

UNIVERSIDADE ESTADUAL PAULISTA
"JÚLIO DE MESQUITA FILHO"
CÂMPUS DE SÃO JOÃO DA BOA VISTA

CRISLAINE MAGALHÃES SOARES

TELEPROTEÇÃO EM LINHAS DE TRANSMISSÃO: Estudo dos protocolos de comunicação

São João da Boa Vista

2025

Crislaine Magalhães Soares

TELEPROTEÇÃO EM LINHAS DE TRANSMISSÃO: Estudo dos protocolos de comunicação

Trabalho de Graduação apresentado ao Conselho de Curso de Graduação em Engenharia Eletrônica e de Telecomunicações do Câmpus de São João da Boa Vista, Universidade Estadual Paulista, como parte dos requisitos para obtenção do diploma de Graduação em Engenharia Eletrônica e de Telecomunicações.

Orientadora: Prof^a Dr.^a Rita de Cássia Domingos

São João da Boa Vista

2025

S676t Soares, Crislaine Magalhães
Teleproteção em linhas de transmissão: Estudo dos protocolos de
comunicação / Crislaine Magalhães Soares. -- São João da Boa Vista,
2025
42 p. : il., tabs.

Trabalho de conclusão de curso (Bacharelado - Engenharia de
Telecomunicações) - Universidade Estadual Paulista (UNESP),
Faculdade de Engenharia, São João da Boa Vista
Orientadora: Rita de Cássia Domingos

1. Telecomunicação. 2. Fibras ópticas. 3. Normas técnicas
(Engenharia). 4. Comunicação. I. Título.

**UNIVERSIDADE ESTADUAL PAULISTA “JÚLIO DE MESQUITA FILHO”
FACULDADE DE ENGENHARIA - CÂMPUS DE SÃO JOÃO DA BOA VISTA
GRADUAÇÃO EM ENGENHARIA ELETRÔNICA E DE TELECOMUNICAÇÕES**

TRABALHO DE CONCLUSÃO DE CURSO

**TELEPROTEÇÃO EM LINHAS DE TRANSMISSÃO: ESTUDO DOS PROTOCOLOS
DE COMUNICAÇÃO**

Aluno: Crislaine Magalhães Soares
Orientador: Prof.^a Dr.^a Rita de Cássia Domingos

Banca Examinadora:

- Rita de Cássia Domingos (Orientadora)
- Plinio Santini Dester (Examinador)
- Edgar Eduardo Benitez Olivo (Examinador)

Os formulários de avaliação e a ata da defesa, na qual consta a aprovação do trabalho, devidamente assinados pela banca encontram-se no prontuário eletrônico do aluno.

São João da Boa Vista, 25 de novembro de 2025

Dedico este trabalho às amizades que criei durante a graduação.

AGRADECIMENTOS

Agradeço a todos que me apoiaram ao longo do processo de graduação, em especial ao meu marido, Vitor Nobre de Carvalho, pelo carinho e pela compreensão, por estar ao meu lado nos momentos de alegria e, principalmente, nos de dificuldade. A caminhada não foi fácil, mas você a tornou mais leve e, certamente, eu não teria chegado até aqui sem o seu apoio.

Aos meus pais, Fabiana Magalhães Sena e Valter da Silva Soares, que, mesmo diante de todas as dificuldades, souberam me orientar pelo caminho correto. Muito obrigada.

Aos meus gestores e colegas de equipe, Alessandro Bonequini e Alex Pereira da Silva, por me ajudarem e por abrirem novas portas de oportunidade na função de gestão atual.

À minha orientadora, Rita de Cássia Domingos, pelos conselhos, orientações e pela disponibilidade constante, que contribuíram de forma significativa para o desenvolvimento e aprimoramento deste trabalho.

À Universidade Estadual Paulista – Câmpus de São João da Boa Vista, pelo ensino de qualidade. À reitoria da Unesp pelo apoio financeiro que recebi durante todo o período de graduação. O auxílio financeiro foi importante, pois sem ele não seria possível concluir o curso.

Por fim, agradeço aos amigos que conquistei ao longo da graduação, que tornaram essa trajetória mais leve, enriquecedora e significativa. Agradeço também a todos os professores e colaboradores da UNESP Câmpus de São João da Boa Vista, que contribuíram de forma essencial para minha formação pessoal e profissional, compartilhando conhecimento, apoio e inspiração ao longo dessa trajetória.

“Se fosse fácil achar o caminho das pedras, tantas pedras no caminho não seriam tão ruins.”
(Humberto Gessinger.)

RESUMO

A operação segura e confiável das redes elétricas depende da atuação eficiente dos sistemas de teleproteção, que utilizam canais de comunicação dedicados para detectar e isolar falhas em tempos reduzidos. Este trabalho apresenta um estudo comparativo entre dois protocolos amplamente empregados nesse contexto: C37.94 e GOOSE. O protocolo C37.94, baseado em enlaces ópticos dedicados, destaca-se pela baixa latência e pela elevada imunidade a interferências eletromagnéticas, sendo adequado a aplicações de teleproteção ponto a ponto. O protocolo GOOSE, definido pela norma IEC-61850 e operando em redes Ethernet, permite a troca rápida de mensagens entre dispositivos eletrônicos inteligentes (IEDs), favorecendo a automação e a interoperabilidade em subestações digitais. A partir de critérios técnicos estabelecidos em normas e documentos do setor elétrico, são analisadas as principais características, vantagens e limitações de cada protocolo, indicando os contextos em que cada um se mostra mais apropriado e discutindo a possibilidade de uso de soluções híbridas em sistemas de proteção e automação.

PALAVRAS-CHAVE: teleproteção; protocolo c37.94; protocolo goose.

ABSTRACT

The safe and reliable operation of power systems depends on the effective performance of teleprotection schemes, which rely on high-speed communication channels to detect and isolate faults. This work presents a comparative study of two communication protocols widely used in this context: C37.94 and GOOSE. The C37.94 protocol, based on dedicated optical links, provides low latency and high immunity to electromagnetic interference, making it suitable for point-to-point teleprotection applications. The GOOSE protocol, defined by IEC 61850 and operating over Ethernet networks, enables fast message exchange among intelligent electronic devices (IEDs), supporting interoperability and automation in digital substations. Using technical criteria established in standards and reference documents, this study analyzes the main characteristics, advantages, and limitations of each protocol, indicating the contexts in which they are most appropriate and discussing the potential use of hybrid architectures in protection and automation systems.

KEYWORDS: teleprotection; c37.94 protocol; goose protocol.

LISTA DE ILUSTRAÇÕES

Figura 1 – Representação do esquema de teleproteção entre duas subestações, destacando o relé, o CIU, o disjuntor e o canal de comunicação utilizado.	17
Figura 2 – Representação das fases de funcionamento de um sistema de teleproteção, incluindo vigilância, detecção, atuação e recuperação.	19
Figura 3 – Meio de comunicação.	22
Figura 4 – Ilustração da fibra óptica monomodo, com destaque para o núcleo estreito que possibilita a transmissão a longas distâncias.	23
Figura 5 – Ilustração da fibra óptica multimodo, mostrando o núcleo mais largo, adequado para transmissões de curta distância.	23
Figura 6 – Estrutura do cabo OPGW, que combina fibras ópticas e condutor metálico para comunicação e proteção.	24
Figura 7 – Topologia C37.94, ilustrando a interligação entre o relé de proteção e o multiplexador por meio de fibra óptica.	25
Figura 8 – Topologia GOOSE, ilustrando a troca de mensagens entre os relés de proteção por meio de um switch Ethernet.	27

LISTA DE TABELAS

Tabela 1 – Principais meios de comunicação utilizados pelos protocolos C37.94 e GOOSE. .	30
Tabela 2 – Requisitos de Comunicação em Sistemas de Teleproteção	31
Tabela 3 – Protocolos de comunicação	32

LISTA DE ABREVIATURAS E SIGLAS

ANEEL	Agência Nacional de Energia Elétrica
BER	<i>Bit Error Rate</i> (Taxa de Erros de Bits)
CMSE	Comitê de Monitoramento do Setor Elétrico
CIU	Unidade de Interface de Comunicação
DNP3	<i>Distributed Network Protocol</i> (Protocolo de Rede Distribuída)
EMI	<i>Electromagnetic Interference</i> (Interferência Eletromagnética)
GOOSE	<i>Generic Object Oriented Substation Event</i>
IED	<i>Intelligent Electronic Device</i> (Dispositivo Eletrônico Inteligente)
IEC	<i>International Electrotechnical Commission</i>
IEEE	<i>Institute of Electrical and Electronics Engineers</i>
LAN	<i>Local Area Network</i> (Rede Local)
LT	Linha de Transmissão
ONS	Operador Nacional do Sistema Elétrico
OPGW	<i>Optical Ground Wire</i>
OPLAT	Ondas Portadoras em Linhas de Alta Tensão
OSI	<i>Open Systems Interconnection</i> (Interconexão de Sistemas Abertos)
PLC	<i>Power Line Carrier</i>
SCADA	<i>Supervisory Control and Data Acquisition</i> (Sistemas de Supervisão e Aquisição de Dados)
SEP	Sistema Elétrico de Potência
SIN	Sistema Interligado Nacional
TCC	Trabalho de Conclusão de Curso
TC	Transformador de Corrente
TP	Transformador de Potencial
UNESP	Universidade Estadual Paulista "Júlio de Mesquita Filho"

UNIFEI	Universidade Federal de Itajubá
VLAN	<i>Virtual Local Area Network</i> (Rede Local Virtual)

SUMÁRIO

1	INTRODUÇÃO	14
2	FUNDAMENTAÇÃO TEÓRICA	16
2.1	Contexto Histórico da Teleproteção	16
2.2	Como Funciona um Sistema de Teleproteção	18
2.3	Regulamentação do ONS para Sistemas de Proteção e Teleproteção	19
2.3.1	Baixa latência	19
2.3.2	Alta confiabilidade	20
2.3.3	Imunidade a interferências eletromagnéticas	20
2.3.4	Sincronização precisa	20
2.3.5	Largura de banda adequada	20
2.3.6	Compatibilidade e interoperabilidade	21
2.4	Meios de Comunicação	21
2.4.1	Fibra Óptica	22
2.5	Protocolos de Comunicação	24
2.5.1	IEEE C37.94	24
2.5.2	GOOSE (IEC 61850)	26
3	METODOLOGIA	30
3.1	Critérios de Análise	30
3.2	Fontes de Pesquisa	33
3.3	Método de Comparação	33
4	ANÁLISE COMPARATIVA DOS PROTOCOLOS	35
4.1	Desempenho e Eficiência	35
4.2	Tecnologia de Rede e Infraestrutura	35
4.3	Escalabilidade e Flexibilidade	36
4.4	Complexidade e Facilidade de Implementação	36
4.5	Aplicações Típicas	37
4.6	Impacto dos Meios de Comunicação	37
4.7	Conclusão da Análise Comparativa	38
5	COMENTÁRIOS FINAIS	40
5.1	Contribuições do Estudo	40
5.2	Limitações e Desafios do Estudo	41
5.3	Oportunidades de Estudos Futuros	41
	REFERÊNCIAS	42

1 INTRODUÇÃO

A teleproteção é um sistema essencial para a segurança das redes de energia elétrica, especialmente nas linhas de transmissão, pois assegura a estabilidade e a confiabilidade da rede. É composta por relés de proteção, redes de comunicação e protocolos padronizados, que, juntos, possibilitam a detecção rápida e eficaz de falhas no sistema, além de implementar ações coordenadas para isolar essas falhas. Dessa forma, minimizam-se os danos aos equipamentos e evitam-se interrupções no fornecimento de energia, algo vital para a continuidade operacional de uma infraestrutura crítica, como o sistema elétrico.

Historicamente, as tecnologias de comunicação utilizadas na teleproteção começaram de forma analógica, com sistemas de transmissão baseados em linhas telefônicas que, embora eficazes para a época, apresentavam limitações quanto à velocidade de transmissão, segurança e resistência a interferências, prejudicando a rapidez e a confiabilidade necessárias à teleproteção. Com o tempo, os meios de comunicação evoluíram com o avanço das telecomunicações e da automação, o que permitiu a implementação de sistemas de teleproteção mais sofisticados e eficientes (CIGRÉ, 2006; PINHO et al., 2020).

A adoção de redes digitais, como a fibra óptica, foi um marco importante na evolução das redes de comunicação, permitindo melhorar a confiabilidade e reduzir a latência nas comunicações entre os dispositivos de proteção. Com sua ampla largura de banda, esse meio permite a troca de dados em alta velocidade, o que é crucial para garantir a atuação imediata dos sistemas de proteção.

A evolução dos métodos de comunicação, de analógicos a digitais, trouxe avanços significativos para a teleproteção. Tecnologias como o *Optical Ground Wire* (OPGW) melhoraram a precisão e a eficiência desses sistemas, proporcionando uma detecção mais rápida e confiável de falhas. Esses avanços tecnológicos permitem que as redes de energia elétrica sejam cada vez mais robustas e preparadas para enfrentar falhas com o mínimo impacto.

Com relação aos protocolos de comunicação, o IEEE C37.94 (TELECOM, 2022) é um dos principais protocolos utilizados em sistemas de teleproteção, definindo métodos de comunicação direta entre dispositivos de proteção, garantindo uma resposta eficiente às falhas detectadas. Além do IEEE C37.94, principal protocolo para comunicação direta entre relés, destaca-se também o *Generic Object Oriented Substation Event* (GOOSE), protocolo da norma IEC 61850, que prioriza mensagens de disparo em redes Ethernet. A escolha correta e a implementação desses protocolos são determinantes para assegurar que o sistema de teleproteção funcione com a eficácia necessária.

Visando assegurar a padronização e a qualidade da teleproteção, o Operador Nacional do Sistema Elétrico (ONS) desempenha papel essencial nesse contexto. Conforme ONS (2021), os sistemas de teleproteção são responsáveis por reduzir significativamente a ocorrência de interrupções em linhas de alta tensão, contribuindo para a estabilidade e para a operação contínua do Sistema Interligado Nacional (SIN)¹. Reconhecendo essa importância, o ONS estabelece diretrizes que orientam e normatizam o funcionamento e a interoperabilidade dos sistemas de proteção, garantindo um sistema elétrico mais

¹ Sistema Interligado Nacional — infraestrutura elétrica que conecta todas as regiões do Brasil em uma única rede.

seguro e confiável. Entre essas diretrizes, destacam-se requisitos cruciais para a comunicação em teleproteção, como baixa latência, confiabilidade, redundância, imunidade a interferências, segurança, capacidade de diagnóstico e sincronização precisa. Tais requisitos são utilizados como parâmetros para assegurar que os sistemas de teleproteção operem de forma ágil e eficiente, minimizando os impactos em caso de falhas.

Neste contexto, a adoção de protocolos como o IEEE C37.94 e o GOOSE é vital para garantir a estabilidade e a segurança do Sistema Interligado Nacional. Considerando a crescente modernização das subestações e a necessidade de sistemas de proteção cada vez mais rápidos, interoperáveis e resilientes, torna-se fundamental compreender as vantagens e limitações das diferentes soluções de comunicação empregadas na teleproteção. Assim, surge a seguinte questão: de que forma as diferenças entre os protocolos C37.94 e GOOSE impactam o desempenho, o determinismo e a confiabilidade da teleproteção, especialmente na transição de tecnologias legadas para arquiteturas digitais de subestação? A motivação para esta investigação decorre do fato de que o C37.94, amplamente consolidado e utilizado há décadas em sistemas de teleproteção, representa uma solução tradicional e determinística baseada em enlaces ópticos dedicados, enquanto o GOOSE, definido pela IEC 61850, é projetado para atender às exigências das subestações digitais, oferecendo maior integração, escalabilidade e flexibilidade. Compreender como essas duas abordagens se comportam e em quais cenários cada uma é mais adequada torna-se essencial para orientar decisões técnicas e acompanhar a evolução das redes elétricas. Dessa forma, o objetivo deste trabalho é realizar um estudo comparativo entre os protocolos C37.94 e GOOSE, analisando as diferenças entre eles e avaliando como suas características influenciam o desempenho e a confiabilidade da teleproteção. Além disso, pretende-se identificar suas principais vantagens, limitações e os contextos em que cada protocolo se mostra mais adequado para aplicação. A organização do trabalho é descrita a seguir.

Na Seção 2, apresenta-se a fundamentação teórica, abordando definições e conceitos básicos necessários ao entendimento do trabalho, bem como uma visão geral dos protocolos de comunicação essenciais à troca de informações entre dispositivos de proteção. A metodologia do estudo é descrita na Seção 3. Os resultados e a discussão dos dados coletados são apresentados na Seção 4. A conclusão e as considerações finais são apresentadas na Seção 5.

2 FUNDAMENTAÇÃO TEÓRICA

Neste capítulo, são apresentadas as definições e os conceitos básicos necessários ao entendimento do trabalho. Inicialmente, apresenta-se um contexto histórico da teleproteção. A seguir, são descritos os regulamentos do ONS, os meios de comunicação e os requisitos de comunicação na teleproteção. Por fim, apresentam-se os protocolos de comunicação voltados à teleproteção.

2.1 Contexto Histórico da Teleproteção

A teleproteção é um sistema desenvolvido para proteger linhas de transmissão por meio da integração de relés de proteção e de canais de comunicação, permitindo monitoramento contínuo, detecção rápida e resposta imediata a falhas. Esse sistema possibilita a comunicação em tempo real entre os componentes da infraestrutura elétrica, garantindo que, ao identificar anomalias, como curtos-circuitos ou sobrecargas, sejam aplicadas medidas corretivas de forma ágil e eficiente. Segundo Pinho et al. (2020), historicamente, a evolução da teleproteção em linhas de transmissão acompanha os avanços tecnológicos e a crescente complexidade das redes elétricas. No início, entre as décadas de 1920 e 1930, a teleproteção era aplicada em sistemas bastante simples, que utilizavam relés eletromecânicos para detectar defeitos. Esses relés, embora inovadores para a época, apresentavam lentidão e imprecisão, tornando-os insuficientes para atender às demandas das redes em expansão.

Na década de 1940, um marco importante na evolução da teleproteção foi o avanço no uso de relés de distância, que permitiam uma detecção mais precisa de falhas por meio da medição da impedância da linha (FILHO; MAMEDE, 2013). Já nos anos 1970, a introdução dos relés eletrônicos representou um avanço significativo, aumentando a precisão e a velocidade de atuação dos sistemas de proteção.

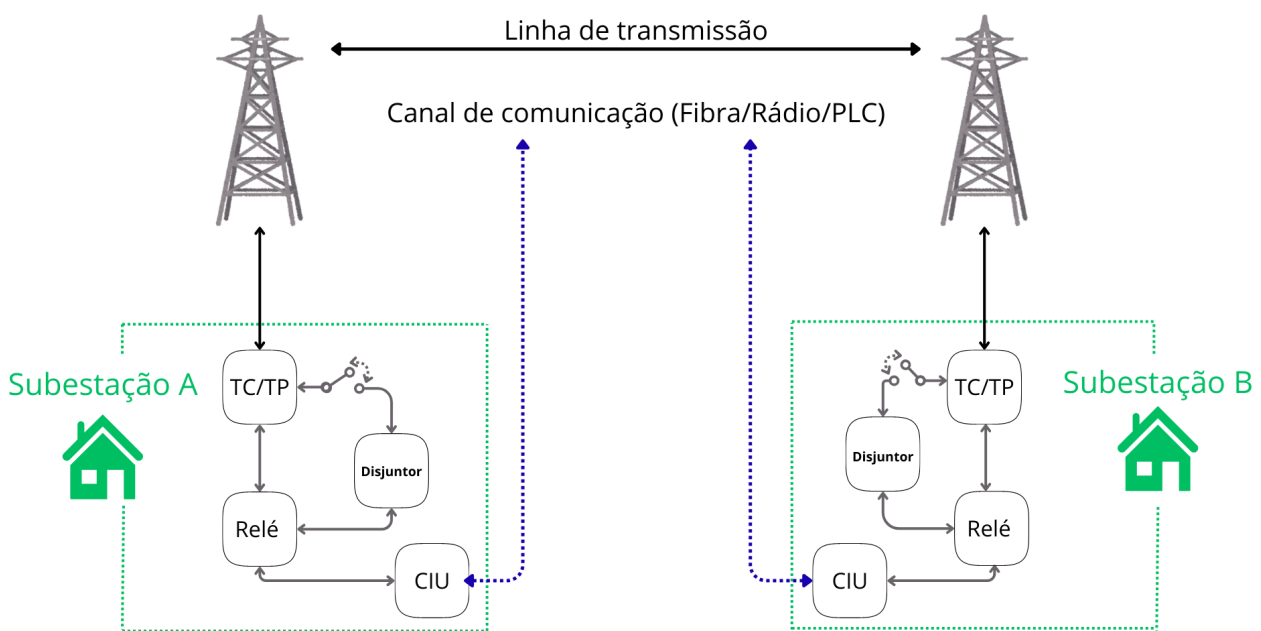
Com os avanços, nas décadas de 1980 e 1990, a teleproteção passou a incorporar relés digitais e ensaios de comunicação óptica, marcando o início da digitalização das proteções. Já nos anos 2000, com o avanço da padronização internacional, foram introduzidos protocolos específicos, como o IEEE C37.94, voltado à comunicação por fibras ópticas, e o GOOSE (IEC 61850), utilizado para a troca de mensagens urgentes em redes Ethernet (CIGRÉ, 2006). Ao longo desse período, também se consolidou o uso de fibras ópticas e de protocolos como o DNP3, que permitiram uma integração mais eficiente com sistemas de supervisão e aquisição de dados (SCADA). A partir de 2010, tecnologias como o rádio digital e a comunicação por linha de potência (PLC)¹. Passaram a complementar os sistemas de teleproteção, mantendo os protocolos IEEE C37.94 e GOOSE entre os mais utilizados. Com isso, o sistema de teleproteção passou a operar com ainda mais eficiência, integrando tecnologias modernas aos seus principais componentes:

- **Relés de proteção:** responsáveis por analisar grandezas elétricas, como corrente e tensão, para identificar falhas na linha de transmissão. Quando detectam um problema, enviam comandos para isolar a parte afetada da rede.

¹ *Power Line Communication* — tecnologia que utiliza os próprios cabos de energia elétrica para transmitir dados.

- **Sistema de comunicação:** permite que os relés instalados nas extremidades da linha troquem informações entre si. Para isso, usam-se meios como a fibra óptica, que garante rapidez e confiabilidade na transmissão de dados.
- **Disjuntores:** entram em ação para interromper o fluxo de corrente elétrica nos trechos com falhas, ajudando a proteger o sistema contra danos mais graves.
- **Transformadores de Corrente (TCs) e de Potencial (TPs):** fornecem medições precisas de corrente e de tensão, fundamentais para o funcionamento adequado dos relés.
- **Unidades de Interface de Comunicação (CIUs):** fazem a ponte entre os relés e o sistema de comunicação, garantindo que os dados circulem de forma eficiente.
- **Sistemas de supervisão e controle:** monitoram o desempenho do sistema de teleproteção em tempo real, permitindo ajustes e intervenções sempre que necessário.

Figura 1 – Representação do esquema de teleproteção entre duas subestações, destacando o relé, o CIU, o disjuntor e o canal de comunicação utilizado.



Fonte: Elaborado pela autora.

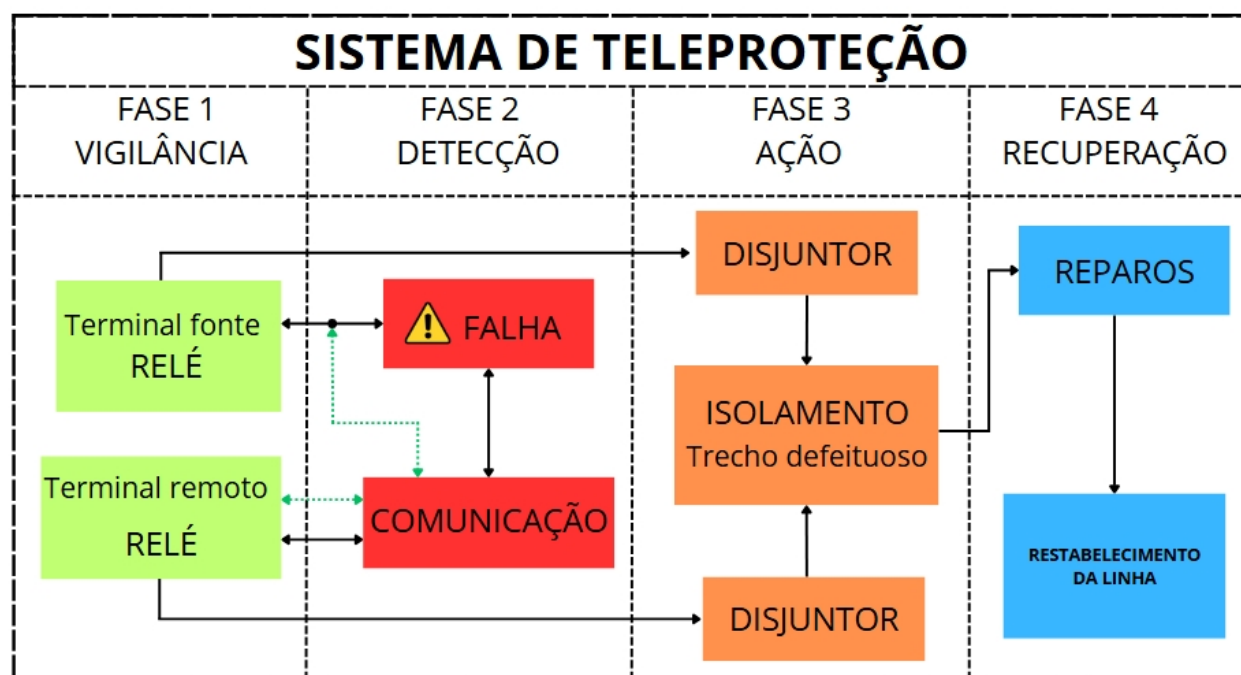
A quantidade de equipamentos em teleproteção depende da capacidade da comunicação, dos relés e da rede elétrica, sem um limite fixo, sendo ajustada conforme as necessidades e a capacidade do sistema.

2.2 Como Funciona um Sistema de Teleproteção

Conforme mostrado no diagrama esquemático da Figura 2, o funcionamento de um sistema de teleproteção pode ser dividido em quatro fases: vigilância, detecção, ação e recuperação. Vejamos, a seguir, a explicação de cada fase.

- **Fase 1:** os relés de proteção são instalados nos terminais das linhas de transmissão, onde monitoram a linha de forma contínua e detectam possíveis falhas. Esses relés medem parâmetros como corrente e tensão, com base nos dados fornecidos pelos transformadores de corrente e de potencial.
- **Fase 2:** quando uma falha é detectada pelo relé de proteção presente no terminal de origem (chamado de terminal de origem), um sinal de comando é enviado ao relé localizado no terminal remoto, por meio do sistema de comunicação já estabelecido. Essa comunicação entre os relés é favorecida pelas unidades de interface de comunicação, que podem utilizar meios como a fibra óptica. Dessa forma, os relés trocam informações sobre a falha detectada, garantindo uma resposta rápida e coordenada para isolar o trecho defeituoso (CIGRÉ, 2006).
- **Fase 3:** com base nas informações trocadas, os relés de proteção em ambos os terminais decidem qual ação tomar para isolar a seção defeituosa da linha. Essa ação envolve o acionamento dos disjuntores, equipamentos responsáveis por interromper o fluxo de corrente elétrica na área afetada. Ao interromper o fornecimento de energia no trecho defeituoso, os disjuntores evitam que a falha cause danos mais graves ao sistema elétrico, minimizando o impacto na infraestrutura e garantindo que as demais partes do sistema continuem operando normalmente. Após o isolamento da falha, o sistema de supervisão e controle entra em ação, auxiliando os operadores na análise do problema.
- **Fase 4:** com o suporte dessas ferramentas, os operadores conseguem identificar com precisão a causa da falha, adotar as medidas corretivas necessárias e realizar os reparos no trecho afetado da linha. Assim que a manutenção é concluída e a linha está novamente em condições adequadas de operação, o fornecimento de energia elétrica é restabelecido de forma segura e eficiente.

Figura 2 – Representação das fases de funcionamento de um sistema de teleproteção, incluindo vigilância, detecção, atuação e recuperação.



*As fases 3 a 4 são "ativadas" somente quando uma falha é detectada durante a vigilância.

Fonte: Elaborado pela autora.

2.3 Regulamentação do ONS para Sistemas de Proteção e Teleproteção

O Operador Nacional do Sistema Elétrico (ONS) é responsável pela coordenação, operação e supervisão do Sistema Interligado Nacional (SIN). Para garantir a confiabilidade e a segurança operativa do sistema elétrico, o ONS estabelece requisitos técnicos por meio dos Procedimentos de Rede, entre os quais se destacam os Submódulos 2.6 e 2.11 (ONS, 2010; ONS, 2021). Esses documentos definem critérios mínimos para o desempenho dos sistemas de proteção, de registro de perturbações e de teleproteção, incluindo requisitos relativos à comunicação, à integridade de sinais, à sincronização e à confiabilidade dos esquemas de proteção.

Com base nesses submódulos, os principais requisitos regulatórios aplicáveis aos sistemas de teleproteção podem ser sintetizados a seguir.

2.3.1 Baixa latência

Embora os Procedimentos de Rede não estabeleçam tempos máximos explícitos de latência, ambos os submódulos determinam que os canais de teleproteção devem atender a requisitos de desempenho relacionados ao *tempo de propagação*, *simetria* e *variação do tempo de propagação*, fatores diretamente associados ao tempo total de resposta da proteção.

O Submódulo 2.6 define, na Seção 8.2.4(a), que os canais devem ser especificados considerando o tempo de propagação e suas variações. De forma equivalente, o Submódulo 2.11, na Seção 5.1.3(a), estabelece que o desempenho adequado do canal depende desses mesmos parâmetros. Esses requisitos

garantem que a comunicação seja suficientemente rápida para permitir a atuação coordenada dos sistemas de proteção.

2.3.2 Alta confiabilidade

A confiabilidade é considerada um requisito essencial nos Procedimentos de Rede. O Submódulo 2.6, na Seção 8.2.4(b), estabelece que os canais de teleproteção devem operar com alto grau de confiabilidade, mesmo sob condições adversas. Adicionalmente, a Seção 8.2.5 determina que devem ser previstos meios de teste que permitam verificar o desempenho do sistema sem comprometer a operação da linha de transmissão.

O Submódulo 2.11 complementa essas exigências ao estabelecer, na Seção 5.1.3(b), requisitos para manutenção da integridade dos sinais em condições degradadas. A Seção 5.1.7 reforça a necessidade de redundância, especificando que os sistemas devem adotar meios independentes que assegurem continuidade da comunicação em caso de falha de um dos canais.

2.3.3 Imunidade a interferências eletromagnéticas

Em ambientes de alta tensão, a presença de campos eletromagnéticos intensos exige que os equipamentos utilizados na teleproteção apresentem robustez diante de perturbações. O Submódulo 2.6, na Seção 8.2.2, estabelece que os equipamentos de telecomunicações e teleproteção devem atender às normas aplicáveis de compatibilidade eletromagnética, garantindo a integridade dos sinais e prevenindo ações indevidas de proteção.

2.3.4 Sincronização precisa

A sincronização temporal é essencial para o correto registro de perturbações e para a análise pós-falta. O Submódulo 2.6 aborda esse aspecto na Seção 7.2.1(i)–(j), que estabelece requisitos de precisão da base de tempo, incluindo um erro máximo de 1 ms na sincronização e de 2 ms entre a detecção e o registro do evento.

O Submódulo 2.11 também aborda a necessidade de sincronismo nas Seções 4.1 e 4.2, que estabelecem diretrizes para a correlação temporal adequada entre registros e eventos, garantindo a coerência entre os dispositivos envolvidos na proteção.

2.3.5 Largura de banda adequada

O dimensionamento da largura de banda é um ponto central para o desempenho dos canais de teleproteção. O Submódulo 2.6, na Seção 8.2.4(a), determina que a largura de banda, a taxa de transmissão e o número de sinais devem ser compatíveis com o esquema de proteção adotado.

De forma semelhante, o Submódulo 2.11 estabelece, na Seção 5.1.3(a), que a taxa de transmissão e a integridade das informações devem ser garantidas para assegurar a adequada atuação da proteção.

2.3.6 Compatibilidade e interoperabilidade

A interoperabilidade entre agentes e equipamentos é fundamental para a operação integrada do SIN. O Submódulo 2.6 trata dessa exigência na Seção 1.3, ao definir que os sistemas de proteção devem estar integrados aos sistemas de telecomunicações, e nas Seções 6.2.2.1 a 6.2.2.4, que estabelecem a padronização dos requisitos entre os terminais de proteção.

O Submódulo 2.11 reforça a necessidade de padronização nas Seções 3.1 e 3.2, assegurando que diferentes agentes utilizem critérios compatíveis entre si. A Seção 5.1.3 também destaca a importância da interoperabilidade entre os canais de teleproteção.

Esses critérios são fundamentais para garantir que os sistemas de teleproteção operem de forma rápida e eficiente, minimizando os impactos em caso de falhas. Além disso, reforçam a importância da documentação adequada, assegurando a confiabilidade global do sistema elétrico. Essa abordagem é respaldada por casos como o blecaute de 2011² (BRASIL, 2011), que reforçou a importância de sistemas de proteção robustos para evitar colapsos regionais.

2.4 Meios de Comunicação

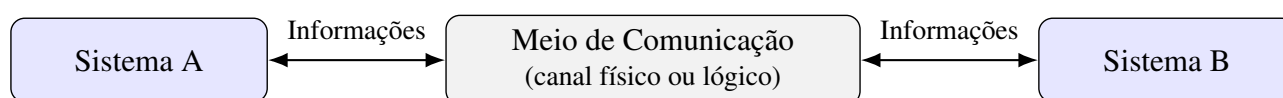
Os meios de comunicação constituem a base física responsável por transportar as informações trocadas entre os relés de proteção em sistemas de teleproteção. A escolha adequada desse meio afeta diretamente a latência, a imunidade a interferências, a disponibilidade e a confiabilidade global do sistema, fatores essenciais para evitar atuações incorretas e garantir o isolamento rápido de falhas em redes de alta tensão.

Diversas tecnologias podem ser empregadas nesse contexto, como rádios digitais, PLC e cabos metálicos blindados. Contudo, essas alternativas apresentam limitações importantes quando aplicadas a esquemas de proteção que exigem baixa latência, elevada imunidade a interferências eletromagnéticas e alta confiabilidade. Esses requisitos são estabelecidos pelos Submódulos 2.6 e 2.11 do ONS, que definem critérios rigorosos para os meios de comunicação utilizados em sistemas de proteção e de teleproteção.

Entre as opções disponíveis, a fibra óptica se destaca por atender plenamente a esses requisitos, oferecendo baixa atenuação, elevada imunidade a ruídos eletromagnéticos e ótimo desempenho tanto em enlaces de curta quanto de longa distância. Além disso, trata-se de um meio de comunicação utilizado por ambos os protocolos analisados neste trabalho, especificamente o IEEE C37.94 e o GOOSE. Isso permite uma comparação técnica consistente entre os protocolos, evitando vieses decorrentes do uso de meios físicos distintos. A Figura 3 ilustra, de forma simplificada, o conceito de um meio de comunicação, indicando como ocorre a transmissão de dados entre dois dispositivos.

² O blecaute de 2011, que afetou as regiões Norte e Nordeste do Brasil, teve origem em falhas de proteção e comunicação no sistema de transmissão de 500 kV, evidenciando a necessidade de aprimoramento dos sistemas de teleproteção e dos Procedimentos de Rede do ONS.

Figura 3 – Representação conceitual de um meio de comunicação, ilustrando a transferência de informações entre dois sistemas por meio de um canal físico ou lógico.



Fonte: Elaborado pela autora.

No que segue, apresenta-se uma descrição das características técnicas da fibra óptica, de seus tipos e de sua aplicação nos protocolos IEEE C37.94 e GOOSE, destacando sua relevância para a operação segura e eficiente das redes elétricas.

2.4.1 Fibra Óptica

A fibra óptica é amplamente empregada em sistemas elétricos devido à sua elevada capacidade de transmissão, baixa atenuação e imunidade a interferências eletromagnéticas. Tais características a tornam especialmente adequada para aplicações de proteção e teleproteção, que exigem desempenho determinístico e alta confiabilidade.

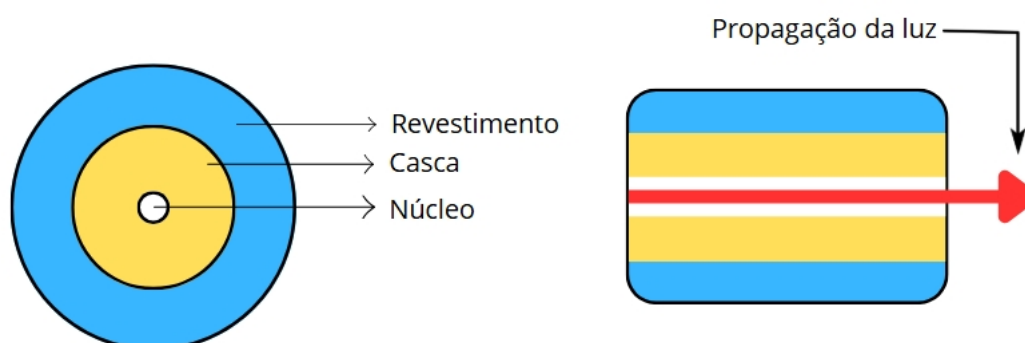
O sinal é transmitido por pulsos de luz guiados por um núcleo transparente, mantendo a estabilidade mesmo sob condições severas de campo eletromagnético em subestações. Além da composição física, o desempenho da fibra óptica deve ser avaliado considerando parâmetros como latência, jitter, taxa de erros de bits (BER), redundância e disponibilidade, conforme definidos pelos Submódulos 2.6 e 2.11 do ONS.

Existem dois tipos principais de fibra óptica, empregados nesse contexto: multimodo e monomodo, cada um adequado a diferentes contextos de aplicação e distâncias específicas.

- **Fibra óptica monomodo:** a fibra óptica monomodo possui um núcleo significativamente mais estreito, com diâmetro entre $8\ \mu\text{m}$ e $10\ \mu\text{m}$, permitindo que somente um modo de luz se propague. Isso minimiza a dispersão modal e possibilita transmissões de longa distância com baixíssima atenuação, especialmente nos comprimentos de onda de 1310 nm e 1550 nm. A Figura 4 ilustra esse tipo de fibra.

Segundo ONS e ANDERSON, em sistemas de teleproteção, a fibra monomodo é amplamente utilizada em enlaces entre subestações elétricas, integrando-se frequentemente à infraestrutura óptica das linhas de transmissão. Esse tipo de fibra permite transmissões de longa distância com baixa atenuação, tipicamente em torno de 0,35 dB/km a 1550 nm, e dispersão modal mínima, garantindo que sinais críticos de proteção sejam transportados com taxa de erros muito baixa ($\text{BER} < 10^{-9}$) (KAMINOW; LI; WILLNER, 2013; KEISER, 2021).

Figura 4 – Ilustração da fibra óptica monomodo, com destaque para o núcleo estreito que possibilita a transmissão a longas distâncias.

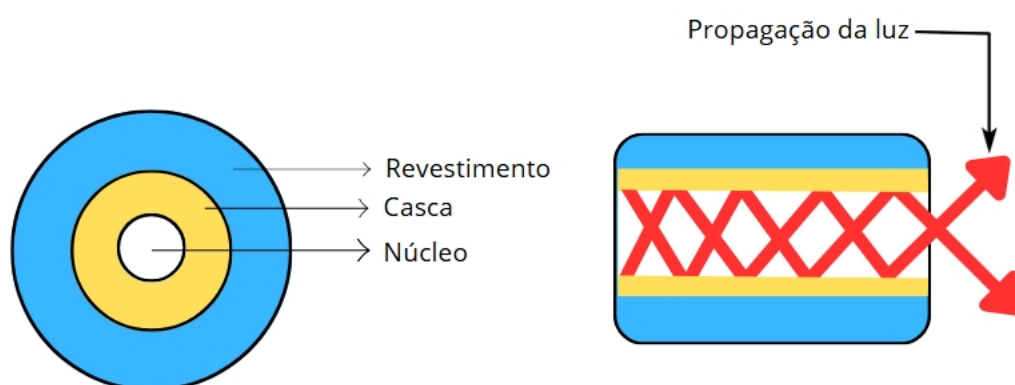


Fonte: Elaborado pela autora.

- **Fibra óptica multimodo:** a fibra óptica multimodo possui um núcleo mais largo, geralmente de $50\ \mu\text{m}$ ou $62,5\ \mu\text{m}$, o que permite a propagação simultânea de múltiplos modos de luz, conforme ilustrado na Figura 5. Essa característica reduz os custos de instalação e facilita a conexão entre dispositivos em distâncias curtas. Entretanto, a maior dispersão modal limita seu alcance típico a aproximadamente 2 km.

Segundo ONS e ANDERSON, em sistemas de teleproteção, a fibra multimodo é amplamente utilizada em enlaces internos de subestações elétricas, conectando relés e outros equipamentos ópticos de proteção. Devido à dispersão modal mais elevada, seu alcance é limitado, com atenuação típica em torno de 2 a 2,5 dB/km a 850 nm, mas ainda apresenta taxa de erros muito baixa ($\text{BER} < 10^{-9}$) para enlaces curtos KAMINOW; LI; WILLNER; KEISER.

Figura 5 – Ilustração da fibra óptica multimodo, mostrando o núcleo mais largo, adequado para transmissões de curta distância.

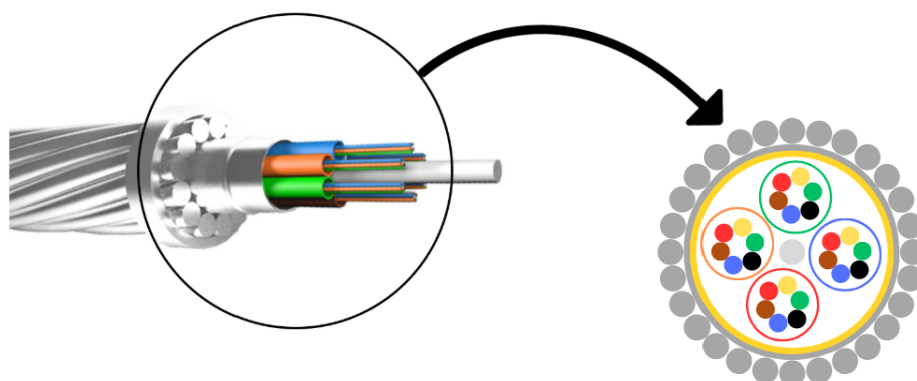


Fonte: Elaborado pela autora.

Em linhas de transmissão de alta tensão, a fibra óptica é frequentemente instalada como cabo *Optical Ground Wire* (OPGW). Esse cabo (ver Figura 6) combina, em um único componente, a função de cabo para-raios, instalado no topo das torres para proteção contra descargas atmosféricas, e a função de meio de comunicação, incorporando fibras ópticas responsáveis pela transmissão de dados com

alta confiabilidade. Dessa forma, o OPGW consolidou-se como uma das principais soluções para a comunicação em sistemas de proteção e de teleproteção associados às redes de transmissão (LEE, 2024).

Figura 6 – Estrutura do cabo OPGW, que combina fibras ópticas e condutor metálico para comunicação e proteção.



Fonte: Lee (2024) adaptada pela autora.

Embora as características físicas da fibra óptica definam seu desempenho básico, em sistemas de teleproteção seu impacto é percebido diretamente na troca de sinais entre relés e demais dispositivos eletrônicos inteligentes (IEDs) da subestação. A influência sobre parâmetros como latência, jitter, BER e determinismo varia conforme o protocolo empregado, seja o protocolo IEEE C37.94, utilizado em enlaces ópticos dedicados, ou o protocolo GOOSE definido pela norma IEC 61850 e transportado por redes Ethernet comutadas. Esses aspectos são detalhados nas subseções a seguir.

2.5 Protocolos de Comunicação

À medida que as redes elétricas se tornam mais complexas, aumenta a necessidade de garantir a continuidade e a segurança do fornecimento de energia. Nesse contexto, os protocolos de comunicação desempenham um papel indispensável nos sistemas de teleproteção. Eles viabilizam uma troca de informações eficiente, confiável e ágil entre os dispositivos de proteção, permitindo a rápida identificação de falhas e a execução de medidas corretivas coordenadas. Por serem projetados para atender a requisitos rigorosos, como baixa latência, alta confiabilidade e segurança, esses protocolos são fundamentais para a operação eficaz e segura das linhas de transmissão. A seguir, apresentam-se os principais protocolos utilizados em sistemas de teleproteção, com ênfase em suas características e contribuições para a segurança e a eficiência na transmissão de energia elétrica.

2.5.1 IEEE C37.94

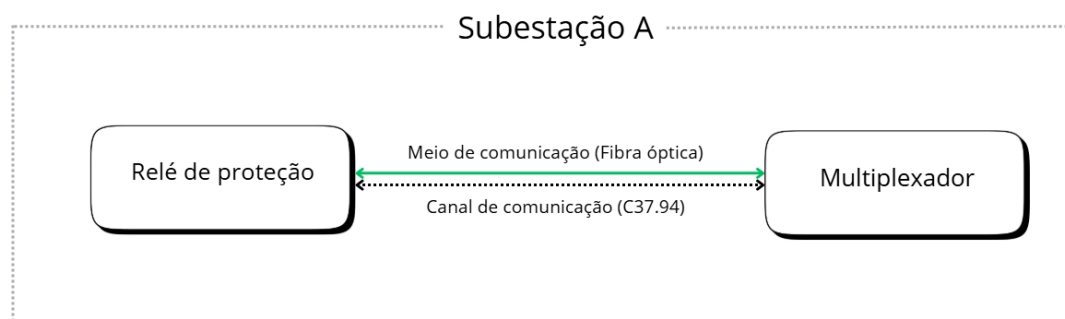
Desenvolvido pelo *Institute of Electrical and Electronics Engineers* (IEEE), o protocolo IEEE C37.94 representa um marco na evolução das comunicações em subestações elétricas, ao definir um padrão de comunicação óptica em múltiplos de 64 kb/s ($n \times 64$ kb/s, com $1 \leq n \leq 12$), destinado à interconexão de relés e dispositivos eletrônicos inteligentes (IEDs) com equipamentos de telecomunicações em subestações elétricas. Embora, do ponto de vista formal, seja uma interface óptica

padronizada que atua principalmente na camada física do modelo *Open Systems Interconnection* (OSI), o padrão é amplamente tratado na prática como um protocolo, por estabelecer regras de codificação, temporização, transmissão e sincronismo que permitem a interoperabilidade entre equipamentos de diferentes fabricantes. Neste trabalho, o termo “protocolo C37.94” é empregado no sentido aplicado, conforme o uso comum no setor elétrico.

Teve origem na década de 1990, quando a necessidade de substituir as conexões de cobre por fibras ópticas em subestações tornou-se evidente devido a problemas de interferência eletromagnética. Entretanto, a padronização formal do protocolo ocorreu apenas em 2002, com a publicação da norma IEEE Std C37.94-2002 (IEEE, 2003). Antes da sua criação, as subestações dependiam de cabos metálicos para conectar dispositivos como relés digitais e sistemas de controle. Esses cabos, porém, eram altamente suscetíveis a ruídos gerados por eventos comuns em ambientes de alta tensão, como curtos-circuito ou manobras abruptas de disjuntores. Tais interferências distorcem os sinais analógicos e digitais, comprometendo a precisão das informações e aumentando o risco de falhas operacionais — como desligamentos não intencionais ou atrasos na detecção de faltas, que poderiam levar a danos catastróficos em equipamentos ou até à interrupção prolongada de energia (ANDERSON, 1999).

O surgimento do protocolo IEEE C37.94 representou, portanto, um avanço significativo, trazendo uma solução de comunicação robusta, imune a interferências e mais confiável.

Figura 7 – Topologia C37.94, ilustrando a interligação entre o relé de proteção e o multiplexador por meio de fibra óptica.



Fonte: Elaborada pela autora.

- Características:

- Escopo e camadas: embora o IEEE C37.94 atue essencialmente na camada física do modelo OSI, definindo também a temporização e a estrutura de trama (elementos de camada de enlace), para transportar $n \times 64$ kb/s sobre uma taxa de linha de 2,048 Mb/s (E1) (IEEE, 2003).
- Modelo de comunicação: o protocolo adota uma topologia de comunicação ponto a ponto (*point-to-point*), estabelecendo um enlace óptico dedicado entre dois dispositivos, geralmente entre relés de proteção e equipamentos de telecomunicações, como multiplexadores. Esse modelo de comunicação garante uma transmissão síncrona, determinística e exclusiva, sem o compartilhamento de banda com outros dispositivos. Isso assegura latência mínima

e alta confiabilidade nas aplicações de teleproteção, características essenciais para uma proteção eficiente e rápida das redes elétricas (IEEE, 2003).

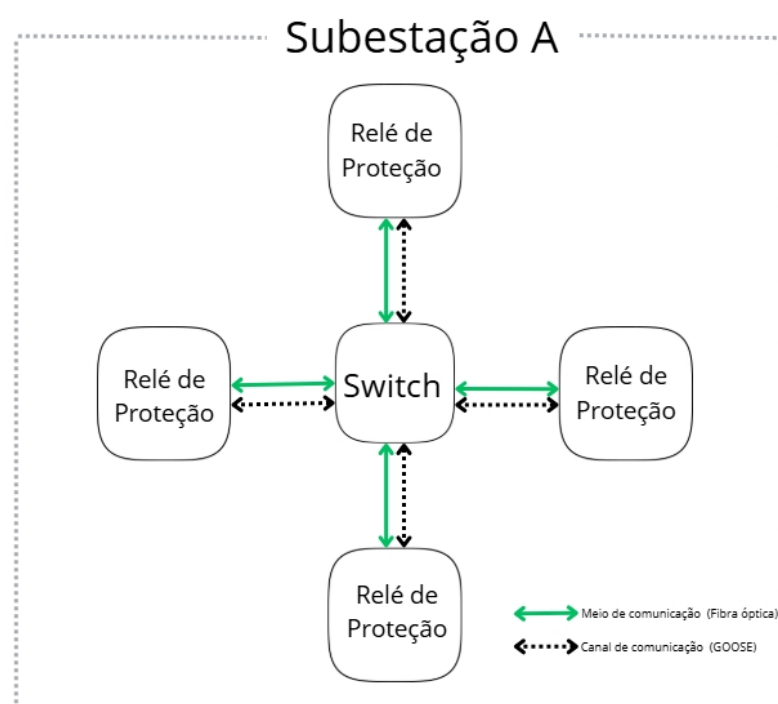
- Meio físico: utiliza fibra óptica multimodo, ideal para distâncias de até 2 km, conectando relés de proteção a disjuntores e outros equipamentos em subestações (CIGRÉ, 2006). Essa escolha se deve à sua alta capacidade de transmissão, baixo custo, facilidade de instalação e imunidade a interferências eletromagnéticas, características essenciais para garantir a confiabilidade e baixa latência exigidas em sistemas de proteção e automação.
 - Desempenho: baixa latência e imunidade à EMI, adequadas às funções críticas de proteção.
- Aplicações: O protocolo IEEE C37.94 é amplamente utilizado em sistemas de proteção diferencial e em esquemas de teleproteção de linhas de transmissão, que exigem troca instantânea de informações entre relés para a rápida detecção e o isolamento de falhas. O padrão garante comunicação confiável e determinística por meio de enlaces ópticos dedicados, imunes a interferências eletromagnéticas, assegurando alto desempenho mesmo em condições adversas. Além da confiabilidade, o IEEE C37.94 favorece a interoperabilidade entre equipamentos de diferentes fabricantes, ao definir uma interface padronizada de comunicação entre relés, IEDs e multiplexadores (IEEE, 2003). Segundo Soares (2020), sua simplicidade e robustez justificam seu uso contínuo em aplicações de teleproteção convencionais. Mesmo com o avanço de protocolos digitais, como o GOOSE, o C37.94 mantém importância em enlaces ponto a ponto, servindo como base confiável para a automação de subestações.
 - Vantagens: entre as principais vantagens do IEEE C37.94 estão a baixa latência e a alta imunidade a interferências eletromagnéticas — fatores essenciais em ambientes de alta tensão, onde qualquer ruído pode comprometer a proteção do sistema. Essa característica assegura uma comunicação estável e precisa, mesmo nas condições mais adversas. Outra grande vantagem é a compatibilidade entre equipamentos de diferentes fabricantes, já que o padrão foi criado justamente para ser universal. Com isso, fica mais fácil integrar novos dispositivos, realizar manutenções ou ampliar o sistema sem depender de soluções proprietárias. A combinação de robustez, confiabilidade e interoperabilidade faz do C37.94 uma escolha muito eficiente para aplicações críticas na proteção e na automação de subestações (IEEE, 2003).
 - Limitações: embora apresente suas qualidades, o IEEE C37.94 apresenta algumas limitações. Um dos principais desafios é o custo de instalação, que pode ser elevado devido à necessidade de infraestrutura específica para sistemas de fibra óptica, especialmente em regiões mais remotas. Além disso, o alcance da fibra multimodo, utilizada na maioria das implementações do padrão, é limitado a distâncias de até 2 km, o que restringe sua aplicação a áreas relativamente próximas da subestação (CIGRÉ, 2006; IEEE, 2003).

2.5.2 GOOSE (IEC 61850)

Com a crescente digitalização das subestações, surgiram protocolos mais flexíveis e integrados, entre eles o protocolo *Generic Object Oriented Substation Event* (GOOSE), definido pela norma

IEC 61850, publicada pela *International Electrotechnical Commission* (IEC), que representa um avanço significativo na modernização das comunicações entre dispositivos de proteção em subestações elétricas. Padronizado em 2003, com a publicação da IEC 61850-8-1, o GOOSE foi desenvolvido para superar as limitações dos sistemas tradicionais baseados em sinais físicos, que exigiam cabeamento dedicado, eram pouco flexíveis e suscetíveis a interferências eletromagnéticas. Nesse contexto, o GOOSE surge como uma solução digital eficiente, permitindo que eventos, como mudanças de estado, comandos de disparo, alarmes ou sinais de falha, sejam transmitidos em redes Ethernet de forma rápida e confiável. Essa funcionalidade permite que os IEDs respondam, em tempo quase real, às ocorrências no sistema elétrico, assegurando maior agilidade e confiabilidade na atuação dos esquemas de proteção.

Figura 8 – Topologia GOOSE, ilustrando a troca de mensagens entre os relés de proteção por meio de um switch Ethernet.



Fonte: Elaborada pela autora.

- Características:

- Escopo e camadas: o protocolo GOOSE atua na camada de enlace de dados (camada 2) do modelo OSI, utilizando quadros Ethernet para a troca direta de mensagens entre IEDs.
- Modelo de comunicação: o GOOSE adota o modelo de comunicação multicast, baseado na arquitetura publisher-subscriber. Nesse modelo, um dispositivo publicador envia mensagens que podem ser recebidas simultaneamente por vários assinantes. Essa abordagem reduz o tráfego de controle e aumenta a eficiência na troca de informações de proteção e de controle. A topologia estrela é frequentemente utilizada na configuração física da rede, na qual todos os dispositivos, como relés de proteção e IEDs, são conectados a um switch central. Esse switch distribui as mensagens multicast aos dispositivos assinantes, assegurando uma comunicação rápida e eficiente na subestação (IGRID, 2025).

- Meio físico: o protocolo é transportado em redes Ethernet, utilizando diferentes tipos de cabeamento, como fibra óptica ou par trançado, conforme as necessidades da aplicação. Em sistemas de proteção, a fibra óptica é preferencialmente adotada por oferecer isolamento elétrico superior, maior imunidade a interferências e comunicação estável e confiável.
 - Retransmissão periódica: enquanto um evento permanecer ativo, o protocolo reenviará periodicamente as mesmas mensagens, aumentando a confiabilidade da entrega das informações e eliminando a necessidade de solicitações adicionais.
 - Desempenho: em termos de desempenho, o protocolo garante tempos típicos de comunicação inferiores a 4 milissegundos, atendendo aos requisitos de aplicações de proteção que exigem resposta imediata (IGRID, 2025).
- Aplicações: o GOOSE é amplamente empregado em sistemas de automação e de proteção de subestações, permitindo a troca rápida e confiável de informações entre dispositivos de diferentes fabricantes. Sua aplicação é essencial em esquemas de proteção diferencial, intertravamento de disjuntores e sistemas de bloqueio e religamento automático, nos quais a atuação precisa e sincronizada é fundamental para a estabilidade do sistema elétrico. Segundo Soares (2020), o GOOSE consolidou-se como elemento central na automação de subestações digitais por oferecer comunicação em tempo quase real, alta interoperabilidade e redução do uso de cabeamento físico em comparação aos sistemas tradicionais. Além disso, o autor destaca que o protocolo pode coexistir com o C37.94 em arquiteturas híbridas, integrando canais ópticos dedicados e redes Ethernet em aplicações de teleproteção.
 - Vantagens: entre suas principais vantagens, destacam-se a baixa latência e a alta confiabilidade, características fundamentais para comunicações de proteção e controle em tempo real. A substituição das conexões ponto a ponto por uma rede Ethernet reduz significativamente o volume de cabeamento e os custos de instalação, além de simplificar a manutenção. Outro aspecto relevante é a interoperabilidade entre equipamentos de diferentes fabricantes, proporcionada pela padronização da IEC 61850, que permite a integração de dispositivos heterogêneos, favorecendo a expansão e a flexibilidade dos sistemas de automação e proteção (THOMAZ, 2018).
 - Limitações: embora tenha vantagens, o protocolo GOOSE apresenta algumas limitações a serem consideradas. Sua operação depende de uma rede Ethernet dedicada, devidamente configurada e isolada das demais comunicações, o que pode elevar os custos de implementação. Além disso, por se tratar de uma comunicação multicast sem confirmação direta de recebimento, o protocolo não garante a entrega absoluta das mensagens, sendo classificado como quase determinístico, característica que, embora adequada à maioria das aplicações de proteção, requer um planejamento criterioso da rede e a implementação de redundâncias para assegurar a confiabilidade da comunicação (ANDRADE et al., 2023).

Embora atuem em camadas distintas do modelo OSI e adotem abordagens tecnológicas diferentes, o IEEE C37.94, por meio de uma interface óptica padronizada essencialmente associada à camada física, e o GOOSE, definido como um protocolo orientado a eventos na camada de enlace Ethernet,

atendem ao mesmo propósito funcional: possibilitar a troca rápida, confiável e determinística de sinais de proteção entre IEDs. Por esse motivo, a comparação entre C37.94 e GOOSE é plenamente justificável. Ainda que utilizem modelos de comunicação distintos — ponto a ponto no caso do C37.94 e multicast no caso do GOOSE —, ambos são empregados como soluções de transporte para sinais críticos de teleproteção, influenciando diretamente o tempo de atuação, a confiabilidade e a arquitetura da subestação.

Dessa forma, observa-se que tanto o C37.94 quanto o GOOSE apresentam características e vantagens específicas em diferentes contextos de aplicação, o que reforça a importância de uma análise comparativa entre ambos.

3 METODOLOGIA

Neste capítulo, são apresentados os critérios de análise, as fontes de pesquisa e o método de comparação entre os dois protocolos. O estudo adota uma abordagem qualitativa, descritiva e comparativa, fundamentada em pesquisa bibliográfica não sistemática, com base na seleção de materiais considerados relevantes para o tema.

3.1 Critérios de Análise

O desenvolvimento deste trabalho adotou critérios técnicos baseados em normas e diretrizes amplamente reconhecidas no setor elétrico, conforme os submódulos 2.6 e 2.11 do ONS (2010, 2021). Esses documentos estabelecem parâmetros fundamentais para a comunicação em sistema de teleproteção, como latência máxima, disponibilidade mínima e imunidade a interferências eletromagnéticas. As tabelas 1, 2 e 3 apresentam um resumo da fundamentação teórica dos principais meios, requisitos e protocolos de comunicação em sistemas de teleproteção, respectivamente. Esses resumos fornecem a base necessária para a análise comparativa dos protocolos C37.94 e GOOSE, a ser realizada na seção 4.

Tabela 1 – Principais meios de comunicação utilizados pelos protocolos C37.94 e GOOSE.

Meio de comunicação	Resumo Geral	Aplicações Típicas
Fibra Óptica Monomodo	A fibra óptica monomodo possui um núcleo estreito ($8\ \mu\text{m}$ a $10\ \mu\text{m}$), permitindo a propagação de um único modo de luz, com mínima dispersão. Isso resulta em transmissões de longa distância com baixa atenuação, especialmente a $1310\ \text{nm}$ e $1550\ \text{nm}$, com atenuação típica de $0,35\ \text{dB/km}$ a $1550\ \text{nm}$.	Enlaces de longa distância entre subestações e centros de controle. Integrada às linhas de transmissão de alta tensão (OPGW).
Fibra Óptica Multimodo	A fibra multimodo possui um núcleo mais largo ($50\ \mu\text{m}$ ou $62,5\ \mu\text{m}$), o que permite múltiplos modos de luz. Isso resulta em maior dispersão modal, limitando o alcance a distâncias típicas de até $2\ \text{km}$, com atenuação de 2 a $2,5\ \text{dB/km}$ a $850\ \text{nm}$. Essa fibra é mais econômica, mas tem maior limite de distância.	Comunicação interna dentro de subestações, conectando IEDs, relés e equipamentos de proteção.

Fonte: Elaborado pela autora.

Nota: O OPGW é um cabo com fibras ópticas integradas, utilizado em linhas de transmissão de alta tensão (instalado no topo das torres), atuando como para-raios e como meio de comunicação simultaneamente.

Tabela 2 – Requisitos de Comunicação em Sistemas de Teleproteção

Requisito	Descrição	Observações
Baixa Latência	Tempo de transmissão extremamente baixo, considerando o tempo de propagação, a simetria e a variação do tempo de propagação, que garantem uma comunicação quase instantânea.	Canais devem ser supervisionados continuamente para detectar variações de atraso, perdas de pacotes ou falhas, conforme os requisitos dos Submódulos 2.6 e 2.11.
Alta Confiabilidade	Garantida por redundância em todos os níveis, incluindo fontes, relés, canais e supervisão, com meios de teste para verificar o desempenho sem comprometer a operação da linha.	Canais independentes e redundantes são necessários para garantir a continuidade da comunicação, mesmo em caso de falha de um deles.
Imunidade a Interferências Eletromagnéticas	Resistência a ruídos e descargas típicas de redes de alta tensão, para preservar a integridade das mensagens de disparo.	Equipamentos devem atender às normas de compatibilidade eletromagnética (CEM), conforme o Submódulo 2.6, Seção 8.2.2. A instalação correta e o aterramento adequado são essenciais para evitar falhas na proteção.
Sincronização Precisa	Precisão na sincronização do tempo para atuação coordenada e para o registro de eventos sob uma referência única, com erro máximo de 1 ms na base de tempo.	Os Submódulos 2.6 e 2.11 estabelecem a precisão necessária para garantir a correlação temporal correta entre os eventos e os dispositivos envolvidos na proteção, com erro máximo de 2 ms entre a detecção e o registro de falhas.
Largura de Banda Adequada	Capacidade de transmissão dimensionada à taxa de transmissão, ao tempo de propagação e à quantidade de sinais trocados, garantindo desempenho adequado para o sistema de proteção.	Em redes compartilhadas, garantir a reserva mínima de largura de banda e a prioridade total às mensagens de teleproteção, conforme o Submódulo 2.6, Seção 8.2.4.
Compatibilidade e Interoperabilidade	Integração eficiente entre dispositivos de diferentes fabricantes, permitindo o funcionamento de um sistema de teleproteção integrado e expandível.	Arquiteturas abertas e padronizadas são necessárias para garantir a interoperabilidade e facilitar a expansão sem comprometer o desempenho, conforme os requisitos do Submódulo 2.6, Seções 1.3, 6.2.2.1 a 6.2.2.4 e do Submódulo 2.11, Seções 3.1 e 3.2.

Fonte: Elaborado pela autora.

Tabela 3 – Protocolos de comunicação

Aspecto	IEEE C37.94	GOOSE (IEC 61850)
Origem / Padronização	Padronização formal em 2002 (IEEE Std C37.94-2002).	Padronizado em 2003 (IEC 61850-8-1).
Motivação	Substituir conexões de cobre suscetíveis à interferência eletromagnética por comunicação óptica robusta.	Superar as limitações de sistemas baseados em sinais físicos e em cabeamento dedicado, com comunicação digital via Ethernet.
Camada OSI	Atua essencialmente na camada física, definindo também a temporização e a estrutura de trama (elementos de enlace).	Camada de enlace de dados (camada 2), usando quadros Ethernet.
Meio de comunicação	Fibra óptica (com múltiplos modos para distâncias curtas, até ~2 km).	Tecnologia: Ethernet (camada 2); meio físico: fibra óptica (preferencial para proteção) ou par trançado.
Latência	Baixa latência adequada a funções críticas de proteção.	Tempos típicos inferiores a 4 ms.
Confiabilidade	Enlace óptico dedicado, síncrono, determinístico e imune a EMI.	Retransmissão periódica das mensagens enquanto o evento estiver ativo.
Características	Comunicação ponto a ponto; interface óptica em múltiplos de $n \times 64$ kb/s ($1 \leq n \leq 12$) a 2,048 Mb/s (E1).	Modelo multicast <i>publisher-subscriber</i> em Ethernet; reenvio periódico de mensagens.
Aplicações	Proteção diferencial e esquemas de teleproteção de linhas, com enlaces dedicados entre relés e telecom (ex.: multiplexadores).	Automação e proteção de subestações (proteção diferencial, intertravamento, bloqueio/religamento); podem coexistir com C37.94 em arquiteturas híbridas.
Vantagens	Baixa latência, alta imunidade às interferências eletromagnéticas e interoperabilidade entre fabricantes.	Baixa latência, alta interoperabilidade e redução de cabeamento físico em relação aos sistemas tradicionais.
Limitações	Custo de instalação e alcance limitado da fibra multimodo (até cerca de 2 km).	Depende de rede Ethernet dedicada e não garante confirmação absoluta de entrega (quase determinística), o que exige planejamento e redundâncias.

Fonte: Elaborado pela autora.

Os critérios de análise adotados na comparação entre os protocolos C37.94 e GOOSE foram:

- Desempenho e Eficiência: avaliação da latência máxima e da velocidade de transmissão de dados, verificando a capacidade de atender aos requisitos de tempo real.
- Tecnologia de Rede e Infraestrutura: análise da compatibilidade de cada protocolo com redes modernas (fibra óptica) e de sua imunidade a interferências eletromagnéticas.
- Escalabilidade e Flexibilidade: verificação da capacidade de cada protocolo de suportar redes de diferentes dimensões e do desempenho em sistemas distribuídos ou de grande porte.
- Complexidade e Facilidade de Implementação: consideração da simplicidade ou complexidade na implementação de cada protocolo, bem como de sua integração com sistemas legados ou modernos.

- Aplicações Típicas: análise das áreas de aplicação de cada protocolo, como subestações inteligentes e sistemas de proteção em redes elétricas.

3.2 Fontes de Pesquisa

Como evidenciado ao longo do desenvolvimento deste trabalho, as principais fontes de pesquisa do estudo são documentos técnicos, normas e trabalhos acadêmicos que abordam os protocolos de comunicação empregados em sistemas de teleproteção. Entre as referências mais relevantes estão os submódulos 2.6 e 2.11 do ONS, que são normas técnicas brasileiras que estabelecem os requisitos mínimos de desempenho e de confiabilidade para sistemas de proteção, registro de perturbações e telecomunicações (ONS, 2010; ONS, 2021). A seleção das fontes não seguiu um método sistemático de busca; priorizaram-se documentos técnicos e acadêmicos com conteúdo diretamente relacionado aos protocolos analisados.

Outra fonte essencial foi a dissertação de Soares (2020), que apresenta uma proposta metodológica para aplicação do protocolo GOOSE em sistemas de proteção e controle. O trabalho aborda a integração entre protocolos convencionais e digitais, com destaque para o uso dos protocolos C37.94 e GOOSE em arquiteturas híbridas voltadas à automação de subestações, demonstrando que essa abordagem contribui significativamente para a eficiência operacional do Sistema Elétrico de Potência (SEP) e reforça a importância de protocolos padronizados para garantir interoperabilidade e segurança.

Complementarmente, foram consultadas fontes técnicas de caráter informativo e institucional, como a Telecom (2022), uma publicação técnica em formato de blog que apresenta uma explicação detalhada sobre o funcionamento e as aplicações do protocolo C37.94 em sistemas de teleproteção, destacando características como simplicidade, robustez e imunidade a interferências eletromagnéticas. É o guia técnico (IGRID, 2025), publicado por uma empresa especializada em automação de subestações, que apresenta uma análise do protocolo GOOSE conforme definido pela norma IEC 61850. Essa fonte descreve como o GOOSE utiliza mecanismos rápidos e confiáveis para transmitir um conjunto de dados entre dispositivos IEDs em subestações elétricas, com tempos de resposta inferiores a 4 milissegundos.

As referências citadas forneceram o embasamento necessário para o desenvolvimento da análise teórica comparativa, permitindo identificar as principais características, vantagens e limitações de cada protocolo, conforme os critérios apresentados na Seção 3.1.

3.3 Método de Comparação

Com base nos critérios definidos na seção 3.1, cada protocolo é avaliado considerando suas características técnicas, limitações e aplicações típicas. A comparação é realizada com foco na capacidade de cada protocolo de atender aos requisitos de desempenho exigidos em diferentes cenários, como em redes de fibra óptica.

A análise considera os pontos fortes e fracos de cada protocolo, buscando identificar em quais contextos cada tecnologia se mostra mais adequada para aplicações de teleproteção. Dessa forma, este trabalho caracteriza-se como um estudo de natureza teórica, com abordagem comparativa, fundamentado em revisão bibliográfica não sistemática e em requisitos técnicos estabelecidos por normas e

documentos do setor elétrico. A análise comparativa é qualitativa e estruturada com base nos critérios definidos na Seção 3.1, sem a realização de ensaios práticos ou de simulações.

4 ANÁLISE COMPARATIVA DOS PROTOCOLOS

Neste capítulo, são apresentadas e discutidas as vantagens e desvantagens dos protocolos, visando uma análise comparativa entre eles. Ambos os protocolos possuem características e formas de implementação distintas, cujos objetivos são garantir a eficiência, a confiabilidade e a segurança da comunicação em sistemas de proteção e de automação de redes elétricas. A análise comparativa dos protocolos C37.94 e GOOSE é conduzida com base nos critérios definidos nas seções 3.1 e 3.3, considerando cinco aspectos principais dos sistemas de teleproteção. A seguir, são abordados os aspectos que influenciam a escolha entre esses protocolos em diferentes cenários operacionais.

4.1 Desempenho e Eficiência

O desempenho temporal é um dos fatores mais determinantes na escolha entre os protocolos, sobretudo porque a atuação da proteção depende diretamente do tempo total de transmissão. Embora ambos atendam aos requisitos do ONS, cada um o faz de forma distinta, o que influencia sua adequação a diferentes funções de teleproteção.

- **C37.94:** o protocolo apresenta comportamento altamente determinístico, pois opera em enlaces ópticos dedicados e livres de congestionamento. Essa característica resulta em latências tipicamente inferiores a 1 ms, com jitter praticamente nulo. Em esquemas diferenciais ou de disparo instantâneo, essa previsibilidade é decisiva: ao manter sempre o mesmo tempo de trânsito, evita alterações na lógica de proteção e falhas de seletividade. Por esse motivo, o C37.94 permanece como referência quando o requisito principal é o tempo de resposta fixo e invariável.
- **GOOSE:** embora seja capaz de atingir tempos de transmissão inferiores a 4 ms em redes bem configuradas, seu desempenho depende diretamente da arquitetura Ethernet, da carga de tráfego e da priorização de pacotes. Isso significa que o GOOSE é rápido, mas não absolutamente determinístico. Em redes estruturadas — com VLANs, QoS e isolamento adequado —, ele funciona com excelente desempenho; porém, em instalações sem engenharia de rede, o jitter pode aumentar. Assim, o GOOSE atende ao requisito de baixa latência, mas não atende à previsibilidade rígida do C37.94.

Dessa forma, o C37.94 é mais adequado para funções de proteção extremamente sensíveis ao tempo, enquanto o GOOSE se ajusta melhor a sistemas em que a latência pode ser ligeiramente variável, desde que mantida dentro dos limites da IEC 61850.

4.2 Tecnologia de Rede e Infraestrutura

A forma como cada protocolo utiliza a infraestrutura de comunicação influencia tanto a confiabilidade quanto a flexibilidade. Embora ambos façam uso de fibra óptica, a natureza dos canais difere significativamente, o que impacta sua aplicação prática.

- **C37.94:** utiliza enlaces ópticos totalmente dedicados, garantindo imunidade natural a interferências eletromagnéticas e eliminando a dependência de elementos intermediários, como switches. Essa abordagem oferece confiabilidade excepcional, sobretudo em pátios de alta tensão. Contudo, operar exclusivamente em enlaces ponto a ponto implica maior custo e menor flexibilidade: qualquer expansão exige a instalação de novas fibras e interfaces, o que dificulta sua adoção em subestações com grande número de dispositivos.
- **GOOSE:** ao operar via Ethernet, aproveita a infraestrutura de automação já existente na subestação. Isso reduz significativamente o cabeamento físico e permite que múltiplos equipamentos troquem informações por meio de VLANs e de mecanismos de priorização. No entanto, essa flexibilidade exige disciplina de engenharia de rede; caso contrário, atrasos e perdas de pacotes podem comprometer a proteção. Assim, o GOOSE apresenta excelente desempenho quando a rede é bem projetada, mas é mais vulnerável em ambientes desestruturados.

Desse modo, o C37.94 prioriza confiabilidade e isolamento físico, enquanto o GOOSE prioriza integração e aproveitamento da infraestrutura existente.

4.3 Escalabilidade e Flexibilidade

A capacidade de expandir ou adaptar o sistema depende diretamente do modelo de comunicação adotado. Nesse aspecto, os protocolos diferem tanto na filosofia quanto na aplicação.

- **C37.94:** sua arquitetura ponto a ponto torna-o pouco escalável. Cada novo canal demanda nova fibra e novas interfaces, o que eleva o custo e o esforço de expansão. Por outro lado, sua simplicidade e previsibilidade fazem com que seja ideal em sistemas estáveis, em que a topologia não muda com frequência e a confiabilidade máxima é prioridade.
- **GOOSE:** foi projetado para sistemas escaláveis. O modelo publisher–subscriber permite adicionar IEDs, modificar lógicas e integrar novos equipamentos sem alterar o cabeamento físico. Mudanças são feitas por meio de configuração, não por intervenção estrutural. Assim, o GOOSE se destaca em ambientes modernos, especialmente em subestações digitais, onde a flexibilidade operacional é um dos principais requisitos.

Portanto, o C37.94 é mais indicado para topologias fixas e confiabilidade máxima, enquanto o GOOSE se ajusta melhor a sistemas dinâmicos e de alta integração.

4.4 Complexidade e Facilidade de Implementação

A complexidade de implantação não apenas afeta o tempo de comissionamento, mas também influencia a probabilidade de erro e o custo de manutenção. Como resultado, cada protocolo apresenta vantagens distintas.

- **C37.94:** destaca-se pela simplicidade. Sua configuração é direta, exige poucos parâmetros e não depende de dispositivos intermediários. Isso reduz o risco de falhas operacionais e acelera o

diagnóstico em campo. Em sistemas em que a manutenção deve ser rápida e previsível, essa simplicidade é uma vantagem significativa.

- **GOOSE:** envolve maior complexidade inicial, pois depende de switches, VLANs, priorização de tráfego e de mecanismos de redundância. Essa complexidade aumenta o risco de erros de configuração, mas também permite uma arquitetura muito mais rica e flexível. Quando a equipe possui domínio da tecnologia, o GOOSE oferece benefícios significativos em automação e integração.

Assim, o C37.94 cumpre integralmente o requisito de simplicidade operacional, enquanto o GOOSE exige maior especialização, mas oferece funcionalidades que o C37.94 não é capaz de oferecer.

4.5 Aplicações Típicas

As escolhas entre IEEE C37.94 e GOOSE decorrem dos requisitos de cada função de comunicação.

- **C37.94:** quando o requisito central é o determinismo estrito e a imunidade a interferências, como em proteção diferencial de linha ou em teleproteção de atuação instantânea, o C37.94 é a opção adequada. Ele estabelece um enlace óptico dedicado, ponto a ponto e síncrono, com latência muito baixa e variação desprezível. Esse comportamento previsível preserva a seletividade e evita atuações indevidas em funções extremamente sensíveis ao tempo (ONS, 2021; TELECOM, 2022). Por outro lado, usar C37.94 para lógicas de automação com muitos destinos implica um aumento de enlaces dedicados, comprometendo a escalabilidade e a flexibilidade da arquitetura. Para automação escalável e interoperável, o GOOSE é a referência.
- **GOOSE:** quando o requisito predominante é integrar numerosos dispositivos, de diferentes fabricantes, trocando sinais lógicos com múltiplos destinos, o GOOSE tende a ser mais apropriado. Intertravamentos, bloqueios, comandos de religamento e a automação de subestações são exemplos. Definido pela norma IEC 61850 e operando por multicast no modelo publisher-subscriber, o GOOSE permite que um evento publicado por um IED seja consumido simultaneamente por diversos assinantes, com tempos típicos inferiores de 4 ms. Isso reduz cabeamento, simplifica a lógica distribuída e facilita mudanças e ampliações sem reconstrução de infraestrutura física, o que o consolidou como espinha dorsal dos sistemas de automação em subestações digitais (IGRID, 2025; SOARES, 2020). Em redes bem projetadas, o comportamento é altamente previsível; porém, em redes mistas ou mal configuradas, a variação de atraso tende a aumentar. Por esse motivo, devido à sua proteção primária extremamente sensível ao tempo, o C37.94 permanece como referência.

4.6 Impacto dos Meios de Comunicação

A eficácia dos sistemas de teleproteção depende não apenas do protocolo utilizado, mas também das características do meio de comunicação. Neste trabalho, são analisados os protocolos C37.94

e GOOSE, com foco na fibra óptica como meio de transmissão. O impacto não está na escolha de diferentes meios físicos, mas na forma como a fibra óptica é utilizada em cada solução.

No caso do C37.94, a fibra óptica é empregada em enlaces dedicados ponto a ponto, criando um canal exclusivo entre os relés e os equipamentos de teleproteção. Essa abordagem garante alta confiabilidade e latência previsível, fundamentais para o desempenho do sistema de proteção. A norma C37.94 foi projetada para distâncias curtas (geralmente até 2 km) e utiliza fibra multimodo, o que facilita a instalação e reduz custos. No entanto, quando são necessários percursos mais longos, o sinal é transportado por equipamentos intermediários, como multiplexadores ou conversores. Embora a interface C37.94 no IED continue padronizada, a necessidade de equipamentos adicionais pode aumentar a complexidade da rede e gerar desafios de manutenção e de custos totais do sistema.

Por outro lado, o protocolo GOOSE utiliza a fibra óptica em uma rede Ethernet, conectando relés de proteção, IEDs e sistemas de supervisão. Isso oferece maior flexibilidade e integração entre dispositivos, permitindo que múltiplos sistemas de proteção compartilhem a mesma infraestrutura de comunicação. Porém, a dependência da rede Ethernet pode afetar o desempenho do GOOSE, já que a qualidade da rede (como latência e perda de pacotes) pode comprometer a eficácia da proteção. Embora o GOOSE não imponha restrições quanto ao tipo de fibra (multimodo ou monomodo), a escolha do meio físico torna-se uma decisão estratégica, considerando fatores como distância, custo e desempenho.

Embora ambos os protocolos utilizem fibra óptica, suas abordagens para a comunicação e o transporte de dados são distintas. O C37.94 se baseia em canais dedicados, o que garante maior previsibilidade e controle, mas limita a flexibilidade em redes de grande escala. Em contraste, o GOOSE se integra a redes compartilhadas, o que oferece maior flexibilidade e escalabilidade, mas com um trade-off em termos de confiabilidade e latência, que dependem da qualidade da infraestrutura de comunicação.

Essa análise demonstra que a escolha entre C37.94 e GOOSE impacta diretamente a flexibilidade, a confiabilidade e a complexidade do sistema de teleproteção. O C37.94 pode ser mais adequado para sistemas que exigem alta confiabilidade e baixo custo operacional, enquanto o GOOSE oferece vantagens em integração e escalabilidade, embora dependa de uma rede de comunicação de alta qualidade para garantir um desempenho ideal.

4.7 Conclusão da Análise Comparativa

De modo geral, o protocolo C37.94 permanece como solução fundamental em sistemas de teleproteção que exigem alta confiabilidade e latência mínima. Sua infraestrutura dedicada de fibra óptica é um grande diferencial em cenários em que a comunicação determinística e livre de interferências é essencial, como em sistemas de proteção de linhas de transmissão (TELECOM, 2022). Em sistemas convencionais, em que a simplicidade, a previsibilidade e a confiabilidade são mais importantes do que a escalabilidade ou a integração de múltiplos dispositivos, o C37.94 mantém sua relevância. Sua principal limitação está na menor flexibilidade para sistemas de grande porte ou subestações digitais, nas quais a expansão e a integração de novos dispositivos tendem a ser mais desafiadoras e caras.

Por outro lado, o GOOSE é a escolha ideal para subestações digitais e sistemas modernos de automação, em que a escalabilidade, a flexibilidade e a interoperabilidade entre IEDs são requisitos essenciais (SOARES, 2020). A arquitetura publisher-subscriber e a comunicação multicast proporcionam alta flexibilidade, permitindo a expansão dinâmica das redes sem a necessidade de reconfiguração significativa da infraestrutura. O GOOSE é especialmente vantajoso em ambientes com nível avançado de automação, nos quais a integração entre dispositivos de diferentes fabricantes torna-se um ponto crítico para a operação do sistema (IGRID, 2025). No entanto, sua dependência da qualidade da rede Ethernet e a possibilidade de falhas de comunicação em ambientes de rede congestionados o tornam menos indicado para aplicações de proteção crítica, nas quais o determinismo absoluto e a resposta imediata são fundamentais.

Em suma, a escolha entre os protocolos C37.94 e GOOSE deve considerar o tipo de sistema de teleproteção, o nível de digitalização da subestação e a infraestrutura disponível. O C37.94 é mais indicado para sistemas convencionais de proteção e teleproteção, nos quais o foco está na alta confiabilidade e na baixa latência. Já o GOOSE é mais adequado para subestações digitais e ambientes de automação, em que a necessidade de integração, escalabilidade e interoperabilidade entre dispositivos de diferentes fabricantes prevalece (IGRID, 2025; SOARES, 2020).

Portanto, a solução mais apropriada não deve ser vista como uma escolha entre um e outro, mas sim como uma decisão contextual, orientada pelas necessidades específicas do sistema. Em muitos casos, pode ser vantajoso adotar uma abordagem híbrida, combinando as vantagens de ambos os protocolos, de modo a maximizar a confiabilidade e a flexibilidade, atendendo a diferentes necessidades operacionais e de escala. A escolha, portanto, depende de uma avaliação cuidadosa dos requisitos técnicos, das características do sistema e da infraestrutura existente, sendo fundamental alinhar o protocolo escolhido aos objetivos estratégicos do sistema de teleproteção.

5 COMENTÁRIOS FINAIS

Este trabalho comparou os protocolos C37.94 e GOOSE, amplamente empregados em sistemas de teleproteção de redes elétricas. Ambos desempenham papéis importantes na proteção e na automação desses sistemas, mas suas características técnicas os tornam mais adequados a diferentes cenários operacionais.

O protocolo C37.94 se destaca pela robustez e pela alta imunidade a interferências eletromagnéticas, sendo especialmente eficaz na interligação entre relés e equipamentos de telecomunicações por meio de enlaces ópticos dedicados. Sua aplicação é frequentemente associada a trechos de menor extensão, como dentro de subestações ou entre instalações próximas, onde a baixa latência e o comportamento determinístico são fundamentais para a teleproteção.

Por outro lado, o protocolo GOOSE oferece maior flexibilidade e escalabilidade, sendo adequado a sistemas mais complexos, como as subestações digitais baseadas na IEC 61850. Sua operação em redes Ethernet e a natureza multicast, sem confirmação direta de entrega, exigem cuidado no projeto e na supervisão da infraestrutura de comunicação, especialmente em aplicações críticas, de modo a garantir a confiabilidade das mensagens de proteção.

A combinação híbrida de ambos os protocolos pode representar uma solução eficaz, aproveitando as vantagens de cada um para atender às demandas de proteção e automação do setor elétrico. Contudo, essa integração requer infraestrutura adicional e um gerenciamento cuidadoso, dado o uso simultâneo de diferentes tipos de comunicação.

Com base na análise realizada, conclui-se que a escolha entre C37.94, GOOSE ou uma solução híbrida deve considerar o contexto de aplicação, o nível de digitalização da instalação e os critérios técnicos apresentados ao longo deste trabalho.

5.1 Contribuições do Estudo

Este trabalho trouxe importantes contribuições para a compreensão dos protocolos de comunicação empregados em sistemas de teleproteção. As principais contribuições incluem:

1. Análise da teleproteção: o estudo destacou a importância da teleproteção para garantir a segurança e a continuidade do fornecimento de energia, apresentando os principais conceitos, requisitos e o papel da comunicação nesse contexto.
2. Comparação dos protocolos C37.94 e GOOSE: o estudo proporcionou uma análise comparativa estruturada entre os protocolos C37.94 e GOOSE, destacando as principais características, como latência, confiabilidade, flexibilidade e escalabilidade. Essa comparação é essencial para entender as vantagens e limitações de cada protocolo, oferecendo uma base sólida para escolher o mais adequado a diferentes cenários de proteção e automação. A escolha correta do protocolo tem impacto direto na eficiência, na segurança e no desempenho das redes de teleproteção.

3. Integração híbrida dos protocolos na teleproteção: o estudo explorou a possibilidade de integrar os protocolos C37.94 e GOOSE a sistemas híbridos de teleproteção, prática já adotada em sistemas modernos. A combinação desses protocolos permite que suas características complementares sejam aproveitadas, otimizando a flexibilidade e a escalabilidade dos sistemas de proteção e automação em redes elétricas.

5.2 Limitações e Desafios do Estudo

Durante o desenvolvimento deste trabalho, um dos principais desafios foi a dificuldade de acesso a materiais acadêmicos que abordassem especificamente os protocolos C37.94 e GOOSE. Embora exista bibliografia sobre o tema, boa parte dela é de acesso restrito ou vinculada a publicações técnicas de mercado, o que limitou a construção de uma base teórica mais abrangente.

Outro aspecto observado foi que o contato mais aprofundado com conceitos de teleproteção ocorreu apenas durante o estágio, por meio de estudos internos e da exposição indireta ao tema no ambiente de trabalho. Esse cenário evidencia que determinados conteúdos relevantes para o setor elétrico ainda são abordados de forma limitada na formação acadêmica. Assim, identifica-se uma oportunidade de que tópicos como proteção de sistemas elétricos e teleproteção sejam abordados em disciplinas optativas, contribuindo para um maior alinhamento entre a formação universitária e as demandas do mercado.

Outro ponto importante foi a ausência de testes práticos. A pesquisa foi desenvolvida exclusivamente de forma teórica, conforme estabelecido na metodologia, o que restringiu a comparação entre os protocolos. A realização de ensaios em laboratório ou em ambientes controlados poderia complementar a análise apresentada, permitindo observar o comportamento dos protocolos C37.94 e GOOSE na prática e fortalecendo os resultados obtidos.

5.3 Oportunidades de Estudos Futuros

Uma importante oportunidade para trabalhos futuros seria a realização de simulações que validem empiricamente as comparações deste estudo, proporcionando uma análise detalhada de como os protocolos C37.94 e GOOSE se comportam em diferentes cenários operacionais.

Outra abordagem interessante seria a implementação de uma arquitetura híbrida, combinando ambos os protocolos em simulações. Isso ajudaria a entender como integrar as vantagens de cada protocolo, minimizando suas limitações e otimizando o desempenho dos sistemas de teleproteção.

REFERÊNCIAS

- ANDERSON, P. M. **Power System Protection**. [S.l.]: IEEE Press, 1999. (IEEE Press Power Engineering Series). Includes bibliographical references and index. ISBN 0-7803-3427-2.
- ANDRADE, M. d. B. et al. Integração do protocolo goose da norma iec 61850 em uma giga de testes para automação elétrica. **Revista do Congresso Brasileiro de Educação em Engenharia – COBENGE**, Rio de Janeiro, v. 51, p. 1–8, 2023.
- BRASIL, B. N. **Apagão no Nordeste afeta milhões de pessoas em sete Estados**. 2011. Acesso em: 3 mai. 2025 (SITE). Disponível em: <https://www.bbc.com/portuguese/noticias/2011/02/110204_apagao_nordeste_rp>.
- CIGRÉ. **International Council on Large Electric Systems - Technical Brochure No. 256: High Voltage Protection and Control Systems**. Paris: CIGRÉ, 2006.
- FILHO, J. M.; MAMEDE, D. R. **Proteção de sistemas elétricos de potência**. Reimpressão. [S.l.]: LTC, 2013. Inclui bibliografia e índice. ISBN 978-85-216-2012-9.
- IEEE. **IEEE Standard for N Times 64 Kilobit Per Second Optical Fiber Interfaces Between Teleprotection and Multiplexer Equipment**. 2003. Approved 2002; published 2003.
- IGRID, T. **What is IEC 61850 GOOSE Messaging?** 2025. Acesso em: 26 out. 2025 (SITE). Disponível em: <<https://www.igrid-td.com/smartguide/iec61850/goose-messaging/>>.
- KAMINOW, I.; LI, T.; WILLNER, A. **Optical Fiber Telecommunications, Volume VI**. 6th. ed. [S.l.]: Academic Press, 2013. ISBN 978-0123877822.
- KEISER, G. **Optical Fiber Communications**. 5th. ed. [S.l.]: McGraw-Hill, 2021. ISBN 978-0073386228.
- LEE, J. **Benefícios do cabo OPGW na indústria de energia: Estrutura e Aplicações**. 2024. Acesso em: 20 abr. 2025 (SITE). Disponível em: <<https://jeanette.anetfiber.com/opgw-cable-benefits-energy-industry-structure-applications/>>.
- ONS, O. N. do S. E. **Submódulo 2.6 – Requisitos mínimos para os sistemas de proteção e de telecomunicações**. 2010. Acesso em: 10 out. 2024 (PDF). Disponível em: <https://www.ons.org.br/ProcedimentosDeRede/M%C3%B3dulo%202/Subm%C3%B3dulo%202.6/Submodulo%202.6_Rev_1.0.pdf>.
- ONS, O. N. do S. E. **Submódulo 2.11 – Requisitos mínimos para o sistema de proteção, de registro de perturbações e de teleproteção**. 2021. Acesso em: 10 out. 2024 (PDF). Disponível em: <https://ecmservice.ons.org.br/ecmprsite/ecmfragmentsdocuments/Subm%C3%B3dulo%202.11-RQ_2020.12.pdf>.
- PINHO, J. T. et al. Evolução dos sistemas de proteção e teleproteção em linhas de transmissão. **Revista Brasileira de Energia**, v. 26, n. 1, p. 45–60, 2020.
- SOARES, P. H. V. **Proposta de metodologia para aplicação do protocolo GOOSE em controle e proteção do sistema elétrico**. 2020. Acesso em: 25 jan. 2025 (PDF). Disponível em: <https://repositorio.unifei.edu.br/jspui/bitstream/123456789/2260/3/Disserta%C3%A7%C3%A3o_2021052.pdf>.
- TELECOM, A. **Teleprotection: C37.94 explained**. 2022. Acesso em: 20 mar. 2025 (SITE). Disponível em: <<https://blog.albedotelecom.com/teleprotection-c37-94/>>.

THOMAZ, B. C. F. **Controle em sistemas de supervisão e telecomunicações utilizadas em subestações de energia elétrica interligadas no sistema elétrica de potência**. 2018. Acesso em: 22 fev. 2025 (PDF). Disponível em: <<https://repositorio.pgsscogna.com.br/bitstream/123456789/53465/1/Breno+Cezar+Faria+Thomaz.pdf>>.