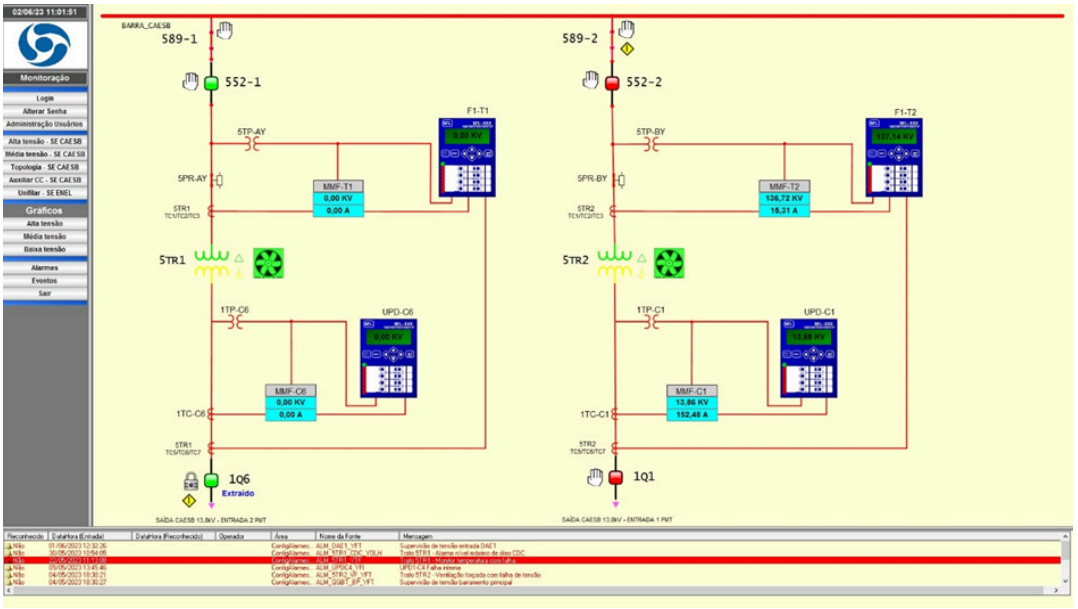

Figura 3 - Foto da Tela do SCADA Elipse - Subestação da CAESB.
Fonte: CAESB.

2.4.Cenário Atual (Arquitetura Atual)

A topologia de rede projetada e executada foi estrela simples sem redundância de switch (Figura 4). Utilizou-se apenas um switch da marca GE, modelo S2024, que atende aos requisitos da Norma 61850, fazendo conexão entre os IEDs da alta e baixa dos transformadores, bem como os IEDs dos alimentadores das unidades: Estação Elevatória de Água Tratada e Estação de Tratamento de Água da CAESB, além de uma unidade da Saneago.

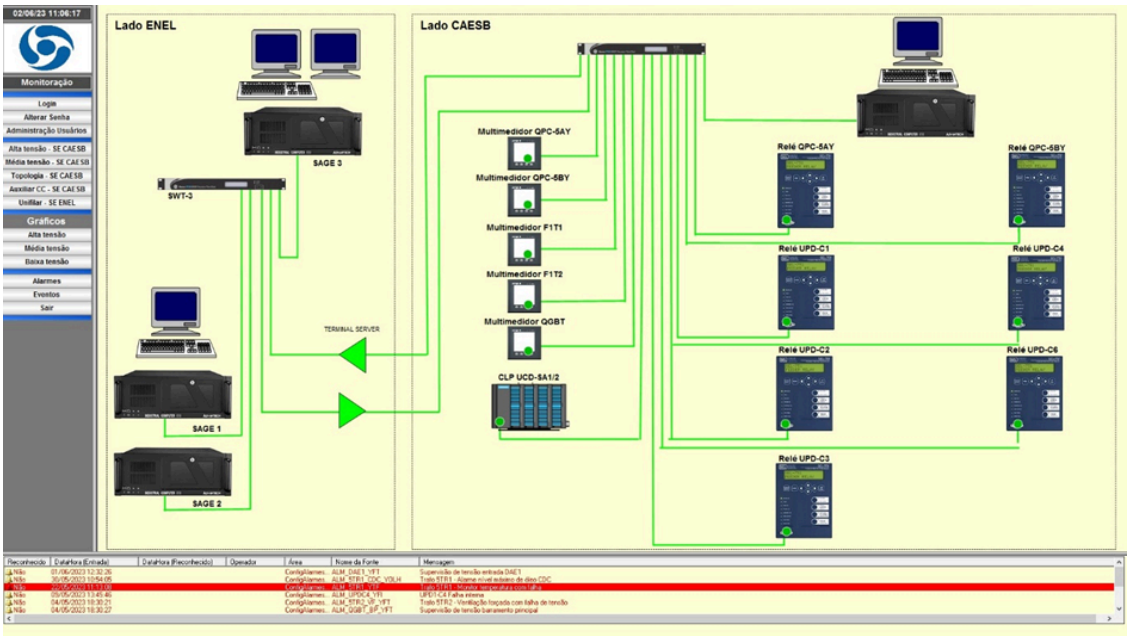

Figura 4 - Foto da Tela do SCADA Elipse – Topologia de rede.
Fonte: CAESB.

Todos os IEDs são conectados ao *switch* ethernet por cabos ópticos e ou cabos Ethernet que facilitam as conexões com os controladores de *bay*, relés de proteção, disjuntores etc.

No caso da proteção dos transformadores, há o relé de retaguarda que faz a proteção de redundância. Se houvesse os NCTIs e/ou MUs poderia ser utilizado o protocolo SV e neste caso seria necessário que o barramento de processo fosse separado do barramento de estação, pois os SVs gerados por uma MU de conversores convencionais ou não convencionais são fluxos de dados contínuos em relação aos SVs (PEREIRA et al, 2014).

Por Norma o SAS tem como um dos requisitos a redundância da Rede Ethernet que evita indisponibilidades, por exemplo, quando um cabo Ethernet falha, o canal de *backup* pode transferir os dados entre os dispositivos que precisam estar comunicando para não haver prejuízo à proteção, comando e controle. O *software* SCADA da CAESB é o Elipse instalado em um IHM local (Figura 4).

Como pontos a serem melhorados no projeto da arquitetura do SAS desta SE seria necessário o equilíbrio de cinco fatores que estão intimamente ligados: Confiabilidade, Disponibilidade, Desempenho, Economia e Capacidade de gerenciamento.

Como o barramento de processo e o barramento de estação têm diferentes tipos de tráfego e têm diferentes requisitos de desempenho é necessário um meio para se obter a separação lógica já que nem sempre é viável uma separação física entre os dois barramentos. Essa necessidade ocorre uma vez que os valores amostrados provenientes de uma unidade de medição (MU) não devem "inundar" todas as portas de um switch Ethernet e devem ir apenas para a porta onde o respectivo relé de assinatura está conectado e do mesmo jeito os sinais GOOSE de comando de *trip* do relé de proteção devem ser encaminhados apenas para a porta onde o assinante está conectado.

Então como ferramenta utilizada para a segregação do tráfego que tem como objetivo a separação lógica de redes devido às funções desempenhadas utilizam-se a VLANs que definem os domínios Multicast e que é uma etapa importante para manter o desempenho exigido e não sobrecarregar os dispositivos da rede.

2.5.Vulnerabilidades de Cibersegurança

A segurança de redes é um ramo da segurança da informação que trata sobre comunicação segura entre dois pontos. Em sua forma mais simplificada, a segurança de redes visa o impedimento de um terceiro mal-intencionado em verificar, ler ou modificar informações referentes à uma comunicação ponto a ponto. Isso pode se dar diretamente à conexão da comunicação ou de forma remota. Os problemas de segurança de redes em áreas interligadas são divididos em: Sigilo ou Confidencialidade, Autenticação, Não repúdio e Integridade (TANENBAUM, 2021).

A Segurança Cibernética é um braço da segurança de redes, que visa a determinação de políticas, modelos e gerenciamento das informações por meio de *framework* ou outras especificações técnicas para mitigação de ataques e revisão das vulnerabilidades (NIST, 2018). Os *frameworks* sugerem uma série de ações que vislumbram o modelo de controles de acesso, padrões de segurança e de avaliação de vulnerabilidades de *software* e *hardware,* além de administração e auditorias.

Uma rede em IEC 61850 está sujeita a vulnerabilidades e por isso ela deve possuir camadas de proteção, procedimentos de melhoria na formação e aplicação de senhas de acessos aos IEDs, sendo bastante recomendado que se utilize redes definidas por *software* (SDN) (TEBEKAEMI, 2016). No experimento da subestação simulada (vide item III), foi feito um teste simples com uma ferramenta computacional bastante conhecida em que se quebraram as senhas de maneira surpreendentemente fácil. Em geral as senhas que os usuários utilizam não são robustas, sendo que por vezes os

usuários utilizam senhas *default* de fábrica e mesmo que fossem utilizadas senhas longas e com caracteres especiais, a vulnerabilidade não seria evitada e o resultado seria apenas o aumento do tempo de invasão.

2.6.Ganhos e Oportunidade para a CAESB

A adoção da IEC 61850 possibilitou à CAESB construir um sistema de automação aberto, onde o custo total da SE ficou menor do que se fosse utilizado esquemas de proteção comando e controle convencionais com o emprego de cabeamento de cobre.

No desenvolvimento, apenas uma parte da Norma foi aplicada, todavia esta SE pode ter mais elementos aplicados no futuro já que é possível instalar novos equipamentos, como MUs, mais switches e GPS. Com uma reconfiguração em toda a rede existente é mais fácil incrementar mais elementos ao SAS com a utilização de equipamentos de qualquer fabricante que possua os requisitos da IEC 61850.

Ademais, o presente trabalho procurou exemplificar o quanto ainda é frágil a segurança de rede em SAS, que mesmo com recomendações padronizadas das normas IEC 61850, estão vulneráveis a ataques em seus equipamentos.

3. Testes e Resultados

3.1.Cenário proposto (arquitetura proposta)

Os testes propostos iniciaram pela montagem e configuração dos equipamentos da rede (Figura 5 e Figura 6) que contou com os equipamentos disponíveis: 3 (três) IEDs (relés de proteção), um *switch* gerenciável, 3 (três) relés biestáveis para simular os disjuntores de campo, um concentrador, um *laptop* com os *softwares* dos IEDs e uma mala de testes com recursos da IEC 61850. Para sincronizar os horários utilizou-se o SNTP por conta da falta de um relógio GPS. Configurou-se as bases de dados do IHM e demais equipamentos no nível estação, permitindo iniciar os testes de comunicação.

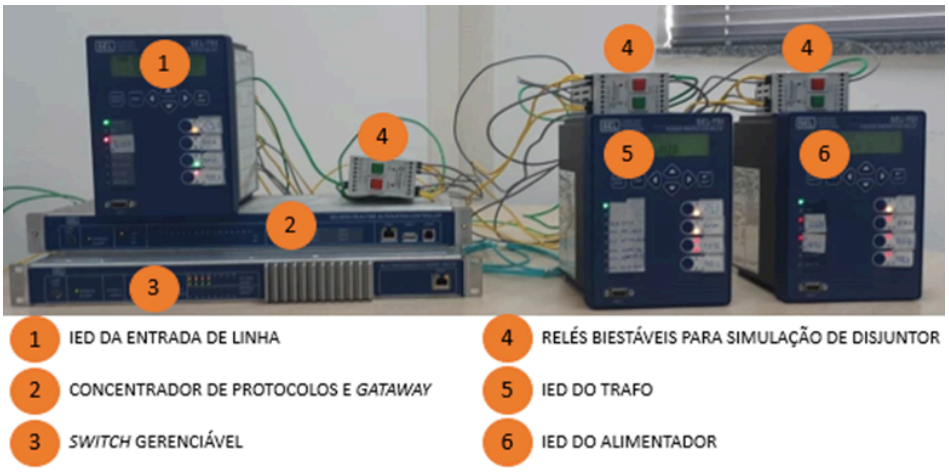

Figura 5 - Montagem Simplificada dos IEDs com arquitetura mínima para o experimento.
Fonte: próprio autor.

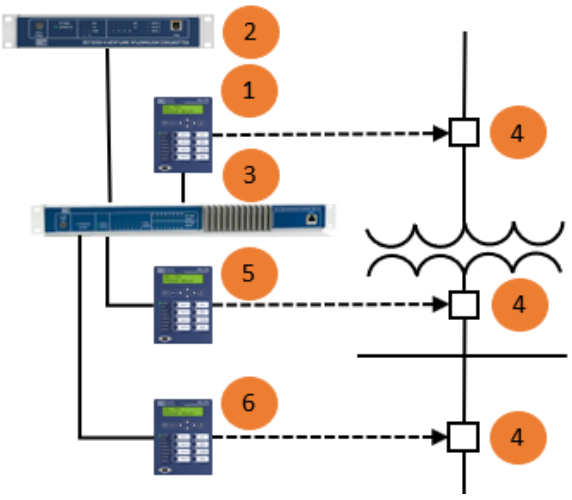

Figura 6 - Representação Unifilar do experimento.
Fonte: próprio autor.

Os objetivos dos testes propostos foram: montar uma rede LAN, criar VLANs, criar um projeto de SAS com a geração de arquivos para simulações das mensagens GOOSE, verificação do desempenho com uma sobrecarga da rede e simular as vulnerabilidades de cibersegurança dessa arquitetura rede.

Para elaboração da linguagem SCL utilizou-se a ferramenta computacional (*AcSELerator Architect*) que inclui as informações sobre a configuração, funcionalidades do SAS e as características da rede de comunicação (Figura 7), obtendo-se um arquivo que representa todo o SAS denominado arquivo SSD (Descrição da Especificação do sistema). O SSD dá origem ao arquivo SCD (Descrição da Configuração da Subestação).

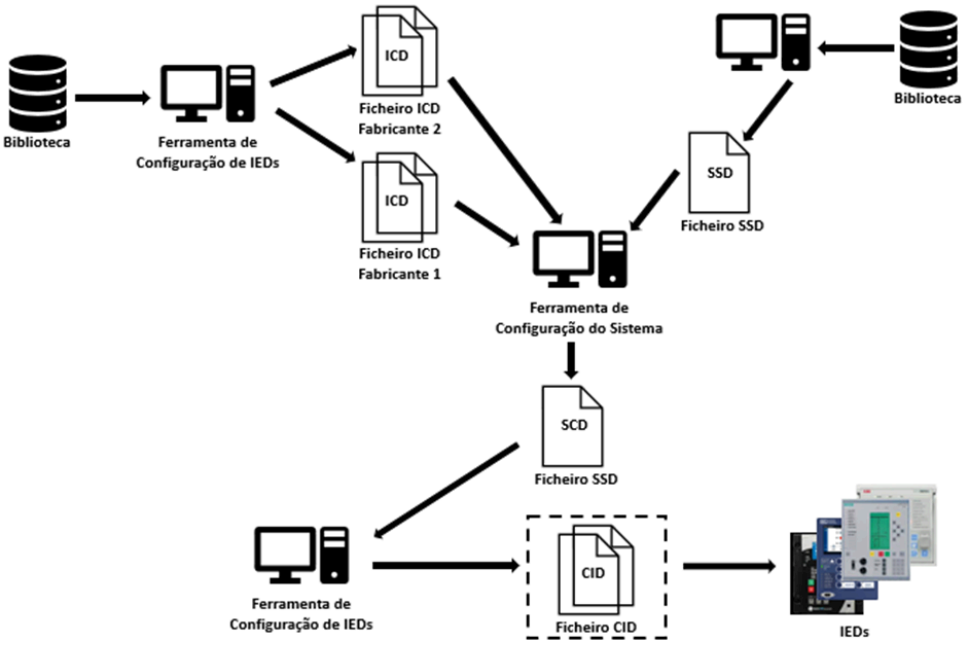

Figura 7 - Processos de criação do arquivo SCL.
Fonte: próprio autor.

O começo dos testes foi simples com aumento da sua complexidade, pouco a pouco, até pela limitação de IEDs e outros elementos importantes. Como exemplo, simulou-se uma

falta envolvendo três relés de proteção apenas para analisar o fluxo de mensagens trocadas por estes IEDs, incluindo as mensagens verticais para o IHM (*status*, alarmes e comandos) e as mensagens horizontais (GOOSE). Cada uma das funções distribuídas deve ser testada, simulando as diversas situações que possam ocorrer. Os IEDs futuros, ou aqueles que não estiverem disponíveis por ocasião do teste, podem ser simulados por uma ferramenta computacional adequada como o *software IEDScout* da OMICRON.

3.2.Testes de Desempenho do Sistema de Comunicação

Os testes de desempenho de um SAS têm a função de verificar se cada função se mantém dentro dos limites de desempenho especificados, mesmo quando a rede de comunicação é submetida a condições críticas de tráfego de mensagens.

Durante os testes de desempenho são verificados os tempos máximos de operação de funções, assim como os tempos máximos que cada mensagem (especialmente as mensagens GOOSE) irá levar desde sua geração em um IED até que seja recebida pelos IEDs subscritores que irão utilizar a informação.

Com a simulação de situações desfavoráveis com maior estresse na rede deve-se considerar a simulação de falhas que evoluam para incluir múltiplas zonas de proteção na subestação, juntamente com falhas de disjuntor. O teste deve mostrar se a LAN pode operar corretamente durante as avalanches de mensagens GOOSE nesta situação, com todas as funções e interações dos IEDs.

3.3.Experimento de Sobrecarga de eventos em uma SE-Simulada

Para que exista uma taxa de mensagens alta a ponto de ser considerada uma sobrecarga de eventos, alguns itens são necessários: uma rede com muitos IEDs, cada IED configurado para envio de muitas mensagens atualizadas em um intervalo pequeno de tempo. Por exemplo, pode-se considerar uma situação hipotética, em que há uma SE Digital com 20 (vinte) *bays*, com dois relés por *bay* (um principal e outro retaguarda), ou seja, totalizando 40 (quarenta) IEDs. Para cada um destes relés haverá 30 (trinta) Datasets, ou seja, um fluxo de 30 (trinta) mensagens diferentes.

Para situações em que um defeito interno dos relés resultar em uma enxurrada de eventos, que poderia ocasionar uma queda de desempenho na rede, propôs-se utilizar uma lógica simples com a função 50BF, avaliando-se o comportamento da proteção em uma falha de disjuntor, por meio de uma ligação via mensagem GOOSE, com e sem a presença de carregamento com frames de alta prioridade.

Nos testes realizados, os IEDs foram montados de forma a simular um sistema de proteção envolvendo uma entrada de linha, um transformador de força e um circuito de saída de um alimentador de 138kV, um transformador de 32MVA e na saída da barra de um alimentador de 13,8kV alimentando as cargas, conforme a Figura 6.

Caso o disjuntor do alimentador de 13,8kV falhe, o IED deve enviar uma mensagem de comando para o disjuntor do transformador a montante para que este abra. O envio deste comando será implementado através da troca de mensagens GOOSE, onde serão realizadas diversas condições adversas de tráfego na rede de comunicação.

Foram realizados testes nos relés em três condições diferentes. O primeiro teste foi feito sob condição natural com tráfego leve. Este teste foi realizado para garantir a funcionalidade da função 50BF e coletar os dados de referência para comparação e análise.

No segundo teste foi definida uma VLAN no switch e procedeu-se um carregamento

GOOSE na rede. O objetivo para a criação da VLAN foi impedir que a avalanche de mensagens GOOSE chegue ao IED que será avaliado.

O terceiro teste contemplou um carregamento da rede através de mensagens GOOSE com a mesma prioridade da mensagem crítica que será checada, conforme o segundo teste, porém, neste caso foi avaliado se a mensagem chegará no IED a montante e o tempo que levará, sem separação do tráfego por redes virtuais.

A corrente foi injetada pela mala de testes no IED do alimentador (relé a jusante), que enviou um comando para abertura do seu disjuntor, a jusante, (Função 50: Tempo= 0s + inércia). Após 100ms o IED do transformador verificou que a corrente permaneceu (portanto o disjuntor não extinguiu a falta), enviando uma informação por meio da rede IEC 61850 via mensagem GOOSE para o relé do transformador a montante. Dessa forma, o IED do transformador recebeu a mensagem GOOSE e enviou um *trip* para a o disjuntor a montante.

3.4.Avaliação da Segurança da Rede

Considerando o cenário hipotético em que o invasor conseguiu com engenharia social o IP de um IED da SE alvo, ilustrada pela SE da Figura 6, então procedeu-se ao ataque no qual será necessário a senha de acesso em primeiro nível e segundo nível.

Para conseguir quebrar a senha será necessário o uso de Força Bruta, considerada na categoria de técnica de sub-ataque pelo ATT&CK for ICS (*Adversarial Tactics, Techniques, and Common Knowledge*), que é uma diretriz para classificar e descrever ataques cibernéticos e intrusões (MITRE, 2022). A Força Bruta, código T1110, consiste em obter acesso a redes quando as senhas são desconhecidas ou quando são obtidos seus *hashes*. Isso também pode ser feito sistematicamente pelo invasor usando mecanismos de repetição ou iteração dos serviços de validação de credenciais.

O acesso por Força Bruta aproveita o conhecimento adquirido de outros comportamentos pós comprometimento, como despejo de credenciais do sistema operacional, descoberta de conta ou descoberta de política de senhas ou combinações desses ataques (MITRE, 2022).

Uma vez configurado o cenário, o objetivo é atacar os comandos elétricos e a lógica de automação dos IEDs, remotamente ou localmente, acessando os privilégios das mensagens GOOSE ou SV e desabilitando o acesso remoto de autenticidade pelo Centro de Operações. A rede de TI funciona como um segundo nível para acessar a rede TO.

Utilizou-se o *software* livre *John The Ripper*, com o objetivo de validar os problemas de ataques cibernéticos na arquitetura proposta tendo como resultados:

- Em 377s todos os IEDs já tinham sido afetados, ou seja, 100% dos IEDs foram invadidos com sucesso;
- Em 987s todos os disjuntores foram abertos com sucesso.

4. Conclusão

O presente trabalho apresentou uma análise da interoperabilidade de IEDs instalados em subestações elétricas de estações de tratamento de água seguindo requisitos da norma IEC 61850.

A subestação analisada é de propriedade da CAESB e foi possível verificar as vantagens do uso da Norma 61850 que na CAESB ainda é incipiente, sendo esta a primeira SE

com está tecnologia. Nesse sentido, o emprego da Norma 61850 possibilitou uma economia substancial durante a construção, com a implementação do protocolo GOOSE entre os IEDs e o MMS na comunicação vertical.

A edição do arquivo SCL mostrou ser uma tarefa relativamente fácil quando se usa IEDs de apenas um fabricante. Havendo outros fabricantes seria necessário o uso dos *softwares* proprietários e esta é apenas uma das dificuldades quando se está projetado um SAS.

O uso indiscriminado de LNs Genéricos também podem causar inconsistências que precisam ser verificadas com cuidado e serem compatibilizados no SCL. Nesse sentido, é importante ressaltar que esses descasamentos não são fixos, e que cada projeto de implementação de interoperabilidade pela Norma IEC 61850 terá suas necessidades de adequação para a devida importação de arquivos entre as ferramentas e correções de nomenclatura.

Outra dificuldade também verificada é o fato de existirem toda uma diversidade de ferramentas de parametrização entre os fabricantes que dificulta um pouco a certificação. Arquivos validados em uma determinada ferramenta não garantem que eles serão interpretados corretamente e aí será necessário conhecimento técnico para a manipulação e devidas alterações.

Uma das formas mais eficientes para certificar a interoperabilidade entre diversas ferramentas é a manipulação dos arquivos SCL dos equipamentos. Dessa forma, ocorre uma acentuada diminuição da quantidade de erros decorrentes do trabalho de configuração manual.

O integrador do SAS deve seguir os procedimentos, conforme descrito neste trabalho, para os testes de conformidade na fabricação do IED (Testes de Aceitação em Fábrica e Testes Aceitação em Campo), sendo uma boa prática um teste de Plataforma ou Prova de Conceito durante a fase de implementação e comissionamento do projeto do SAS para certificação da interoperabilidade. Além dos testes de conformidade de cada IED específico, os testes do SAS completo, incluindo IEDs de diferentes fabricantes interligados por uma rede de comunicação, devem ser realizados em laboratório, de modo a identificar e corrigir possíveis problemas, tornando mais rápida a fase de testes de campo e o início da operação do SAS.

O experimento de sobrecarga de mensagens GOOSE mostrou que mesmo em momentos de alto tráfego na rede não houve perda de desempenho das características da rede ethernet e da norma IEC 61850, que utiliza a técnica das VLANs como forma de separar o tráfego, tendo apresentado um resultado bastante satisfatório com um tempo de médio de 0,33ms em relação à uma rede sem carregamento. A repetição das mensagens GOOSE de evento, que é bastante comum para que ocorra a garantia de sua entrega, mesmo quando um pacote é perdido, provocando um carregamento extra na rede, não demonstrou prejuízos no desempenho da proteção. Nesse sentido, no terceiro teste foi verificada uma diferença média em relação ao teste de referência de 1,67ms, sendo relativamente pequena.

Por fim, deve-se destacar a necessidade de preparação adequada dos profissionais técnicos e engenheiros envolvidos com as áreas de proteção, controle, automação de subestações, comunicação e sistemas de computação para que o padrão IEC 61850 possa fornecer o modelo adequado de informação ao fabricante, *softwares* e equipamentos para a realização de análise e assinatura das mensagens com a finalidade de certificação.

5. Referências

ALBUQUERQUE, P.U.B.; ALEXANDRIA, A.R. *Redes Industriais*, 2ª ed.. 2. ed. Fortaleza: Editora Ensino profissional, 2009.

JÚNIOR, P.S.P.; MARTINS, C.M.; PEREIRA, P.S.. *Testes de Performance em IEDs Através de Ensaios Utilizando Mensagens GOOSE*, Anais do IX STPC - Nono Seminário Técnico de Proteção e Controle – Belo Horizonte – MG, Junho 2008.

LACERDA, S.L.M.C., RIBEIRO, G.H.. *Dispositivos Eletrônicos Inteligentes (IEDs) e a Norma IEC-61850: União que Está Dando Certo*. João Pessoa – PB. 2008.

MITRE. *Brute Force I/O. ATT&CK for ICS*, 2022. Disponível em: <https://attack.mitre.org/techniques/T1110/>.

NIST. *Framework for Improving Critical Infrastructure Cybersecurity*. National Institute of Standards and Technology, v. 1.1, p. 1–55, 2018.

PEREIRA, A.C.; PAULINO, M. E. C.; SIQUEIRA, I. P.; CACERES, D.; ROSAS, G. B.. *A Importância dos Testes Funcionais e de Interoperabilidade para a Integração de Sistemas de Proteção e Automação Utilizando a Norma IEC61850*, Belo Horizonte – MG, Junho 2008.

PEREIRA JÚNIOR, P.S.; MARTINS, C.M.; ROSA, R.R.; PEREIRA, P.S.; LOURENÇO, G.E.; LELLYS, D.; MAKIYAMA, D.. *Aplicação do Barramento de Processo da IEC 61850-9-2 (Process Bus) e Testes com o Carregamento da Rede Ethernet*, SENDI, Santos-SP, Novembro 2014.

SEL. *Redes de comunicação em subestações de energia elétrica - Norma IEC 61850*. O Setor Elétrico, Edição 54, Capítulo VII, p. 56-61, Julho, 2010.

TANENBAUM, A.; FEAMSTER, N.; WETHERALL, D.. *Redes de Computadores*, 6ª Edição, *Bookman*, 2021.

TEBEKAEMI, E.; WIJESEKERA, D.. *Designing an IEC 61850 Based Power Distribution Substation Simulation/Emulation Testbed For Cyber-Physical Security Studies*. In: Proceedings of the First International Conference on Cyber-Technologies and Cyber-Systems, p. 41-49, 2016.