

Desafios da automação de subestações no contexto da segurança cibernética

Tema: Sistemas de Controle, Automação e Proteção

Autores: Fernando Moreira Ribeiro

Co-Autores: Rafael Douglas Costa Dutra, Marisa Lages Murta

Empresa: Cemig Distribuição S.A.

Resumo

Este artigo explora os desafios e soluções adotadas pela Cemig Distribuição (Cemig D) para garantir a segurança e a eficiência de sua rede operativa de automação de subestações. Com a adoção de redes Ethernet e protocolos padronizados como IEC 61850, surgiram questões críticas relacionadas à segurança cibernética, incluindo o acesso remoto seguro aos sistemas e a proteção contra ameaças. Para enfrentar esses desafios, a Cemig D implementou uma arquitetura de rede com segregação de sistemas, utilizando uma zona desmilitarizada (DMZ) e servidores de proxy reverso, garantindo o isolamento da rede operativa da rede corporativa e controlando rigorosamente o acesso. Além disso, são discutidos os desafios remanescentes, como a necessidade de monitoramento proativo de falhas e o desenvolvimento de ferramentas de auditoria e controle de acesso para garantir a inviolabilidade da rede operativa. A implementação de soluções avançadas de segurança cibernética e o aprimoramento da equipe especializada são apontados como passos essenciais para garantir a resiliência e a continuidade operacional.

1. Introdução

Ao longo das últimas décadas, principalmente a partir da década de 1990, o processo de operação das subestações de energia na Cemig D sofreu várias alterações, começando pela centralização da operação, passando pela digitalização dos relés de proteção e dos meios de comunicação e mais recentemente foram incorporados elementos da indústria 4.0 com o objetivo de otimizar a operação e manutenção, reduzindo os custos e aumentando a eficiência operacional.

Ao longo do processo de transformação das subestações, a automação se tornou um elemento crucial e com a evolução das tecnologias foi sendo consolidada a aplicação dos padrões de redes ethernet tanto para comunicação interna, quanto para comunicação externa das subestações. Com isso, tornou-se a ser necessária a criação de uma rede operativa segura e robusta capaz de suportar as demandas da operação em tempo real das subestações de energia da Cemig Distribuição.

Para atender os requisitos de robustez e segurança foi necessário incorporar o conceito de segurança cibernética à rede operativa. Isso significa que a rede operativa deve estar em um ambiente completamente apartado e todas as ações executadas dentro da rede operativa devem ser controladas e rastreáveis.

Este artigo visa fazer uma reflexão sobre os desafios da automação e apontar os caminhos que devem ser percorridos para prover recursos e funcionalidades para as equipes de operação e manutenção sem comprometer a segurança cibernética da rede operativa.

2. Desenvolvimento

2.1 Breve histórico da automação de subestações na Cemig D

Até o início da década de 1990, a maioria das subestações de energia elétrica da Cemig D contava com relés eletromecânicos, medidores analógicos, chaves e botoeiras na casa de controle. Nesse período a operação era realizada presencialmente por operadores em regime de revezamento 24/7 nas subestações mais importantes do sistema.

Com a evolução do sistema elétrico e demandas por melhorias nos índices de qualidade de energia, aliado aos altos custos da operação local a Cemig D iniciou, em meados da década de 1990, a construção de Centros de Operação Regionais (CORs) e a instalação de Unidades Terminais Remotas (UTRs) nas subestações. As UTRs eram responsáveis por coletar os principais pontos de supervisão, controle e proteção dos equipamentos da subestação e enviar as informações via canal analógico para um sistema SCADA instalado nos CORs, que passaram a concentrar a operação e controle de um grupo de subestações. Ao longo da década de 2000 e início da década de 2010, com a evolução tecnológica dos relés de proteção, a Cemig D começou a adotar relés eletrônicos e relés digitais em suas subestações, bem como a aplicação de protocolos de comunicação seriais, como IEC-103 e DNP3, para integração dos pontos de proteção e controle entre os relés e a UTR. Neste período foi realizado também a unificação dos CORs em um único Centro de Operação da Distribuição (COD) localizado em Belo Horizonte.

Em meados da década de 2010, a Cemig D possuía um parque de mais de 380 subestações com soluções de automação diversas, como:

- Subestações com relés eletromecânicos e/ou digitais integrados via contatos discretos em uma UTR, responsável pela coleta e envio de pontos de supervisão e controle entre a subestação e o SCADA do COD;
- Subestações com solução de automação proprietária, onde a integração entre os relés digitais e a UTR ocorria via um protocolo e uma arquitetura de rede proprietários do fabricante da solução;
- Subestações com solução de automação utilizando o protocolo DNP3, onde a integração entre os relés de proteção e a UTR era realizado através do protocolo DNP3, havendo casos de integração via DNP3 serial ou DNP3 ethernet.

Diante do cenário existente e buscando padronizar uma solução de automação robusta, confiável, com mais funcionalidades e que proporcione uma maior interoperabilidade entre os fabricantes, a partir de 2016 foi definida a adoção dos padrões da Norma IEC61850 para o barramento de estação em todas as soluções de automação das subestações da Cemig D. Paralelamente, passaram a ser adotados requisitos mínimos para o link de comunicação da subestação, já que até então era comum a disponibilização de links de comunicação serial para a solução de automação. Desta forma, passou a ser exigida a criação de uma Rede Operativa de Dados (ROD) multisserviço para atender às demandas da nova Solução de Automação de Subestações (SAS).

2.2 Solução de Automação de Subestações da Cemig D

A rede de automação de subestações da Cemig D foi projetada para garantir a operação eficiente e segura do sistema elétrico, conectando dispositivos de controle, medição e proteção. Ela utiliza protocolos de

comunicação padronizados, principalmente aqueles definidos pela norma IEC 61850, para permitir a troca de informações em tempo real entre os equipamentos. A rede integra sistemas como relés de proteção, medidores, dispositivos de controle e sistemas SCADA, otimizando a gestão de falhas e o monitoramento remoto. Além disso, a arquitetura deve ser resiliente e segura, com redundância e proteção contra ameaças cibernéticas. A solução também possibilita a análise de dados para decisões mais rápidas e precisas, melhorando a confiabilidade e a eficiência do sistema elétrico.

A solução de automação de subestações padronizada pela Cemig D é aderente à norma IEC61850 e disponibiliza acesso a serviços como:

- Supervisão e controle remoto através do COD;
- Acesso remoto às oscilografias dos IEDs de proteção;
- Acesso remoto aos dados de medição de perdas e consumo próprio da subestação;
- Acesso remoto aos IEDs para verificação e alteração de parâmetros;
- Acesso remoto a dados de telemetria para monitoramento de ativos;
- Monitoramento em tempo real da rede de automação.

A solução de Automação adotada pela Cemig D apresenta uma segregação entre os dispositivos com funções distintas, sendo configuradas inclusive VLANs distintas para cada tipo de serviço, deixando a rede mais segura e eficiente.

Entre as diferentes redes configuradas nas subestações da Cemig D, a rede de proteção e controle, que conecta os relés de proteção, recebe uma atenção especial, sendo a única rede configurada com redundância em uma topologia em dupla estrela, conferindo uma maior confiabilidade, disponibilidade e resiliência, devido a sua importância na solução.

Para prover acesso total aos serviços previstos, o link de comunicação da subestação exerce função primordial, devendo prover segurança, alta disponibilidade e possuir banda dimensionada para trafegar todos os serviços previstos.

A figura 1 apresenta um croqui de uma rede de automação típica de uma subestação construída pela Cemig D.

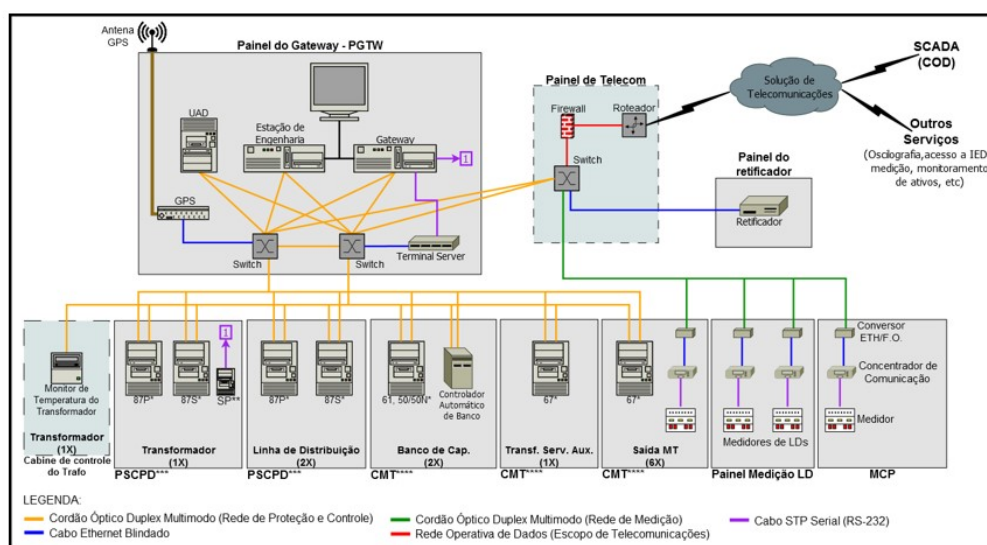


Figura 1: Arquitetura de rede típica de uma subestação da Cemig D.

2.3 Desafios e requisitos de segurança cibernética para acesso remoto aos serviços providos pelo sistema de automação de subestações

Com a adoção de soluções baseadas em redes Ethernet para conectar os serviços oferecidos pela solução de automação de subestações, foi necessário a Cemig D considerar os requisitos de cibersegurança na operação de suas instalações.

A segurança cibernética para acesso remoto às redes de automação de subestações de energia enfrenta uma série de desafios, principalmente devido à natureza crítica e sensível da infraestrutura elétrica. Uma das principais dificuldades é garantir que os sistemas de automação, que operam em tempo real, estejam protegidos contra acessos não autorizados, enquanto ainda permitem intervenções e monitoramentos remotos. A ameaça de ataques cibernéticos, que representam uma preocupação constante em sistemas de missão crítica, torna a implementação de uma segurança robusta ainda mais crucial.

Um requisito fundamental para garantir a segurança cibernética em redes operativas é sua completa separação das redes corporativas, impedindo qualquer contato direto da rede operativa com a internet. Além disso, os acessos diretos às redes operativas devem ser altamente restritos, rastreáveis e realizados a partir de ambientes seguros. Nesse contexto, a segmentação de rede, o uso de firewalls e outras soluções de controle de tráfego são essenciais para isolar os sistemas críticos das subestações de outras partes da rede e impedir acessos indevidos.

Existem ainda desafios relacionados à implementação de atualizações e patches de segurança em tempo hábil. A infraestrutura de automação é frequentemente composta por dispositivos e sistemas com variados ciclos de vida e que, muitas vezes, não são projetados para se atualizar automaticamente. Isso exige que as equipes de automação monitorem continuamente as vulnerabilidades e implementem atualizações de forma controlada para evitar interrupções nos serviços, sem comprometer a segurança.

Diante dos desafios e requisitos determinados pelas necessidades de segurança cibernética, as equipes de automação da Cemig D se viram diante de um problema: como prover acesso remoto aos serviços da solução de automação de subestações para as equipes de operação, pós operação, proteção, medição, gestão de ativos etc. sem comprometer os requisitos de segurança cibernética?

2.4 Solução para acesso aos serviços da rede operativa da Cemig D

Para atender os requisitos de segurança cibernética da rede operativa e prover acesso aos dados das subestações para os usuários da rede corporativa, a Cemig D criou uma zona desmilitarizada (DMZ), onde fica instalado um servidor de proxy reverso, que é responsável por fazer a ponte entre os usuários da rede corporativa e os servidores das aplicações instalados na rede operativa, conforme ilustrado na arquitetura de rede apresentada na figura 2.

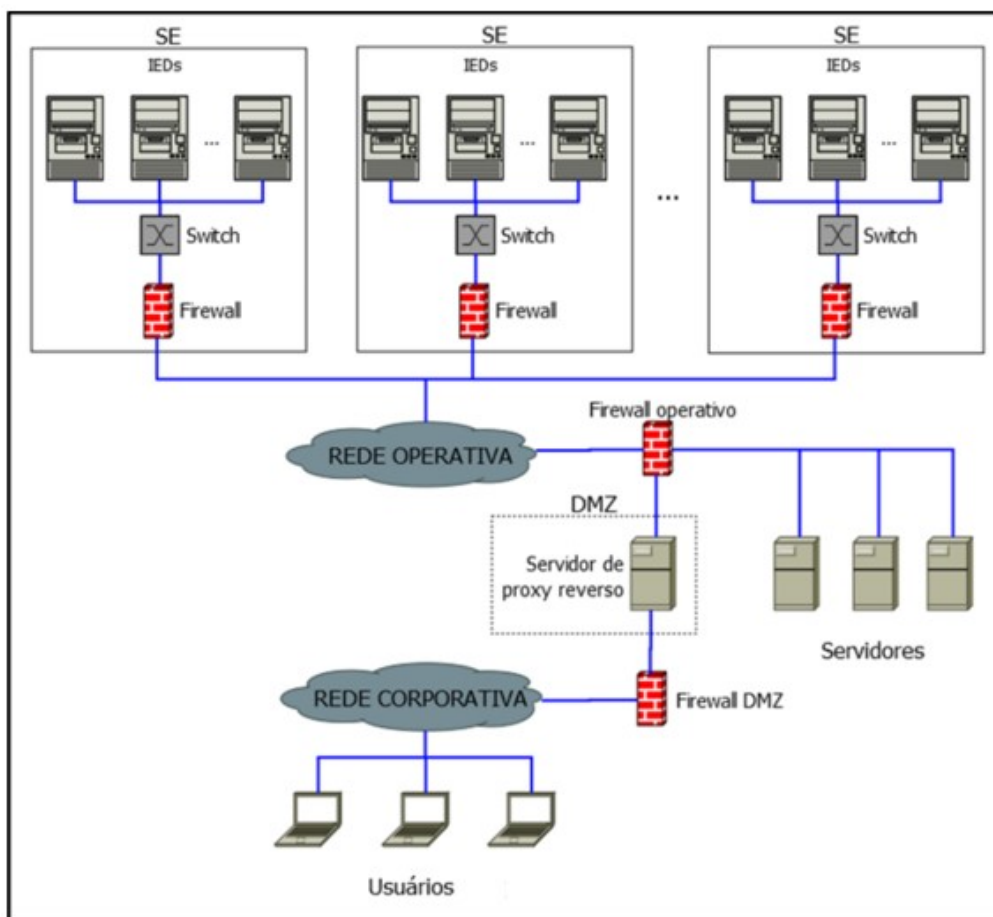


Figura 2: Arquitetura básica da solução de integração dos serviços da rede operativa na rede corporativa. A segregação entre a rede operativa e a rede corporativa é uma prática essencial para garantir a segurança e a integridade dos sistemas de automação. Para isso, é necessária a utilização de uma arquitetura DMZ, que atua como uma camada intermediária entre as redes internas e externas, isolando as redes operativas dos acessos externos ou corporativos. Na DMZ, são instalados servidores e dispositivos que precisam de comunicação com a rede externa, mas sem comprometer a segurança da rede interna. Dessa forma, mesmo que um dispositivo na DMZ seja comprometido, a rede operativa permanece protegida.

Além da DMZ, o uso de um servidor de proxy reverso é uma técnica complementar que contribui para a segurança da segregação. O proxy reverso atua como intermediário entre os clientes externos e os servidores internos, garantindo que as requisições externas sejam filtradas e que o tráfego malicioso seja bloqueado antes de alcançar os sistemas sensíveis. Essa solução não apenas melhora a segurança, como também aumenta a eficiência na gestão do tráfego de dados, pois o proxy pode realizar cache de conteúdos estáticos e reduzir a carga sobre os servidores internos. Ao colocar o servidor de proxy reverso na DMZ, a rede operativa ganha uma camada adicional de proteção contra ataques cibernéticos diretos.

Essa solução de segregação, com a combinação da DMZ e do servidor de proxy reverso, oferece uma série de benefícios para as redes de automação. Ela assegura a integridade e a disponibilidade dos sistemas operativos, minimizando os riscos de acessos não autorizados ou de ataques cibernéticos. A segregação também facilita o monitoramento e a auditoria, uma vez que o tráfego entre as redes operativas e corporativas pode ser mais facilmente controlado e analisado. Dessa forma, a implementação dessa arquitetura não só aprimora a segurança cibernética, mas também garante maior resiliência e estabilidade para as operações críticas de energia.

O SINAPE, sistema de coleta e análise de oscilografias desenvolvido pelo CEPEL e o Sigma, plataforma computacional para gestão de transformadores desenvolvido pela Treotech, ilustrados na figura 3 correspondem a duas aplicações implementadas pela Cemig D.

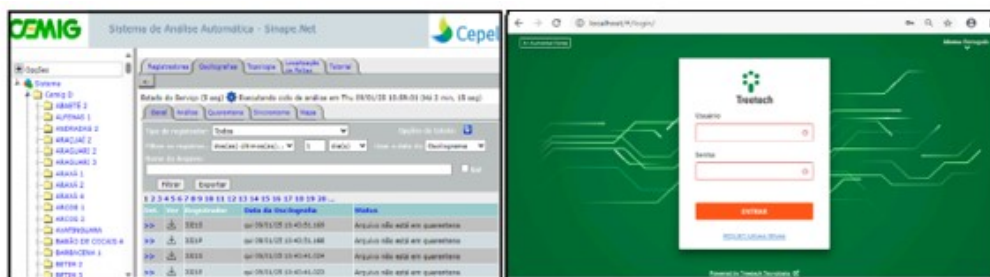


Figura 3: Sinape e Sigma - aplicações de apoio às equipes de operação, manutenção e engenharia

O SINAPE.Net é uma ferramenta web desenvolvido para auxiliar análise de oscilografias em linhas de transmissão e distribuição. Ele realiza análises automáticas de distúrbios e disponibiliza a localização georreferenciada de faltas. Além disso, permite análises manuais e possibilita o download dos arquivos para análise em outras plataformas. Embora focado em linhas de transmissão/distribuição, o SINAPE.Net também gerencia arquivos de outros equipamentos, como transformadores e disjuntores, oferecendo pesquisa e download de dados. Atualmente, o SINAPE.Net é utilizado na Cemig D para gerenciar arquivos de oscilografias em mais de 120 subestações.

Sigma é uma plataforma de TI, desenvolvida em ambiente web, para a gestão de ativos em concessionárias de energia elétrica, incorporando as filosofias de Smart Grid e IoT. Ela automatiza processos essenciais como manutenção preditiva, preventiva e corretiva, e faz a gestão de recursos humanos e materiais [5]. Atualmente, a Cemig D utiliza o Sigma para gestão de transformadores com potência de 40 MVA instalados em subestações estratégicas.

2.5 Desafios para a automação da Cemig D

Apesar da construção de uma solução de acesso seguro a serviços da rede operativa existem serviços, como o acesso remoto aos relés digitais de proteção para consulta e ajuste de parâmetros, que exigem um controle ainda maior para manter a rede operativa inviolável e segura. Dentre os desafios que a automação da Cemig D precisa superar, destaca-se a implementação de uma ferramenta capaz de gerenciar todas as ações dos usuários enquanto navegam pela rede operativa, possibilitando a realização de auditorias em todas as atividades realizadas, além de possibilitar o controle de acesso, logs das atividades realizadas e gestão de senha dos dispositivos.

Outro desenvolvimento necessário é o monitoramento completo da rede de automação. Apesar de construir redes resilientes, com redundâncias, ainda não foi implementado um sistema robusto capaz de identificar as falhas e mau funcionamento de parte da rede e emitir alertas para as equipes de manutenção, antes que essas falhas impactem o correto funcionamento da solução de automação. Algumas iniciativas pontuais de monitoramento e testes pilotos foram realizados, mas há necessidade de uma solução completa para todas as instalações.

Apesar de compartilharem a mesma tecnologia de redes ethernet, as redes operativa e corporativa devem ser tratadas de maneira distinta e, portanto, é recomendável que a equipe responsável por operar e manter a rede operativa seja distinta da equipe responsável pela rede corporativa. A rede operativa, responsável pelo controle e automação de sistemas críticos, exige alta disponibilidade e extrema confiabilidade, com a manutenção focada em garantir a continuidade do serviço e minimizar falhas. Ela costuma ser mais rígida e isolada, com atualizações e ajustes realizados com cautela para evitar impactos no desempenho. Já a rede corporativa, voltada para as operações empresariais gerais, como e-mails e sistemas administrativos, tem

maior flexibilidade e está sujeita a alterações frequentes, com foco em produtividade e colaboração. Sua manutenção envolve gestão de dados, backups, segurança de acesso e atualizações periódicas, sem a urgência de uma rede operativa, mas com ênfase na proteção contra ameaças cibernéticas. Ambas exigem monitoramento, mas a rede operativa exige vigilância constante e em tempo real, enquanto a corporativa é mais flexível e voltada para a gestão de dados e desempenho organizacional. Nesse contexto, é necessário o desenvolvimento de uma equipe de automação dedicada por atuar no nível de tecnologia de informação voltada para as aplicações da rede operativa.

3. Conclusão

A implementação de soluções de acesso seguro aos serviços da rede operativa da Cemig D, com o uso de uma arquitetura de DMZ e servidores de proxy reverso, tem sido fundamental para garantir a integridade e a segurança da infraestrutura de automação das subestações. Essa abordagem proporciona a segregação necessária entre as redes operativa e corporativa, permitindo o acesso remoto a dados e serviços sem comprometer a proteção dos sistemas críticos. A utilização dessa arquitetura avançada fortalece a segurança cibernética, minimizando riscos e permitindo a comunicação segura e eficiente entre as equipes operacionais e os sistemas de controle e supervisão das subestações.

No entanto, apesar dos avanços na segurança e na infraestrutura de automação, a Cemig D ainda enfrenta desafios significativos. A necessidade de controle rigoroso sobre o acesso aos relés digitais de proteção, bem como a gestão eficiente dos usuários e suas ações na rede operativa, exige o desenvolvimento de ferramentas adicionais de monitoramento e auditoria. A implementação de soluções que permitam um rastreamento detalhado das atividades, controle de acessos e gestão de senhas se apresenta como um passo crucial para garantir a inviolabilidade da rede operativa. Esses desafios exigem um investimento contínuo em tecnologia e processos para garantir a continuidade e a segurança das operações.

Um dos principais desafios que a Cemig D precisa superar é o monitoramento proativo da rede de automação. Embora a infraestrutura seja projetada com redundâncias e alta disponibilidade, a falta de um sistema automatizado para detectar falhas antes que afetem o desempenho geral da solução de automação é uma lacuna significativa. O desenvolvimento de um sistema robusto para identificar falhas e emitir alertas antecipados é essencial para garantir a resiliência da rede operativa. A adaptação da equipe de automação para atuar com foco nas particularidades da rede operativa, separada da rede corporativa, também será crucial para enfrentar os desafios operacionais e manter a segurança e a eficiência da infraestrutura a longo prazo.

4. Referências bibliográficas

- [1] CEMIG DISTRIBUIÇÃO. *Plano Diretor Integrado de Automação e Telecomunicação*. Belo Horizonte: Cemig Distribuição, 2016. Documento Interno.
- [2] BRANQUINHO, M.; LEAL, R. *Perigos do acesso remoto a sistemas de controle industriais*. O Setor Elétrico, Edição 187, Fascículo: Segurança Cibernética, p. 28-32, jun. 2022. Disponível em: https://www.os-etoreletrico.com.br/wp-content/uploads/2022/06/Edicao-187_fasciculo-seguranca-cibernetica.pdf. Acesso em: 20 jan. 2025.

- [3] Murta, Marisa Lages; Ribeiro, Fernando Moreira; Soares, Paulo César, “*Sistema de Automação para Subestações Compactas Integradas (SECI) da Cemig Distribuição*” (XXIII Seminário Nacional de Distribuição de Energia Elétrica – SENDI – 2018).
- [4] Murta, Marisa Lages; Ribeiro, Fernando Moreira; Dutra, Rafael Douglas Costa, “*Implantação da Solução de Coleta e Análise Automática de Oscilografias para Subestações da Cemig Distribuição*” (XXIV Seminário Nacional de Distribuição de Energia Elétrica – SENDI – 2023).
- [5] TREETECH. Sigma EAM. Treetech, [s.d.]. Disponível em: <https://www.treetech.com.br/sigma-eam/>. Acesso em: 20 jan. 2025.
- [6] BRANQUINHO, Thiago; BRANQUINHO, Marcelo. *Segurança Cibernética Industrial: As Infraestruturas Críticas Mundiais Correm Perigo. Aprenda a Proteger Redes e Sistemas de Controle com uma Metodologia Comprovada na Prática*. Rio de Janeiro: Alta Books, 2021.
- [7] DUTRA, Rafael Douglas Costa. *O PROCESSO DE DIGITALIZAÇÃO DE UMA SUBESTAÇÃO DA DISTRIBUIÇÃO UTILIZANDO O SISTEMA “SCADA”*. 2016. Trabalho de Conclusão de Curso (Bacharelado em Engenharia Elétrica) – Pontifícia Universidade Católica de Minas Gerais, Belo Horizonte, 2023.