UNIVERSIDADE FEDERAL DE ITAJUBÁ

PROGRAMA DE PÓS-GRADUAÇÃO EM ENGENHARIA ELÉTRICA

Proposta de Integração Segura de Redes entre Agentes de Transmissão, Aplicadas no sistema Especial de Potência N/NE/SE para Mitigação de Vulnerabilidades das Mensagens GOOSE

Neemias Werneck Ferreira

Rio de Janeiro, março de 2025

UNIVERSIDADE FEDERAL DE ITAJUBÁ
PROGRAMA DE PÓS-GRADUAÇÃO EM ENGENHARIA ELÉTRICA

Neemias Werneck Ferreira

Proposta de Integração Segura de Redes entre Agentes de Transmissão, Aplicadas no sistema Especial de Potência N/NE/SE para Mitigação de Vulnerabilidades das Mensagens GOOSE

Dissertação submetida ao Programa de Pós-Graduação em Engenharia Elétrica como parte dos requisitos para obtenção do Título de Mestre em Ciências em Engenharia Elétrica.

Área de Concentração: Sistemas Elétricos de Potência

Orientador: Prof. Dr. Paulo Márcio da Silveira
Coorientador: Prof. Dr. Carlos A. Villegas Guerrero

Março de 2025
Rio de Janeiro

Agradecimentos

Chegar até aqui foi uma jornada desafiadora, mas também de grande aprendizado e crescimento. Essa conquista não é apenas minha, mas também daqueles que, direta ou indiretamente, contribuíram para que este momento fosse possível. Expresso minha mais profunda gratidão a todos que fizeram parte dessa caminhada.

Agradeço aos meus gestores da empresa onde trabalho, por me proporcionarem a oportunidade de atuar em um projeto de grande importância para o setor elétrico brasileiro. A experiência adquirida e o apoio recebido foram fundamentais para o meu crescimento profissional e acadêmico.

Aos meus orientadores, Paulo Márcio e Carlos Villegas, minha sincera gratidão pela paciência, dedicação e pelos valiosos ensinamentos compartilhados ao longo desta jornada. Suas orientações foram essenciais para que este trabalho alcançasse o nível desejado.

Aos meus pais, que me ensinaram desde cedo o valor da honestidade, do caráter e do trabalho árduo. Tudo que sou hoje reflete os princípios e a educação que recebi de vocês.

À minha irmã, por ser uma fonte constante de motivação e incentivo, sempre me desafiando a ir além e a dar o meu melhor em tudo que faço.

Ao meu avô, que, embora não esteja mais presente fisicamente, continua sendo uma grande inspiração em minha vida. Sei que ele ficaria imensamente orgulhoso desta conquista.

À minha esposa, Marcela, minha companheira em todos os momentos, que esteve ao meu lado com amor, paciência e apoio incondicional. Seu incentivo e sua presença tornaram essa caminhada mais leve e significativa.

E, acima de tudo, agradeço a Deus, pois sei que tudo vem Dele e tudo é para a Sua glória. Sem Ele, nada disso seria possível.

"Portanto, quer comais, quer bebais ou façais qualquer outra coisa, fazei tudo para a glória de Deus." 1 Coríntios 10:31

Resumo

O presente trabalho teve como objetivo propor uma metodologia para integração segura de redes de comunicação entre agentes de transmissão, aplicada a um Sistema Especial de Proteção (SEP), para mitigação de vulnerabilidades das mensagens GOOSE, utilizando a norma IEC 61850. A metodologia combinou pesquisa documental e análise qualitativa de propostas de quatro fornecedores, sendo a proposta mais aderente às especificações estabelecidas a avaliada através de testes de Prova de Conceito (PoC), e cujos resultados nortearam a metodologia sugerida neste trabalho.

Os resultados dos testes de PoC validaram a arquitetura que propõe switches SDN (*Software-Defined Networking*) para garantir segurança e desempenho na comunicação entre agentes distintos no SEP. Quatro testes principais foram conduzidos: filtragem de mensagens por MAC, Ethertype e VLAN; limitação de banda; desabilitação de portas físicas e lógicas; e medição do tempo de transmissão. Os resultados indicaram que a solução atende aos requisitos de segurança e desempenho, mantendo os tempos de transmissão dentro dos limites aceitáveis estabelecidos pela norma IEC 61850.

Apesar da eficácia da arquitetura escolhida, sugere-se uma investigação sobre o tipo de criptografia aplicada nas mensagens GOOSE. Estudos recentes revelaram que o algoritmo RSA, recomendado pela norma IEC 62351, não atende aos requisitos de latência de 3 ms devido à sua alta complexidade computacional. Como alternativa, sugere-se investigar o algoritmo de criptografia simétrica AES (*Advanced Encryption Standard*) com a técnica CMAC (*Cipher-based Message Authentication Code*), que demonstra ser capaz de atender às restrições de tempo da IEC 61850 com desempenho superior ao RSA.

A pesquisa contribui significativamente para o avanço da segurança cibernética e da comunicação eficiente em redes de transmissão de energia elétrica em uma aplicação de SEP real, oferecendo uma solução prática e viável para mitigar vulnerabilidades e garantir a integridade e autenticidade das mensagens GOOSE na comunicação entre agentes distintos. A implementação das melhorias propostas pode fortalecer ainda mais a infraestrutura de comunicação do SEP, assegurando um desempenho otimizado e uma operação segura e confiável.

Palavras-Chaves: Segurança Cibernética; Comunicação IEC 61850; Mensagens GOOSE; Criptografia AES; Redes SDN.

Abstract

The present work aimed to propose a methodology for the secure integration of communication networks between transmission agents, applied to a Special Protection System (SPS), to mitigate vulnerabilities of GOOSE messages, using the IEC 61850 standard. The methodology combined documentary research and qualitative analysis of proposals from four suppliers, with the most adherent proposal to the established specifications being evaluated through Proof of Concept (PoC) tests, and whose results guided the methodology suggested in this work.

The PoC test results validated the architecture that proposes SDN (Software-Defined Networking) switches to ensure security and performance in communication between different agents in the SPS. Four main tests were conducted: message filtering by MAC, Ethertype, and VLAN; bandwidth limitation; disabling physical and logical ports; and transmission time measurement. The results indicated that the solution meets security and performance requirements, keeping transmission times within acceptable limits established by the IEC 61850 standard.

Despite the effectiveness of the chosen architecture, an opportunity for improvement in the encryption of GOOSE messages was identified. Recent studies revealed that the RSA algorithm, recommended by the IEC 62351 standard, does not meet the 3 ms latency requirements due to its high computational complexity. As an alternative, the adoption of the AES (Advanced Encryption Standard) algorithm with the CMAC (Cipher-based Message Authentication Code) technique was suggested, which demonstrates the ability to meet the time constraints of IEC 61850 with superior performance to RSA.

In conclusion, the research significantly contributes to the advancement of cybersecurity and efficient communication in power transmission networks in a real SPS application, offering a practical and viable solution to mitigate vulnerabilities and ensure the integrity and authenticity of GOOSE messages in communication between different agents. The implementation of the proposed improvements can further strengthen the SPS communication infrastructure, ensuring optimized performance and secure and reliable operation.

Keywords: Cybersecurity; IEC 61850 Communication; GOOSE Messages; AES Encryption; SDN Networks.

Lista de Figuras

Lista de Tabelas

Lista de Siglas e Abreviaturas

ABRATE - Associação Brasileira das Empresas de Transmissão de Energia Elétrica

AES - *Advanced Encryption Standard*

ANATEL - Agência Nacional de Telecomunicações

ANEEL - Agência Nacional de Energia Elétrica

CIP - *Critical Infrastructure Protection*

CMAC - *Cipher-based Message Authentication Code*

DACU - *Data Acquisition and Control Unit*

ENISA - *European Network and Information Security Agency*

GOOSE - *Generic Object Oriented Substation Event*

GSI - Gabinete de Segurança Institucional

HSR - *High-availability Seamless Redundancy*

IED - *Intelligent Electronic Device*

IDS - *Intrusion Detection System*

IEC - *International Electrotechnical Commission*

LAN - *Local Area Network*

MMS - *Manufacturing Message Specification*

NERC - *North American Electric Reliability Corporation*

NIST - *National Institute of Standards and Technology*

NIS - *Network and Information Security*

ONS - Operador Nacional do Sistema Elétrico

PAC - *Protection, Automation and Control*

PRP - *Parallel Redundancy Protocol*

PTP - *Precision Time Protocol*

RADIUS - *Remote Authentication Dial-In User Service*

SEB - Setor Elétrico Brasileiro

SDN - *Software Defined Networking*

SNTP - *Simple Network Time Protocol*

SV - *Sampled Values*

TACACS - *Terminal Access Controller Access-Control System*

VLAN - *Virtual Local Area Network*

Sumário

1 Capítulo 1 - Introdução

1.1 Considerações iniciais

A força motivadora desta pesquisa se refere ao fato de que há um interesse latente em obter maior robustez em segurança cibernética. No mundo, proliferam os casos de ataques cibernéticos às infraestruturas críticas, em particular às redes de energia elétrica. Como rede sociotécnica catalizadora de muitos outros domínios da sociedade, o setor elétrico destaca-se não apenas por sua vulnerabilidade e exposição, mas principalmente pela extensão dos possíveis danos que ataques cibernéticos podem causar, amplificados pela capilaridade com outros setores críticos da sociedade [1].

As infraestruturas críticas de uma nação incluem diversos setores, entre eles, o sistema elétrico desempenha um papel catalizador ao transmitir e distribuir um insumo essencial aos demais setores de infraestrutura. Simultaneamente, o setor elétrico depende de outros setores para o fornecimento de insumos energéticos (água, óleo, gás, diesel, carvão etc.), além de informações e meios de comunicação, finanças e outros. Assim, a segurança cibernética do setor elétrico depende não apenas de sua exposição própria aos ataques, mas de sua extensão e integração continental, bem como interdependência com os demais setores críticos [2].

No Brasil, entre 2018 e 2021 foram realizados diversos trabalhos de pesquisas e debates entre várias empresas relacionadas com o tema segurança cibernética do setor de energia e de infraestruturas críticas em geral. Destacam-se os realizados pelo Gabinete de Segurança Institucional (GSI), Operador Nacional do Sistema Elétrico (ONS), Agência Nacional de Energia Elétrica (ANEEL), Agência Nacional de Telecomunicações (ANATEL), e Associação Brasileira das Empresas de Transmissão de Energia Elétrica (ABRATE) entre outros, contendo pesquisas também sobre o tema segurança cibernética das infraestruturas críticas. No segmento governo alguns decretos têm muita relevância no atual estágio da regulação de segurança cibernética do Setor Elétrico Brasileiro (SEB) [3].

A ANEEL, seguindo a agenda regulatória, atendendo a solicitação do ONS, que gerou o processo ANEEL 48500-000027_2020-40, publicou a Nota Técnica 50/2020 que abriu a Tomada de Subsídios (TS) 007/2020, em 25/05/2020, com a finalidade de obter contribuições para a regulamentação associada à segurança cibernética do SEB. A Nota Técnica contém uma pesquisa sobre, dentre outros assuntos, os padrões e as melhores práticas de gerenciamento de

segurança, normas e padrões utilizados pelas empresas do setor: agentes, prestadores de serviços e fornecedores no brasil e no exterior [2].

A Rotina Operacional RO-CB.BR.01 e a Resolução 964/2021 [3] da ANEEL foram emitidas com base em um conjunto de padrões utilizado pelo ONS, compatíveis com boas práticas utilizadas internacionalmente. Estratégias, diretrizes, estrutura de governança e controles de segurança cibernética aplicáveis serão avaliados no ambiente em que se situa o Setor Elétrico Brasileiro, como parte das redes de infraestruturas críticas do país [3].

A segurança cibernética no Brasil pode ser avaliada como parte da Estratégia Nacional de Transformação Digital, que objetiva modernizar os setores sociais e produtivos do país, através da automação e da digitalização dos processos. Com a digitalização do setor elétrico, baseada na norma IEC 61850, os meios de comunicação para sua operação e gestão aumentam as superfícies de ataque com as vulnerabilidades próprias destes domínios [4].

A norma IEC 61850 globalmente organiza o fluxo de informações em Subestações de Energia (SE), definindo uma classe comum de dados que permite uma semântica padronizada. As informações podem ser construídas, processadas e transmitidas vertical ou horizontalmente [5].

A comunicação vertical, do tipo servidor-cliente, que conectam equipamentos ao sistema de supervisão e aquisição de dados, é implementada utilizando o protocolo MMS (*Manufacturing Message Specification*) [2]. O mecanismo *multicast*, aplicado para troca de comunicações horizontais entre IEDs (*Intelligent Electronic Devices*) é definido através do protocolo GOOSE (*Generic Object Oriented Substation Event*) [1].

As mensagens do tipo GOOSE destinam-se a trafegar dentro da camada de enlace de dados do modelo *Open Systems Interconnection* (OSI) e sua implementação é descrita na IEC 61850-8-1 [6]. Os pré-requisitos de alto desempenho para troca de mensagens entre IEDs exigem a abstração de processos de segurança, como autenticação do publicador e criptografia de mensagens. Técnicas de ataque, como saturação de rede ou manipulação de quadro Ethernet, podem ser postas para explorar essa vulnerabilidade e impedir que a SE se comporte de forma adequada [6].

A técnica de saturação de rede consiste em cobrir em abundância a rede com mensagens GOOSE que contenham o mesmo significado do publicador. Isso impossibilita o processamento adequado das mensagens reais remetidas pelo editor ao dispositivo assinante. O objetivo da técnica de manipulação do quadro Ethernet é reconhecer mensagens GOOSE e

modificar o valor dos dados das mensagens, fazendo com que o dispositivo assinante descarte as mensagens genuínas subsequentes do dispositivo publicador, ou faça com que o dispositivo assinante se comporte de maneira diferente e injustificada [6].

Observa-se que as melhores práticas de configuração de rede são postas para mitigar essas e outras formas de ataques que podem ocorrer em subestações de energia, essas práticas usam a implementação adequada de *Virtual Local Area Network* (VLANs), bloqueio de portas não utilizadas e novas tecnologias de gerenciamento ou controle de fluxo dos dados, tais como *Software Defined Networking* (SDN) [7].

O Sistema Especial de Proteção (SEP) está intimamente relacionado ao funcionamento do sistema elétrico de potência, pois evita o colapso de uma parte do sistema elétrico ou de todo o sistema. Desta forma, o SEP permite otimizar o funcionamento dos sistemas elétricos, permitindo um maior aproveitamento das redes de transporte, acrescentando maiores níveis de segurança operacional e permitindo uma utilização mais econômica da rede elétrica. Com isso, SEPs destinados ao controle da estabilidade transitória apresentam requisitos especiais de tempo de atuação, pois estão associados a fenômenos mais rápidos, os quais, em alguns casos, são capazes de gerar a perda de estabilidade do sistema [8].

Em junho de 2021, o ONS divulgou a implementação de um novo SEP para a interligação Norte-Nordeste-Sudeste (N/NE/SE). Devido aos importantes reforços da rede de transmissão em corrente alternada das interligações N/NE/SE para permitir o escoamento da geração na região Norte e dos parques eólicos na região Nordeste, uma reavaliação completa do SEP inicial na interligação N-SE era necessária. Espontaneamente, este SEP tem a necessidade de comunicações com vários agentes. Para tal, tem-se como expectativa que o atraso entre IED local de origem e IED local de destino (passando pela Master) mais o tempo de disjuntor e dos equipamentos e enlaces *Wide Area Network* (WAN), não ultrapasse um total de 100 ms [7].

No presente estudo de caso, busca-se propor melhor desempenho na proteção contra-ataques cibernéticos na comunicação entre IEDs de agentes distintos. Para tanto, será investigada a vulnerabilidade na troca das mensagens GOOSE, avaliando várias arquiteturas. Com base na arquitetura selecionada, será investigado o potencial de mitigação de vulnerabilidades do GOOSE entre agentes, a fim de minimizar a suscetibilidade de falha em uma das infraestruturas críticas brasileira, em especial as subestações [9].

A empresa em estudo é um dos maiores grupos privados de transmissão de energia elétrica do Brasil, exclusivamente dedicada à construção, operação e manutenção de ativos de transmissão, com 13.211 km de linhas em operação e 1.918 km de linhas em construção, totalizando 15.129 km de extensão e 104 subestações. Além disso, possui ativos em operação com nível de tensão entre 230 e 525 kV. A empresa aqui abordada receberá o nome fictício de "Delta" com o objetivo de preservar a confidencialidade dos seus dados.

1.2 Descrição do problema

As subestações digitais são projetadas com base nas diretrizes da IEC 61850 para automatização de sistemas elétricos. Na qual possui os princípios de interoperabilidade entre os IEDs, o que possibilita a comunicação entre os dispositivos de diversos fabricantes que fazem parte dos sistemas de monitoramento, proteção e controle de uma subestação elétrica, com desempenho garantido durante o processo de troca de informações [5].

A interoperabilidade definida pela IEC 61850 tem por padrão os protocolos de comunicação MMS, GOOSE e SV (*Sampled Values*). Além disso, conforme estabelecido na IEC 61850, a redundância de mensagens via protocolos PRP (*Parallel Redundancy Protocol*) e HSR (*High-availability Seamless Redundancy*) busca atender ao requisito de disponibilidade da rede, já no que tange a requisitos de sincronização de tempo recomendam-se os protocolos SNPT (*Simple Network Time Protocol*) e PTP (*Precision Time Protocol*) do padrão IEEE 1588 [6].

Na comunicação horizontal, entre agentes interconectados, utiliza-se o protocolo GOOSE que influencia diretamente no comportamento da subestação (SE). Contudo, as mensagens do tipo GOOSE e SV não implementam nenhuma característica de segurança a nível de enlace nas suas transmissões *multicast*. A performance das mensagens GOOSE estão descritas na IEC 61850-5 [4] e são enquadradas nos tipos 1 e 1A. As mensagens do tipo 1 (Mensagens Rápidas), geralmente contém um conteúdo binário, mas pode ter um valor analógico. As mensagens do tipo 1A são mensagens críticas em uma subestação cujo requisito de desempenho exige uma transmissão na ordem de 3 ms no caso mais crítico [7].

A latência introduzida pela criptografia e autenticação de mensagens é o principal impedimento para implementação dessas técnicas a nível de enlace. A norma IEC 62351 define os métodos computacionais de baixo consumo, mas não é suficiente para atender aos pré-requisitos de desempenho impostos pela IEC 61850-5 [4]. Essas mensagens não podem ser

processadas usando métodos de segurança em nível de quadro (criptografia e autenticação de mensagens). Consequentemente, as mensagens GOOSE são inerentemente vulneráveis [10].

Portanto, para mitigar a suscetibilidade nas mensagens GOOSE, o presente trabalho de dissertação busca verificar e analisar uma tecnologia que possibilite às subestações digitais terem maior segurança cibernética, sem impactar na performance gerada quando aplicada a norma IEC 61850.

1.3 Justificativa

A proposta de integração segura de redes entre agentes de transmissão, aplicadas no sistema especial de potência N/NE/SE, para mitigação de vulnerabilidades das mensagens GOOSE, surge em um contexto em que os ciberataques estão mais frequentes e desenvolvidos, compenetrado nas fragilidades dos sistemas. A segurança na comunicação entre os agentes é uma das garantias na manutenção das operações em SEs [7].

Desta forma, medir, analisar e controlar a suscetibilidade no transporte das mensagens GOOSE é imprescindível para preservação do desempenho das redes de infraestrutura críticas de um país. O SEP, além de otimizar o funcionamento dos sistemas elétricos e potencializar o aproveitamento das redes de transporte, aumenta os níveis de segurança operacional [8].

Com a aplicação no SEP N/NE/SE, espera-se uma atenuação significativa na vulnerabilidade da comunicação GOOSE, resultando em melhores níveis desempenho. Isso permitirá que a norma IEC 61850 seja aplicada de forma eficiente, proporcionando mecanismos que garantam uma troca de informações mais segura e confiável entre um ou mais IEDs [7].

Este trabalho se restringe em analisar dados – propostas de arquiteturas de vários fabricantes, parecer da prova de conceito e especificações de implantação do SEP N/NE/SE – coletados por um dos agentes envolvidos no referido SEP.

O escopo em análise enquadra a investigação de ciberataque e proposta de segurança no nível 1 (rede de processos), com interface aos níveis 0 e 2, conforme arquitetura cibernética do setor elétrico. A pesquisa almeja de forma mais objetiva, analisar o comportamento da aplicação da comunicação GOOSE para aplicação no sistema especial de proteção N/NE/SE.

1.4 Objetivos

1.4.1 Objetivo geral

Propor uma estratégia de integração segura de redes de comunicação que mitigue a vulnerabilidade das mensagens GOOSE, de acordo com as boas práticas e regulamentos associados à norma IEC 61850, para interface entre agentes de transmissão na implantação do Sistema Especial de Proteção N/NE/SE no SIN.

1.4.2 Objetivos específicos

Têm-se como objetivos específicos os tópicos descritos abaixo:

a) Investigar infraestruturas críticas nacionais e do Setor Elétrico Brasileiro no contexto da Segurança Cibernética;

b) Entender o contexto das subestações digitais, e os requisitos das normas IEC 61850 e IEC 62351;

c) Estudar os conceitos de ataques cibernéticos, riscos e arquitetura do SEP N/NE/SE;

d) Avaliar várias filosofias de arquiteturas de rede propostas por diferentes fabricantes para integração segura entre agentes no SEP N/NE/SE;

e) Analisar o desempenho da melhor arquitetura através de ensaios em laboratório (Prova de Conceito);

f) Determinação de uma proposta de rede que possa ser utilizada para segurança cibernética em subestações digitais, em especial integração segura de redes para interface entre agentes de transmissão mitigação de vulnerabilidades das mensagens GOOSE.

1.5 Estrutura metodológica

Esta pesquisa é de natureza quantitativa e descritiva, tendo como principais características o levantamento e a justificativa dos dados sobre o objeto em estudo [11]. A abordagem quantitativa utilizada nesta pesquisa deve-se à mensuração numérica, classificação e análise com base em dados, ao utilizar a ferramenta *Wireshark* [12].

O Estudo de Caso é o método mais adequado a essa pesquisa, pois segundo Yin [13],

> *"estudo de caso é um modo de se investigar um fenômeno empírico seguindo um conjunto de procedimentos pré-especificados e que pode ser utilizado".*

O foco desta pesquisa é direcionado na situação presente, ou seja, à forma como a empresa Delta mensura e integra de forma segura as redes entre agentes de transmissão. Além disso, o estudo de caso é indicado quando se torna necessário compreender algo mais profundo sobre determinado tema pouco explorado, como é pretendido pela estratégia proposta do SEP N/NE/SE para mitigação da vulnerabilidade das mensagens GOOSE.

Para o desenvolvimento do trabalho foi realizada uma ampla pesquisa bibliográfica sobre os itens pertencentes ao assunto em apostilas, livros, normas, projetos e artigos, tanto nacionais como internacionais, a fim de reunir informações relevantes ao tema, além do conhecimento de profissionais atuantes nas áreas de estudos, subestações digitais, infraestruturas críticas, segurança cibernética e requisitos da IEC 61850.

1.6 Organização do trabalho

Essa dissertação está dividida em cinco capítulos. O primeiro é a introdução, composta pelas considerações iniciais, descrição do problema, justificativa, objetivos, estrutura metodológica e organização da pesquisa.

No segundo capítulo é abordada a revisão da literatura, para auxiliar nos estudos teóricos sobre o tema, como os conceitos relacionado a segurança cibernética e suas tecnologias, e as especificações da IEC 61850 e IEC 62351.

No terceiro capítulo considera a revisão da literatura sobre sistemas especiais de proteção, com ênfase no SEP N/NE/SE, e arquiteturas de integração entre agentes.

O quarto capítulo representa toda metodologia da pesquisa. Nele está a descrição das etapas da pesquisa, os métodos utilizados na coleta e análise de dados.

O quinto capítulo apresenta os resultados da pesquisa. Refere-se ao estudo de caso propriamente dito, à caracterização da unidade de análise e identificação de qual ação impactou na performance do nível de atendimento.

Por fim, o sexto capítulo trata das conclusões obtidas pelo estudo e as propostas para futuras pesquisas.

2 Capítulo 2 - Segurança Cibernética

2.1 Redes de Infraestruturas Críticas

A infraestrutura crítica do país inclui setores, instalações, serviços, bens e sistemas que, se interrompidos ou destruídos, pode ter sérios impactos sociais, econômicos, políticos e internacionais. A segurança da infraestrutura crítica tornou-se uma tendência global após os ataques terroristas nos Estados Unidos da América em 11 de setembro de 2001 [1].

No Brasil, essa predisposição ganhou força desde 2006, depois que uma organização criminosa atacou várias instalações no estado de São Paulo, levando o governo brasileiro a identificar qual infraestrutura do país deveria ser protegida caso ocorresse uma nova ocorrência desses casos. Consequentemente, a infraestrutura crítica brasileira inclui principalmente os setores de telecomunicações, energia, transporte, finanças e água, para os quais foram criados os *clusters* técnicos para a segurança de infraestruturas críticas, pelo decreto nº 9668/2019 [14].

Esses grupos foram encarregados de apresentar propostas para aprimorar continuamente a identificação e a classificação das infraestruturas críticas; identificar possíveis ameaças e vulnerabilidades dessas infraestruturas; e sugerir medidas de controle para reduzir os riscos às infraestruturas críticas na área prioritária em questão. Como essas infraestruturas atendem às necessidades sociais, sua segurança vai além do escopo das próprias organizações responsáveis, exigindo a implementação de políticas públicas que garantam a segurança social [14].

A interdependência entre infraestruturas críticas é um fator determinante para a cibersegurança nacional, sobretudo devido à dependência ou interferência de umas sobre as outras ou de uma área prioritária de uma infraestrutura crítica sobre outra, nomeadamente quando ocasionada por ciberataques. Deve-se observar que essa dependência acelera e amplifica as consequências de qualquer evento ou ataque de rede de infraestrutura crítica [15].

A Figura 1 ilustra as possíveis interdependências entre os setores sociotécnicos de água, gás, saneamento, logística, comunicação, finanças, dados e emergência, e a centralidade do setor de eletricidade como catalisador dessas funções, fornecendo energia para o seu funcionamento e, ao mesmo tempo, dependendo do apoio desses setores para o seu próprio funcionamento [1].

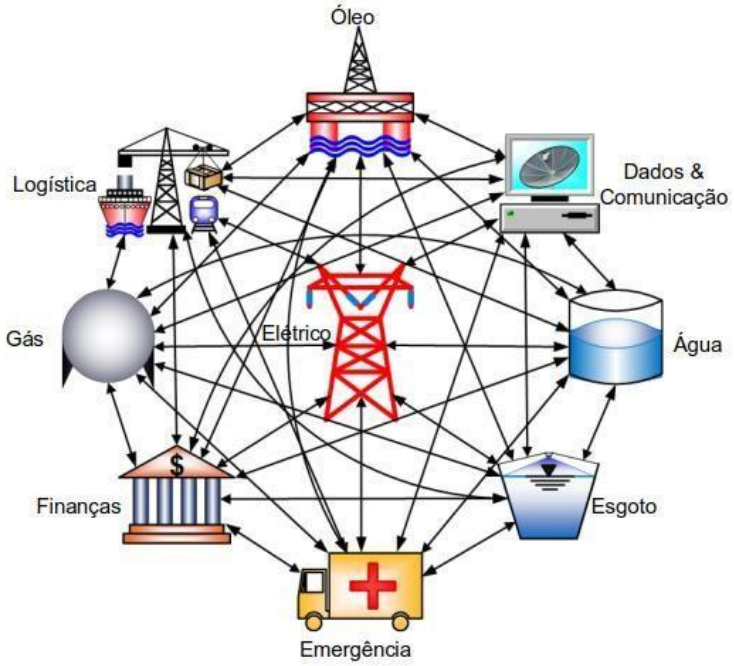

Figura 1 - Centralidade do Setor Elétrico nas Infraestruturas Críticas [1]

Eventos e falhas em um destes setores podem ser propagados aos demais, dependendo das relações de interdependência. Ademais, a Figura 2 representa a estrutura básica da rede de um sistema sociotécnico crítico e sua relação com eventos que impactam o seu desempenho e as consequências associadas.

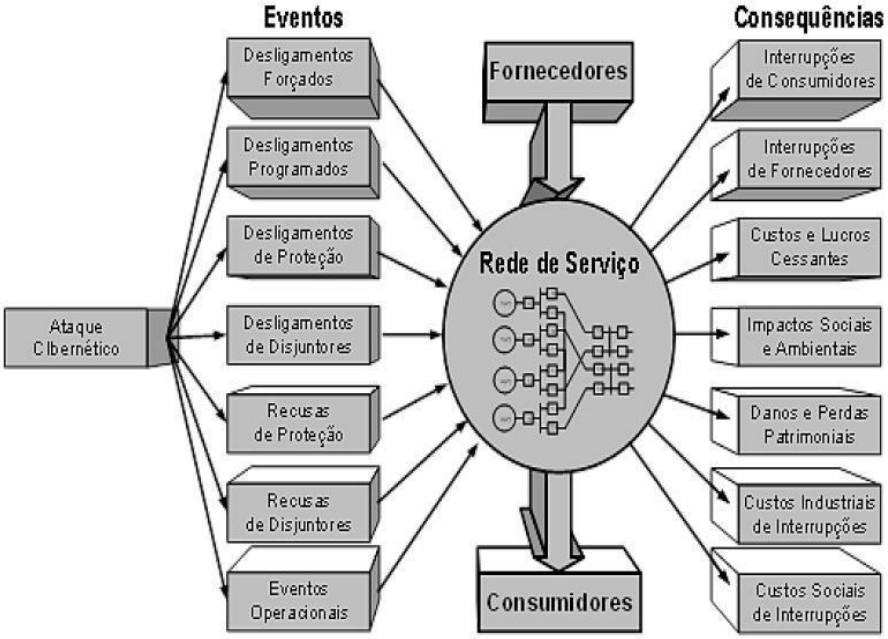

Figura 2 - Avaliação de Desempenho e Risco [1]

A rede é constituída por um conjunto de ativos interligados, alimentados por fornecedores e suprindo um grupo de consumidores, representados na parte central da figura.

De acordo com [1], diversos tipos de ataques cibernéticos podem provocar eventos imprevistos em redes sociotécnicas. Entre os principais tipos citam-se:

- *Sniffer* - Análise de tráfego não autorizada;
- *Replay* – Repetição não autorizada do tráfego capturado;
- *Spoof* – Personificação de um usuário autorizado;
- DoS - Negação de serviço ou sobrecarga de rede;
- Erro - Erros de operadores;
- Social - Engenharia social de usuários autorizados;
- Vírus - Infecção por vírus de componentes do sistema;
- Destruição - Destruição de dados de controle/negócios/configuração;
- Modificação - Modificação de dados de controle/negócios/configuração;
- Desvio - Desvio de funções e mecanismos de segurança do sistema;
- Físico - Comprometimento dos mecanismos de segurança física;
- Natural - Atos da natureza causando indisponibilidade do sistema.

Um ataque cibernético a uma rede sociotécnica como o Sistema Interligado Nacional (SIN) pode desencadear eventos de desligamento forçado de disjuntores, interferência em funções nos dispositivos de proteção ou programados, bem como recusa de atuação das proteções e bloqueio de comandos de interrupção, ou desencadear eventos operacionais inesperados no próprio setor ou em setores interdependentes [16].

A tendência de uso generalizado de dispositivos *Internet of Things* (IoT) em redes sociotécnicas e infraestruturas de missão crítica aumenta a probabilidade de ataques e apresenta desafios para essas infraestruturas. Devido à necessidade de encontrar um equilíbrio entre segurança e privacidade, assim como criar coisas novas [15], esses ataques resultam na interrupção do serviço para consumidores e provedores de rede, aumento de custos e necessidade de recuperar lucros cessantes, consequências sociais e ambientais, danos e perdas patrimoniais, assim como custos sociais e industriais de interrupções [1].

Diversas consequências resultam destes fatores imprevistos apresentados na Figura 2. Entre os mais importantes, de interesse para avaliação de desempenho e risco da rede de infraestrutura, constam: as interrupções no fornecimento de serviço aos consumidores, parceiros e clientes; as interrupções do fornecimento do serviço contratado; os lucros cessantes empresariais; as perdas patrimoniais e de investimentos; as perdas de produção industrial e os custos sociais relacionados [15]. Consequências similares podem ser listadas para todos os tipos de redes de infraestrutura, conforme representadas no lado direito da Figura 2, contextualizando os objetivos desta pesquisa.

2.2 Segurança Cibernética no Brasil

Observa-se que, no Brasil, entre 2018 e 2021, foram conduzidos inúmeros estudos e debates entre diversas empresas relacionadas ao tema da segurança cibernética no setor de energia e infraestruturas críticas em geral. Destacam-se os trabalhos realizados pelo GSI, ONS, ANEEL, ANATEL, ABRATE, entre outros, que também abordaram a segurança cibernética das infraestruturas críticas [3].

No segmento governo alguns decretos têm muita relevância no atual estágio da regulação de segurança cibernética do setor elétrico brasileiro. A Figura 3 mostra os mais relevantes [17].

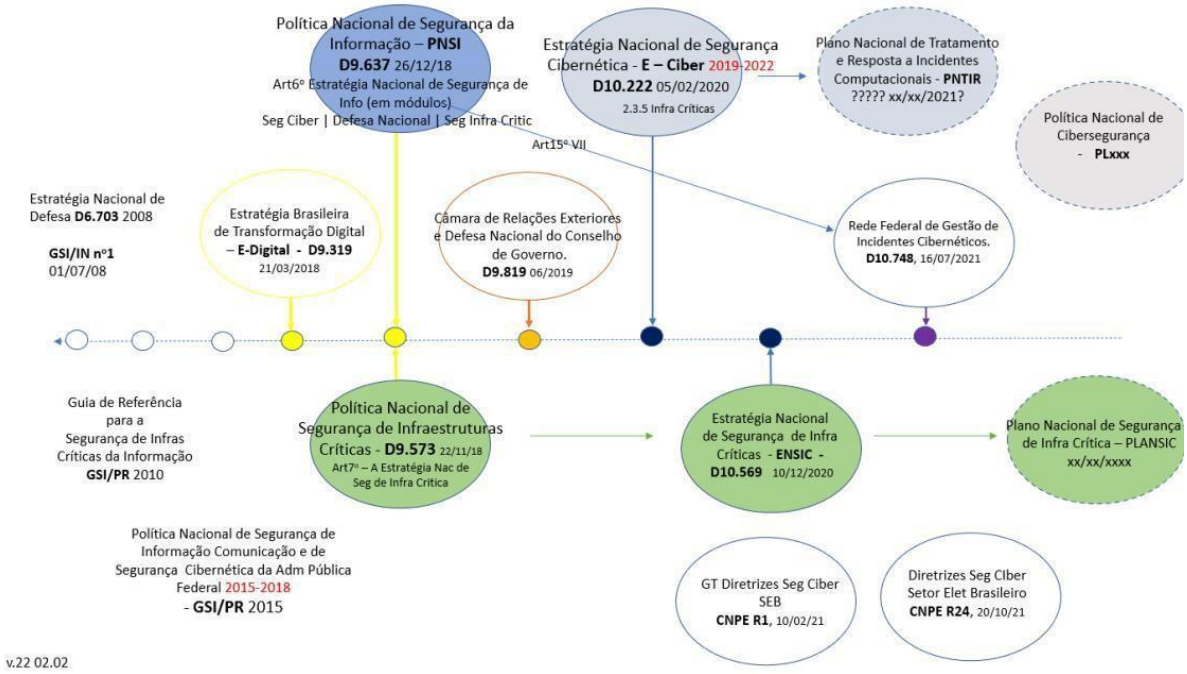

Figura 3 - Quadro Legal da Segurança Cibernética [16]

No Decreto 9.319, de 21/03/2018, a Estratégia Brasileira de Transformação Digital, E-Ciber, balizou e determinou a elaboração das políticas - Política Nacional de Segurança das Infraestruturas Críticas (PNSI), D9.573, de 23/11/2018, e Política Nacional de Segurança da Informação, D9.637, de 26/12/2018 - e das suas estratégias - Estratégia Nacional de Segurança Cibernética (E-Ciber), D10.222, de 05/02/2020, e Estratégia Nacional de Segurança das Infraestruturas Críticas (ENSIC), D10.569, de 10/12/2020 - cujos planos ainda estão em estágio de elaboração - Plano Nacional de Tratamento e Resposta a Incidentes Computacionais (PNTIR1), e o Plano Nacional de Segurança das Infraestruturas Críticas (PLANSIC2). A Política Nacional de Segurança Cibernética, uma das Iniciativas Estratégicas da ENSIC, em elaboração desde 2016, está na Casa Civil para as devidas providências [3].

A Rede Federal de Gestão de Incidentes Cibernéticos, D10.768, de 14/07/2021, e a Resolução 24, de 20/10/2021, tratam sobre resiliência sistêmica [3].

A E-Ciber foi um documento relevante para a elaboração da estratégia de pesquisa deste trabalho. Em seu diagnóstico do cenário brasileiro, destaca-se que as empresas desperdiçam tempo ao realizar pesquisas sobre as mesmas questões relacionadas ao tema. Embora existam boas iniciativas gerenciais nessa área, elas são fragmentadas e pontuais, dificultando a convergência de esforços no setor. Além disso, a falta de alinhamento normativo, estratégico e operacional frequentemente gera retrabalho, prejudicando a absorção de lições aprendidas e comprometendo a eficácia prolongada dessas ações [2].

Decorrentes dessas Políticas e Estratégias os reguladores, particularmente a ANEEL e ONS, produziram documentos regulatórios conforme linha do tempo mostrada na Figura 4.

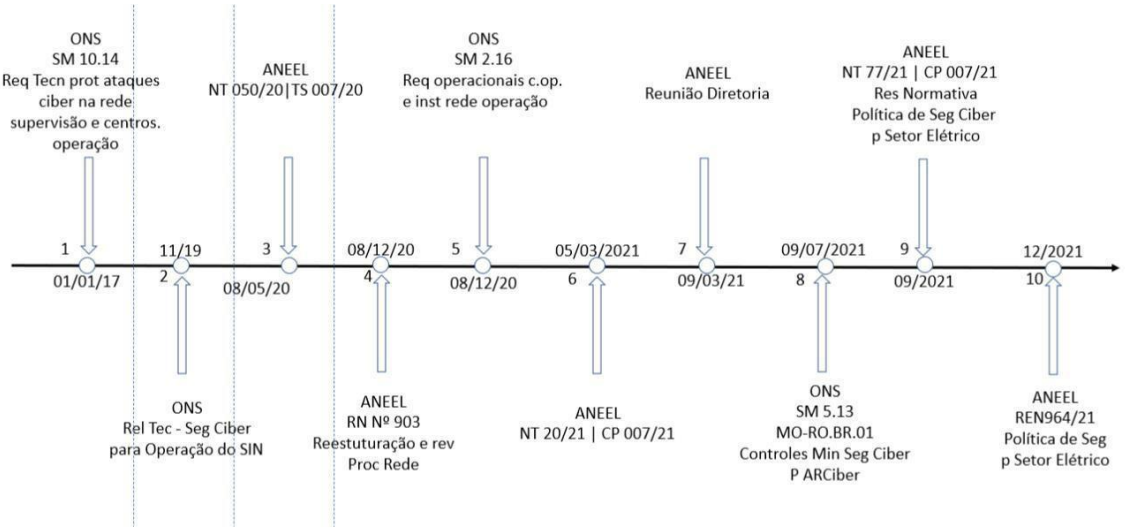

Figura 4 - Quadro Regulatório de segurança cibernética proposto pela ANEEL e ONS [17]

A ANATEL iniciou a jornada de regulação com tomada de subsídios TS 52/2018. Após análise e interação com o setor de telecomunicações resultou na Resolução 740/2020, de 21/12/2020 - Regulamento de Segurança Cibernética Aplicada ao Setor de Telecomunicações [17].

A ABRATE encaminhou à ANEEL, em 2018, uma proposta de uma estrutura de gerenciamento de risco para o setor de transmissão baseado no NIST CSF (*Cybersecurity Framework*) e no C2M2 (*Cybersecurity Capability Maturity Model)* [2].

A ANEEL, seguindo a agenda regulatória, atendendo a solicitação do ONS, que gerou o processo ANEEL 48500-000027_2020-40, publicou a Nota Técnica 50/2020 que abriu a Tomada de Subsídios TS 007/2020, em 25/05/2020, com a finalidade de obter contribuições para a regulamentação associada à segurança cibernética do Sistema Elétrico Brasileiro. A Nota Técnica continha uma pesquisa sobre, dentre outros assuntos, os padrões e as melhores práticas de gerenciamento de segurança, normas e padrões utilizados pelas empresas do setor: agentes, prestadores de serviços e fornecedores no brasil e no exterior [2].

Após a Tomada de Subsídios, a ANEEL realizou a Consulta Pública CP 007/2021 aberta por meio da Nota Técnica 20/2021, de 05/03/2021, com o objetivo de receber subsídios para a Análise de Impacto Regulatório (AIR) sobre segurança cibernética no Setor Elétrico Brasileiro. Com isso, determinou ao ONS emitir documento operativo no sentido de detalhar essas diretrizes, apresentando as referências, os conceitos, as atribuições e as orientações técnicas complementares relacionadas com a política de segurança e com os recursos tecnológicos para proteção contra-ataques cibernéticos [2].

O ONS emitiu o Submódulo 5.13, Rotina Operacional RO-CB.BR.01 [3] - Controles mínimos de segurança cibernética para o Ambiente Regulado Cibernético que teve a sua vigência iniciada em 09/07/2021 [3].

Continuando o processo, a ANEEL emitiu uma nova Consulta Pública, CP 007/2021/2, sobre uma Minuta de Resolução Normativa para a segurança cibernética no setor elétrico elaborada como resultado da primeira consulta pública. Após as contribuições, a ANEEL emitiu a Resolução Normativa 964 [3], em 14/12/2021, sobre a política de segurança cibernética.

2.3 Segurança Cibernética no Mundo

No cenário internacional, as principais referências em segurança cibernética para o setor elétrico são as regras CIP (*Critical Infrastructure Protection*) [18] da NERC (*North American Electric Reliability Corporation*) [19] e o framework do NIST (*National Institute of Standards and Technology*) [20]. Há um sombreamento das atividades entre os dois órgãos dos Estados Unidos, mas em geral o framework do NIST serve como recomendação para os agentes. Além disso, o NIST emite diretrizes para as agências dos Estados Unidos da América (EUA), como a FERC (*Federal Energy Regulatory Commission*), a qual está vinculada à NERC. Essa, portanto, é uma regulação obrigatória para os agentes do sistema elétrico dos EUA [21].

Além disso, a jurisdição da FERC/NERC, consequentemente as regras do CIP, abrange o BES (*Bulk Electric System*) dos EUA, ou seja, os grandes geradores e transmissores de energia. O que tem uma certa equivalência à Rede Básica do Sistema Elétrico Brasileiro. Os outros sistemas, como transmissão local e distribuição são de competência dos Estados. Portanto, não há uma regra geral para esses sistemas nos EUA [21].

Cabe ressaltar que os EUA, por terem uma grande infraestrutura de energia elétrica e por serem uns dos países mais avançados em tecnologia, são naturalmente os maiores alvos de ataques cibernéticos. Assim, os regulamentos relativos à segurança cibernética desenvolvidos pelos EUA estão entre os mais completos. Dessa forma, outros países desenvolvidos em regulação, como Austrália e Canadá, seguem as regras do NIST e NERC. Além disso, o México também está sujeito à regulamentação do NIST e NERC nas interligações com os EUA. A Europa, embora não sujeita ao NIST e NERC, usa diretamente os textos da CIP em sua regulamentação, assim como a IEC 62443 [22]. A Nova Zelândia emitiu sua própria regulamentação também derivada do NIST e NERC [16].

Na União Europeia, o órgão que propõe a regulamentação para a segurança cibernética é a ENISA (*European Network and Information Security Agency*). Ela publicou, em 2016, a Diretiva NIS (*Network and Information Security*), que foi, em seguida, incorporada pelos países membros. Embora tenha havido certa flexibilidade durante a incorporação, pois alguns países como a França já possuíam regulação para segurança cibernética, o processo de incorporação à regulação de cada país foi concluído em 2018 [16].

2.4 Arquitetura Cibernética de Referência

A Segurança Cibernética do Setor Elétrico pode ser avaliada considerando uma arquitetura em camadas, modelada segundo o padrão original *Purdue Enterprise Reference Architecture and Methodology* (PERA) [23] e adaptada para o contexto nacional brasileiro.

Neste sentido, a Figura 5 mostra uma visão genérica das camadas de domínios de segurança a nível nacional e suas conexões, derivadas deste arquétipo, que será utilizada como modelo de referência neste trabalho. Ressalta-se que este modelo é apenas conceitual, para orientar a proposição de políticas, controles e tecnologias aplicáveis de segurança cibernética ao SEB e úteis para fomentar uma discussão nacional sobre a sua regulamentação [1].

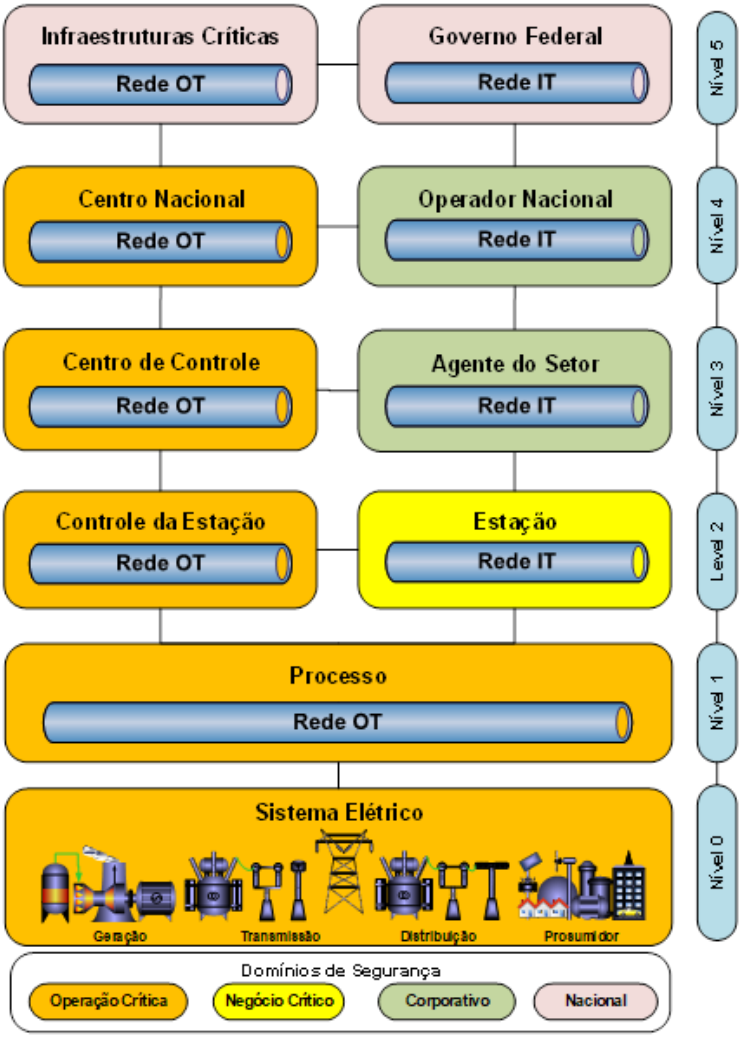

Figura 5 - Arquitetura Cibernética do Setor Elétrico [2]

Seguindo o modelo PERA da Purdue [23], uma arquitetura de ativos de Tecnologia da Informação (TI) ou Tecnologia Operacional (TO) pode ser dividida em seis camadas

hierárquicas, identificadas por seis níveis numéricos, apresentados na Figura 5, que interagem ou estão relacionados por redes de comunicação, conforme a classificação a seguir.

- Nível 0 – Rede de Campo;
- Nível 1 – Rede de Processo;
- Nível 2 – Rede de Estação;
- Nível 3 – Rede do Centro de Controle;
- Nível 4 – Rede Corporativa;
- Nível 5 – Rede Externa.

O Nível 0, equivalente à camada mais baixa, também denominado por Rede de Campo, compreende todos os itens físicos de alta e baixa tensão das instalações elétricas do SIN, ou seja, os equipamentos dos sistemas energéticos, tais como disjuntores, transformadores, reatores, geradores etc. Genericamente, este nível refere-se a qualquer instalação física das estações de geração, transmissão, distribuição ou consumo de energia elétrica. Utilizando interfaces e protocolos de comunicação de IoT, todos os ativos podem se comunicar, em potencial, com outros equipamentos ou itens do mesmo nível ou das camadas superiores da arquitetura [1].

O Nível 1, a segunda camada, também conhecido como Rede de Processos, abrange todos os ativos de hardware e software que monitoram, medem ou controlam diretamente todos os equipamentos do sistema elétrico, como barramentos, alimentadores, disjuntores, transformadores, reatores etc. Estes ativos incluem os meios e as redes de comunicação local e os protocolos de comunicação que interligam estes equipamentos a nível de campo, os quais coletam continuamente sinais do Nível 0 (processo) [1].

O Nível 2, a terceira camada, também chamado de Rede de Estação, é composto por todos os itens de hardware e software que supervisionam, monitoram e controlam centralizadamente uma subestação ou usina. Estes ativos incluem, normalmente, as redes e os processadores das salas de comando, os processadores de interfaces humana, assim como os protocolos de comunicação e controle destas instalações [24].

O Nível 3, a quarta camada, também denominado por Rede do Centro de Controle, compreende todos os itens de hardware e software e os protocolos de comunicação que supervisionam, monitoram e controlam, a nível corporativo, as subestações e usinas de um agente e interagem diretamente com o centro de controle do ONS. Este Nível pode possuir

subníveis, dependendo da estrutura hierárquica de centros de controle utilizada por cada agente do SIN [24].

O Nível 4, a quinta camada, também conhecido como Rede Nacional, engloba todos os itens de hardware e software e os protocolos de TI e TO do ONS que interagem com os Centros de Controle dos agentes no Nível 3, para processar tarefas operacionais, comerciais, de engenharia e administrativas, e com os demais agentes e entidades setoriais, de mercado e governamentais [24].

O Nível 5, a sexta camada, chamado de Rede Externa, compreende os centros de controle binacionais, internacionais e de monitoramento setorial, os centros de controle de outros setores críticos e todos os itens de entidades externas que se comunicam com o ONS na realização de atividades de negócios, operação, engenharia e administração [1].

Destaca-se que os níveis a partir do Nível 2 estão divididos em dois domínios relacionados aos ativos de TI e TO de todos os agentes, representando a separação típica entre estes ativos e constituindo domínios tradicionais de segurança cibernética em cada Nível.

2.5 Norma IEC 61850

A *International Electrotechnical Comission* – IEC desenvolveu o padrão IEC 61850 para superar os problemas de interoperabilidade entre dispositivos de diferentes fornecedores no sistema de automação da subestação. A IEC 61850 define os modelos de dados e protocolos de comunicação que permitem a digitalização de infraestruturas elétricas e integram os dispositivos com as comunicações dentro deste tipo de instalações. Um conceito central é o de *dataset*, que agrupa dados específicos para facilitar a comunicação eficiente entre dispositivos eletrônicos inteligentes (IEDs) [2].

A arquitetura do Sistema de Automação da Subestação (SAS) conforme a norma IEC 61850 é projetada para integrar diversos dispositivos e sistemas de controle, proteção e monitoramento. Essa arquitetura utiliza uma rede de comunicação baseada em Ethernet para interligar os IEDs, permitindo a troca de informações em tempo real e a implementação de funções avançadas de automação. A comunicação horizontal entre os dispositivos é realizada através do protocolo GOOSE, enquanto a comunicação vertical utiliza o protocolo MMS, garantindo a interoperabilidade e a eficiência operacional [6].

A Figura 6 apresenta a divisão da arquitetura do SAS em três níveis (Estação, *Bay* e Processo), conforme especificado na IEC 61850-5 [1]. Ela também ilustra os barramentos de Estação e de Processo, que são as redes de comunicação responsáveis pela conexão entre os dispositivos alocados nos diferentes níveis mencionados. Além disso, a Figura 6 mostra a direção do fluxo de informações dentro de uma subestação e os protocolos típicos utilizados em cada barramento: MMS para supervisão e controle, GOOSE para a transmissão rápida de eventos de subestação e SV para o envio ágil de dados analógicos de corrente e tensão através da rede de comunicação.

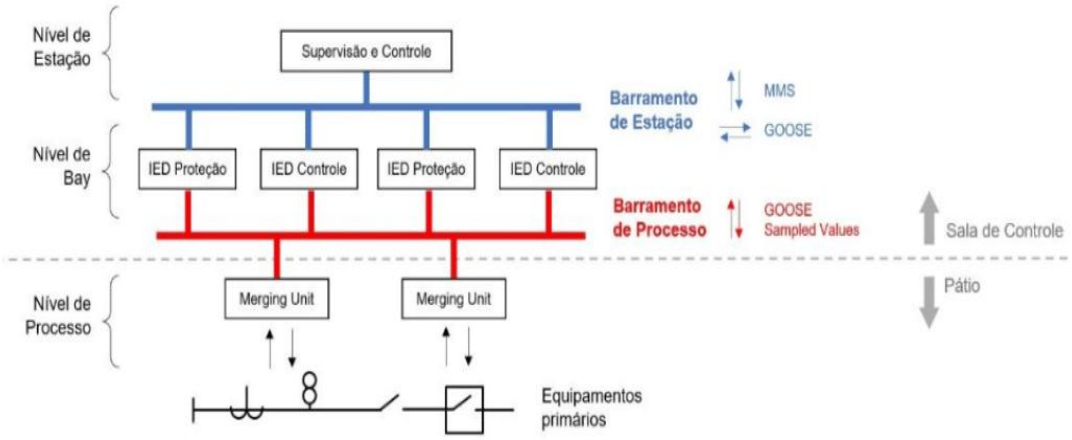

Figura 6 - Arquitetura do Sistema de Automação da Subestação [25]

Em resumo, a norma IEC 61850 define a arquitetura do SAS em termos de níveis e barramentos para facilitar a comunicação e integração dos IEDs, melhorando a confiabilidade e flexibilidade do sistema. Cada nível da arquitetura abrange: dispositivos de campo (Nível 0), equipamentos de controle e proteção (Nível 1), sistemas de supervisão e controle local (Nível 2), e sistemas de supervisão e controle remoto – Centro de Controle (Nível 3).

A IEC 61850 define os protocolos de comunicação utilizados no âmbito de uma subestação e abre caminho para a digitalização e padronização. A progressiva integração da TO com a TI introduz novas vulnerabilidades. As informações entre os dispositivos são distribuídas na forma de quadros Ethernet, que podem ser facilmente detectados, alterados ou gravados e reproduzidos [4].

O benefício de uma decisão baseada no padrão IEC 61850 depende da estratégia de implementação apropriada. Os ganhos se estendem a facilitar a construção do campo, como redução de cabos, serviços relacionados ao comissionamento e jornada de trabalho, e documentação de procedimentos de projeto e manutenção. A decisão deve ser tomada em planejamento e com visão global para que as vantagens sejam reais e assimiladas em todas as

fases de instalação, manutenção e operação da subestação. As principais razões para decidir sobre a IEC 61850 são [6]:

a) **Interoperabilidade:** O padrão define muito claramente os protocolos de comunicação (MMS, GOOSE, SV). Também, conforme estabelecido na IEC 61850, a redundância de mensagens via protocolos PRP e HSR busca atender ao requisito de disponibilidade, já a sincronização de tempo aplica-se através dos protocolos SNTP e PTP do padrão IEEE 1588. Isso permite que equipamentos de diferentes fabricantes e gerações trabalhem juntos. A compatibilidade deve ser assegurada pela aprovação de todos os IEDs, infraestrutura de comunicação, ferramentas de software e sistemas de monitoramento.

b) **Facilidade de substituição:** A troca de dispositivos é simplificada ao separar fisicamente o pátio dos IEDs da sala de controle. Isso permite que o gerenciamento da tecnologia e o ciclo de vida dos dispositivos sejam tratados de forma independente.

c) **Documentação:** Dado que o padrão define os arquivos de configuração (*System Specification Description* - SSD, *Configured IED Description* - CID, *System Configuration Description* - SCD) com base numa linguagem padronizada (*System Configuration Description Language* - SCL), gerar uma documentação pode ser realizada com certa facilidade. O maior impacto é cultural.

d) **Facilidade de Transformação:** Transformação de ideias de projeto, normalização da filosofia ou implementar novos recursos é mais fácil sem a necessidade de mudanças físicas (cabo ou relé opcional);

e) **Administração de Ativos:** Com implementação completa de padrões têm-se informações inteligentes sobre todos os ativos e a gestão se torna mais eficiente. Pode-se monitorar desempenho, histórico e disponibilidade em tempo real.

f) **Virtualização:** O desenvolvimento de tecnologias de virtualização para execução das funções do sistema PAC (*Protection, Automation and Control*) contribui para a distribuição de funções.

g) **Disponibilidade:** Potencial de maior disponibilidade, o que facilita ter funções redundantes (*backups*) em diferentes equipamentos. Também agiliza a substituição de dispositivos.

Os desafios são reais à medida que as equipes e empresas precisam estar qualificadas para os avanços da tecnologia nos produtos adquiridos aderentes à norma IEC 61850.

2.5.1 Aplicações da norma IEC 61850 em esquemas de proteção

O sistema de fornecimento de energia elétrica deve manter padrões muito elevados de continuidade de serviço e minimizar sua indisponibilidade em caso de condições inaceitáveis de operação. Essas condições são criadas por fatores como incidentes naturais, acidentes, falhas de equipamentos, equívocos humanos e outros eventos que não podem ser totalmente evitados na prática. O sistema PAC, em particular os esquemas de proteção, tem grande responsabilidade nesse sentido, identificando e tomando as medidas essenciais, com o menor impacto sistêmico possível. Considerando a importância do esquema de proteção para o sistema elétrico, ele deve ser projetado considerando os seguintes aspectos [6]:

a) **Confiabilidade:** Fornecer o desempenho certo quando solicitado e não aleatório quando não solicitado.

b) **Seletividade:** Separar a menor parte do sistema de energia para suprimir interrupções.

c) **Velocidade de atuação:** Reduzir o tempo de influência do obstáculo (falha) no sistema de energia.

d) **Simplicidade:** Minimizar o número de dispositivos e circuitos para atendimentos da proteção.

e) **Econômico:** Maximizar o desempenho de proteção com os custos mais baixos.

Ao avaliar o uso de novas tecnologias, métodos, filosofias, entre outros, é importante verificar se esses aspectos são atendidos tanto pelos critérios da própria empresa de energia quanto pelos órgãos de regulação e controle da rede elétrica. Além disso, deve-se determinar se há ganhos ou perdas em relação à situação anterior, para posteriormente avaliar se a mudança é positiva ou não [6].

O benefício mais óbvio da implementação da norma IEC 61850 para funções de proteção é substituir a forma como as informações são trocadas, passando da fiação tradicional para a comunicação usando os protocolos GOOSE e SV. Outro potencial vantagem é a livre alocação de funções através da segregação em nós lógicos (*logical nodes*), concedendo maior flexibilidade, principalmente na redundância dos esquemas de proteção. Assim, torna-se

possível implementar muitas das funções de proteção atualmente postas em esquemas de proteção tradicionais usando IEC 61850 [6], tais como:

a) Proteção de Barramentos;

b) Falha de Disjuntor;

c) SEP – Sistema Especial de Proteção;

d) Teleproteção.

2.5.2 Requisitos de segurança cibernética e a norma IEC 61850

Em uma aplicação baseada na IEC 61850, a segurança cibernética é muito significante, pois toda a infraestrutura de comunicação utiliza uma solução padronizada, consequentemente é conhecida e deve ser protegida para garantir a confidencialidade, integridade e, especialmente, disponibilidade dos fluxos de dados e informações, de acordo com os objetivos de proteção definidos na norma ISO / IEC 27000 (triângulo CIA). O princípio dos sistemas PAC é atender aos pré-requisitos de escalabilidade, eficiência, desempenho, interoperabilidade, redundância e disponibilidade com ênfase em longos ciclos de vida sem interrupção. Assim, esses requisitos não são afetados pelos instrumentos de defesa cibernética [6].

Um dos conceitos-chave nessas estratégias, introduzidas no padrão, é o conceito de "defesa em profundidade", do vocábulo em inglês DiD - *Defense in depth*. O princípio básico deste conceito é não confiar em uma única maneira como medida de segurança para impedir invasões. Desta forma, várias camadas de proteção devem ser implementadas, aumentando assim a segurança do sistema.

Para definir as necessidades de segurança cibernética, é essencial estabelecer os padrões que devem ser usados para garantir a disponibilidade. Este é um problema muito complexo, pois existem vários padrões, com objetivos diferentes, e todos com aspectos importantes a serem tratados. Eles não se complementam, tornando difícil determinar quais se aplicam. Na Figura 7 tem-se uma visão geral de algumas normas IEC / ISO, demonstrando-se o foco de cada uma. [6].

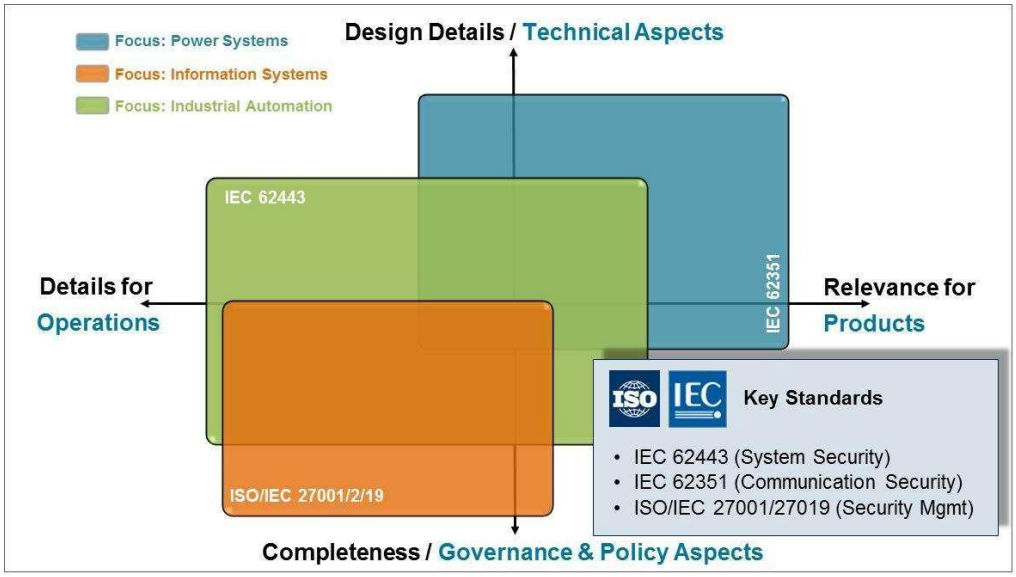

Figura 7 - Visão geral das normas IEC/ISO [6]

A norma IEC 61850 não fornece detalhes sobre segurança cibernética. No entanto, eles são abordados na IEC 62351-6 (Gerenciamento de sistemas elétricos e troca de informações associadas - Comunicação e segurança de dados - Parte 6: Segurança para IEC 61850) [26]. O foco está na prevenção de replicação, que requer autenticação de mensagens de extensões de segurança para evitar invasões e, assim, garantir a integridade da mensagem. A razão para usar o mecanismo de extensão é que ele deve garantir a integridade do nível do processo e o desempenho das mensagens GOOSE e SV, assim como o período de garantia do tráfego de rede entre a origem e o destino [6].

2.5.3 R-GOOSE

O R-GOOSE (*Routable Generic Object Oriented Substation Event*) é uma extensão do protocolo GOOSE, definido pela norma IEC 61850, que permite a comunicação entre dispositivos eletrônicos inteligentes (IEDs) em subestações elétricas distintas. Diferente do GOOSE tradicional, que opera em redes locais (LAN), o R-GOOSE é projetado para funcionar em redes maiores, como redes de área ampla (WAN), utilizando endereçamento IP. Essa característica torna o R-GOOSE uma solução ideal para aplicações que requerem comunicação entre subestações geograficamente distribuídas [6].

A principal vantagem do R-GOOSE é a sua capacidade de roteamento, que permite a transmissão de mensagens GOOSE através de diferentes segmentos de rede, mantendo a interoperabilidade e a eficiência operacional. Isso é particularmente útil em cenários onde a

comunicação entre subestações é crítica para a operação do sistema elétrico, como em esquemas de proteção e controle distribuídos.

Além disso, o R-GOOSE mantém as propriedades de tempo real e alta prioridade do GOOSE tradicional, garantindo que as mensagens sejam entregues de forma rápida e confiável. A implementação do R-GOOSE também segue os requisitos de segurança cibernética definidos pela norma IEC 62351, que especifica mecanismos de autenticação e integridade para proteger as mensagens contra-ataques cibernéticos.

A adoção do R-GOOSE em subestações digitais representa um avanço significativo na modernização das infraestruturas elétricas, proporcionando maior flexibilidade, escalabilidade e segurança na comunicação entre dispositivos. Conforme destacado em [6], a integração do R-GOOSE com outras tecnologias de comunicação e proteção pode melhorar a resiliência e a eficiência dos sistemas de energia, contribuindo para a estabilidade e a confiabilidade da rede elétrica.

2.6 Norma IEC 62351

A segurança cibernética é uma preocupação crescente nos sistemas de energia. Para atender aos requisitos de segurança, como autenticação e integridade para mensagens genéricas de evento de subestação orientada a objeto (GOOSE), o padrão IEC 62351-6 recomenda o uso de assinaturas digitais – uso de criptografia para assegurar que a identidade do remetente seja verificada, e que o conteúdo da mensagem não seja alterado durante a transmissão. Além disso, especifica explicitamente o uso do algoritmo de assinatura digital *RSASSA-Probabilistic Signature Scheme* (PSS) baseado no RFC 3447. Os sistemas de energia são executados em tempo real e as medidas de segurança cibernética implementadas devem atender estritamente aos requisitos de tempo [26].

De acordo com esse padrão, a variante do RSA (*Rivest Shamir Adleman*) – método de encriptação, utilizada para esse fim, deve seguir rigorosamente a RFC 3447 [26] e ser compatível com a RFC 2313 [27]. Além disso, o IEC 62351-6 especifica que a confidencialidade das mensagens GOOSE não pode ser garantida, pois o algoritmo de criptografia não pode atender ao rigoroso requisito de tempo de 3 ms. Em [10], destacam-se os desafios práticos de proteger as trocas de mensagens baseadas na IEC 61850 com aplicação das diretrizes definidas pela IEC 62351-6.

O desafio de obter desempenho em tempo real para proteger o GOOSE e SV com assinaturas digitais RSA foi analisado em [28] usando-se IEDs com recursos limitados em execução em diferentes plataformas. Da mesma forma, em [28], avaliou-se o desempenho do algoritmo de assinatura digital RSA de 1024 bits para proteger a mensagem GOOSE em diferentes plataformas.

Na literatura [27]–[28], todas as análises e avaliações para proteger as mensagens GOOSE foram baseadas nas assinaturas digitais RSA sem especificar o esquema exato de assinatura. No entanto, como já foi mencionado, para proteger as mensagens GOOSE, o padrão IEC 62351-6 específica explicitamente o uso do RSA-*Probabilistic Signature Scheme* baseado no *Signature Scheme* com Apêndice (RSASSA-PSS), conforme RFC 3447, que também é compatível com RFC 2313 (ou seja, versão PKCS 1.5).

Isso significa que o padrão IEC 62351-6 complementa o padrão IEC 61850, e especifica perfis de segurança para proteger a troca de mensagens baseadas na IEC 61850. É importante que esses mecanismos de segurança cibernética não causem atrasos nas mensagens GOOSE além dos limites permitidos. [26].

De acordo com a norma IEC 61850, por exemplo, os protocolos de comunicação implementados pelo SEP devem garantir a interoperabilidade entre todos os equipamentos incluindo a integração de futuros dispositivos relacionados a possíveis extensões do SEP. A solução deve garantir a compatibilidade de integração de cada IED local com o IED mestre.

3 Capítulo 3 – Sistemas Especiais de Proteção (SEP)

3.1 Sistemas Especiais de Proteção (SEP)

Os SEPs são modelos especiais que, ao detectar condições atípicas no SIN por meio de dispositivos de medição, são obrigados a proceder de forma a garantir a integridade do sistema, bem como dos equipamentos, prejudicando o menor número possível de consumidores [9]. O SEP pode ser classificado em três regimes diferentes, conforme previsto em [9].

a) O **Esquema Regional de Alívio de Carga** decide reduzir gradualmente a carga, automaticamente para normalizar a frequência do sistema quando está se encontra baixa.

b) O **Esquema de Controle de Emergência** é um circuito especial que, ao detectar uma condição anormal no sistema eléctrico, através de um equipamento (como exemplo, o relé de proteção), toma medidas imediatas para proteger a integridade das linhas de transmissão e dos demais ativos do sistema.

c) O **Esquema de Controle de Segurança** é um sistema especial que, quando vários imprevistos são descobertos, age imediatamente por meio de ações automatizadas para prevenir novas violações e manter o sistema estável.

O SEP opera sob demanda e, automaticamente, através de equipamentos e Controladores Lógicos Programáveis (CLPs), quando o sistema está instável ou sujeito a eventos que levam a desligamentos graduais, para conservar o sistema como um todo. As ações realizadas podem ser: abertura de linha, divisão de barramento, corte de carga, controle de geração, isolamento de transformadores, inserção/retirada de carga, dentre outras. [29].

Porém, cada SEP instalado tem uma finalidade específica, que é solucionar ou evitar determinado problema, que pode afetar a qualidade do fornecimento de energia elétrica, dos equipamentos de uma pequena parte do sistema, de uma grande região, ou do SIN como um todo [29].

Desta forma, para operar o SIN com segurança, são necessários vários esquemas de proteção eficazes e confiáveis [9]. Assim sendo, os SEPs são sistemas automatizados de proteção e controle instalados no SIN (geração e transmissão) que permitem melhorar a utilização do sistema, aumentando a confiabilidade contra possíveis perturbações pontuais. Além disso, a estrutura e o controle desses sistemas são definidos pelos Procedimentos de Rede

(PRs) do ONS, onde incluem-se os requisitos técnicos e consideram-se os principais cenários de operação. O modo de operação do SEP está descrito no PR, no módulo plano especial [9].

O SEP possibilita a visualização da situação operacional do sistema (operação / falha de linha de transmissão, sobrecarga, sobretensão, baixa frequência etc.) e introduz lógicas de controle, sendo que essas lógicas estão associadas a diferentes condições do sistema. Assim, para cada condição, a respectiva lógica deve ser acionada. O SEP atua de acordo com a lógica pré-definida em relação ao estado do sistema no momento da falha. Cada SEP pode ter uma lógica diferente e sua operação representa uma ação corretiva / preventiva (corte de geração, corte de carga, abertura de linha de transmissão, inserção e retirada de carga reativa para controle de tensão, separação de barramento, entre outros). A lógica no mesmo SEP pode usar mesmas ações de maneiras diferentes em diferentes dispositivos ou pontos do sistema [9].

3.1.1 Aplicação do SEP no Cenário Internacional

De modo geral, conforme se descreve em [30], no cenário internacional, o SEP é uma estratégia eficaz para aumentar a confiabilidade do sistema de energia. Este método é frequentemente empregado como esquemas de proteção secundária. O SEP também é denominado como regime de proteção especial, além disso é referido com diferentes nomes ao redor do mundo, como *System Integrity Protection Scheme* (SIPS), *Bonneville Power Administration* (BPA), *Remedial Action Scheme* (RAS) e outros como *Special Protection Scheme* (SPS, melhor tradução para o que se chama de SEP no Brasil).

Na Índia, no final dos anos 90, o conceito de SEP foi introduzido para aumentar a confiabilidade do sistema de energia. Na rede elétrica indiana, diferentes SEPs foram projetados e implementados com sucesso, como na Usina Termelétrica de Bhusawal, que permitiu melhorar a estabilidade da rede [31].

Já na Austrália os SEPs operam para controle de frequência e carregamento de rede. O Basslink HVDC (*High-Voltage Direct Current)*, isto é, corrente contínua em alta tensão que atua como interconector no controlador de frequência e conecta as cidades Tasmânia e Victoria. É o SEP mais complexo da Austrália, que fornece uma transferência de energia significativa com controle de frequência (exportação de 600 MW e importação de 300 MW). Para efeitos de comparação, a carga do sistema da Tasmânia é aproximadamente 1500 MW [30].

3.1.2 Aplicação do SEP no Cenário Nacional

No Brasil, o SEP associado ao corredor de transmissão de 765 kV da Usina de Itaipu tem papel fundamental para manter a estabilidade do SIN. O corredor de transmissão de 765 kV pode transportar um fluxo de alta potência, de até aproximadamente 6.600 MW. Assim, qualquer contingência envolvendo este corredor de transmissão apresenta grandes riscos à estabilidade do SIN. Desse modo, um SEP confiável e eficiente é necessário para maximizar a produção de energia elétrica em Itaipu e reagir rapidamente a contingências que possam comprometer a confiabilidade geral do SIN [32].

O ONS realizou um estudo sobre o corredor de 765 kV, o relatório ONS RE 3/031/2012 [33], onde definiu os requisitos de desempenho e redundância para este SEP. O requisito de tempo de resposta total para o esquema é de 200 ms, desde o início da contingência até a abertura do disjuntor. O SEP de 765 kV é baseado em unidades de aquisição e controle de dados, do inglês *data acquisition and control units* (DACU), instaladas nas cinco subestações do sistema de transmissão de 765 kV: Foz do Iguaçu, Ivaiporã, Itaberá e Tijuco Preto em Itaipu, e na subestação de 500 kV de Ibiúna [32].

A DACU local é responsável por adquirir os dados binários da subestação – *status* dos reatores de derivação da linha de transmissão (abertos ou fechados), bancos de capacitores em série, disjuntores e chaves seccionadoras –, adquirir também os dados analógicos – magnitudes de tensões, correntes, potência ativa e potência reativa –, e por fim, verificar a consistência dos dados adquiridos. Cada DACU local envia todos esses dados para os controladores mestres, fisicamente localizados em Itaipu, por meio do protocolo de comunicação GOOSE [34].

O controlador mestre recebe esses dados e executa o algoritmo do SEP e, dependendo da contingência e do estado do sistema no momento, envia sinais de comando para Itaipu com o número de unidades a serem desligadas ou a redução de geração de energia, ou ainda, as linhas que serão disparadas nos barramentos de 500 kV ou 345 kV da subestação Tijuco Preto [34].

A topologia do SEP é totalmente redundante com dois sistemas (A e B) trabalhando em um princípio dual, conforme Figura 8. Cada subestação possui no mínimo duas DACUs, que enviam os dados para os dois controladores mestres através de túneis de comunicação configurados em sistemas de comunicação redundantes e multiplexados. Um deles é baseado em uma hierarquia digital síncrona de fibra multiplexada, do inglês *synchronous digital*

hierarchy (SDH), e o outro em um sistema de rádio de micro-ondas, assim, fornecendo links de comunicação redundantes e independentes para os Sistemas A e B [32].

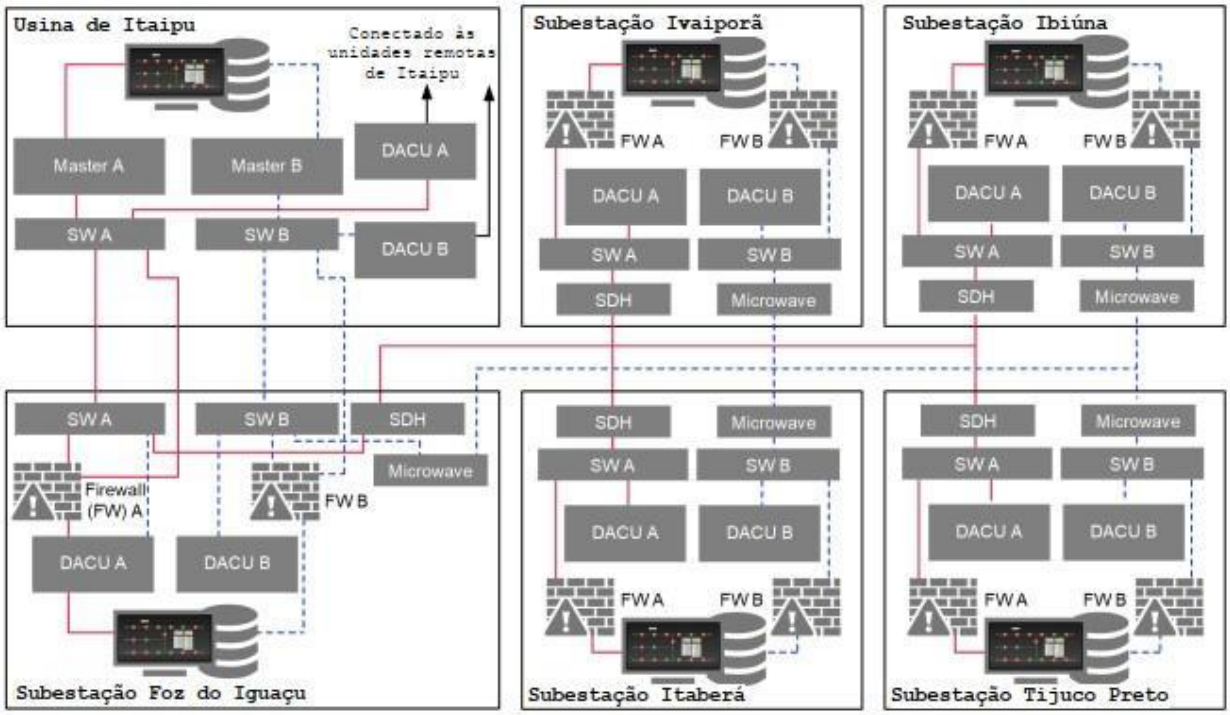

Figura 8 - Arquitetura de Rede Simplificada [32]

As linhas vermelhas sólidas são comunicações do Sistema A e as linhas azuis pontilhadas são comunicações do Sistema B. Além do SEP aplicado ao corredor da Usina de Itaipu, tem-se o SEP empregado à interligação Norte–Sudeste (N-SE) que é composto por uma rede de CLP em subestações de 500 kV da interligação, com lógicas para fazer face de contingências simples, duplas e triplas em qualquer trecho da interligação Norte-Nordeste-Sudeste (N/NE/SE).

Essas lógicas promovem o corte de geração nas usinas de Serra da Mesa, Tucuruí, Estreito, Lajeado e Peixe Angical, tendo sido posteriormente incorporadas ações de *run-up* ou *run-back* (processo de aumentar ou diminuir gradualmente a potência em um sistema de transmissão) nos bipolos Xingu – Estreito e Xingu – Terminal Rio, após a entrada em operação desses equipamentos. Tais ações são comandadas pela Lógica 4 do SEP associado ao sistema HVDC da SE Xingu, a partir do recebimento de sinais do CLP Master de Serra da Mesa do SEP associado à interligação N-SE, havendo assim uma interação entre os esquemas.

Em função da obsolescência dos equipamentos do referido esquema e da necessidade de revisão completa das suas lógicas, devido à nova configuração do SIN, em especial da entrada em operação das SE 500 kV Gilbués e Serra Pelada, e linhas de transmissão associadas,

foi proposto um novo SEP associado às Interligações N/NE/SE. Conforme informado pela ONS, este esquema substituirá a infraestrutura do SEP originalmente instalado e as ações da Lógica 4 do SEP associado ao sistema HVDC da SE Xingu.

3.1.3 Arquitetura do Projeto SEP N/NE/SE

Para atendimento às premissas e ações supracitadas, apresenta-se na Figura 9 a arquitetura geral proposta para o novo SEP.

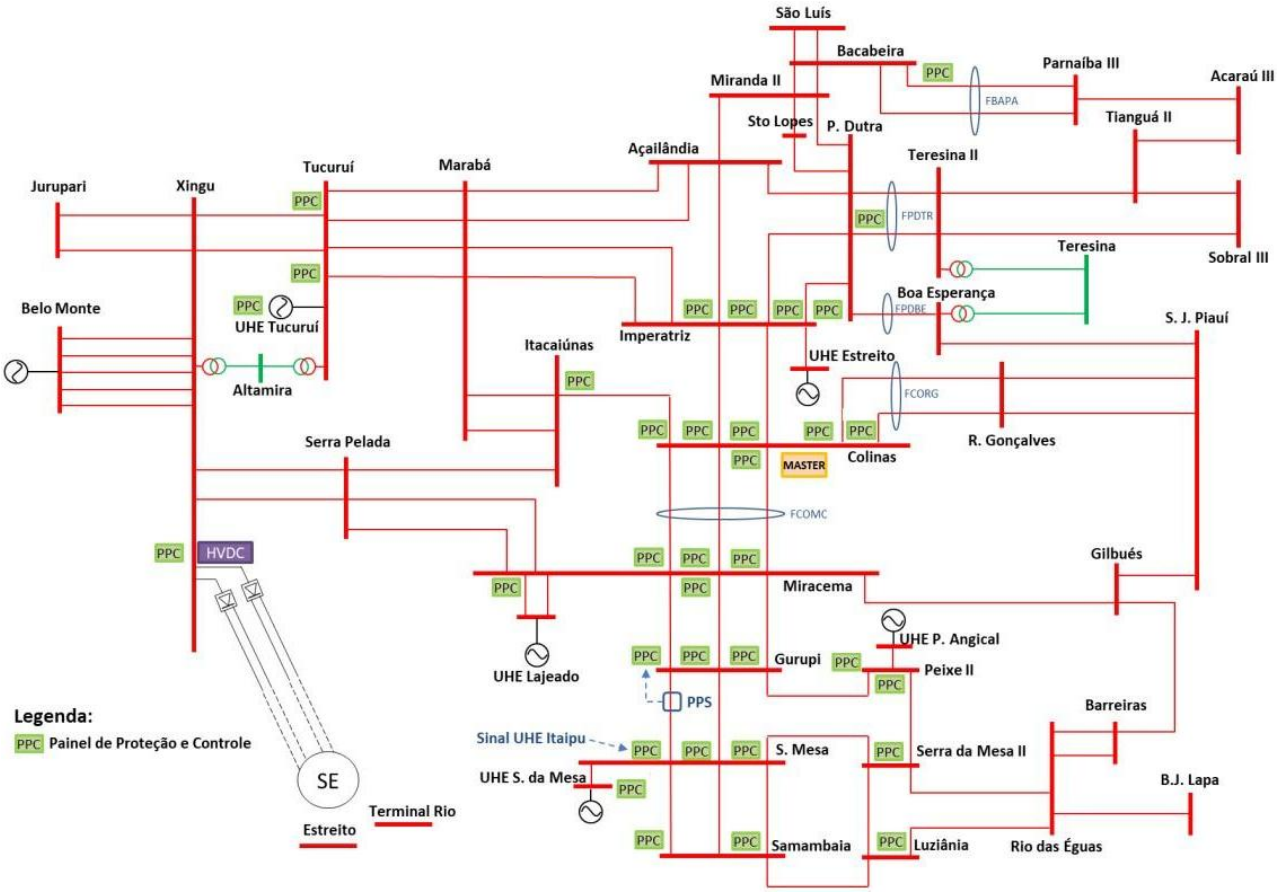

Figura 9 -Arquitetura geral proposta para o SEP N/NE/SE [35]

No diagrama são representados os painéis de proteção e controle (PPC) que contemplam os equipamentos das cadeias redundantes do SEP. Salienta-se que o número exato de painéis necessários pode ser modificado em função da solução a ser proposta pelo fabricante responsável pela implantação do SEP [35].

Conforme o diagrama, observa-se que os IEDs de usina apenas serão necessários nas Usinas Hidroelétricas Serra da Mesa e Tucuruí (únicas usinas com PPC), que terão corte seletivo de unidades geradoras (UG). Para essas usinas deverão ser fornecidos IEDs redundantes que permitam realizar a função de seleção e desligamento de unidades geradoras,

ou envio de sinais a sistemas internos redundantes das usinas que realizem essa função, sendo integrados ao SEP através da rede de comunicação [7].

O SEP também terá interação com outros dois esquemas existentes: a recepção no IED de Gurupi do sinal da PPS (Proteção contra Perda de Sincronismo) de Gurupi - Serra da Mesa C1, que hoje comanda o corte de 4 UG na Usina Hidroelétrica (UHE) Tucuruí por meio do SEP original da interligação N-SE, e a recepção de um sinal no IED de Serra da Mesa a partir do SEP do tronco de 765 kV associado à UHE Itaipu, para comando de corte de 4 UG na UHE Tucuruí [7].

3.1.3.1 Rota de comunicação do Projeto SEP N/NE/SE

Devido à criticidade do SEP para a segurança e operação otimizada do SIN, foi proposto a premissa de que as rotas de comunicação redundantes devem utilizar meios físicos de comunicação independentes, com estruturas de transmissão distintas, de forma a eliminar as possibilidades de falha comum.

A Figura 10 apresenta as rotas de comunicação Principal e Redundante propostas para o referido projeto de SEP. Nessa figura, uma das cadeias do sistema de comunicação redundante é representada em preto, e a outra em azul, considerando a disponibilidade de cabos OPGW (*Optical Ground Wire*) como meio físico. Salienta-se que não é prevista a necessidade de comunicação entre IEDs locais de subestações distintas, sendo imperativo, entretanto, que todos os IEDs locais tenham acesso à rede para comunicação com o IED Master [35].

O ONS recomendou que a elaboração da proposta técnica apresentada aos fabricantes para elaboração do SEP, seja única, e que seja coordenada pelo agente com maior participação no SEP em termos de equipamentos a serem instalados, podendo ter a participação dos demais [7].

Nesse sentido, cabe ressaltar que a escolha do fabricante para a implantação do SEP é de responsabilidade do agente proprietário do IED Master, mediante a criticidade da interconexão, uma vez que todos os equipamentos associados ao SEP serão integrados neste IED, ou seja, os 13 agentes distintos com os seus respectivos IED locais se comunicam com o IED Master e não entre si [35].

Neste contexto, a Figura 11 mostra a arquitetura geral do SEP com cada enlace da Rota A e B e subestações [35].

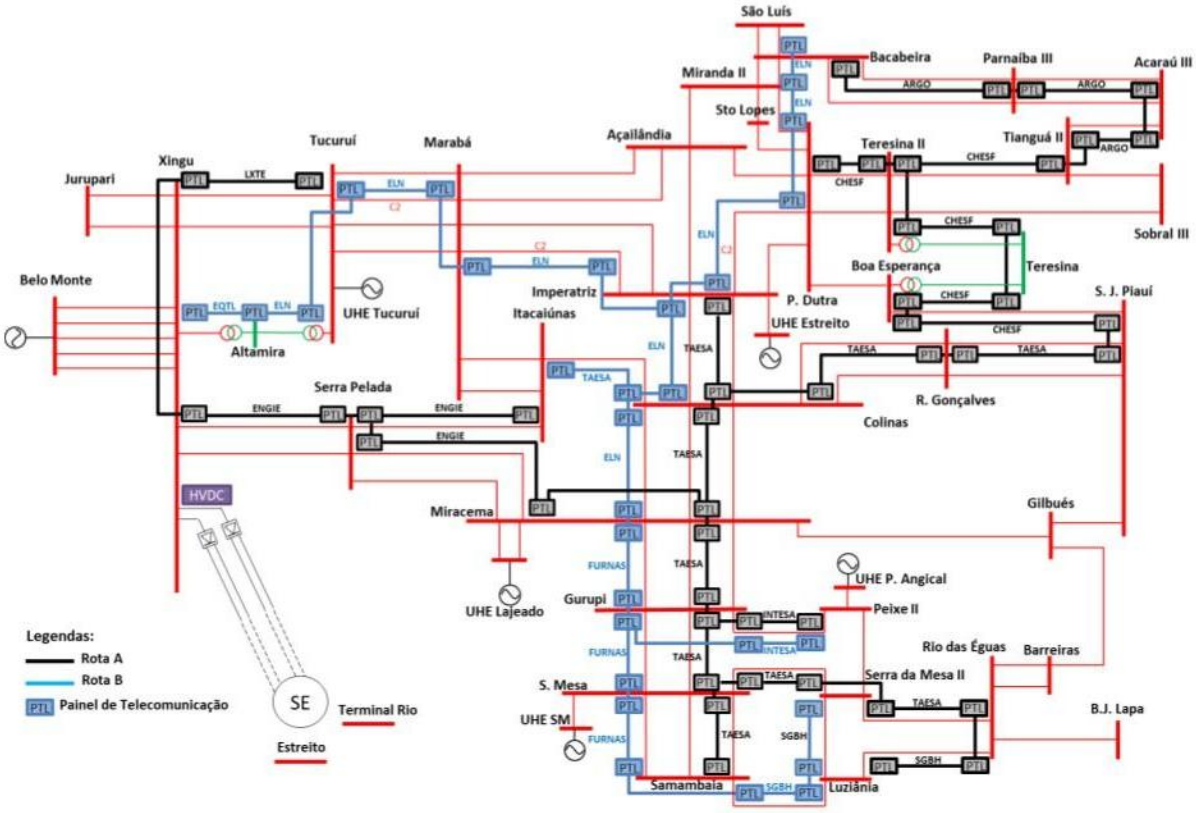

Figura 10 - Infraestrutura geral das rotas de comunicação do SEP [35]

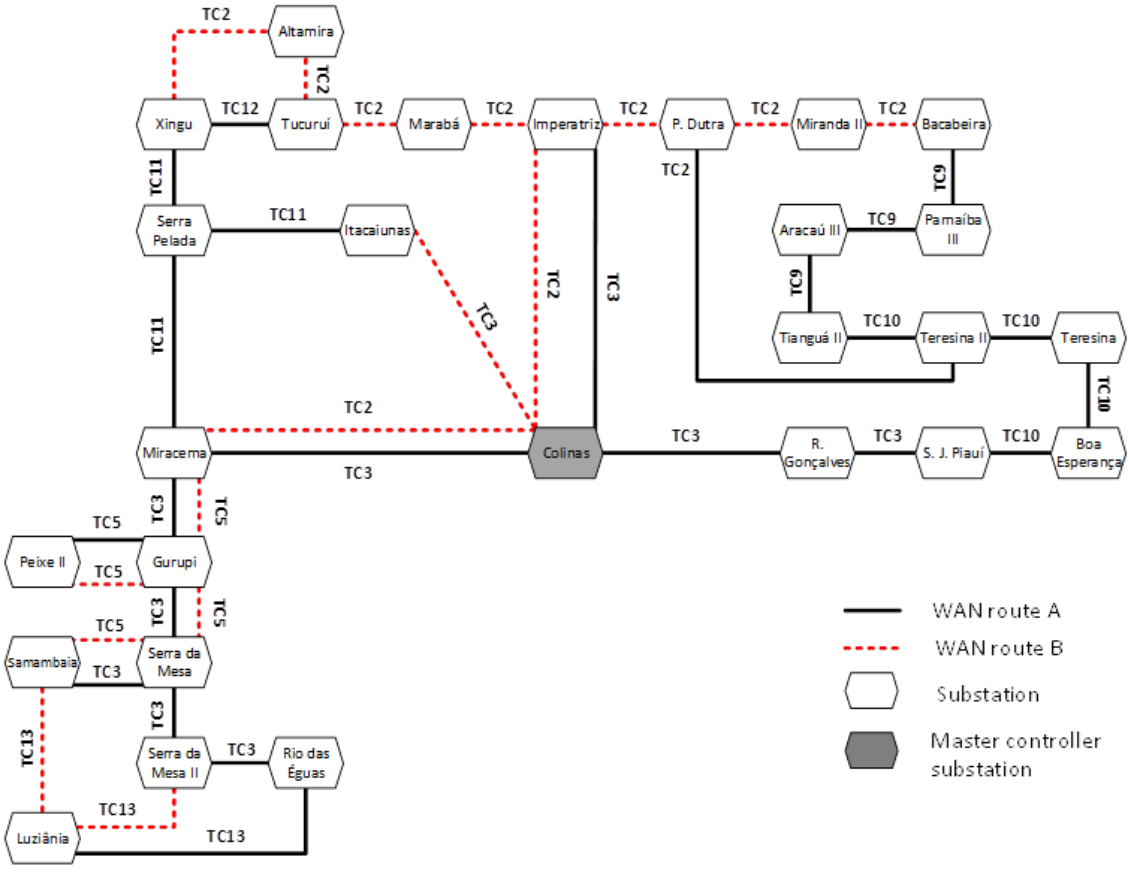

Figura 11 -Arquitetura de Rede Geral do SEP [35]

3.1.3.2 Lógica do Projeto SEP N/NE/SE

O SEP associado às interligações N/NE/SE prevê ações para três categorias distintas de fenômenos, com os seguintes objetivos [7]:

a) Alívio de carregamento decorrentes de contingências duplas ou triplas nas Interligações N/NE/SE (Lógica 1);

b) Evitar perda de sincronismo entre os sistemas Norte, Nordeste e Sudeste, quando tem perdas duplas ou triplas nas Interligações N/NE/SE (Lógica 2);

c) Controle de tensão na área Goiás-Brasília (Lógica 3).

Adicionalmente, haverá duas lógicas que não serão processadas no IED Master, mas que utilizarão a infraestrutura deste SEP [7]:

a) Corte de geração na Usina Hidrelétrica Tucuruí por comando do SEP associado ao tronco de 765 kV;

b) Corte de geração na Usina Hidrelétrica Tucuruí por atuação da PPS (Proteção contra Perda de Sincronismo) de Serra da Mesa – Gurupi.

Para desempenhar os objetivos propostos no projeto, as lógicas do SEP devem utilizar as seguintes premissas [7]:

a) Identificação dos cenários de interação (Norte, Sudeste ou Nordeste Exportador) pelo IED Master do SEP;

b) Pré-habilitação das lógicas de estabilidade pelos fluxos de referência (FNNE – Fluxo Norte e FCOMC – Fluxo Colinas);

c) Identificação das contingências duplas e triplas, para as lógicas de estabilidade, a partir do monitoramento por IEDs locais dos estados dos dois terminais das linhas de transmissão em questão;

d) Identificação pelos IEDs locais de sobrecargas inadmissíveis em linhas de transmissão a partir do monitoramento de corrente em apenas um terminal;

e) Identificação de sobretensão em linhas de transmissão, pelos IEDs locais.

Esclarece-se que o fluxo de referência FNNE será composto no IED Master pelo somatório dos fluxos de potência ativa provenientes das LTs 500 kV Colinas – Ribeiro Gonçalves C1 e C2, Presidente Dutra – Teresina C1 e C2, Presidente Dutra – Boa Esperança e

Bacabeira – Parnaíba C1 e C2, considerando-se este FNNE positivo para o cenário Nordeste importador. O fluxo de referência FCOMC será composto no IED Master pelo somatório dos fluxos de potência ativa da LT 500 kV Colinas – Miracema C1, C2 e C3, sendo considerado positivo para o sentido Colinas – Miracema [7].

As seguintes ações serão realizadas pelo SEP:

a) Comando de *run-up* ou *run-back* nos bipolos Xingu – Estreito e Xingu – Terminal Rio, a depender do cenário operativo;

b) Corte de unidades geradoras nas UHE Tucuruí e Serra da Mesa;

c) Abertura das linhas de conexão de 500 kV associadas às UHE Estreito, Lajeado e Peixe Angical (corte total das usinas), nas SE Imperatriz, Miracema e Peixe II, respectivamente;

d) Abertura de linhas de transmissão nas SE Luziânia e Samambaia, e de bancos de capacitores na SE Samambaia, com objetivo de mitigar sobretensões;

e) By-pass temporizado dos bancos de capacitores série (BCS) dos circuitos da LT Serra da Mesa – Samambaia (instalados na SE Samambaia) e da LT S. da Mesa 2 – Luziânia (instalados na SE Luziânia).

3.2 Comunicação Entre os Agentes Distintos

Em subestações da rede básica associadas com múltiplos agentes, é comum que os dispositivos dos agentes diferentes precisem trocar sinais contendo informações de proteção e controle. Esquemas de falha do disjuntor, seletividade lógica, supervisão baseada nos estados dos equipamentos primários, bloqueios, oscilografia e proteção de barras são frequentemente associados a essas informações [36].

Os painéis de interface são amplamente utilizados, mas têm limitações quando se trata de conectar sistemas com comunicação baseada em redes Ethernet. A aplicação dos barramentos de estação e de processo, conforme definidos pela norma IEC 61850, é um exemplo desses sistemas. Esses barramentos geralmente usam protocolos como GOOSE, para digitalização e troca de sinais binários; SV para digitalização de sinais secundários de transformadores de corrente e potencial; MMS para supervisão e controle; e PTP para sincronismo de tempo.

3.2.1 Métodos de Interconexão entre Agentes Localizados na mesma Subestação

O método mais popular para este caso, e único esquema até agora aplicado, consiste em conectar os sistemas de agentes distintos por meio do seccionamento da cablagem nos painéis de interface, que servem como ponto de concentração e compartilhamento de sinais. O diagrama esquemático para o caso de agentes com painéis separados é mostrado na Figura 12. Na medida em que essa metodologia fornece um isolamento físico e não requer conexão com as redes de comunicação dos agentes, ela apresenta forte resiliência às ameaças cibernéticas [36].

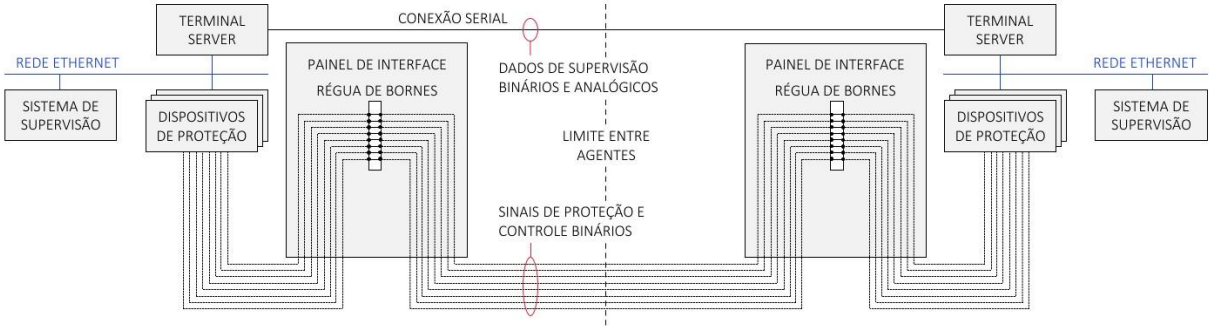

Figura 12 - Interface via cablagem elétrica utilizando painéis separados

Uma alternativa em relação a essa sistematização se baseia no envio de sinais internos da rede via protocolos de comunicação para módulos de entradas e saídas digitais (Módulos de Interface).

Os módulos funcionam como equipamento de fronteira entre agentes, coletando dados da rede interna e transformando-os em sinais elétricos por meio do acionamento dos respectivos contatos (saídas binárias). O módulo do agente receptor sensibiliza as entradas binárias e converte os sinais em mensagens de protocolo de comunicação internamente na rede. Um diagrama esquemático deste tipo de solução é mostrado na Figura 13.

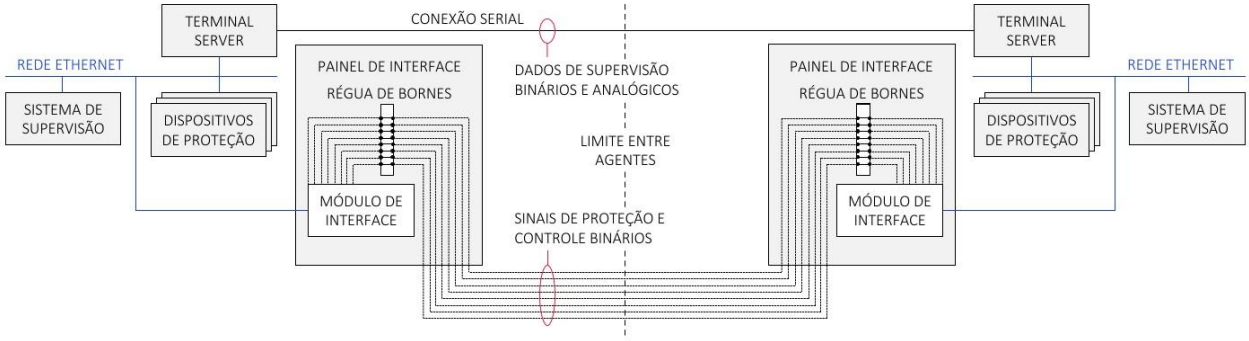

Figura 13 - Interface entre agentes via módulos com protocolo

Os protocolos que permitem a comunicação entre os módulos de fronteira e os dispositivos da rede interna devem permitir a implementação de esquemas de proteção e controle. Eles podem ser implementados de acordo com padrões internacionais ou proprietários se forem dispositivos e módulos do mesmo fabricante. O protocolo GOOSE, definido pela norma IEC 61850, é o protocolo principal utilizado nessa abordagem. É um protocolo aberto que permite a interoperabilidade entre dispositivos e módulos de diferentes fabricantes [36].

A conexão direta das redes entre agentes não é viável na maioria das vezes. Aumenta a vulnerabilidade aos riscos cibernéticos, dificulta a gestão do tráfego e pode comprometer as performances. Esses problemas surgem da abordagem insegura que os equipamentos convencionais de redes Ethernet, incluindo os switches de comunicação, usam.

Os switches estão mais centrados na conectividade do que no controle e na segurança. É necessário incorporar dispositivos de proteção, como *firewalls*, que limitam os tipos de protocolo e monitoram a origem e o destino das mensagens. Os serviços baseados em camada 2, como GOOSE, são mais difíceis de integrar porque o controle dos *firewalls* é feito usando camadas mais altas do modelo de rede.

Com o avanço da digitalização, a tendência é que a interface entre módulos de interface de agentes distintos localizados na mesma subestação se torne cada vez mais baseada em comunicação digital, utilizando protocolos padronizados como o GOOSE da norma IEC 61850. Essa abordagem permite uma maior flexibilidade e eficiência na integração de dispositivos de diferentes fabricantes, além de facilitar a implementação de esquemas avançados de proteção e controle. A digitalização também possibilita a redução de cablagem física e a simplificação da infraestrutura, ao mesmo tempo em que melhora a resiliência. No entanto, este cenário impõe desafios à segurança cibernética.

3.2.2 Redes Convencionais de Comunicação

O “plano de controle” e o “plano de dados” são conceitos fundamentais para as arquiteturas de redes de comunicação. Algoritmos, protocolos ou regras pré-estabelecidos são usados pelo plano de controle para tomar decisões.

Após a decisão sobre o que fazer com uma mensagem específica, o plano de controle envia a instrução para o plano de dados. O plano de dados então codifica a mensagem nas portas de destino certas ou a descarta. Vale ressaltar que, o plano de controle e o plano de dados são aplicáveis tanto aos switches Ethernet convencionais quanto aos switches SDN.

No caso dos switches convencionais, o plano de controle e o plano de dados são implementados no mesmo equipamento. Aprendizagem da tabela MAC (controle de acesso ao meio), regras de segregação e priorização de tráfego, e algoritmos de recomposição são alguns dos recursos do plano de controle.

Estes recursos estão espalhados em diferentes switches da rede de comunicação e funcionam com base em informações de outros equipamentos, o que os torna imprevisíveis e vulneráveis nas redes tradicionais [37]. Estas deficiências incluem condições do sistema não previstas e intencionais maliciosas. Os seguintes exemplos de ataques de camada 2 são incluídos, embora não sejam exclusivos de:

a) **Ataques às tabelas MAC**: forçam os switches a atualizarem suas tabelas MAC, processo no qual abre-se uma janela de aprendizagem onde as mensagens recebidas são encaminhadas para todas as portas, permitindo o reconhecimento da rede por um invasor;

b) **BPDU (*Bridge Protocol Data Unit*) falsificação**: destinado aos switches, o ataque dispara recomposições indevidas no algoritmo de convergência de redes denominado RSTP (*Rapid Spanning Tree Protocol),* sendo utilizado para reconhecimento ou comprometimento da performance da rede;

c) **ARP (*Address Resolution Protocol)* falsificação**: destinado aos dispositivos finais, o ataque consiste no envio de mensagens ARP adulteradas com o intuito do redirecionamento do tráfego a um endereço de rede específico.

As técnicas de *spoofing* apresentadas possuem alvos diferentes, mas ambas são utilizadas para interceptação de mensagens e geralmente antecedem outros tipos de ataques [38].

Além disso, a integração de redes convencionais com tecnologias emergentes, como a virtualização e a digitalização, pode oferecer novas oportunidades para melhorar a eficiência e a segurança das comunicações. A utilização de *firewalls* e outros dispositivos de proteção é essencial para mitigar os riscos cibernéticos associados às redes tradicionais. A implementação de protocolos de comunicação padronizados, como o GOOSE da norma IEC 61850, facilita a interoperabilidade entre dispositivos de diferentes fabricantes, promovendo uma maior flexibilidade e eficiência na gestão das redes de comunicação [38].

Por fim, a evolução para redes definidas por software (SDN) representa uma mudança significativa na forma como as redes de comunicação são gerenciadas e operadas. A separação

dos planos de controle e dados permite uma maior centralização e automação das funções de rede, melhorando a capacidade de resposta a eventos e a resiliência contra-ataques cibernéticos. A adoção de SDN em ambientes de infraestrutura crítica pode proporcionar benefícios substanciais em termos de segurança, desempenho e flexibilidade operacional [38].

3.2.3 Redes Definidas por Software

A arquitetura de uma rede definida por software (*Software-defined networking* - SDN) foi criada nos anos 2000 para atender às demandas de sistemas de tecnologia da informação, que eram caracterizadas por um grande volume de dados e mudanças frequentes de topologia [39]. Ao longo dos anos, descobriu-se que as características que foram inicialmente desenvolvidas para estes sistemas podem ser usadas para beneficiar ambientes de infraestrutura crítica, que, por outro lado, tendem a ser estáticos e recebem um número limitado de mensagens e serviços.

Diferentemente das arquiteturas de rede convencionais, a arquitetura SDN depende da separação dos planos de controle e dados. Todos os fluxos necessários para a operação do sistema são programados preventivamente em uma entidade central chamada Controlador, que recebe o plano de controle [40]. Os comutadores (também conhecidos como switches) SDN, ou equipamentos de rede, recebem as instruções do controlador por meio do protocolo padronizado conhecido como OpenFlow [41]. O plano de dados utilizado nos switches SDN obedece às diretrizes estabelecidas pelo controlador. Os diagramas conceituais para redes convencionais e SDN são mostrados na Figura 14.

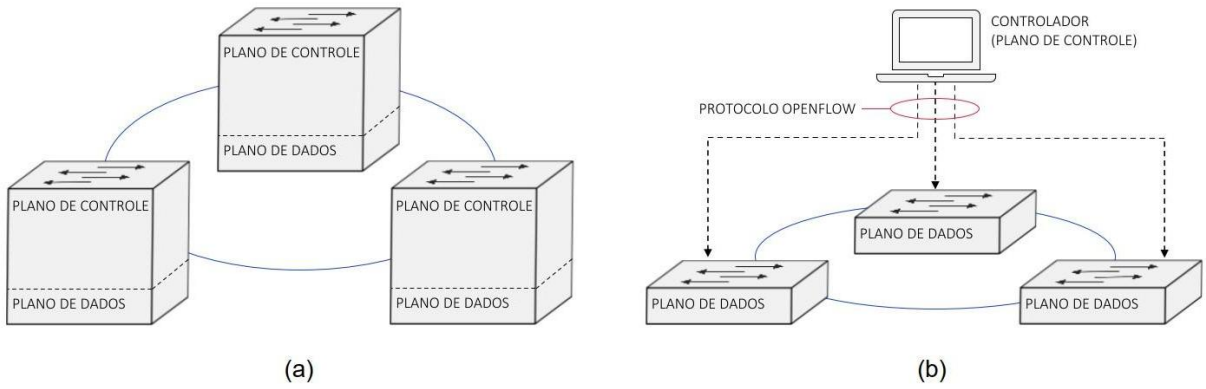

Figura 14 - (a) Arquitetura de comunicação tradicional; (b) Arquitetura SDN [36]

Vale ressaltar que as duas arquiteturas diferem no modo de operação dos seus equipamentos. Ambas são interoperáveis porque têm os mesmos padrões e protocolos de comunicação.

3.2.3.1 Inspeção Multicamadas

O alcance e a profundidade da inspeção de mensagens é outra distinção significativa entre as duas arquiteturas, convencional e SDN. Os dispositivos de comunicação que são projetados usando arquiteturas convencionais normalmente examinam uma camada particular do modelo de comunicação OSI.

Por exemplo, os switches verificam os dados do cabeçalho Ethernet, os roteadores verificam os protocolos da camada de rede e os *firewalls* filtram as conexões pela camada de transporte. Por outro lado, a arquitetura SDN permite a inspeção de todas as camadas do modelo OSI em um único dispositivo. Os campos disponíveis para a implementação da SDN em ambientes de tecnologia da operação estão listados na Tabela 1 [42],[43].

Tabela 1 - Campos inspecionados pela arquitetura SDN [42], [43]

Nome	Valores configuráveis	Descrição
InPort	Qualquer porta do *switch*	Porta de ingresso no *switch*
ArpTpa	Qualquer endereço IPv4 válido	Endereço IPv4 de destino no ARP
ArpSpa	Qualquer endereço IPv4 válido	Endereço IPv4 de oringem no ARP
EthDst	Qualquer endereço MAC válido	Endereço de destino Ethernet
EthSrc	Qualquer endereço MAC válido	Endereço de origem Ethernet
EthType	0 a 65535	Tipo do quadro Ethernet
Ipv4Dst	Qualquer endereço IPv4 válido	Endereço IPv4 de destino
Ipv4Src	Qualquer endereço IPv4 válido	Endereço IPv4 de origem
TcpDst	0 a 65535	Porta TCP de destino
TcpSrc	0 a 65535	Porta TCP de origem
UdpDst	0 a 65535	Porta UDP de destino
UdpSrc	0 a 65535	Porta UDP de origem
VlanPcp	0 a 7	VLAN PCP
VlanVid	Nenhum, atual ou de 1 a 0494	VLAN ID

A Tabela 1 mostra a flexibilidade e a precisão que a arquitetura SDN oferece para a operação de uma rede de comunicação. Os dispositivos que implementam o plano de dados desta arquitetura podem ser chamados de "comutadores" porque não estão limitados a uma camada específica do modelo OSI. No entanto, por razões de simplicidade e uniformidade textual, esta dissertação mantém a designação de "switches SDN” para estes dispositivos.

3.2.3.2 Funcionamento

As instruções de encaminhamento enviadas pelo controlador são armazenadas nas tabelas dos switches SDN. Ao receber uma mensagem, os dados em seu cabeçalho são comparados com as entradas da tabela. Em caso de correspondência entre as informações da mensagem e as regras listadas na tabela, cada entrada contém uma ação específica que será executada. O direcionamento da mensagem para uma porta ou um grupo de portas de destino é

a maioria das ações, mas eles também podem adicionar ou remover VLANs e configurar uma fila de prioridade para egresso.

O diagrama esquemático de funcionamento de um switch SDN é mostrado na Figura 15. Neste exemplo, o switch recebe duas mensagens diferentes do protocolo GOOSE (GOOSE #1 e GOOSE #2). No caso da mensagem GOOSE #1, após ser processada pelo switch, ela é enviada para as portas C2 e C4 porque as informações no cabeçalho da mensagem encontram correspondência na linha 30 da tabela de regras do switch. A mensagem GOOSE #2, por outro lado, não encontra nenhuma entrada relevante na tabela de regras e é descartada automaticamente pelo switch.

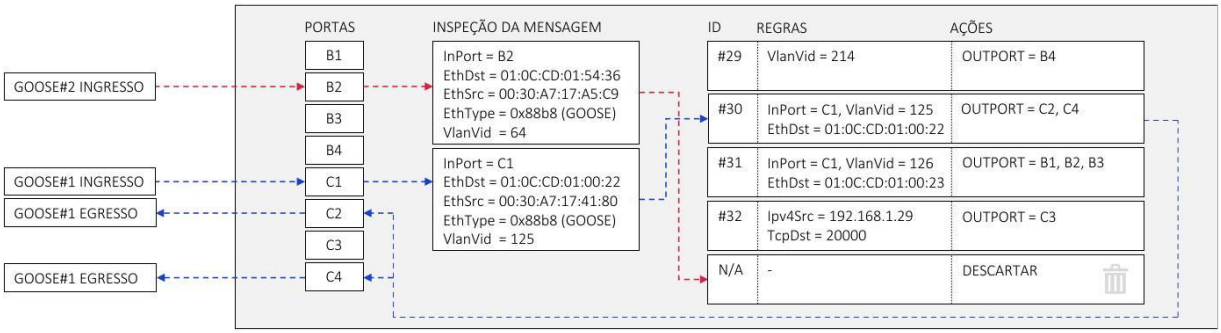

Figura 15 - Exemplo de funcionamento de um switch SDN [42]

A princípio, os switches SDN descartam todo o tráfego por padrão, devido à divisão do plano de controle e do plano de dados. Isso também é chamado de “bloquear por padrão e permitir por exceção” [44]. Eles não usam algoritmos de recomposição e aprendizagem. As instruções do controlador controlam o encaminhamento de mensagens e o chaveamento para rotas reservas, tornando a arquitetura SDN mais segura e com controle de tráfego melhor do que as arquiteturas convencionais.

3.2.3.3 Segurança Cibernética em Redes SDN

Como os switches SDN não possuem tabelas MAC e não utilizam mensagens BPDUs para convergência da rede, as redes SDN com regras predefinidas são imunes aos ataques de tabela MAC e BPDU *spoofing*. Além disso, quando todo o tráfego ARP entre os dispositivos é configurado, os ataques de falsificação ARP são eliminados [38].

O *Simple Network Management Protocol* (SNMP), ou protocolo de gestão de rede simples, é usado para supervisionar switches SDN. Nesses casos, o serviço de criptografia dos dados é disponibilizado entre o controlador (também conhecido como gerente SNMP) e os switches (também conhecidos como agentes SNMP). Para garantir a confidencialidade dos

dados, em [43] propõe-se usar o protocolo SNMPv3 e uma criptografia de chave simétrica AES-128.

3.2.3.4 Integração de Redes entre Agentes

A viabilidade do SDN como um novo método de troca de informações entre agentes pode ser avaliada com base nos detalhes da arquitetura apresentados na Seção 3.2.1. Na arquitetura sugerida, cada agente tem um switch SDN conectado à sua rede interna. Isso serve como um perímetro eletrônico para aplicações de controle e proteção. Eles podem ser conectados ponto a ponto ou por meio de uma infraestrutura de rede compartilhada.

A Figura 16 mostra um diagrama esquemático deste tipo de solução. O switch SDN correspondente pode acessar o tráfego interno da rede quando está conectado à rede Ethernet do agente. As mensagens de estado e alarmes dos equipamentos primários, bem como os disparos e intertravamentos dos dispositivos de proteção e controle, podem estar na rede. Protocolos como o GOOSE geralmente fornecem essas informações. É um desafio compartilhá-los de forma segura sobre a infraestrutura Ethernet ao sistema do outro agente [36].

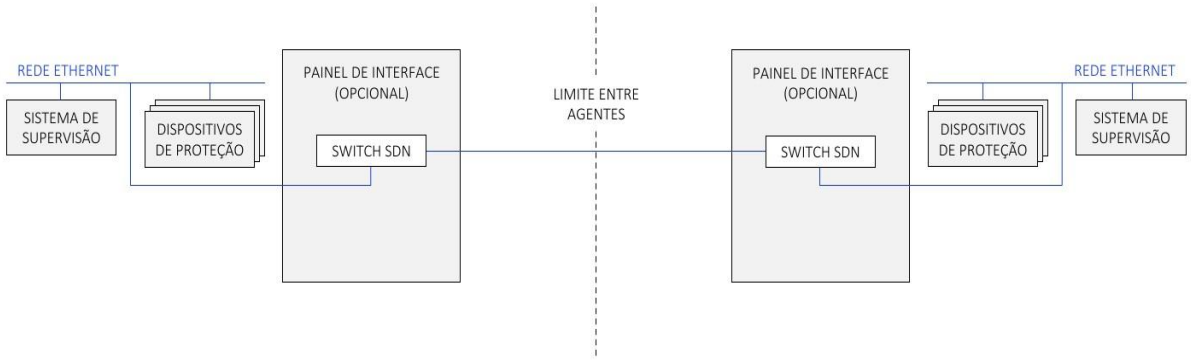

Figura 16 - Interface entre agentes via arquitetura SDN

A segurança fornecida pela abordagem de bloquear por padrão e permitir por exceção, associada ao controle de fluxo granular, são as principais características que permitem o uso da arquitetura SDN para a interligação de redes Ethernet. Nessa solução, cada agente configura em seu switch as permissões para o ingresso e o egresso de mensagens de sua rede; isso naturalmente inclui apenas os serviços necessários para as aplicações de proteção, controle e supervisão. A arquitetura SDN normalmente bloqueia todos os outros tráfegos de mensagens inesperados ou indesejados [36].

A solução com a arquitetura SDN também exige duas condições para que a informação que vem da rede de um agente atinja a rede do outro. Isso o torna semelhante aos métodos existentes baseados no seccionamento elétrico. O agente transmissor deve configurar uma regra de permissão de egresso em seu interruptor SDN. Além disso, a regra de permissão de ingresso deve ser configurada no interruptor na outra extremidade da comunicação. Tal condição é crucial porque diminui a probabilidade de uma configuração de egresso incorreta em um agente afetar a segurança e a performance das aplicações que trafegam sobre a rede interna do outro agente [36].

Os barramentos de estação ou barramentos de processo entre agentes podem ser conectados com a solução com interface via SDN, devido aos avanços nas tecnologias de rede e protocolos de comunicação usados nas subestações de energia. Estes barramentos formam redes de comunicação Ethernet que são usadas para transmitir informações entre dispositivos de proteção e controle ou entre estes e módulos de digitalização, que são instalados próximos aos equipamentos primários no pátio das subestações, os quais são denominados *merging units* (MU) [45].

A escalabilidade da interface SDN é significativa, pois elimina o painel de interface do projeto elétrico. Isso se deve ao fato de que a expansão de réguas de bornes, o lançamento de novos cabos ou a instalação de novos painéis não são mais necessários. Ou seja, o conceito de painel de interface é modernizado. Por exemplo, ao adicionar um novo vão na subestação, precisa-se apenas aumentar a quantidade de pontos, configurando a publicação e recepção das novas mensagens GOOSE e novas regras correspondentes a este novo fluxo nos switches SDN [45].

A implementação da SDN oferece novos caminhos para a integração de sistemas e melhorias nos sistemas de proteção, controle e supervisão de subestações [36]. Esta solução permite a implementação de esquemas clássicos de controle e proteção, como seletividade lógica, falha de disjuntor e até esquemas de proteção de barras compartilhando a rede de comunicação. A aplicação da tecnologia SDN para interface permite o compartilhamento virtual entre agentes de qualquer informação de seus sistemas, como medições de tensão e correntes digitalizadas, no contexto da aplicação de barramento de processos segundo a norma IEC 61850 [36].

A Figura 17 ilustra uma aplicação potencial da interface SDN no contexto da digitalização de sistemas de proteção e controle baseados no protocolo SV. Nessa situação, a

merging unit (MU) transmite mensagens SV ao relé assinante da proteção de barras (87B) do agente oposto.

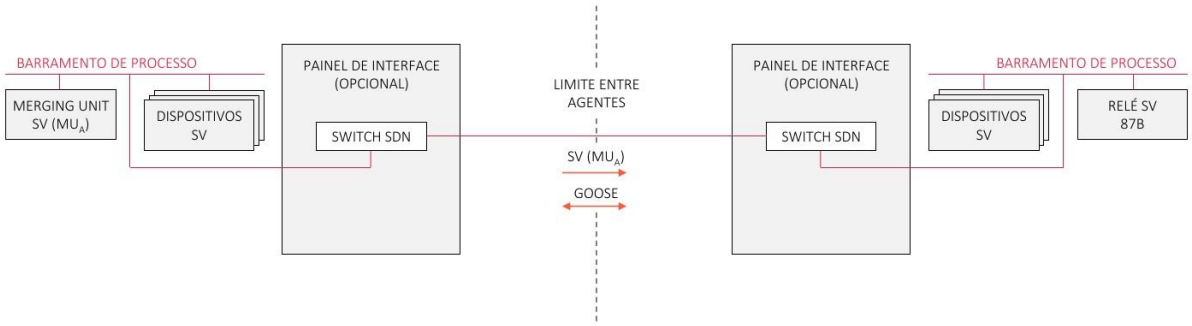

Figura 17 - Interface SDN para proteção de barras via SV [36]

4 Capítulo 4 – Metodologia da Pesquisa

4.1 Considerações Iniciais

A presente pesquisa lida com um estudo de caso em uma empresa multinacional do setor de transmissão de energia elétrica, sendo um dos principais players do Brasil no segmento, com apenas 14 anos de existência. A Delta (nome fictício) possui 104 subestações, entretanto, o estudo de caso delimita-se somente a 9 delas, as quais fazem parte do projeto do SEP N/NE/SE. A Delta é a empresa detentora do IED Master do referido SEP, portanto, foi a responsável pela determinação da melhor proposta de arquitetura de comunicação entre agentes distintos que vise mitigar as vulnerabilidades na troca de mensagens GOOSE. As diretrizes determinadas como parte do presente trabalho de mestrado foram aplicadas pelo corpo de engenharia da empresa Delta na seleção da proposta.

4.2 Classificação da Pesquisa

Essa pesquisa articula a combinação do referencial teórico entre segurança cibernética, sistemas especiais de proteção e requisitos de comunicação com base no framework proposto pela norma IEC 61850, em um estudo de caso no Sistema Especial de Proteção N/NE/SE, ao determinar uma proposta para mitigação de vulnerabilidades das mensagens GOOSE na comunicação entre agentes distintos.

As pesquisas científicas são em geral divididas entre básica e aplicada. A básica costuma investigar conhecimentos novos relacionados ao avanço da ciência, já a aplicada utiliza o conhecimento da básica para aplicações práticas, voltada para solucionar problemas. Este projeto trata-se de uma pesquisa aplicada com abordagem qualitativa de classificação descritiva e estudo de caso [11].

Inicialmente essa pesquisa pode ser considerada descritiva, pois descreve as características do fenômeno sistemas especiais de proteção e tem por finalidade identificar possíveis lacunas para melhorar a comunicação entre agentes distintos, pois tenta compreender como está a performance ofertada entre a troca das mensagens GOOSE e de qual maneira a ocorrência desse fenômeno pode elevar a segurança com alto desempenho de tráfego [11].

Também, como método de pesquisa, o estudo de caso tem como intuito investigar, analisar e propor aperfeiçoamento em um processo através de uma única unidade de exame. Ao observar o cenário do sistema especial de proteção N/NE/SE pretende-se obter um melhor

resultado por meio da observação do desempenho das mensagens GOOSE na ferramenta *Wireshark* e os IEDs escolhidos [12].

Quanto à natureza dos dados, a abordagem qualitativa apresenta-se como a mais apropriada, pois o objetivo está em encontrar a melhor alternativa para mitigar a vulnerabilidade na comunicação GOOSE entre agentes distintos, que atenda aos critérios de segurança cibernética definidos pelo Operador Nacional do Sistema Elétrico. Os critérios julgados como relevantes para a seleção da alternativa, foram determinados e aplicados pelo corpo de engenharia da empresa Delta – empresa detentora do IED Master do SEP – na análise das propostas de vários fornecedores do SEP e, por consequência, na identificação da melhoria no processo [11].

Para isso, a partir de benchmarking entre propostas de 4 fornecedores, e através de resultados dos testes das provas de conceito que foram aplicadas à alternativa escolhida, determina-se a metodologia com melhores características de segurança cibernética para o SEP. Desta forma, busca-se definir uma proposta de rede que mitigue a vulnerabilidade na comunicação GOOSE entre agentes distintos.

4.3 Técnicas de Coleta de Dados

Nesta pesquisa, adota-se a técnica de pesquisa documental, pois precisa-se da coleta de dados em fontes primárias, como documentos pertencentes a arquivos públicos, instituições particulares, domicílios e fontes estatísticas [12].

Desta forma, os dados foram coletados diretamente dos documentos de Parecer das Soluções dos Fornecedores e da Prova de Conceito para o SEP N/NE/SE da empresa Delta, e das especificações atribuídas pelo ONS no Relatório de Implantação do SEP N/NE/SE [7], e detalhado no documento Requisitos Mínimos da Rede LAN e WAN (RM-REDE) para a Implantação do Sistema Especial de Proteção Norte/Nordeste/Sudeste (SEP N/NE/SE) [46].

Após a coleta dos dados sobre as propostas das soluções dos fornecedores, tais informações foram contrastadas com as especificações. Como resultado desta análise, foi determinada a arquitetura de rede entre agentes que justifique ser submetida à prova de conceito. Assim, das informações práticas obtidas na prova de conceito, procurou-se definir uma proposta de integração segura de redes entre Agentes de Transmissão, que vise mitigar as vulnerabilidades das mensagens GOOSE no SEP N/NE/SE.

4.4 Procedimento para Análise dos Dados

A análise dos dados é uma das fases mais importantes da investigação, pois, a partir dela, serão apresentados os resultados e a conclusão da pesquisa, fechamento esse que poderá ser final ou apenas parcial, deixando margem para pesquisas posteriores [12].

Com base nas especificações do relatório de implementação do SEP e esmiuçado no documento Requisitos Mínimos da Rede LAN e WAN (RM-REDE) [46] para a Implantação do Sistema Especial de Proteção Norte/Nordeste/Sudeste (SEP N/NE/SE) [7], conforme premissas do ONS, analisou-se e verificou-se se os equipamentos e as soluções propostas como um todo atendem a cada um desses requisitos mínimos.

Desta forma, inicialmente foi realizada uma análise qualitativa na avaliação das propostas dos fornecedores (4). O fornecedor mais bem qualificado na análise foi convocado para verificação do atendimento dos requisitos, através de testes de Prova de Conecito (Poc).

Este trabalho teve foco em 4 testes realizados para examinar qual o nível de segurança e performance de melhoria na utilização da tecnologia para mitigar a vulnerabilidade na comunicação de mensagens GOOSE entre agentes distintos no SEP N/NE/SE.

4.4.1 Propostas dos Fornecedores

São participantes da proposta quatro fornecedores, são empresas com ampla experiência na solução para comunicação entre agentes distintos. Nas análises, estes fornecedores serão chamados de Empresa 1, 2, 3 e 4. Cada *player* possui sua particularidade na solução.

A Empresa 1, conforme pode ser visto na Figura 18, apresenta em sua proposta uma arquitetura considerando uma subestação com múltiplos agentes. O ponto central da arquitetura é a utilização exclusiva de multiplexador – MUX (equipamento WAN), esse equipamento vem integrado com software de gerência que permite a realização de criptografia entre os MUXs. Além disso, a aplicação não prevê uso de switches em conjunto com o MUX.

As ligações em azul e preta são análogas, e representam uma conexão dupla, para implementação do protocolo de redundância (PRP), sendo as duas ligações em azul conduzidas por um caminho e as ligações em preto por outro caminho. Assim, cada linha representa uma porta Ethernet tanto no IED como no equipamento WAN, trafegando a 100 Mb/s e utilizando MPLS-TP (*Multiprotocol Label Switching - Transport Profile*) - tecnologia de roteamento de pacotes. A ligação entre equipamentos WAN tem banda de 10Gb/s e utiliza criptografia

Advanced Encryption Standard (AES). Adotando essa solução proposta, garante o tempo de 150 ms para as lógicas de estabilidade de *run-up/back*. Além disso, o fornecedor estima o tempo de transmissão na ordem de 4 ms entre IEDs e o equipamento WAN, e de 8 ms entre o seu equipamento WAN e o equipamento WAN do detentor da Master, onde os dados serão entregues.

Vale destacar ainda, que nessa arquitetura, o acesso ao supervisório local pode ser feito por outros equipamentos da rede LAN (*Local Area Network*) do agente, ou pode ser feito por uma das portas Ethernet do equipamento WAN caso o dono do IED também seja o dono do multiplexador. Destaca-se que, como o equipamento WAN também atua como *firewall*, ele poderia proporcionar a proteção da rede do agente com relação ao que vem da rede do SEP. Entretanto, o servidor de supervisão e gerência na Master estão ligados na LAN da Delta para que sejam feitos os acessos remotos aos serviços. Contudo, esse mesmo servidor está ligado também no equipamento WAN de outro agente.

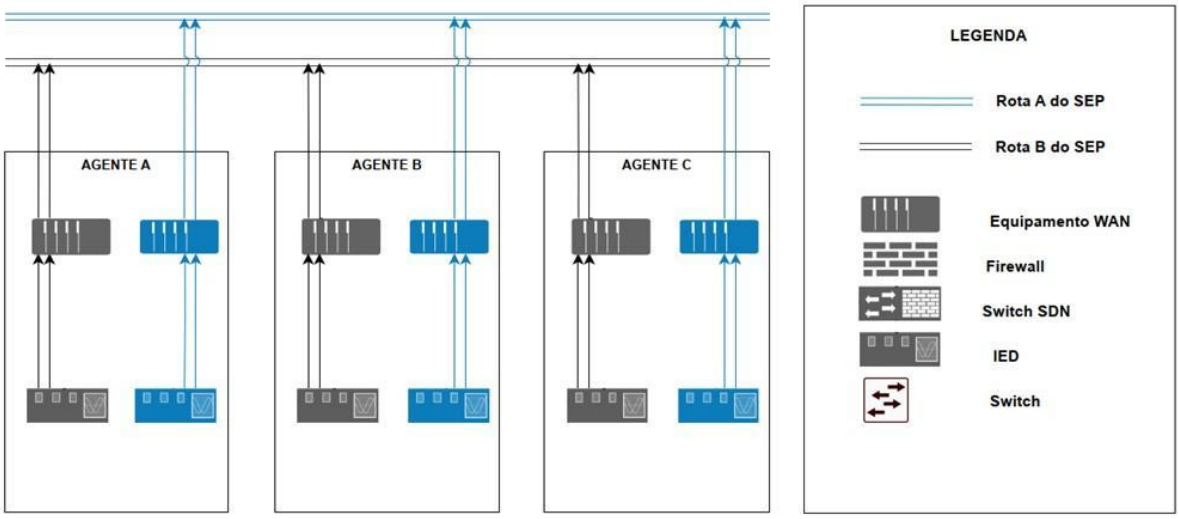

Figura 18 - Arquitetura para SE com múltiplos Agentes da Empresa 1. Fonte: Elaboração própria

Na arquitetura proposta pelo fornecedor, o IED do agente A é conectado diretamente no MUX, com redundância de porta. Nessa proposta, o equipamento WAN do fornecedor também atua como equipamento de segurança, protegendo a comunicação com os agentes B e C durante a troca de mensagens GOOSE.

A Empresa 2 apresentou em seu projeto uma proposta que busca delimitar as zonas de segurança, protegendo tanto a rede do SEP quanto a rede dos agentes contra a possibilidade de disseminação de ataques. Nesse caso, existe um *firewall* que restringe os limites da rede do agente, e outro que protege a entrada na rede do SEP. Cabe a observação que esse *firewall* de

entrada na rede do SEP tem características de switch gerenciável por HTTPS ou *Secure Shell* (SSH) - protocolo de rede criptográfico para operação de serviços de rede de forma segura sobre uma rede insegura - e com capacidade de sincronismo via PTP, tanto para mensagens R-GOOSE (*Routable Generic Object Oriented Substation Event*) em L3 (switch de camada 3, que opera tanto em camada de enlace de dados quanto na camada de rede) e em L2 (switch de camada 2, camada de enlace) .

Conforme destaca a Figura 19, assume-se que a rede de processo é segura com uso de GOOSE, uma mensagem de camada 2 (não permitindo o uso do *firewall*) atuando a partir da camada 3, com proposta de atuação com R-GOOSE ao encapsular o pacote de camada 2 e rotear na rede. A empresa sugere como equipamento de segurança o uso de um switch proprietário utilizando função ACL (*Access Control List).* No entanto, como diferencial, tem a implementação de R-GOOSE, recentemente recomendado para comunicação em WANs. Tem, ainda, suporte a PRP. Cada agente deverá ter dois switches, sendo que cada IED deve ser ligado nos dois switches. Um dos switches deve ser ligado na rede principal (rota A) e o outro na rede alternada (rota B).

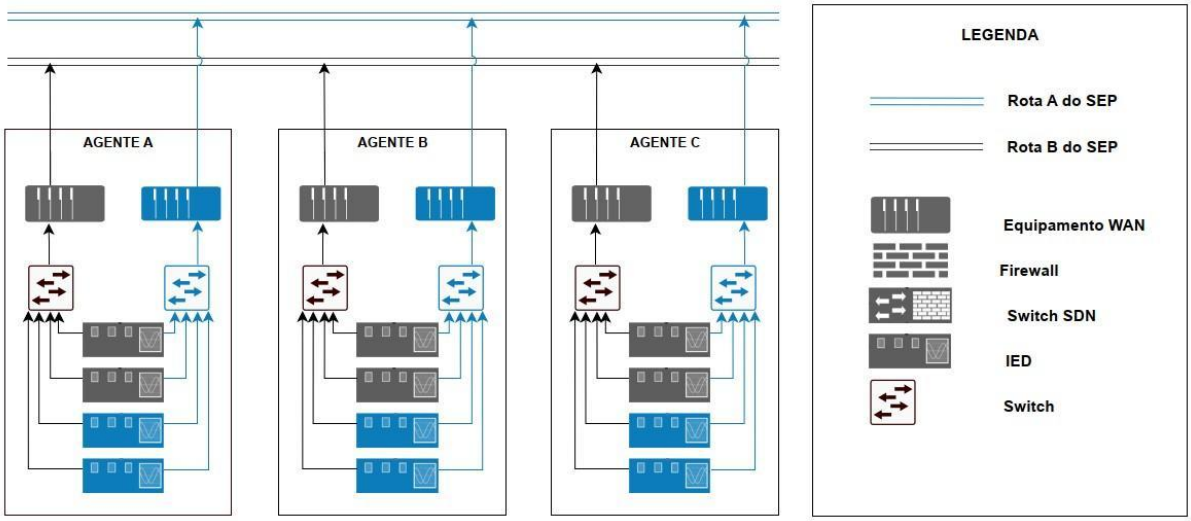

Figura 19 - Arquitetura para SE com múltiplos Agentes da Empresa 2. Fonte: Elaboração própria

Na arquitetura proposta pelo fornecedor, o IED do agente A é conectado diretamente a um switch com função ACL, em uma arquitetura em PRP. Nessa proposta, o switch com função ACL atua como equipamento de segurança. O equipamento de segurança é interligado ao equipamento WAN que faz a comunicação entre agentes B e C trocando mensagens GOOSE.

A Empresa 3 expôs uma solução para os IEDs locais, responsáveis pela aquisição dos sinais de tensão, corrente e estados necessários para cada vão de linha, para comunicação com

o multiplexador do SEP proposto. A referida empresa indicou o uso de switches SDN na arquitetura como um componente segregador de tráfego e de segurança cibernética, por consequência, isolando e controlando o que entra e sai.

Sendo assim, conforme Figura 20, é proposto o uso do switch SDN para segregar as mensagens dos agentes. Onde, cada agente pode utilizar o switch SDN como equipamento de segurança entre o equipamento WAN e o IED local.

É ressaltado que a porta do IED conectada no switch tem todos seus protocolos desabilitados permitindo apenas a passagem de GOOSE, assim como a porta entre o switch SDN e o equipamento WAN. Vale destacar ainda, que os switches SDN interligam estes IEDs e o equipamento WAN da sua respectiva cadeia. Sendo assim, tem-se um switch SDN por cadeia, conectado ao MUX (equipamento WAN) de saída para cada rota. Além disso, têm-se a possibilidade de configuração de uma mensagem GOOSE com publicação lenta para os valores com requisitos de tempo não críticos, como por exemplo analógicos e monitoramento, e outra mensagem GOOSE com publicação rápida para estado e contingências na interface entre o switch e o MUX.

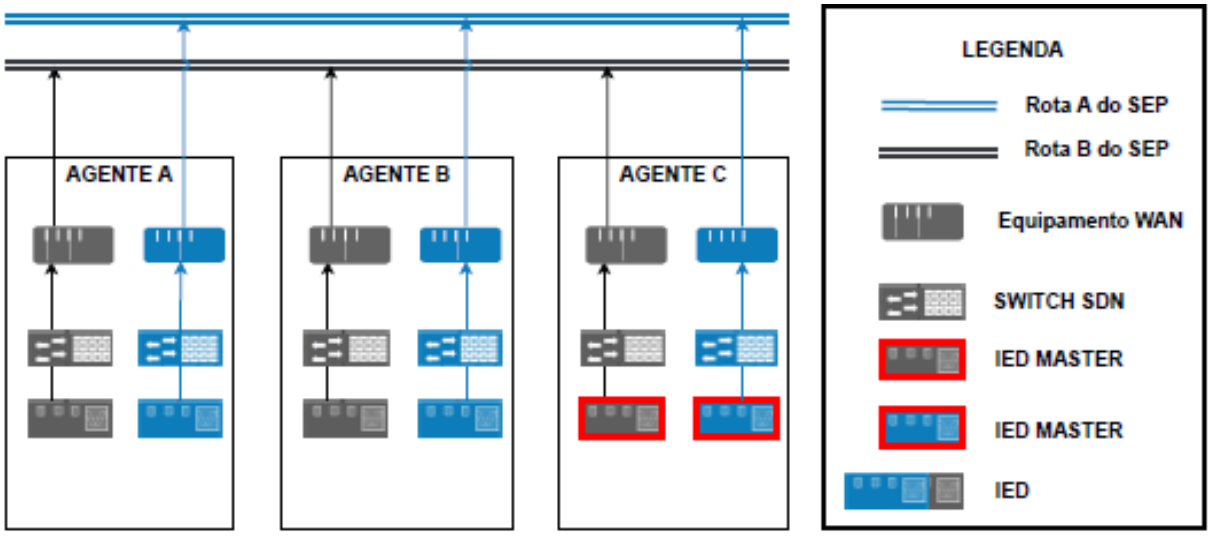

Figura 20 - Arquitetura para SE com múltiplos Agentes da Empresa 3. Fonte: Elaboração própria

Na arquitetura proposta pelo fornecedor, o IED do agente A é conectado diretamente a um switch SDN. Nessa proposta, o switch SDN atua como equipamento de segurança. O equipamento de segurança é interligado ao equipamento WAN que faz a comunicação entre agentes B e C trocando mensagens GOOSE.

A Empresa 4 apresentou, conforme Figura 21, uma arquitetura com os switches interligando os IEDs e o equipamento WAN da sua respectiva cadeia. Sendo assim, tem-se um

switch por cadeia, conectado ao MUX (equipamento WAN) de cada rota. Na solução proposta, existe um *firewall* entre o switch e os IEDs. Os agentes são segregados por VLANs, tanto na cadeia principal quanto na alternada. Assim, cada agente possui sua VLAN na cadeia principal e outra VLAN na cadeia alternada. O *firewall* que fica entre o IED e o switch do SEP é responsável por filtrar a comunicação do IED com a rede do SEP.

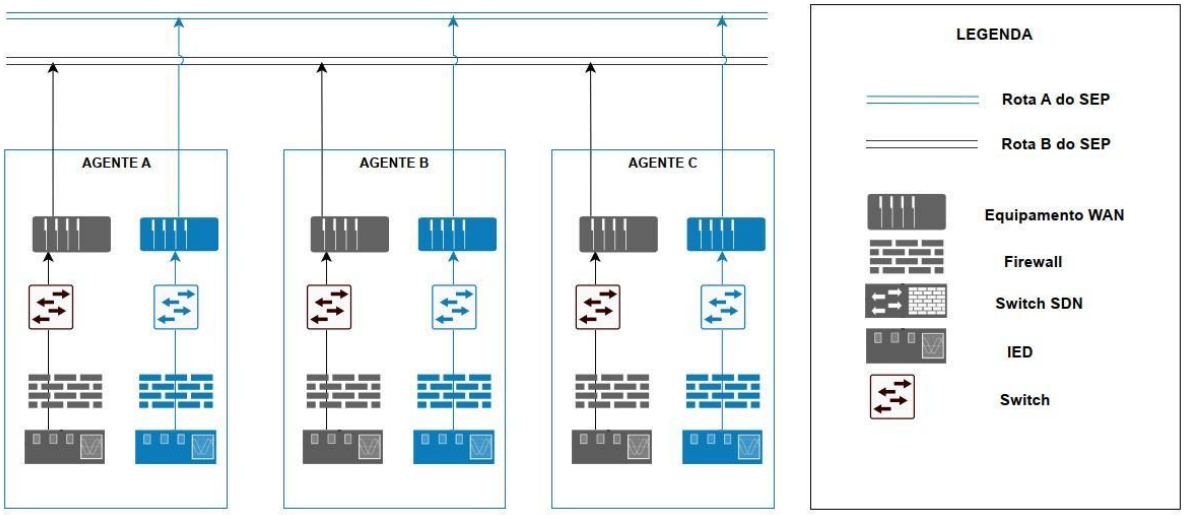

Figura 21 - Arquitetura para SE com múltiplos Agentes da Empresa 4. Fonte: Elaboração própria

Na arquitetura proposta pelo fornecedor, o IED do agente A é conectado diretamente a um *firewall*, que atua como equipamento de segurança. O *firewall* é interligado com o switch, que por sua vez e conectado ao equipamento WAN que faz a comunicação entre agentes B e C trocando mensagens GOOSE.

4.4.2 Especificações para análise das propostas de fornecedores

Nesta seção são abordadas as especificações fundamentais conforme hipótese e interesse desse estudo de caso, e todos os critérios são requisitos mínimos da rede LAN e WAN (RM-REDE) para o SEP N/NE/SE conforme ONS [3], [46].

Como aspecto geral, a arquitetura proposta deve ser flexível para permitir adequações e expansões nas lógicas e infraestrutura física, que possam ser necessárias em decorrência da expansão da rede, mesmo que as novas expansões sejam feitas com fornecedores distintos da solução original, bem como com equipamentos de diferentes fabricantes.

Os dois principais requisitos explorados nesse estudo de caso sobre a arquitetura da rede do SEP são:

1. Os dados analógicos e digitais necessários para implementação da lógica do SEP devem ser enviados somente através de mensagens GOOSE pela rede do SEP;

2. Para a rede do SEP é obrigatório que seja prevista a segmentação da rede com recursos como a utilização de VLANs e a priorização de mensagens GOOSE, garantindo isolamento e a qualidade de serviço destas mensagens. Esses recursos devem ser definidos no projeto básico.

Já para a arquitetura da rede de monitoramento, têm-se como principais exigências:

3. Devem ser previstos, entre o ponto de coleta do Agente e o sistema de monitoramento da Master, a utilização de equipamentos e protocolos de segurança sob responsabilidade do Agente.

4. O protocolo utilizado para troca de informações entre o ponto de coleta de cada Agente e o gerenciamento central da Master é de responsabilidade do Agente responsável pela Master, podendo ser, inclusive, *Hypertext Transfer Protocol Secure* (HTTPS).

5. O protocolo utilizado para troca de informações entre o ponto de coleta de cada Agente e o gerenciamento central da Master deve dar suporte a criptografia das informações.

6. Os equipamentos do SEP devem ser monitorados através de SNMP (versão a cargo do Agente) até o ponto de coleta. Protocolos proprietários não são recomendados para a rede de monitoramento.

7. A porta conectada à rede de monitoramento do equipamento, por onde trafega SNMP, deve ser distinta da porta da rede do SEP, por onde trafega GOOSE.

8. O ponto de coleta deve disponibilizar para o sistema de monitoramento central da Master as variáveis relacionadas aos equipamentos da LAN do SEP, sendo estes o equipamento de segurança e os IEDs (se este tiver monitoramento SNMP disponível) que minimamente são: Estado (*up* e *down*) de todas as interfaces; Estado (*up* e *down*) dos equipamentos; Taxa de erro de todas as interfaces; Taxa de envio e recebimento de todas as interfaces; Carga de CPU.

Com destino à arquitetura da rede de supervisão as obrigações essenciais são:

9. Os IEDs do SEP devem ser supervisionados através do protocolo MMS da norma IEC 61850.

10. A porta de supervisão do equipamento, por onde trafega MMS, deve ser distinta da porta da rede do SEP, por onde trafega GOOSE. No entanto, caso necessário, pode ser compartilhada com a porta da rede de monitoramento do SEP, devendo ser observada a segmentação lógica entre essas redes.

11. Além dos pontos de supervisão do SEP definidos no RT-ONS-DPL 0131/2021 [25], devem ser monitorados os nós lógicos LCCH (*Logical Node for Comunication Channel Supervision*) e LGOS (*Logical Node for GOOSE Supervision*), para supervisão do canal de comunicação e das mensagens GOOSE que trafegam no IED, respectivamente.

12. O ponto de coleta de supervisão pode ser um sistema supervisório ou um Gateway.

13. É obrigatório que o sistema de supervisão na Master possua IHM (Interface Homem-Máquina) para visualização gráfica de todas as medições de fluxo, falhas de IEDs, falhas GOOSE e de canal conectado ao IED, linhas com estado aberto ou inconsistente e qualquer outra informação de supervisão que se faça necessária.

Sobre os IEDs locais e IED da master, estes devem possuir hardware modular com capacidade de expansão futura.

A respeito do sincronismo temporal, este deve ser realizado com protocolo PTP ou IRIG-B (*Inter-ange instrumentation group timecode*), sendo que o SNTP não é indicado e a precisão temporal entre os IEDs que compõe o SEP deve se manter em até 1ms. A arquitetura e protocolo utilizados são de escolha do Agente, conforme definido pela ONS [46].

Nos aspectos de segurança, deve-se adotar a sistemática descrita a seguir:

14. O controle de acesso de todos os equipamentos dentro do SEP (IEDs e dispositivos de rede) deve ser feito através de Controle de Acesso Baseado em Papéis (RBAC - *Role-based access control*).

15. Cada Agente deve criar e manter sua base de usuários e papéis em seu sistema RBAC. É recomendável que seja utilizado um protocolo aberto para armazenar essa estrutura, como por exemplo, o *Lightweight Directory Access Protocol* (LDAP).

16. Todos os IEDs devem se conectar ao equipamento de segurança do SEP, que é capaz de filtrar e limitar o tráfego da rede do SEP. Adicionalmente, cada Agente deverá ter seu *firewall* para segurança da sua própria rede.

    16.1. Esse dispositivo pode ser um switch SDN, um *firewall* capaz de filtrar na camada 2 ou um switch capaz de desabilitar o aprendizado dinâmico de endereço MAC e fazer uma lista de controle de acesso (ACL - *Access Control List*).

    16.2. Esse equipamento deve minimamente filtrar os campos: Endereço MAC de origem e destino, *Ethertype* e VLAN.

17. O equipamento de segurança deve possuir um mecanismo para limitar a banda de cada fluxo de rede. Esse mecanismo visa limitar os efeitos de um possível ataque de negação de serviço (DoS – *Denial-of-service*) através de um fluxo permitido dentro da rede do SEP.

18. Todos os Agentes devem possuir um sistema centralizado de logs, como o *Syslog*, para os equipamentos do SEP sob sua responsabilidade.

19. Os logs devem notificar qualquer modificação nas configurações tanto dos equipamentos de rede quanto dos IEDs.

20. O sistema de log deve ser usado como base para auditoria de todas as ações tomadas nos equipamentos.

21. Todos os serviços não utilizados dentro da rede do SEP devem ser desabilitados nos equipamentos do SEP, sejam eles IEDs ou dispositivos de comunicação.

22. Nas interfaces de rede do SEP, apenas o protocolo GOOSE deve estar habilitado, visto que nenhum outro serviço trafega pela rede.

23. Todas as interfaces de rede não utilizadas devem ser desabilitadas via software ou hardware. Isso deve ser feito tanto nos dispositivos de rede quantos nos IEDs, quando possível.

24. O acesso a todos os dispositivos deve ser feito exclusivamente através do RBAC.

25. Todo equipamento deve ser capaz de reportar logs de segurança para um servidor (syslog).

26. A rede do SEP deve contar também com um sistema de detecção de intrusão (IDS - *Intrusion Detection System*).

26.1. É fortemente recomendável que cada Agente possua seu próprio IDS.

26.2. O Agente responsável pela Master deve ter um IDS para todo o tráfego SEP.

26.3. O IDS da Master deve minimamente receber todo o tráfego direcionado aos IED Master através de espelhamento de porta.

Não menos importantes acerca do desempenho:

27. O atraso entre IED local de origem e IED local de destino (passando pela Master), desconsiderando o tempo dos equipamentos e enlaces WAN, não deve ultrapassar um total de 37 ms mesmo em condições de sobrecarga no sistema, exceto para medidas analógicas.

27.1. Os IEDs e a Master, assim como equipamentos de segurança e qualquer outro equipamento inserido na proposta do fornecedor, devem ser devidamente dimensionados pelos fornecedores para garantir esse atraso máximo de 37 ms. O atraso máximo deve ser devidamente aferido nos testes de aceitação de fábrica e comissionamento.

28. O atraso máximo na WAN é definido como o somatório dos tempos gastos pelo quadro desde a entrada no Equipamento WAN de saída na subestação de origem até a saída no Equipamento WAN de entrada na subestação da Master. O atraso de comunicação em rede WAN não deve ultrapassar o tempo máximo de 63 ms.

4.4.3 Contextualização do Método Proposto

O principal objetivo deste capítulo foi definir especificações baseadas em normas e regimentos, as quais subsidiarão, posteriormente, a seleção da melhor arquitetura de rede, em termos de segurança cibernética, dentre 4 propostas de diferentes fornecedores. Assim, será desenvolvida a prova de conceito (PoC - *proof of concept*), cujos critérios de testes a serem aplicados serão definidos com base nas características da arquitetura selecionada. Finalmente, após validação prática do desempenho da arquitetura escolhida, determinar-se-á a proposta a ser recomendada neste trabalho para implantação do SEP com garantia de mitigação de vulnerabilidades na troca de mensagens GOOSE entre agentes.

5 Capítulo 5 – Resultados da Pesquisa

5.1 Objetivo da pesquisa

Este estudo de caso se restringe em analisar dados coletados pela empresa Delta (nome fictício) de quatro fornecedores reconhecidos no mercado, seguindo as especificações e critérios determinados no Capítulo 4. A pesquisa se aplica no setor elétrico e, de forma mais objetiva, busca-se determinar a melhor proposta de segurança cibernética entre agentes de transmissão distintos, em redes baseadas na norma IEC 61850, para mitigação de vulnerabilidades das mensagens GOOSE.

5.2 Análise das Propostas

Nessa seção são abordados os pontos fortes e fracos de cada proposta, contrapondo com as especificações e a norma IEC 61850, para isso, são considerados os fatores: Tempo e Banda; Disponibilidade e Segurança. Desta forma, são analisados os seguintes aspectos:

- Arquitetura: com facilidade de ser ampliada, fácil operação e manutenção, e equipamento de segurança com capacidade filtrar os campos;
- Filtro: Endereço MAC de origem e destino, Ethertype e VLAN;
- Limitação de banda: capacidade de limitação de banda;
- Desativar serviços: capacidade de desativar serviços não utilizados;
- Latência: o equipamento de segurança deve atender o limite de latência.

No final dessa secção e com base nessa análise, será feito um quadro comparativo considerando os seguintes critérios de avaliação: “Não Atende”; “Atende Parcialmente”; “Atende”; “Supera”. No qual, os critérios terão as pontuações 0, 1, 2 e 3, de forma respectiva, com objetivo em descobrir qual proposta tem maior aderência com as especificações determinadas no Capítulo 4.

5.2.1 Empresa 1

Pontos fortes apresentado pela Empresa 1.

Tempo e Banda:

1. Menor atraso na comunicação devido a não haver necessidade de conversão de Ethernet para SDH.

2. Banda disponível muito superior às necessidades do SEP, com 100 Mb/s entre IED e MUX (Multiplexador) e 10Gb/s entre multiplexadores.

Disponibilidade e Segurança: Não houve pontos de destaque.

Pontos fracos demonstrados pela Empresa 1.

Tempos e Banda:

1. As estimativas de banda e atraso de comunicação apresentados com pouco detalhamento, sem justificar a diretriz de tempo exposta no subcapitulo 4.4.2, item 27.1.

Disponibilidade e Segurança:

1. Não foram previstos mecanismos de redundância para o sistema de gerência e supervisão, apesar de existirem diversos modelos de disponibilidade bem conhecidos para arquiteturas virtualizadas, tais como redundância ativa-ativa (múltiplos operam simultaneamente) e ativa-passiva (um componente principal está ativo enquanto um ou mais componentes permanecem em *backup*).

2. Os dispositivos de supervisão dos IEDs da Delta e dos Masters da cadeia principal e alternada estão ligados no mesmo MUX (equipamento WAN). Isso torna esse MUX um ponto único de falha, o que não está de acordo com as especificações, conforme item 10 da seção 4.4.2.

3. A criptografia proposta pelo fornecedor não utiliza RBAC, portanto, não estando alinhado com o item 24 da seção 4.4.2. A criptografia entre equipamentos WAN protege contra-ataques de interceptação e *spoofing*, caso seja possível interceptar a comunicação e inserir um equipamento intermediário. Esse cenário é muito pouco provável dentro SEP e seria notificado por queda de enlace e interrupção de transmissão de GOOSE nos sistemas de gerência. Além disso, como existem circuitos de comunicação com segregação de tráfego, as mensagens GOOSE de um IED só chegam ao IED Master, de forma que a privacidade dos dados já é naturalmente preservada.

4. Além disso, ao verificar a necessidade de uso de switches para implementação do SEP, já não garante que há informação falsa inserida na comunicação com o esquema de criptografia a partir do MUX. Portanto, o sistema de criptografia não traz vantagens claras e insere maior complexidade no sistema, em dissenso com o item 5 da seção 4.4.2.

5. Não foi explicitamente previsto o uso de *firewall* entre o IED e a LAN do agente, embora tenha sido comentado que o uso desse *firewall* é perfeitamente adequado à solução

proposta, podendo inclusive ser utilizado o *firewall* do próprio MUX (equipamento WAN), caso o agente em questão tenha um multiplexador híbrido dentro da subestação. Esse arranjo, embora reduza custos, aumenta a complexidade de configuração do SEP, além de demandar mais um switch interno do MUX exclusivamente para a conexão entre a LAN e o IED do SEP.

Em resumo, a arquitetura proposta é pouco escalável, pois interliga o IED diretamente ao equipamento WAN. Embora essa arquitetura tenha baixa escalabilidade, ela reduz a quantidade de equipamentos necessários para processar dados, o que melhora o impacto da latência.

Na solução apresentada, o equipamento WAN também desempenha a função de equipamento de segurança. Segundo o fornecedor, ele possui funcionalidade de *firewall* L2 para controlar a entrada do tráfego no SEP. No entanto, não foram especificados os campos disponíveis para essa filtragem. Na apresentação, foi mencionado apenas o uso de uma faixa de endereços *Media Access Control* (MAC), o que é insuficiente para garantir a segurança do SEP.

A proposta também menciona a capacidade de limitação de banda para proteção contra-ataques de negação de serviço. Contudo, não foi apresentado nenhum mecanismo que assegure a prevenção ou o sucesso desses ataques.

Em relação à desativação de serviços, não foram detalhados os mecanismos de *hardening* que podem ser aplicados ao sistema proposto.

5.2.2 Empresa 2

Pontos fortes abordados pela Empresa 2.

Tempos e Banda:

1. A solução proposta pode ser usada com SDH ou MPLS-TP, conforme decisão do cliente. Caso haja a possibilidade de MPLS-TP, isso aumentaria a banda disponível e reduziria os atrasos de transmissão.

2. Suporte ao protocolo de sincronização de tempo IEEE 1588 e a norma IEC 61850.

Disponibilidade e Segurança:

1. O sistema proposto apresenta alta disponibilidade em termos de rede de comunicação, pois o volume de tráfego gerado na rede de trânsito é equivalente ao gerado pelo

PRP, mas com maior disponibilidade, sendo que cada Master irá receber tanto o conjunto de informações da cadeia principal quanto da cadeia alternada.

2. A configuração proposta para os switches com uso de VLAN e ACL permite uma restrição criteriosa dos fluxos de entrada no SEP, assim como garante um controle de banda máxima por porta, promovendo maior segurança na rede. Os switches dão suporte ao SNMP e são gerenciados por HTTPS ou por SSH, apresentando autenticação remota via *Remote Authentication Dial-In User Service* (RADIUS) e *Terminal Access Controller Access-Control System* (TACACS). Também é proposto um multiplexador, que permitiria a migração para MPLS-TP, garantindo bandas maiores disponíveis para o SEP.

Pontos fracos evidenciados na proposta da Empresa 2.

Tempos e Banda:

1. A empresa não justificou sobre os tempos associados ao *firewall*, ACL e *storm control* - estabelece uma taxa máxima de dados na porta, visando garantir proteção da rede do SEP contra-ataques de negação de serviço gerado a partir de um dos agentes que tenha sido invadido. Portanto, não sendo possível garantir o tempo 37 ms requerido no item 27 da seção 4.4.2.

2. Não foi estimada a banda ocupada na rede do SEP pelo tráfego de gerência e segurança. Semelhante ao anterior, em desarmonia com item 17 da seção 4.4.2.

Disponibilidade e Segurança:

1. Não foi indicado o uso de IDS, que pode ser uma ferramenta interessante para aumentar o nível de segurança da solução em desacordo com item 26 da seção 4.4.2.

Em síntese, a arquitetura proposta apresenta dificuldades de configuração e manutenção devido à complexidade do PRP, sem oferecer um ganho significativo de redundância, já que a arquitetura do SEP possui duas rotas distintas.

A solução apresentada para o equipamento de segurança é um switch com função ACL, capaz de realizar filtros por endereço MAC de origem e destino, Ethertype e VLAN. No entanto, sua configuração é complexa em comparação com outras propostas, sendo também pouco escalável e por consequência limitada.

O equipamento proposto garante o controle de banda máxima por porta e possui a capacidade de desativação de serviços. Contudo, essa desativação é de baixa escalabilidade, pois não pode ser realizada de forma centralizada.

5.2.3 Empresa 3

Pontos fortes abordados pela Empresa 3.

Tempos e Banda:

1. Simplicidade no monitoramento de desempenho de tempo e banda, através do fornecimento de um software para gerenciamento de fácil interpretação.

Disponibilidade e Segurança:

1. Possibilidade de redundância total de monitoramento e gerência do switch, pois o SDN permite monitoramento por *OpenFlow* e por SNMP.

2. A possibilidade de criação das regras visando segurança cibernética no switch SDN são bastante robustas e incluem todos os campos de camada 2/3/4, além de porta de entrada e saída e *meters*.

3. Coordenação da atuação entre as Unidades Master.

Pontos fracos evidenciados na proposta da Empresa 3.

Tempos e Banda:

1. O IED proposto possui no máximo 2 portas não sendo possível o uso de PRP na solução.

2. Não apresentou proposta de sincronismo, como a empresa anteriormente mencionada. Deixou a cargo do cliente.

Disponibilidade e Segurança:

1. Não esclareceu como funciona a proteção contra *spoofing*.

2. Não mencionou a parte de log de autenticação e acesso nos IEDs, software e switches, em contraste com as demais propostas.

3. Não mencionou se o switch é capaz de notificar modificações em sua configuração via SNMP, diferente das outras empresas.

De forma concisa, o equipamento de segurança é um switch com função SDN, capaz de realizar filtros por endereço MAC de origem e destino, Ethertype e VLAN. O equipamento possui um diferencial importante: maior granularidade na configuração dos filtros, permitindo separação por usuários ou por tipo de comunicação.

O equipamento proposto garante o controle de banda máxima por porta, com fácil configuração, que pode ser realizada através de gerência centralizada. Além disso, permite a desativação de serviços que não estão em uso, também de forma centralizada.

Em relação à latência, o equipamento de segurança proposto reduz o tempo de processamento, pois o encaminhamento das informações é pré-definido.

5.2.4 Empresa 4

Pontos fortes abordados pela Empresa 4.

Tempos e Banda:

1. A empresa garante a capacidade de limitação de banda.

Disponibilidade e Segurança:

1. Possui sistema que monitora o desempenho da rede, saúde dos equipamentos e mudança de configuração nos switches.

2. Atendimento ao ARCiber. Ex: Possui sistema de inventário dos ativos do SEP; possui autenticação de múltiplos fatores.

Pontos fracos evidenciados na proposta da Empresa 4.

Tempos e Banda:

1. Sugeriu o uso de VXLAN (*Virtual Extensible LAN*) em uma rede exclusivamente de camada 2, segmentada por VLAN. No próprio documento destaca a importância de se manter na camada 2 para garantir a latência do SEP, porém ao utilizar VXLAN o tráfego sobe para camada 3.

Disponibilidade e Segurança:

1. Não foi demonstrado um cenário onde o *firewall* pode ser utilizado exclusivamente em camada 2, sem a necessidade de VXLAN. Não ficou claro se o *firewall* pode ser utilizado em camada 2.

Resumidamente, a arquitetura proposta é simples e facilmente escalável. No entanto, foi sugerido o uso de R-GOOSE para comunicação entre os agentes, o que não é viável, pois não é aceito na especificação.

Em relação ao equipamento de segurança, foi proposto o uso de um *firewall*, mas não foram fornecidos detalhes sobre a capacidade do equipamento de operar na camada 2, realizando filtros por endereço MAC de origem e destino.

O fornecedor garante a capacidade de limitação de banda, mas não explicou como isso seria implementado. Além disso, não foram fornecidos detalhes sobre como seria realizada a desativação dos serviços não utilizados.

5.2.5 Resultado da Análise das Propostas

Com base nas especificações da seção 4.4.2 e nos aspectos considerados na análise das propostas (seção 5.2.4) – arquitetura, filtro, limitação de banda, desativar serviços e latência – foram determinados 10 quesitos que permitam uma comparação didática e correspondente avaliação das propostas apresentadas. Esses quesitos examinam elementos gerais das 27 especificações, bem como elementos específicos, conforme exposto na Tabela 2.

Tabela 2 - Comparação das Propostas. Fonte: Elaboração própria

Quesito	Empresa 1	Empresa 2	Empresa 3	Empresa 4
Arquitetura Simplificada. Especificação geral seção 4.4.2.	Não Atende	Atende parcialmente	Atende	Atende
Equipamento de Segurança com tráfego de proteção, sem inserir atraso significativo na rede. Especificação: item 27, da seção 4.4.2.	Atende parcialmente	Atende parcialmente	Supera	Não Atende
Todos IEDs conectados ao equipamento do SEP. Especificação: item 18 da seção 4.4.2.	Atende	Atende	Atende	Atende
Equipamento de segurança filtrando os campos: Endereço MAC origem e destino, Ethertype e VLAN. Especificação: itens 16.1. e 16.2. da seção 4.4.2.	Atende Parcialmente	Atende parcialmente	Atende	Atende
Firewall capaz de filtrar na camada 2. Especificação: 16. da seção 4.4.2.	Atende parcialmente	Atende	Atende	Não Atende
Firewall para segurança da rede. Especificação item 16.1 da seção 4.4.2.	Não Atende	Não Atende	Atende	Não Atende

Equipamento de segurança com mecanismo para limitar a banda de cada fluxo de rede. Especificação: item 17 da seção 4.4.2	Atende Parcialmente	Atende parcialmente	Atende	Atende Parcialmente
Conexões entre IEDs da LAN e rede dos Agentes protegidas por um equipamento de segurança. Especificação: item 16 da seção 4.4.2.	Atende parcialmente	Atende	Atende	Atende
Rede com utilização de VLANs e priorização de mensagens GOOSE. Especificação: item 2 na seção 4.4.2.	Atende Parcialmente	Atende parcialmente	Supera	Atende Parcialmente
Atraso entre IED local de origem e IED local de destino (passando pela Master) e dos equipamentos e enlaces WAN < 37 ms. Especificação: item 27.1. da seção 4.4.2.	Atende Parcialmente	Atende	Supera	Atende Parcialmente

A Tabela 2 com a avaliação qualitativa das propostas dos fornecedores, será transformada com as respectivas pontuações na Tabela 3 a seguir.

Tabela 3 - Comparação da Pontuação das Propostas dos Fornecedores. Fonte: Elaboração própria

Quesito	**Empresa 1**	**Empresa 2**	**Empresa 3**	**Empresa 4**
Arquitetura Simplificada	0	1	2	2
Equipamento de Segurança com Tráfego de Proteção, sem inserir atraso significativo na rede.	1	1	3	0
Todos IEDs conectados ao equipamento do SEP	2	2	2	2
Equipamento de segurança com tráfego de rede filtrando os campos: Endereço MAC origem e destino, Ethertype e VLAN	1	1	2	2
Firewall capaz de filtrar na camada 2	1	2	2	0
Firewall para segurança da rede	0	0	2	0

Equipamento de segurança com mecanismo para limitar a banda de cada fluxo de rede	1	1	2	1
Conexões entre IEDs da LAN e rede dos Agentes protegidas por um firewall	1	2	2	2
Rede com utilização de VLANs e priorização de mensagens GOOSE	1	1	3	1
Atraso entre IED local de origem e IED local de destino (passando pela Master) - desconsiderando o tempo de disjuntor e dos equipamentos e enlaces WAN < 37 ms	1	2	3	1

Com base da Tabela 3 tem-se o resultado exposto na Tabela 4, após o somatório da pontuação das empresas em cada um dos requisitos apresentado.

Tabela 4 - Resultado da Pontuação da Comparação das Propostas. Fonte: Elaboração própria

Fornecedores	**Empresa 1**	**Empresa 2**	**Empresa 3**	**Empresa 4**
Resultado	9	13	23	11

O resultado da análise ressalta o uso da arquitetura baseada em switches SDN como um diferencial para chegar no objetivo de obter segurança cibernética e mitigar a vulnerabilidade das mensagens GOOSE. Tal diferencial se destaca pela superioridade do switch SDN em termos de granularidade (políticas e controles detalhados a fluxos de dados específicos), segurança, flexibilidade e capacidade de adaptação às mudanças dinâmicas na rede. A opção por não realizar testes com ACLs ou *firewalls stateful* no modo transparente se baseou na compreensão de que essas tecnologias, embora eficazes em certos contextos, não oferecem o mesmo nível de proteção e adaptabilidade que o switch SDN pode proporcionar, especialmente quando o foco está em garantir segurança robusta e filtragem eficiente na camada 2.

Desta forma, em adição ao resultado da pontuação da comparação das propostas, destaca-se a proposta da Empresa 3, e por consequência será submetida à prova de conceito.

5.3 Aplicação dos Testes para Prova de Conceito

Conforme se destacou no subcapítulo anterior, a arquitetura proposta pela Empresa 3 apresentou maior aderência às especificações determinadas, portanto, os testes de Prova de Conceito (PoC – *proof of concept*) são aplicados com base nessa proposta.

Assim, para validação da proposta selecionada a partir da avaliação do cumprimento das especificações, são considerados 4 critérios que norteiam os testes aplicados na PoC. Tais testes são recomendados devido às especificações 16, 17, 21, 22, 23 e 27 do item 4.4.2. A Tabela 5 apresenta a relação entre as especificações e os critérios de testes de PoC.

Tabela 5 - Relação entre as especificações e testes de PoC

ID	Especificações	Testes de PoC
1	16) Todos os IEDs devem se conectar ao equipamento de segurança do SEP, que é capaz de filtrar e limitar o tráfego da Rede do SEP. Adicionalmente, cada Agente deverá ter seu *firewall* para segurança da sua própria rede. Esse dispositivo pode ser um switch SDN, um *firewall* capaz de filtrar na camada 2 ou um switch capaz de desabilitar o aprendizado dinâmico de endereço MAC e fazer ACL (*Access Control List*). Esse equipamento deve minimamente filtrar os campos: Endereço MAC de origem e destino, Ethertype e VLAN.	1º - Teste do requisito utilizando como equipamento de segurança um switch SDN. Neste teste serão configuradas (utilizando o controlador) regras no switch a fim de filtrar as mensagens por MAC de origem e destino, Ethertype e VLAN. Já para a comprovação das mensagens GOOSE nos switches de origem e destino aplica-se espelhamento de portas e utiliza-se o software Wireshark para a análise do resultado.
2	17) O equipamento de segurança deve possuir um mecanismo para limitar a banda de cada fluxo de rede. Esse mecanismo visa limitar os efeitos de um possível ataque de negação de serviço através de um fluxo permitido dentro da rede do SEP.	2º - A arquitetura SDN deve permitir a implementação de contadores de mensagens ou de largura de banda para cada regra criada, de forma a fornecer maior visibilidade acerca dos serviços que trafegam ou que são descartados pela rede. Deve-se permitir, ainda, a definição de limites com relação à rajada de mensagens em curtos intervalos de tempo ou com relação à largura de banda. Na arquitetura SDN, estes recursos são referenciados como “medidores” e contribuem para melhorar a visibilidade e a qualidade do serviço da rede, pois impõem limites ao consumo de banda utilizado pelos serviços permitidos.

3	21) Todos os serviços não utilizados dentro da rede do SEP devem ser desabilitados nos equipamentos do SEP, sejam eles IEDs ou dispositivos de comunicação. 22) Nas interfaces de rede do SEP, apenas o protocolo GOOSE deve estar habilitado, visto que nenhum outro serviço trafega pela rede. 23) Todas as interfaces de rede não utilizadas devem ser desabilitadas via software ou hardware. Isso deve ser feito tanto nos dispositivos de rede quantos nos IEDs, quando possível.	3º - Mostrar no switch SDN que as portas físicas não utilizadas podem ser desabilitadas. Quanto as portas lógicas dos serviços podem-se utilizar uma ferramenta de escaneamento de rede (por exemplo NMAP) para mostrar que os serviços não utilizados foram desabilitados nos equipamentos do SEP.
4	27) Os IEDs e a Master, assim como equipamentos de segurança e qualquer outro equipamento inserido na proposta do fornecedor, devem ser devidamente dimensionados pelos fornecedores para garantir esse atraso máximo de 37 ms. O atraso máximo deve ser devidamente aferido nos testes de aceitação de fábrica e comissionamento. 27.1) O atraso entre IED local de origem e IED local de destino (passando pela Master) desconsiderando o tempo dos equipamentos e enlaces WAN, não deve ultrapassar um total de 37 ms mesmo em condições de sobrecarga no sistema, exceto para medidas analógicas.	4º - Medir o tempo de transmissão na plataforma de testes e estimar os tempos máximos envolvidos na aplicação real.

Para realização da prova de conceito, foi montado dentro da instalação da Empresa 3 uma bancada de testes, conforme Figura 22, composta pelos seguintes equipamentos:

1) IED MASTER – Função: Simulação do IED responsável pelas lógicas do SEP;
2) GATEWAY FEP (*Front-End Processor*) – Função: Equipamento usado para controle, monitoramento e automação. Dentro da arquitetura do SEP e da PoC, este equipamento é utilizado como ponto de concentração dos pacotes GOOSE para não sobrecarregar o IED MASTER;
3) SWITCH SDN – Função: Equipamento de segurança na interface entre agentes;
4) IED LOCAL AGENTE A – Função: IED local dos agentes que fazem comunicação com o IED master;
5) IED PARA MEDIÇÃO DE TEMPO – Função: Modelo de IED próprio da Empresa 3 utilizado dentro da arquitetura para análise dos tempos de comunicação.
6) Notebook conectado a bancada de testes para acesso as ferramentas e gerências.

Para análise dos dados e demonstração das informações, foram utilizadas as seguintes ferramentas:

1) Software de gerência dos IEDs do fabricante, para configuração e análise de tempo entre o fluxo dos pacotes;
2) Software de gerência do switch com função SDN, para configuração do equipamento e análise de dados;
3) Software Wireshark, para análise do fluxo de pacotes entre os equipamentos;
4) Software NMAP (*Network Mapper*), que é uma ferramenta de código aberto usada para descobrir portas TCP e UDP abertas em dispositivos de uma rede.

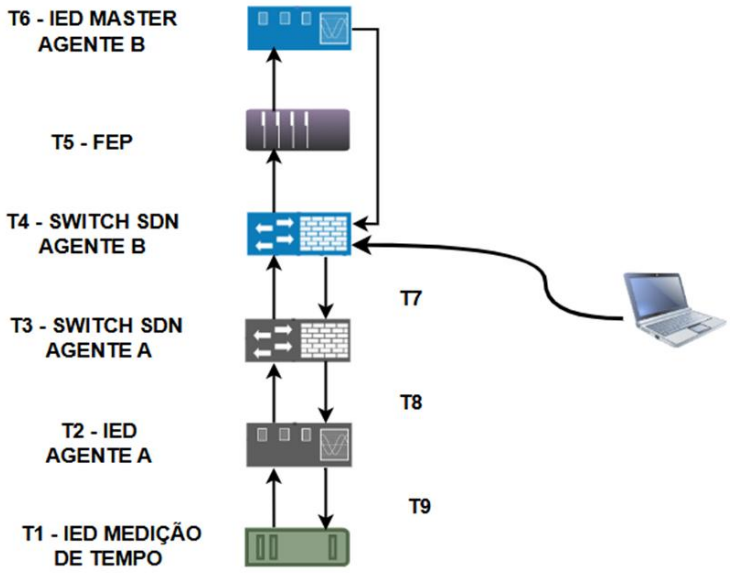

Figura 22 - Bancada de testes montada para realização da prova de testes. Fonte: Elaboração própria

Nos testes realizados em bancada o IED do agente A é o publicador possuindo endereço MAC 00-30-A7-12-14-39 enquanto o agente B possui o IED assinante com o endereço MAC 01-0C-CD-01-00-10. O protocolo de comunicação utilizado será restritamente o GOOSE.

O teste 1 visa provar que o equipamento de segurança ofertado pela Empresa 3 é capaz de filtrar as mensagens por MAC de origem e destino, Ethertype e VLAN.

Para realização do teste foi utilizado o software de gerenciamento do equipamento de segurança, onde foram configurados os filtros. Com o uso da ferramenta *Wireshark*, foram

analisados os fluxos de pacotes GOOSE, e a capacidade dos equipamentos de filtrar os pacotes que estão sendo trafegados.

Esse teste representa a comunicação de um dos agentes com o agente responsável pelo IED Master que possui as lógicas de atuação do SEP. No cenário real do SEP, o IED LOCAL (agente A), envia GOOSE com a informação do estado do terminal da LT, atuação de sobrecarga da LT e o fluxo em tempo real.

O IED Master (agente B), envia fluxo para todos relês, sendo assinado pelo IED Local responsável pela ação. O fluxo entre a Master e os IED locais podem conter ações como corte de máquina de geração e abertura da LT.

A Figura 23 demonstra a tela de gerência do switch SDN, com uma regra configurada permitindo o fluxo publicado pelo IED do agente A para a Master do agente B. Abaixo descrição dos campos.

InPort: Porta 23 (Origem do fluxo publicado pelo IED do agente A)

VlanVId: Vlan 16 (Vlan utilizada para comunicação entre o agente A com a Master do Agente B)

EthType: Goose (Protocolo permitido para o fluxo de comunicação entre o agente A e o agente B)

EthDsT: Regra permitindo a comunicação para o endereço MAC do agente B (Fluxo permitido do IED A com endereço MAC 00-30-A7-12-14-39 de origem na porta 23, para o endereço MAC do agente B 01-0C-CD-01-00-10).

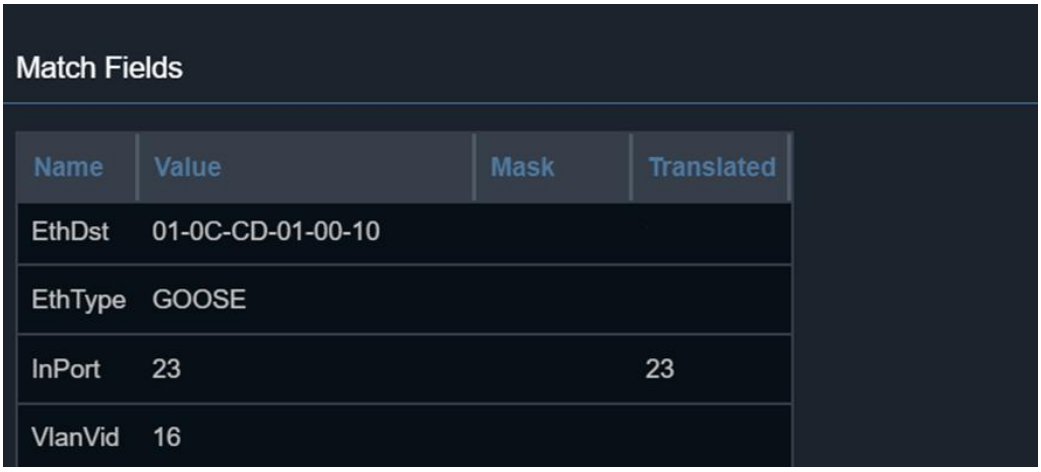

Figura 23 – Gerência do equipamento de segurança. Fonte: Elaboração própria

No caso da Figura 24 ilustra-se a tela do Wireshark com os filtros aplicados na gerência do switch SDN, nos campos Destination (MAC de destino), Source (MAC de origem), Type (EthType) e 802.1Q (VLAN), configurado no DataSet da mensagem GOOSE publicada pelo agente A.

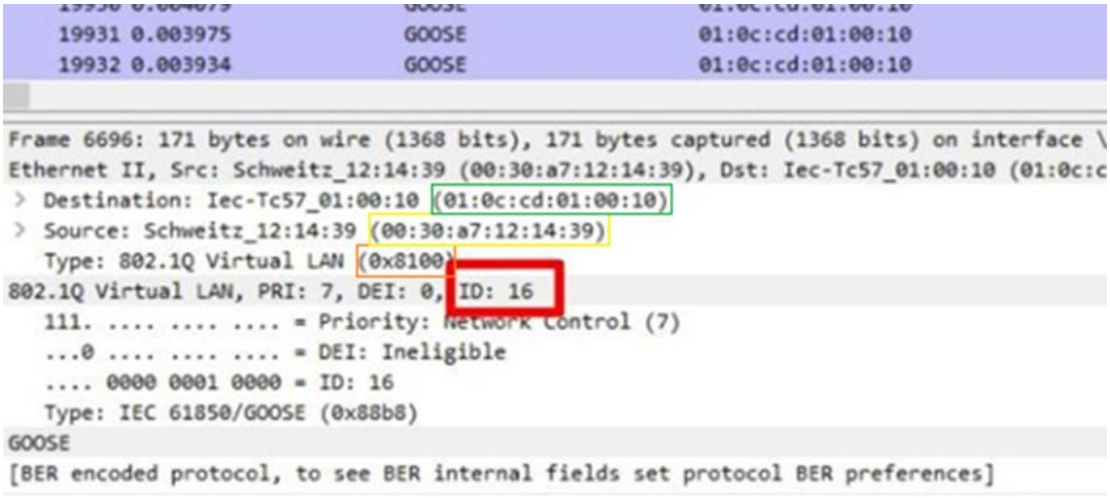

Figura 24 – Tela da ferramenta Wireshark com filtro de MAC de destino. Fonte: Elaboração própria

Das evidências apresentadas nas Figuras 22 e 23, conclui-se que houve a capacidade do equipamento (switch SDN) em aplicar os filtros listados no requisito.

Assim, prossegue-se com a aplicação do 2° teste de prova de conceito, onde o equipamento de segurança deve possuir um mecanismo para limitar a banda de cada fluxo de rede. Esse mecanismo visa limitar os efeitos de um possível ataque de negação de serviço através de um fluxo permitido dentro da rede do SEP.

A banda antes do filtro era de aproximadamente 450 kbps para fluxo entre o IED do agente A para o IED master do agente B. Então, foi realizado um filtro para 250 kbps no campo "*Meter EnTries*" da gerência do switch SDN, conforme demonstrado na Figura 25.

Por outro lado, na Figura 26 é demonstrado no software *Wireshark* o monitoramento do fluxo GOOSE entre os 2 agentes. Pode-se notar que, conforme esperado, após a aplicação do filtro tem-se uma diminuição do fluxo de dados de 450 kbps para 250 kbps, a partir do instante 50 s. Com isso, comprova-se a capacidade do equipamento (switch SDN) em fazer limitação de banda de cada fluxo de rede.

Figura 25 - Gerência do equipamento de segurança. Fonte: Elaboração Própria

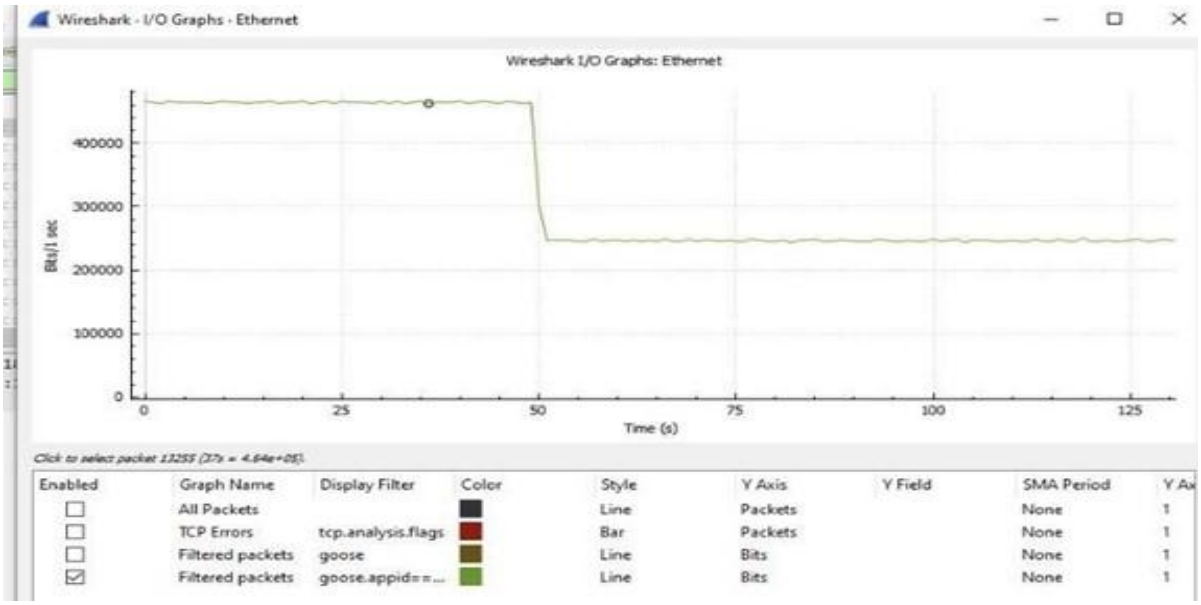

Figura 26 - Monitoramento do Tráfego pelo Wireshark. Fonte: Elaboração Própria

Já no 3° teste de PoC procura-se mostrar no switch SDN que as portas físicas não utilizadas podem ser desabilitadas. Também, testa-se a capacidade de desabilitar portas lógicas TCP e UDP. Para os testes foi utilizado o próprio software de gerenciamento do equipamento de segurança (switch SDN) para desabilitação das portas físicas e lógicas. Para comprovação da desabilitação das portas lógicas utiliza-se a ferramenta ZENMAP como recurso.

Na Figura 27 pode-se observar em destaque as portas ativas 1, 5 e 11 no switch SDN do agente A. As demais portas estão desabilitadas fisicamente. As portas ativas estão sendo utilizadas da seguinte forma: Porta 1 – Comunicação com o equipamento de segurança do

agente B; Porta 5 – Comunicação com o IED LOCAL do agente A; Porta 11 – Comunicação com o *notebook*.

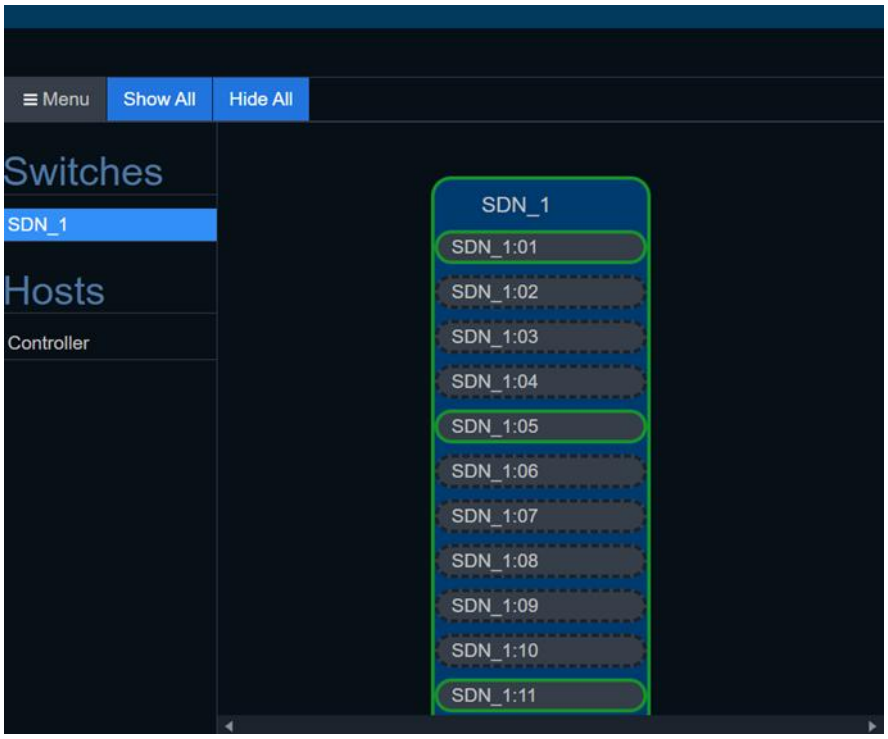

Figura 27 – Gerência do equipamento de segurança – Demonstração de portas físicas habilitadas.
Fonte: Elaboração Própria

O switch SDN funciona com a regra de "negar por padrão", com isso toda porta lógica que não tiver uma regra ativa, o fluxo de dados não é liberado. A Figura 28 ilustra a capacidade do equipamento de segurança (switch SDN) em fazer filtro TCP e UDP no fluxo de origem e destino. No equipamento de gerência, o filtro pode ser feito no campo "*Flow Entries*" podendo ser escolhido quais portas podem ser liberadas nos campos" TcpDst TcpSrc e UdpDst e UdpSrc". Para comprovação da funcionalidade foi utilizado o software ZENMAP para o IP 172.30.99.45, que é o IP configurado no *notebook* que está interligado com o equipamento de segurança e, posteriormente, foi repetido o processo com o IP 172.30.99.43, que é o IP do equipamento de segurança.

Entre os 2 equipamentos existem apenas uma regra configurada para liberação das portas TCP 80 e 443 para acesso a gerência do switch SDN através do protocolo HTTP e HTTPS. Com isso, o filtro se mostrará eficaz se demonstrar que apenas as portas com regra no equipamento de segurança estão ativas e as demais bloqueadas.

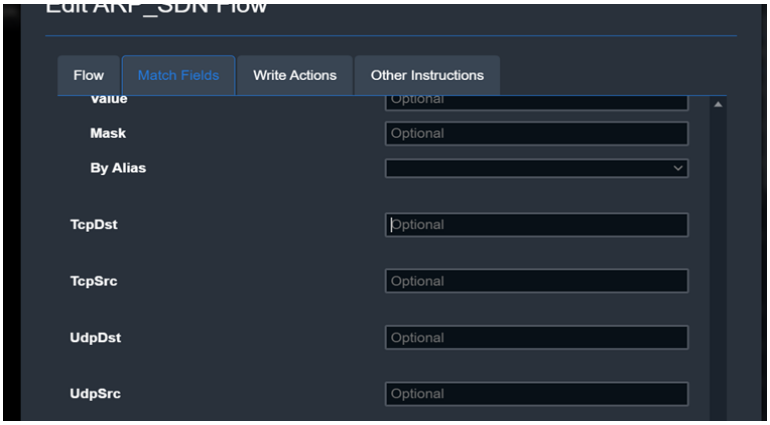

Figura 28- Gerência equipamento de segurança. Fonte: Elaboração Própria

O teste foi iniciado com a varredura de portas no IP 172.30.99.45 que está configurado no *notebook*. Pode-se perceber, através da Figura 29, que diversas portas TCP e UDP estão ativas no *notebook*. Posteriormente foi feita uma nova varredura para o IP 172.30.99.43, configurado no switch SDN.

Na Figura 30, pode-se notar que apenas as portas TCP 80 e 443 estão ativas, pois são as únicas portas que possuem regras de libração no equipamento, comprovando assim a capacidade do equipamento em desativar portas físicas e logicas que não estão em uso.

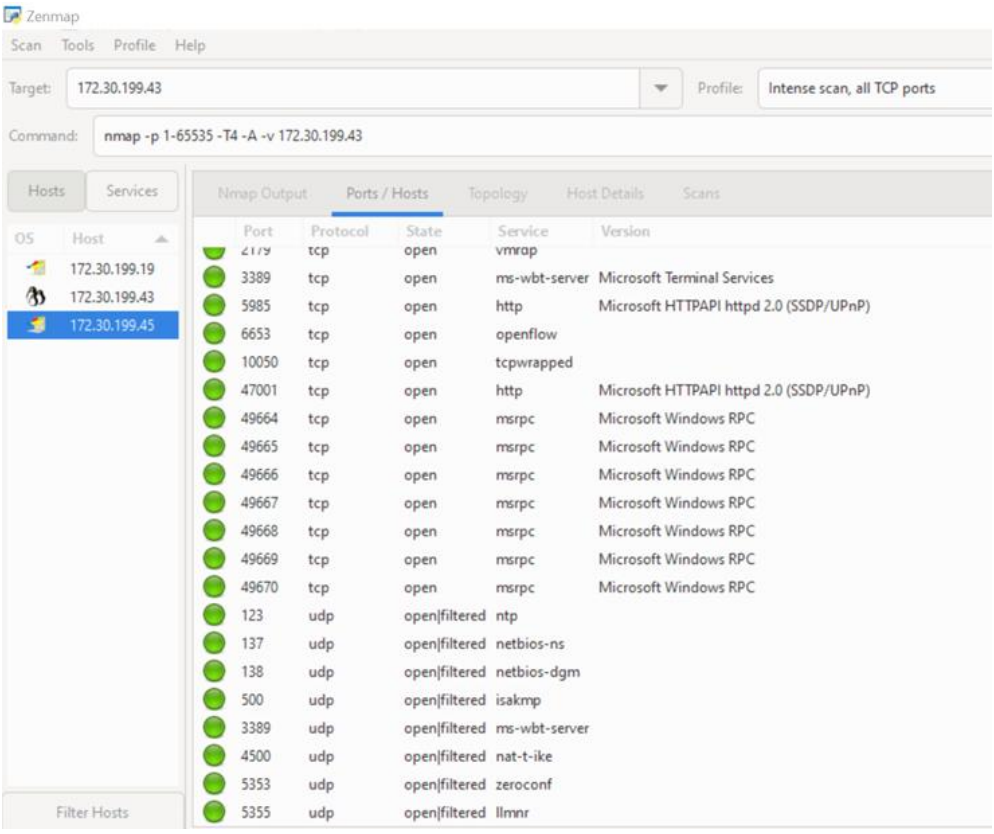

Figura 29 –Varredura de portas no notebook através do ZENMAP –. Fonte: Elaboração Própria

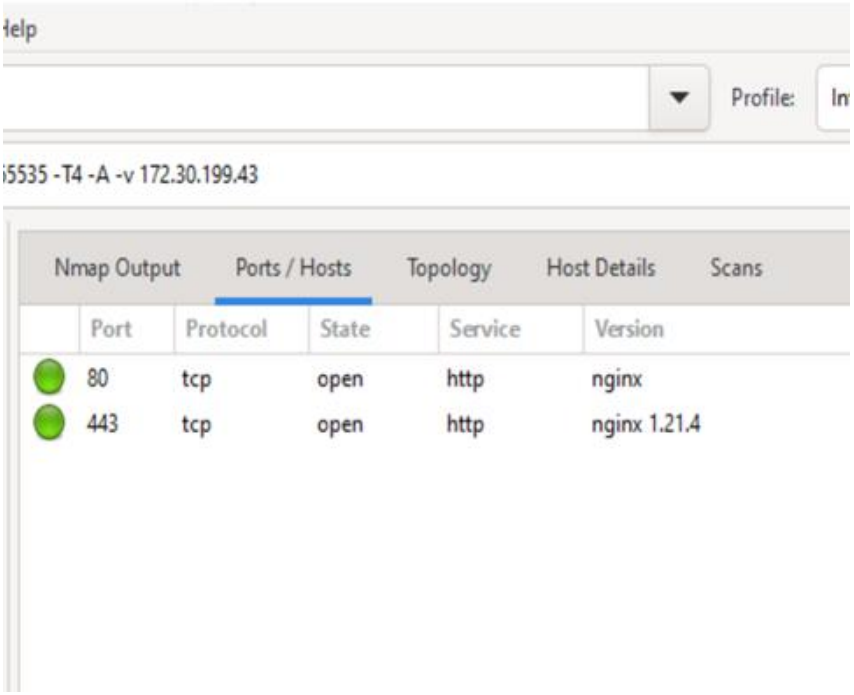

Figura 30 –Varredura de portas do switch SDN através do ZENMAP. Fonte: Elaboração Própria

Por fim, o 4º teste da PoC que visa verificar se o atraso entre o IED local de origem e o IED local de destino (passando pela Master), desconsiderando o tempo dos equipamentos e enlaces WAN, não deve ultrapassar um total de 37 ms, mesmo em condições de sobrecarga no sistema, exceto para medidas analógicas.

Para esse teste, utiliza-se toda a estrutura montada para a bancada de teste, de acordo com a Figura 22. O tempo total do fluxo do pacote GOOSE será considerado da saída (*OUT*) do IED de medição com o tempo "T1", passando pelos equipamentos do agente A e B e retornando (*IN*) para o equipamento de medição no "T9".

Foram realizados 71 testes onde foi medido o tempo de transferência do GOOSE, entre a atuação da saída virtual "OUT101" e a atuação da entrada virtual "IN101", no IED. No campo "ELEMENT" do registro de eventos do IED, apresentado na Figura 31, tem-se a captura de tempo que levou o pacote para percorrer todos os equipamentos da bancada entre "T1" e "T9", para alguns dos testes realizados. Além disso, conforme fluxo destacado na Figura 22, em "T5" ocorreu a concentração das mensagens para não sobrecarregar o IED Master.

#	DATE	TIME			ELEMENT	STATE
185	06/12/2022	21:10:35.5068	35,5068		SER archive	cleared
183	06/12/2022	21:16:48.7686	48,7686		OUT101	Deasserted
182	06/12/2022	21:16:48.7951	48,7951	26,5	IN101	Asserted
179	06/12/2022	21:16:52.4946	52,4946		OUT101	Deasserted
178	06/12/2022	21:16:52.5241	52,5241	29,5	IN101	Asserted
175	06/12/2022	21:16:55.8746	55,8746		OUT101	Deasserted
174	06/12/2022	21:16:55.8992	55,8992	24,6	IN101	Asserted
171	06/12/2022	21:16:58.3456	58,3456		OUT101	Deasserted
170	06/12/2022	21:16:58.3762	58,3762	30,6	IN101	Asserted
167	06/12/2022	21:17:01.0026	1,0026		OUT101	Deasserted
166	06/12/2022	21:17:01.0361	1,0361	33,5	IN101	Asserted
163	06/12/2022	21:17:03.4366	3,4366		OUT101	Deasserted
162	06/12/2022	21:17:03.4641	3,4641	27,5	IN101	Asserted
159	06/12/2022	21:17:06.1576	6,1576		OUT101	Deasserted
158	06/12/2022	21:17:06.1871	6,1871	29,5	IN101	Asserted
155	06/12/2022	21:17:08.6296	8,6296		OUT101	Deasserted
154	06/12/2022	21:17:08.6551	8,6551	25,5	IN101	Asserted
151	06/12/2022	21:17:14.1906	14,1906		OUT101	Deasserted
150	06/12/2022	21:17:14.2151	14,2151	24,5	IN101	Asserted
147	06/12/2022	21:17:17.3226	17,3226		OUT101	Deasserted
146	06/12/2022	21:17:17.3551	17,3551	32,5	IN101	Asserted
143	06/12/2022	21:17:22.8126	22,8126		OUT101	Deasserted
142	06/12/2022	21:17:22.8391	22,8391	26,5	IN101	Asserted
139	06/12/2022	21:17:28.4736	28,4736		OUT101	Deasserted
138	06/12/2022	21:17:28.5071	28,5071	33,5	IN101	Asserted
135	06/12/2022	21:17:31.1346	31,1346		OUT101	Deasserted
134	06/12/2022	21:17:31.1592	31,1592	24,6	IN101	Asserted
131	06/12/2022	21:17:34.3626	34,3626		OUT101	Deasserted
130	06/12/2022	21:17:34.3872	34,3872	24,6	IN101	Asserted
127	06/12/2022	21:17:37.3176	37,3176		OUT101	Deasserted
126	06/12/2022	21:17:37.3433	37,3433	25,7	IN101	Asserted
123	06/12/2022	21:17:40.0026	40,0026		OUT101	Deasserted
122	06/12/2022	21:17:40.0272	40,0272	24,6	IN101	Asserted
119	06/12/2022	21:17:42.6736	42,6736		OUT101	Deasserted
118	06/12/2022	21:17:42.6992	42,6992	25,6	IN101	Asserted
115	06/12/2022	21:17:48.4386	48,4386		OUT101	Deasserted
114	06/12/2022	21:17:48.4632	48,4632	24,6	IN101	Asserted

Figura 31 - Eventos Monitorados no IED. Fonte: Elaboração Própria

Na tabela 6, apresenta-se a análise de tempo dos 71 testes realizados. Pode-se notar que o tempo médio ficou em torno de 26,37 ms, o tempo máximo em 33,5 ms e o menor tempo foi de 23,6 ms. Com isso, pode-se perceber que o tempo de processamento dos pacotes, passando pelos equipamentos da bancada, incluindo os equipamentos de segurança com regras aplicadas, está dentro do limite estabelecido pelas especificações, de 37 ms.

Tabela 6 - Tempos Alcançados nos Testes. Fonte: Elaboração Própria

Tempo (ms)	**Descrição**
26,37	Média do tempo de atuação da LAN
2,362	Desvio padrão
23,6	Menor Tempo de Atuação do SEP
33,5	Maior Tempo de Atuação do SEP
37	Tempo Máximo permitido pelo RM

Assim, a PoC teve como objetivo validar a arquitetura de rede proposta pela Empresa 3, que se destacou por sua aderência às especificações de segurança cibernética e mitigação de vulnerabilidades das mensagens GOOSE. A arquitetura utiliza switches SDN para garantir segurança e desempenho na comunicação entre agentes distintos no SEP. Resumindo, têm-se as seguintes conclusões, considerando os testes realizados e os respectivos critérios estabelecidos:

- Filtragem de Mensagens por MAC, Ethertype e VLAN: O teste foi bem-sucedido, demonstrando que o switch SDN pode aplicar filtros eficazes, conforme evidenciado pelo uso do software Wireshark para monitorar os pacotes.
- Limitação de Banda: O teste mostrou que o switch SDN pode implementar contadores de mensagens e limitar a largura de banda, melhorando a visibilidade e a qualidade do serviço da rede.
- Desabilitação de Portas Físicas e Lógicas: O switch SDN conseguiu desabilitar portas físicas e lógicas, conforme comprovado pelo uso da ferramenta ZENMAP para escanear portas abertas antes e depois da aplicação dos filtros.
- Medição do Tempo de Transmissão: Os testes confirmaram que o tempo de transmissão ficou dentro do limite permitido, com uma média de 26,37 ms e um desvio padrão de 2,362 ms.

5.3.1 Proposta deste trabalho

Com base nos resultados favoráveis à proposta da Empresa 3, determinou-se que a arquitetura a ser aplicada no SEP, para garantir a mitigação de vulnerabilidades das mensagens GOOSE entre agentes, deve seguir o esquema mostrado na Figura 20. Basicamente, essa arquitetura propõe o uso de switches SDN como componentes para segregar o tráfego e aumentar a segurança cibernética, isolando e controlando o que entra e sai da rede. O switch SDN é utilizado para segregar as mensagens dos agentes, funcionando como um equipamento de segurança entre o equipamento WAN e o IED local. Além disso, a porta do IED conectada ao switch tem todos os seus protocolos desabilitados, permitindo apenas a passagem de mensagens GOOSE.

No entanto, embora a arquitetura proposta pela Empresa 3 tenha se mostrado eficaz, há espaço para melhorias, especialmente no que diz respeito à criptografia das mensagens GOOSE. Apesar de não fazer parte do escopo de testes da PoC, em [47], destaca-se a dificuldade de

atender à latência exigida pela IEC 61850 utilizando o algoritmo RSA para assinatura digital das mensagens GOOSE. O estudo demonstra que o RSA, devido à sua complexidade computacional, não é viável para dispositivos com baixa capacidade de processamento, como os IEDs, pois não consegue atender ao requisito de latência de 3 ms estabelecido pela norma IEC 61850.

Como alternativa, em [47] sugere-se a utilização do algoritmo de criptografia simétrica AES (*Advanced Encryption Standard*) com a técnica CMAC (*Cipher-based Message Authentication Code*). Os resultados experimentais indicam que o AES, mesmo quando aplicado a toda a carga útil de um pacote GOOSE, atende às restrições de tempo definidas pela IEC 61850, com um tempo de comunicação fim-a-fim significativamente menor que o RSA.

Desta forma, propõe-se estudos mais profundo visando a substituição do algoritmo RSA por outro algoritmo mais eficiente, para ser utilizando em conjunto com a arquitetura de rede proposta pela Empresa 3. Como possibilidade, temos a utilização do AES como algoritmo de criptografia simétrica pode proporcionar os seguintes benefícios:

- **Redução de Latência:** O AES apresenta tempos de cifragem e decifragem significativamente menores que o RSA, permitindo que as mensagens GOOSE sejam transmitidas e processadas dentro do limite de 3 ms exigido pela IEC 61850. Isso é crucial para garantir a comunicação em tempo real entre os IEDs.
- **Maior Segurança**: O AES oferece um nível de segurança equivalente ou superior ao RSA, garantindo a integridade e autenticidade das mensagens GOOSE. A técnica CMAC utilizada com o AES proporciona uma autenticação robusta, protegendo contra-ataques de falsificação de mensagens.
- **Eficiência Computacional:** A implementação do AES é mais eficiente em termos de uso de recursos computacionais, o que é particularmente importante para dispositivos com baixa capacidade de processamento, como os IEDs. Isso permite uma operação mais eficiente e confiável da rede de comunicação do SEP.

Portanto, a adoção do AES como algoritmo de criptografia simétrica na arquitetura proposta pela Empresa 3 pode, portanto, melhorar significativamente o desempenho e a segurança da rede, atendendo às exigências da norma IEC 61850 e garantindo uma comunicação eficiente e segura entre os IEDs.

6 Capítulo 6 – Conclusões

A pesquisa realizada teve como objetivo principal analisar e propor uma estratégia de comunicação baseada na IEC 61850 entre agentes distintos no SEP, que vise mitigar as vulnerabilidades das mensagens GOOSE.

A metodologia adotada combinou pesquisa documental e análise qualitativa das propostas de quatro fornecedores distintos. A pesquisa foi classificada como aplicada, com abordagem descritiva, visando solucionar problemas práticos relacionados à segurança cibernética e comunicação eficiente entre os agentes do SEP.

Os fornecedores foram avaliados com base em critérios de tempo e banda, disponibilidade e segurança, com base em 27 critérios selecionados de diretrizes da IEC 61850 e especificações do ONS. A análise das propostas revelou pontos fortes e fracos de cada fornecedor, destacando a Empresa 3 como a mais aderente às especificações estabelecidas.

Com base na análise das propostas supracitadas, foi realizada a Prova de Conceito para validar a arquitetura proposta pela Empresa 3, que utiliza switches SDN para garantir segurança e desempenho na comunicação entre agentes distintos no SEP. Quatro testes principais foram conduzidos: Filtragem de Mensagens por MAC, Ethertype e VLAN; Limitação de Banda; Desabilitação de Portas Físicas e Lógicas; e Medição do Tempo de Transmissão. Como resultado dos testes realizados, comprovou-se que o switch SDN apresenta vantagens na implementação eficaz de estratégias de segurança cibernética garantindo o desempenho de tempo requerido na aplicação do SEP, tais como: capacidade de filtragem, permitindo que apenas dados legítimos circulem na rede do SEP; contagem de mensagens e limitação de largura de banda, prevenindo ataques de negação de serviço e mantendo a estabilidade da rede, versatilidade na desabilitação de portas físicas e lógicas não utilizadas, reduzindo a superfície de ataque da rede e prevenindo acessos não autorizados; e tempo de transferência entre IEDs dentro do limite permitido de 37 ms.

Apesar da eficácia da arquitetura proposta pela Empresa 3, foi identificada uma oportunidade de aprimoramento na criptografia das mensagens GOOSE. Análises feitas em [47] revelaram que o algoritmo RSA, recomendado pela norma IEC 62351, não atende aos requisitos de latência de 3 ms devido à sua alta complexidade computacional.

Assim, como alternativa, o presente trabalho propõe a adoção de um novo algoritmo de criptografia buscando mais eficiência, podendo ser o algoritmo simétrica AES com a técnica

CMAC, pois experimentos feitos em [47] demonstraram que o AES é capaz de atender às restrições de tempo da IEC 61850, mesmo quando aplicado a toda a carga útil de um pacote GOOSE, com um desempenho significativamente superior ao RSA. Portanto, para pesquisas futuras, recomenda-se um estudo mais aprofundado visando a troca por um algoritmo mais eficiente que o RSA, para ser implementado na arquitetura de rede da Empresa 3. A adoção do algoritmo de criptografia aumenta a segurança, tornando a rede de comunicação do SEP mais robusta e confiável.

De modo geral, a pesquisa demonstrou que a arquitetura proposta pela Empresa 3, utilizando switches SDN, é eficaz para garantir a segurança e o desempenho na comunicação entre agentes distintos no SEP. Assim, a proposta de melhoria, baseada na substituição do algoritmo RSA para aprimorar ainda mais a segurança e a eficiência da rede, atendendo às exigências da norma IEC 61850.

Em conclusão, a pesquisa contribui significativamente para o avanço da segurança cibernética e da comunicação eficiente em redes de transmissão de energia elétrica de um caso real, como é o SEP N/NE/SE, oferecendo uma solução prática e viável para mitigar vulnerabilidades e garantir a integridade e autenticidade das mensagens GOOSE entre Agentes. A implementação das melhorias propostas pode fortalecer ainda mais a infraestrutura de comunicação do SEP, assegurando um desempenho otimizado e uma operação segura e confiável.

Para estudos futuros, sugere-se explorar o desempenho de vários algoritmos de criptografia na arquitetura da Empresa 3, que possam oferecer ainda mais eficiência e segurança, mantendo a latência dentro dos limites aceitáveis para a comunicação GOOSE. A investigação de novas técnicas criptográficas pode revelar soluções que atendam melhor às necessidades específicas do SEP, proporcionando uma camada adicional de proteção contra possíveis ataques cibernéticos.

Além disso, é importante avaliar o impacto dos switches SDN em diferentes cenários de redes de energia elétrica. Realizar estudos em ambientes variados, considerando diferentes topologias e cargas de trabalho, permitirá uma compreensão mais abrangente da eficácia dos switches SDN. Isso ajudará a identificar possíveis limitações e oportunidades de melhoria na aplicação dessa tecnologia em redes de transmissão de energia.

Por fim, desenvolver métodos avançados de detecção de anomalias e intrusões que possam ser integrados aos switches SDN é uma área promissora para futuras pesquisas. A

criação e teste de técnicas inovadoras de monitoramento e resposta a ameaças cibernéticas em tempo real aumentarão a capacidade de proteção das redes de comunicação do SEP, garantindo uma operação ainda mais segura e confiável.

Referências

[1] SIQUEIRA, I. P. Rede de Infraestruturas Críticas – Análise de Desempenho e Riscos dos Setores de Energia, Petróleo, Gás, Água, Finanças, Logística e Telecomunicações, Editora Interciencia, Rio de Janeiro, 2013.

[2] SIQUEIRA, I. P; CASTRO, N. Segurança Cibernética do Setor Elétrico Brasileiro: Desafios Regulatórios e Tecnológicos. UFRJ. GESEL. Rio de Janeiro, Agosto, 2021.

[3] Relatório Segurança Cibernética para Operação do Sistema Integrado Nacional, anexo à carta ONS 0766/DTA/2019 de 10/12/2019 – Proposta de Procedimentos de Rede de Segurança Cibernética.

[4] RODRÍGUEZ, M. et al. A Fixed-Latency Architecture to Secure GOOSE and Sampled Value Messages in Substation Systems. Spain, Volume: 9, Pages 51646 – 51658, March 2021.

[5] TAKEDA, A. H; GUITIERREZ, T. I. S. A primeira subestação digital do sistema interligado nacional, subestação Lorena. XVI STPC – Seminário Técnico de Proteção e Controle. Rio de Janeiro. Outubro, 2022.

[6] FLORES, P, H; Onça, A; Aplicações da norma IEC 61850 – Sistemas De Automação Operando Com Redes De Comunicação – XVSTPC, 2021.

[7] Operador Nacional do Sistema Elétrico. Sistema Especial De Proteção - SEP Associado às Interligações Norte-Nordeste-Sudeste. RT-NOS DPL 0131/2021. Rio de Janeiro. Junho, 2021.

[8] FLORINDO, T. P. Estudo de caso baseado nos esquemas especiais de proteção do procedimento de rede: (controle de emergência no Sul do Rio Grande do Sul para contingência da LT 525 KV Nova Santa Rita/Povo Novo). 2019. 82p. – Instituto Federal de Santa Catarina, Câmpus Florianópolis. 2019.

[9] SILVEIRA, M. G; FRANCO, P. H. Segurança Cibernética em Redes IEC 61850: Como Mitigar Vulnerabilidades Das Mensagens GOOSE. Schweitzer Engineering Laboratories, Inc. São Paulo, 2021.

[10] HOHLBAUM, F. et al. Cyber security practical considerations for implementing IEC 62351. in Proc. PAC World Conf., Dublin, Republic of Ireland, Jun. 2010, pp. 21–24.

[11] DIEHL, A. A. Pesquisa em ciências sociais aplicadas: métodos e técnicas. São Paulo: Prentice Hall, 2004.

[12] GIL, A. C. Como elaborar projetos de pesquisa. 5a. Edição ed. São Paulo: Editora Atlas S.A., 2010.

[13] YIN, R. K. Estudo de caso. Porto Alegre: Bookman, 2003.

[14] Presidência da República, Secretaria Geral, Subchefia para Assuntos Jurídicos. Decreto nº 9 669, de 2 de Janeiro de 2019.

[15] SIQUEIRA, I. P. Cyber Security of Electrical Networks, Tutorial presented during the International Seminar of Smart Grids, Rio de Janeiro, 2018.

[16] LEWIS, T. Critical Infrastructure Protection in Homeland Security: Defending a Networked Nation. Disponível em: https://www.wiley.com/nosus/Critical+Infrastructure+Protection+in+Homeland+Security%3ª +Defending+a+Networked+Nation%2C+3rd+Edition-p-9781119614531. Acessado em: 09 de dezembro de 2023.

[17] UTCAL – Segurança Cibernética – Melhores Práticas de Segurança Cibernética – Quadro Legal e Regulatório do Setor Elétrico Brasileiro e Internacional Relacionado à Segurança Cibernética, 2022.

[18] PROOFPOINT. Critical Infrastructure Protection (CIP). Disponível em: https://www.proofpoint.com/us/threat-reference/critical-infrastructure-protection-cip. Acesso em: 23 fev. 2025.

[19] NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION. About NERC. Disponível em: https://www.nerc.com/aboutnerc/Pages/default.aspx. Acesso em: 23 fev. 2025.

[20] NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. About NIST. Disponível em: https://www.nist.gov/about-nist. Acesso em: 23 fev. 2025.

[21] CEER Cybersecurity Work Stream, CEER Paper on Cybersecurity in the Clean Energy for All Europeans Package, 4 June 2020, Ref: C20-CS-58-03.

[22] INTERNATIONAL ELECTROTECHNICAL COMMISSION. IEC 62443 - Industrial communication networks - Network and system security. Disponível em: https://www.iec.ch/standards/62443. Acesso em: 23 fev. 2025.

[23] WILLIAMS, T.J. The Purdue Enterprise Reference Architecture and Methodology (PERA), Institute for Interdisciplinary Engineering Studies Purdue University, West Lafayette, IN, 1990.

[24] ALVES, V. et al. Segurança Cibernética e Políticas Públicas no Brasil, XI Simpósio de Excelência em Gestão e Tecnologia, 2014. Disponível em: https://www.researchgate.net/publication/275272400. Acessado em: 10 de dezembro de 2023.

[25] IEC 61850: 2016 SER Series Communication networks and systems for power utility automation. Disponível em: https://www.iec.ch/standards/61850. Acesso em: 23 fev. 2025.

[26] FAROOQ, A. M; HUSSAIN, S. M. S; USTUN, T. S. Performance Evaluation and Analysis of IEC 62351-6 Probabilistic Signature Scheme for Securing GOOSE Messages. IEEE ACCESS. Japan. March, 2019.

[27] Public-Key Cryptography Standards (PKCS) #1: RSA Encryption Version 1.5, document RFC 2313, IETF, Mar. 1998.

[28] D. Ishchenko and R. Nuqui, ‘‘Secure communication of intelligent electronic devices in digital substations,’’ in Proc. IEEE/PES Transmiss. Distrib. Conf. Expo. (T&D), Denver, CO, USA, Apr. 2018, pp. 1–5.

[29] GUARINI, M. C. Análise de segurança de esquemas de proteção para sistemas elétricos de potência. Dissertação (Mestre em Engenharia Elétrica) – COPPE, Rio de Janeiro, 2009.

[30] AHMED, K. S. et al. Special Protection Schemes: A Survey and Vision for the future. Applied Mechanics and Materials. Vol. 839, Pages 49-53, June 2016.

[31] BALLAL, M. S. et al. Special Protection Scheme at BTPS Power Station. Journal of The Institution of Engineers (India): Series B. India. March, 2016.

[32] ABBOUD, R. et al. Case Study: Modern RAS Applied to Furnas 765 kV Transmission Corridor Improves Itaipu Power Plant and Brazilian Power System Stability. 49th Annual Western Protective Relay Conference Spokane, Washington, October, 2022.

[33] OPERADOR NACIONAL DO SISTEMA ELÉTRICO. Relatório RE 3/031/2012. Disponível em: https://www.ons.org.br/AcervoDigitalDocumentosEPublicacoes/2012-ONS-Relatorio-Anual.pdf. Acesso em: 23 fev. 2025.

[34] POORNENDU K. et al. Data Acquisition and Controlling in Thermal Power Plants using a Wireless Sensor Network and LabVIEW. Vol. 4. International Journal of Engineering Research & Technology (IJERT). July, 2005.

[35] Jogaib R.; et al. Fornecimento de bens e serviços para implementação do sistema de proteção, controle, supervisão e rede lan do sistema especial de proteção Norte/Nordeste/Sudeste. Julho, 2022

[36] GONÇALVES, E; et al. Proposta De Integração Segura De Redes Para Interface Entre Agentes De Transmissão. XVI STPC - Seminário Técnico De Proteção E Controle. Rio de Janeiro, Outubro, 2022.

[37] P. Garcia, M. Cabral, et al. Aplicação da Tecnologia SDN na Modernização de parte dos Esquemas de Controle de Emergência do Setor de 50 Hz da Itaipu Binacional. Apresentado no XIV STPC, novembro de 2018.

[38] C. Gray, "How SDN Can Improve Cybersecurity in OT Networks", proceedings of the 22nd Conference of the Electric Power Supply Industry, Kuala Lumpur, Malásia, Setembro 2018.

[39] N. Feamster, J. Rexford, E. Zegura, "The Road to SDN: An Intellectual History of Programmable Networks". ACM Queue, dezembro de 2013.

[40] Y. Lopes. "SMARTFlow, SisteMa Autoconfigurável para Redes de Telecomunicações IEC 61850 com arcabouço OpenFlow". Tese (Mestrado em Engenharia de Telecomunicações) - Universidade Federal Fluminense. Niterói, 2013.

[41] Open Networking Foundation, "OpenFlow". Disponível em [www.opennetworking.org/sdn-resources/openflow]. Acesso em: 7 de setembro de 2023.

[42] SEL-5056, Software-Defined Network Flow Controller, manual de instruções, julho de 2022.

[43] SEL-2740S, Software-Defined Network Switch, manual de instruções, abril de 2022.

[44] NIST Special Publication 800-53, Revision 5. Security and Privacy Controls for Information Systems and Organizations, setembro de 2020.

[45] IEC 61869-9, Instrument transformers – Part 9: Digital interface for instrument transformers. Disponível em: https://webstore.iec.ch/en/publication/24663. Acesso em: 23 fev. 2025.

[46] Requisitos Mínimos Da Rede LAN e WAN (RM-Rede) para A Implantação Do Sistema Especial De Proteção Norte/Nordeste/Sudeste (SEP N/NE/SE). Rio de Janeiro, 2022.

[47] SCARSELLI, R. B.; SOARES, L. F.; MORAES, I. M. Uma Avaliação de Algoritmos Criptográficos em Redes IEC 61850: Uma Abordagem Prática. In: Anais do Simpósio Brasileiro de Segurança da Informação e de Sistemas Computacionais (SBSeg), 2019. p. 1-10.