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[(1)]
Engenheiro Eletricista pelo Centro de Educação Superior de Brasília (IESB), Mestre em Engenharia de Elétrica pela Universidade Federal do ABC (UFABC), Especialista em Engenharia de Automação de Sistemas Elétricos (INATEL/SEL), atualmente cursa MBA em Saneamento Ambiental pelo FESPSP. Atua como Analista de Sistemas de Saneamento da Companhia Ambiental de Saneamento do Distrito Federal – CAESB.
Thales Sousa[(2)]
Professor Associado do curso de Engenharia de Energia da Universidade Federal do ABC - UFABC. Coordenador do grupo de pesquisa CNPQ Grupo de Planejamento, Operação e Regulação do Sistema Elétrico de Potência - GPOR-SEP. Coordenador e Pesquisador de Projetos de Pesquisa e Desenvolvimento de agências de fomento, ANP e ANEEL. Consultor na área de estudos elétricos em Sistemas Elétricos de Potência.

Endereço[(1)]**:** Rua 35 Sul Lote 11 Torre 2 Apartamento 501, Águas Claras - Brasília - Distrito Federal - CEP: 71931-180 - Brasil - Tel: +55 (61) 99914-3344 - e-mail: marciopsilva@caesb.df.gov.br.

RESUMO

A energia elétrica é um insumo essencial para Estações de Tratamento de Água e Esgoto, que demandam alto consumo energético e, frequentemente, subestações em níveis de subtransmissão (34,5 ou 138 kV). Subestações mais antigas utilizam sistemas analógicos com relés eletromecânicos e cabeamento de cobre, enquanto subestações modernas adotam dispositivos eletrônicos com integração em rede, exigindo protocolos avançados, como os definidos pela norma IEC 61850. Essa norma padroniza a comunicação e estabelece requisitos mínimos de *hardware*, sendo fundamental para aumentar a confiabilidade e o desempenho das redes. Neste contexto, o trabalho apresenta uma análise qualitativa de uma subestação da CAESB, focando em segurança cibernética, desempenho da rede e conformidade com a IEC 61850. Os resultados obtidos se mostraram coerentes com testes laboratoriais e referências bibliográficas.

PALAVRAS-CHAVE: Cibersegurança, Estações de Tratamento de Água e Esgoto, IEC 61850, Interoperabilidade, Subestações.

INTRODUÇÃO

Com o avanço constante da tecnologia e a necessidade de melhorias da eficiência dos processos envolvidos e da confiabilidade do fornecimento de energia, nos últimos anos observou-se uma grande mudança nos padrões construtivos de subestações de energia elétrica. As subestações estão cada vez mais digitalizadas e automatizadas, dispendendo a 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.

Na busca por otimizar, simplificar, aumentar o desempenho e a confiabilidade das subestações de energia elétrica, a Norma internacional IEC 61850 torna-se imprescindível, pois adota protocolos de comunicação padronizados e delimita os requisitos mínimos de *hardware* para os dispositivos utilizados nas mesmas.

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

Todavia, uma das premissas da norma é a utilização 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 (Figura 1). 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.

Assim, 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 desta forma os custos de projeto, engenharia, comissionamento, monitoramento, diagnóstico e manutenção e gerenciamento em geral.

Nesse sentido, 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 está renovação, ou seja, a renovação pode tornar-se mais onerosa porque não seria possível simplesmente substituir um equipamento integrante do SAS, sendo necessário substituir todo o SAS.

Com a aplicação dos conceitos da IEC 61850, modificações em esquemas de proteção e/ou automação que teriam a intervenção física são evitadas, pois a maioria das implementações focam no barramento de estação e na troca de mensagens GOOSE entre equipamentos, tornando à implementação de um barramento de processos e de troca de mensagens SV muito mais fáceis, rápidas e mais baratas.

Neste contexto, 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 de pontos de vulnerabilidade em segurança de dados (*Cyber Security*), desempenho da rede de dados e validação de requisitos previstos na Norma 61850.

OBJETIVOS

OBJETIVO GERAL

Analisar uma arquitetura real de equipamentos em uma subestação de subtransmissão que alimenta uma planta de saneamento ambiental, verificando a interoperabilidade entre os equipamentos de diferentes fabricantes, desempenho e verificando possíveis vulnerabilidades de Cibersegurança na arquitetura.

OBJETIVOS ESPECÍFICOS

- Estudo de arquitetura de rede;
- Testes de interoperabilidade entre equipamentos de diferentes fabricantes com o foco no *hardware*;
- Validar uma topologia padrão para redes de *switches* de uma subestação que atenda empresas do mesmo seguimento que a CAESB;
- Subsidiar uma especificação de *switches* para subestações da CAESB;
- Testar a integração dos equipamentos com sistemas supervisórios e sistemas externos à subestação;
- Testar requisitos de segurança cibernética em subestações de subtransmissão: configuração de equipamentos e sistemas, comunicação entre os diversos componentes, integração com sistemas supervisórios, todos de acordo com recomendações das normas vigentes;
- De maneira secundária, demonstrar a aplicação de metodologias de manutenção baseada em condição, evidenciando como o uso de recursos digitais, como o monitoramento remoto, pode contribuir para a antecipação de falhas, para o aumento da disponibilidade operacional e a consequente para a redução do *OPEX*, com foco no caso real da CAESB.

METODOLOGIA UTILIZADA

A metodologia para realização do presente trabalho se deu, inicialmente, a partir de uma Revisão da Literatura relacionada à Norma IEC 61850.

Em seguida, foi realizada uma análise do projeto da Subestação de Suprimento da Unidade de Tratamento de Água do Sistema Corumbá da CAESB inaugurado em 2022.

O próximo passo foi a análise qualitativamente da topologia de rede de dados da subestação com os equipamentos aplicados: *Switches*, CLPs e Dispositivos Eletrônicos Inteligentes - IEDs de diferentes fabricantes, observando possíveis vantagens, desvantagens, erros e acertos deste empreendimento de maneira a propor um teste de aceitação dos equipamentos, metodologia de comissionamento de acordo com a Norma IEC 61850.

Por fim, foi realizada a validação da metodologia proposta a partir da simulação de diferentes cenários de renovação dos ativos de automação e proteção em outras subestações da CAESB.

SISTEMA CONSIDERADO

A construção de subestações é uma atividade que vem se desenvolvendo desde o final do século XIX, ou seja, há mais de 100 anos. E 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. Cada geração de tecnologia resolve uma determinada necessidade, tendo sido agregadas às instalações, criando o que se convencionou chamar de "ilhas de dados" dentro da subestação (Cascaes et al, 2008).

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, faz-se necessário a utilização da Norma IEC 61850, que propõe uma arquitetura de comunicação única entre os dispositivos independente do fabricante e da função exercida na subestação.

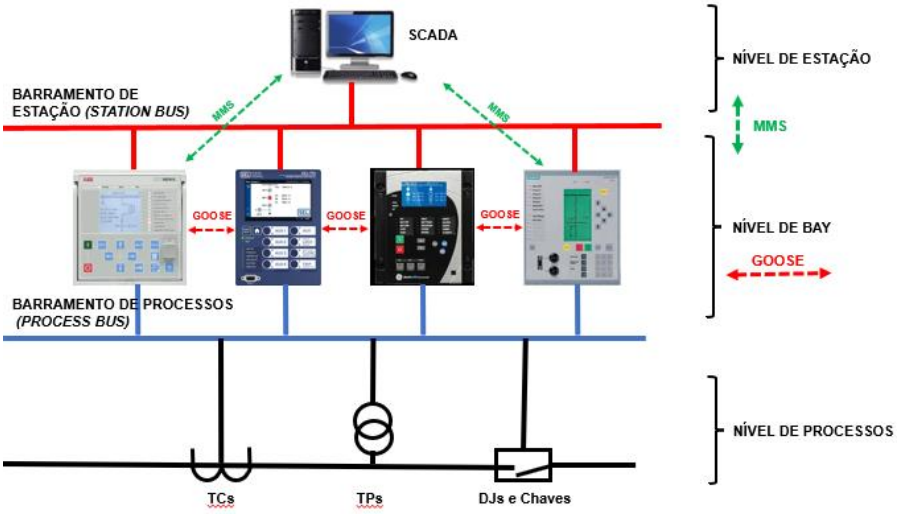
NORMA IEC 61850

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, tendo sido adotada a tecnologia TCP/IP. Portanto, todos os conceitos oriundos das redes de computadores comerciais, como endereços IP, endereços MAC, LAN, WAN, roteamento, frames e datagramas têm sido utilizados na automação e proteção de subestações. O transporte das informações entre dois dispositivos é encapsulado em TCP/IP, tendo sido utilizado em todo mundo há mais de 20 anos (Cascaes et al, 2008).

Com a tecnologia TCP/IP consagrada, a norma IEC 61850 tem o foco na modelagem dos dispositivos de automação das subestações. A norma é muito mais do que um protocolo de comunicação, mas sim uma arquitetura de automação de subestações. Possui 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 IED`s (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, servidores etc.

Figura 1 Barramento de comunicação da IEC 61850 e os níveis do SAS.



Fonte: o próprio autor.

SUBESTAÇÃO

A subestação ilustrada na Figura 2 é a subestação mais moderna da CAESB e está localizada em Valparaíso - 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: Google, 2023.

A experiência da CAESB com a Norma 61850 foi implementada pela primeira vez na subestação que alimenta o complexo Corumbá, a partir do emprego do protocolo GOOSE entre os IEDs e o SMS na comunicação vertical.

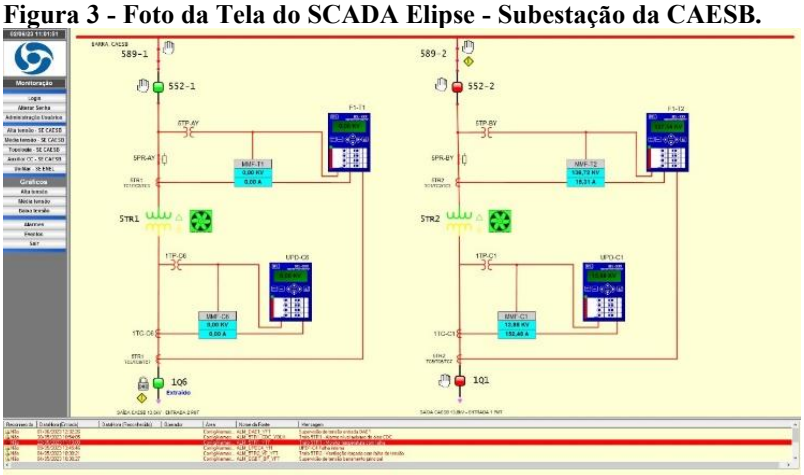
Os funcionários da empresa estão em formação para conseguir dar a devida manutenção nesta subestação, quebrando paradigmas a partir da adoção de ferramentas não convencionais, baseada em análise de dados e análise de desempenho de redes.

SISTEMA SCADA (*SUPERVISORY CONTROL AND DATA ACQUISITION*)

Um Sistema de Automação de Subestação (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* Homem-Máquina) local (Fontes, 2015).

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. A Figura 3 ilustra a interface do sistema SCADA da subestação da CAESB.

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

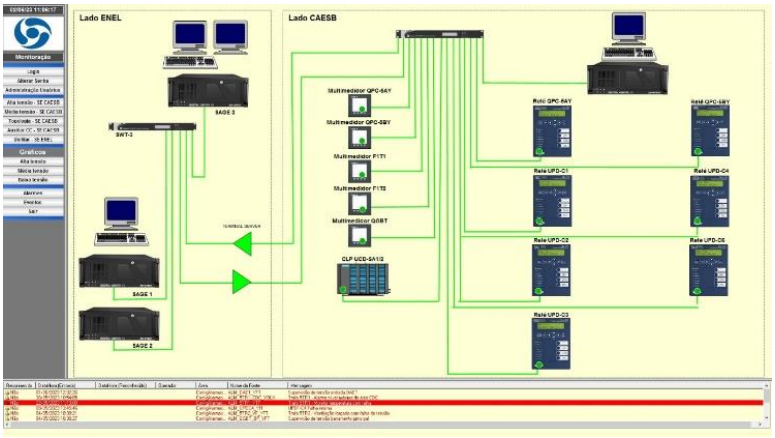


Fonte: Sistema Supervisório Local da Subestação da CAESB, 2023.

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 é muito moderno e que atende aos requisitos da Norma 61850. O *switch* faz a 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: Sistema Supervisório Local da Subestação da CAESB, 2023.

Todos os IEDs são conectados ao *switch ethernet* por cabos ópticos e ou cabos *Ethernet*, facilitando 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.

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 subestação seria necessário o equilíbrio de cinco fatores que estão intimamente ligados: Confiabilidade, Disponibilidade, Desempenho, Economia, 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 separação lógica já que nem sempre é viável uma separação física entre os dois barramentos. Isto 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. 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.

Assim, 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*, que são uma etapa importante para manter o desempenho exigido e não sobrecarregar os dispositivos da rede.

VULNERABILIDADES DE CIBERSEGURANÇA

A cibersegurança é um ramo da segurança da informação que trata sobre comunicação segura entre dois pontos. Em sua forma mais simplificada, a cibersegurança visa o impedimento de um terceiro mal-intencionado em verificar, ler ou modificar informações referentes à uma comunicação ponto a ponto. Isso pode ser dar diretamente à conexão da comunicação ou de forma remota (Tanenbaum, 2021).

Os problemas de segurança de redes em áreas interligadas são divididos em: Sigilo ou Confidencialidade, Autenticação, Não repúdio e Integridade (Tanenbaum, 2021).

A cibersegurança 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. 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.

Um dos *frameworks* de cibersegurança mais conhecido e mais seguido por administradores de rede é o divulgado no guia de infraestrutura crítica. O documento apresenta uma Estrutura Básica, que é uma lista de Funções, Categorias, Subcategorias e Referências Informativas que descrevem atividades específicas de cibersegurança, comuns em todos os setores com infraestrutura crítica (Nogueira, 2007).

As funções do *framework* do NIST, descrito no documento, são: Identificar (ID), Proteger (PR), Detectar ou Diagnosticar (DE), Responder (RS) e Recuperar (RC) (Nogueira, 2007).

GANHOS E OPORTUNIDADE PARA A CAESB

Neste contexto, o presente trabalho buscou 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.

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

Em relação à adoção da IEC 61850, foi aplicada apenas uma parte da mesma, sendo que outros elementos podem ser aplicados no futuro, já que é possível instalar novos equipamentos na subestação, como MUs, *switches* e GPS. Neste ponto, deve-se destacar que realizada uma reconfiguração em toda a rede existente torna-se mais fácil incrementar o número de elementos ao SAS, utilizando-se equipamentos de diferentes fabricantes, desde que possuam requisitos da IEC 61850.

Adicionalmente, a inserção da CAESB no estado da arte para SAS permite que o seu corpo técnico se atualize nesta tecnologia.

TESTES E RESULTADOS

ARQUITETURA PROPOSTA

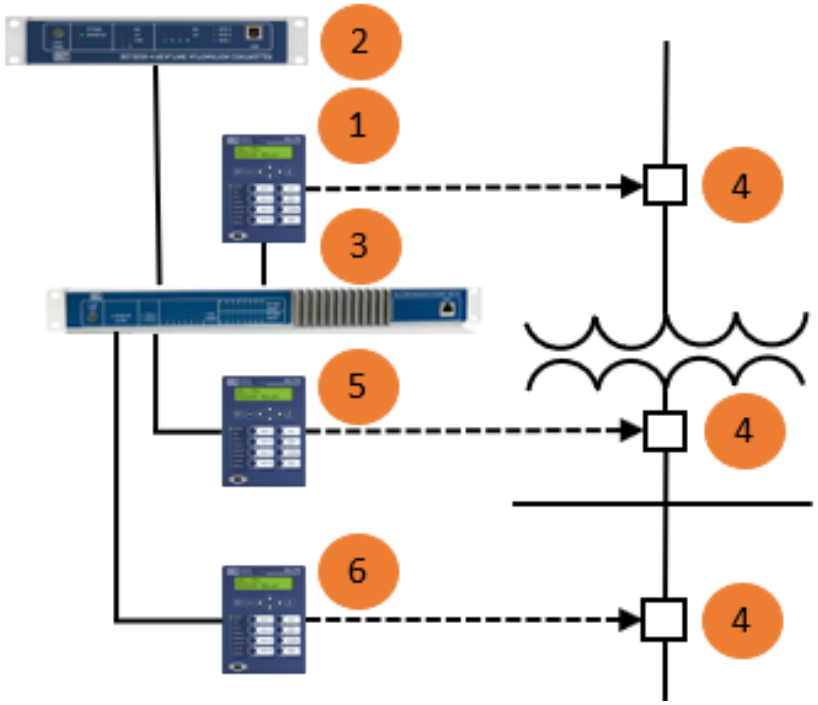
O teste proposto no presente trabalho iniciou a partir da montagem e configuração dos equipamentos da rede proposta, ilustrada nas Figuras 5 e 6 e contou com os seguintes equipamentos: 3 (três) IEDs (relés de proteção), um *switch* gerenciável, 3 (três) relés biestáveis para simular os disjuntores de 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. Ademais, foram configuradas as bases de dados do IHM e demais equipamentos.

Todas as informações apresentadas nesse sistema têm por finalidade fornecer uma maior quantidade de informações para a adequada tomada de decisões pelos vários usuários que interagem com o sistema, seja a partir de um SCADA local ou um SCADA remoto (Figura 3).

Figura 5 - Arquitetura Proposta Simplificada.

Fonte: o próprio autor.

Figura 6 - Representação Unifilar do experimento.

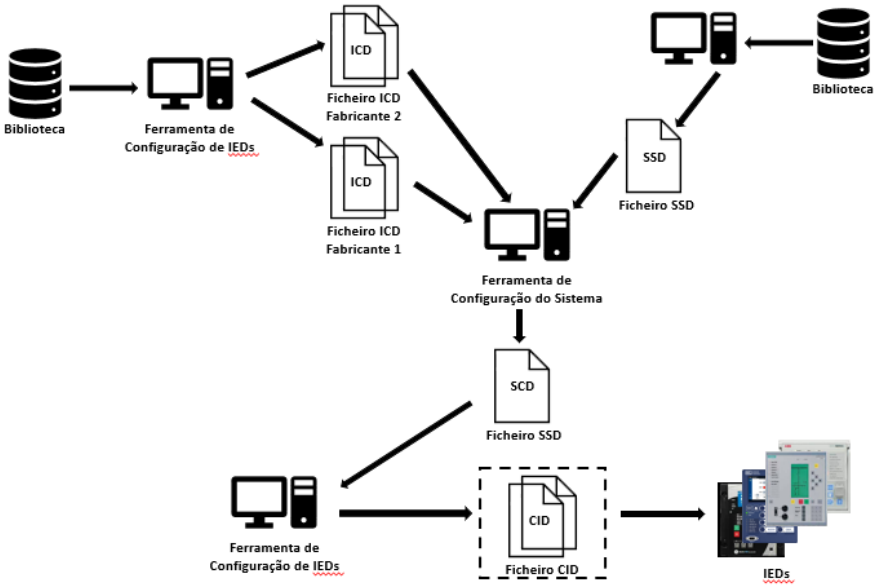


Fonte: o próprio autor.

A partir da montagem e configuração dos equipamentos da rede proposta, foram realizados um conjunto de testes com os seguintes objetivos 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 da arquitetura da 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 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). A Figura 7 ilustra os processos de criação do arquivo SCL.

Figura 7 - Processos de criação do arquivo SCL e implantação do CID nos IEDs.



Fonte: o próprio autor.

Inicialmente foram realizados testes simples, aumentando a sua complexidade, até alcançar a limitação de IEDs e de outros elementos importantes.

Como exemplo dos testes realizados, foi simulada uma falta envolvendo três relés de proteção, com o objetivo de 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). Neste sentido, 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 devem ser simulados por uma ferramenta computacional adequada, como por exemplo, o *software IEDScout* da OMICRON.

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 especificado, 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 *stress* 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.

EXPERIMENTO DE SOBRECARGA DE EVENTOS EM UMA SUBESTAÇÃO 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 IED´s, sendo que cada IED deve ser configurado para envio de muitas mensagens atualizadas em um intervalo pequeno de tempo.

Para o teste de sobrecarga de eventos, considerou-se uma subestação digital com 20 (vinte) *bays*, com dois relés por *bay* (um principal e outro retaguarda), totalizando 40 (quarenta) IEDs. Neste caso, para cada um destes relés haveria 30 (trinta) *Datasets*, ou seja, um fluxo de 30 (trinta) mensagens diferentes. Adicionalmente, consideraram-se situações de defeito interno dos relés em que resultaria em uma enxurrada de eventos, ocasionando uma queda de desempenho na rede.

Dessa forma, para o teste proposto, foi utilizada uma lógica simples com a função 50BF, de maneira a avaliar 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.

Os IEDs foram montados de forma a simularem 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 ilustrado na Figura 6.

Na hipótese do disjuntor do alimentador de 13,8kV falhar, 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.

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

Para o segundo teste foi criada uma VLAN no *switch* e um carregamento GOOSE na rede. O objetivo para a criação da VLAN é impedir que a avalanche de mensagens GOOSE chegasse 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 será 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, e quando o IED do transformador a montante recebe a mensagem GOOSE envia um *trip* para o disjuntor a montante.

REDES DE CIBERSEGURANÇA - EXPERIMENTO DE INTRUSÃO EM UMA SUBESTAÇÃO SIMULADA

Para o teste de intrusão em uma subestação simulada, considerou-se a situação onde o invasor conseguiu com engenharia social o IP de um IED da subestação alvo, representada pela subestação ilustrada na Figura 6. Neste caso, para realização do ataque, seria necessária a senha de acesso em primeiro nível e segundo nível.

Para conseguir quebrar a senha seria necessário o uso de Força Bruta, classificada 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 utilizando 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 (NIST, 2018).

Uma vez configurado o cenário, o objetivo é atacar os comandos elétricos e a lógica de automação dos IED's, 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.

No teste de intrusão proposto utilizou-se o *softwar*e livre *John The Ripper*, com o objetivo de validar os problemas de ataques cibernéticos na arquitetura proposta. Os resultados obtidos foram:

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

CONCLUSÕES E RECOMENDAÇÕES

O presente trabalho apresentou uma análise de uma arquitetura real de equipamentos em uma subestação de subtransmissão que alimenta uma planta de saneamento ambiental, verificando a interoperabilidade entre os equipamentos de diferentes fabricantes, o desempenho e as possíveis vulnerabilidades de cibersegurança na arquitetura.

Os testes foram realizados em bancada, tendo sido observados vários pontos de grande importância para a compreensão da vasta gama de possibilidades de adequações que podem surgir em projetos de implementação de SAS, TAFs de IEDs, comissionamentos e cuidados com a segurança de dados.

Para a subestação da CAESB analisada verificou-se, mesmo que ainda incipiente, visto que essa foi a primeira subestação com está tecnologia, as vantagens do emprego da Norma 61850. Neste sentido, o emprego da Norma 61850 possibilitou uma economia substancial durante a construção com a implementação do protocolo GOOSE entre os IEDs e o SMS na comunicação vertical.

A priori, a edição do arquivo SCL pode ser uma tarefa relativamente fácil quando se usa IEDs de apenas um fabricante. Todavia, com a implantação de outros fabricantes seria necessário o uso de *softwares* proprietários, sendo esta apenas uma das dificuldades quando se está projetado um SAS. Ou seja, não há um *software* universal que possa ser utilizado para todos os IEDs de diferentes fabricantes, podendo causar erros no arquivo ICD gerado pelo *software* do fabricante e inconsistências.

Nesse sentido, uma forma eficiente 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.

Outra dificuldade obervada é o fato de existirem 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 nessa manipulação para as devidas alterações.

Um ponto que foi possível perceber é que o *hardware* impacta diretamente na interoperabilidade, pois dois IEDs em conformidade com a Norma e com os arquivos SCL devidamente coerentes entre eles, não irão interoperar nos pontos em que não possuírem funcionalidades coerentes entre eles (funções, nós lógicos, adequação aos protocolos da Norma etc.), excessos de GGIO e necessidade de *softwares* para cada tipo de fabricante.

O experimento de sobrecarga de mensagens GOOSE realizado mostrou que mesmo em momentos de alto tráfego na rede não houve perda de desempenho devido às características da rede ethernet e da norma IEC 61850 que utiliza a técnica das VLANs como forma de separar o tráfego. Neste caso, foi obtido um resultado bastante satisfatório com tempo médio de 0,33ms em relação à uma rede sem carregamento, mesmo quando da ocorrência de 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. Mesmo nestes caos, não houveram prejuízos no desempenho da proteção. Como visto no terceiro teste, a diferença média em relação ao teste de referência foi de 1,67ms sendo relativamente pequena.

Adicionalmente, foram exploradas as vulnerabilidades que uma rede em IEC 61850 está sujeita. Um teste simples com uma ferramenta computacional bastante conhecida foi capaz de quebrar as senhas de maneira surpreendentemente fácil. Em geral as senhas que os usuários utilizam não são robustas, por vezes os usuários nem trocam as 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.

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 a modelagem de informação adequada ao fabricante, *softwares*, equipamentos para realização de análise e assinatura das mensagens com a finalidade de certificação.

REFERÊNCIAS BIBLIOGRÁFICAS

1. CASCAES PEREIRA, A.; PAULINO, M. E. C.; SIQUEIRA, I. P. de; 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, jun. 2008.

2. FONTES, Marcel da Costa. *Projeto de plataforma didática compatível com a norma IEC61850 para comissionamento de sistema digital de controle e proteção de subestação de energia elétrica*. 2015. 129f. Dissertação (Mestrado Profissional em Energia Elétrica) - Centro de Tecnologia, Universidade Federal do Rio Grande do Norte, Natal, 2015.

3. VARDHAN, Harsh; RAMLACHAN, R.; SZELA, Wojciech; GDOWIK, Edward. *Deploying digital substations: experience with a digital substation pilot in North America*. PECO, USA, 2017.

4. INTERNATIONAL ORGANIZATION FOR STANDARDIZATION. *ISO 9506-2: Industrial automation systems — Manufacturing Message Specification — Part 2: Protocol specification*. 2. ed. [S.l.: s.n.], 2003. ISBN 5935522004.

5. LEITE, Matheus Felipe Ayello. *Interoperabilidade com base na norma IEC 61850: revisão sistemática e estudo de caso*. Trabalho de Conclusão de Curso (TCC), 2021.

6. JÚNIOR, P. S. P.; MARTINS, C. M.; PEREIRA, P. S. *Testes de performance em IEDs através de ensaios utilizando mensagens GOOSE*. In: *Anais do IX STPC - Nono Seminário Técnico de Proteção e Controle*, Belo Horizonte – MG, jun. 2008.

7. MITRE. *Brute Force I/O*. ATT&CK for ICS, 2022. Disponível em: https://attack.mitre.org/techniques/T1110/. Acesso em: 02 jun. 2025.

8. NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. *Framework for improving critical infrastructure cybersecurity – version 1.1*. v. 1.1, p. 1–55, 2018.

9. NOGUEIRA, Bruno Vazquez. *Protocolo de comunicação IEC-61850*. Salvador – BA, 2007.

10. CARDOSO, P. *Avaliação do impacto em comissionamento e testes de funcionamento numa subestação com protocolo CEI 61850*. 2013. Dissertação (Mestrado) – Faculdade de Engenharia da Universidade do Porto (FEUP), Porto, 2013.

11. PEREIRA JÚNIOR, Paulo Sergio; MARTINS, Cristiano Moreira; PEREIRA, Paulo Sergio; LOURENÇO, Gustavo Espinha. *Experimento de sobrecarga com 15.000 mensagens GOOSE por segundo em uma rede IEC 61850 e a investigação de suas consequências*. In: *XX SNPTEE*, Recife – PE, nov. 2009.

12. PEREIRA JÚNIOR, Paulo S.; MARTINS, Cristiano M.; ROSA, Rodrigo R.; PEREIRA, Paulo S.; LOURENÇO, Gustavo E.; LELLYS, Denys; MAKIYAMA, Diego. *Aplicação do barramento de processo da IEC 61850-9-2 (Process Bus) e testes com o carregamento da rede Ethernet*. In: *SENDI*, Santos – SP, nov. 2014.

13. TANENBAUM, A.; FEAMSTER, N.; WETHERALL, D. *Redes de computadoras*. 6. ed. Porto Alegre: Bookman, 2021.