UNIVERSIDADE ESTADUAL PAULISTA "JÚLIO DE MESQUITA FILHO"
CAMPUS DE ILHA SOLTEIRA

WU MU CHANG

COMUNICAÇÃO DE DADOS DE MEDIÇÃO, CONTROLE E PROTEÇÃO EM SUBESTAÇÕES DIGITAIS USADO A NORMA IEC 61850

Ilha Solteira - SP
2025

WU MU CHANG

COMUNICAÇÃO DE DADOS DE MEDIÇÃO, CONTROLE E PROTEÇÃO EM SUBESTAÇÕES DIGITAIS USADO A NORMA IEC 61850

Trabalho de Conclusão de Curso apresentado à Universidade Estadual Paulista (UNESP), FEIS, Ilha Solteira-SP, para obtenção do título de Grau acadêmico Bacharelado em Engenharia Elétrica.

Orientador(a): Prof. Dr. Jonatas Boas Leite

Ilha Solteira - SP

2025

FICHA CATALOGRÁFICA
Desenvolvida pela Diretoria Técnica de Biblioteca e Documentação

Wu, Mu Chang.
W959c Comunicação de dados de medição, controle e proteção em subestações digitais usado a norma IEC 61850 / Wu Mu Chang. -- Ilha Solteira: [s.n.], 2025
84 f. : il.

Trabalho de conclusão de curso (Graduação em Engenharia Elétrica) - Universidade Estadual Paulista. Faculdade de Engenharia de Ilha Solteira, 2025

Orientador: Jonatas Boas Leite
Inclui bibliografia

1. Automação em subestações. 2. IEC 61850. 3. GOOSE. 4. Sampled values. 5. Protocolos de comunicação. 6. Modelo OSI.

Elaborada por Raiane da Silva Santos - CRB-8/9999

UNIVERSIDADE ESTADUAL PAULISTA
"JÚLIO DE MESQUITA FILHO"
Câmpus de Ilha Solteira

ATA DE DEFESA DE TRABALHO DE GRADUAÇÃO

Aos cinco dias do mês de dezembro do ano de dois mil e vinte e cinco, o discente ***Wu Mu Chang,*** matriculado sob o nº 182053751, tendo como banca examinadora o seu orientador, *o Prof. Dr. Jonatas Boas Leite, o Prof. Dr. Fábio Bertequini Leão e o Doutorando Thiago Lombarde Vitoriano,* apresentou o Trabalho de Graduação intitulado **"Comunicação de Dados de Medição, Controle e Proteção em Subestações Digitais usado a Norma IEC 61850",** obtendo a nota 10,0 (DEZ) e conceito APROVADO.

Prof. Dr. Jonatas Boas Leite
- Orientador-

Wu Mu Chang
- Discente-

Prof. Dr. Fábio Bertequini Leão
- Membro da Banca -

Doutorando Thiago Lombarde Vitoriano
- Membro da Banca -

Faculdade de Engenharia – Departamento de Engenharia Elétrica
Avenida Professor José Carlos Rossi, 1370 - CEP 15.385-000, Ilha Solteira - SP - Brasil
Tel (18) 37431150 - Fax (18) 3742-2735 - www.feis.unesp.br

AGRADECIMENTOS

Agradeço primeiramente ao meu orientador do trabalho de Graduação, Jonatas Boas Leite, pelo devido suporte ao longo do processo de pesquisa e desenvolvimento.

Aos meus amigos, colegas de classe e professores pelos ensinamentos ao longo do caminho.

Aos serviços da biblioteca da UNESP que me permitiram encontrar um espaço confortável para o desenvolvimento do trabalho.

Aos ex-colegas de trabalho da empresa Siemens Energy Brasil LTDA, pelos ensinamentos durante o meu estágio. Foi durante esse período que despertei o interesse em buscar entender melhor o funcionamento de subestações de energia elétrica na vida real.

E, por fim, à família por me incentivar a estudar na Faculdade de Engenharia de Ilha Solteira.

RESUMO

Este trabalho apresenta um estudo sobre a comunicação de dados de medição, controle e proteção em subestações digitais, utilizando a norma IEC 61850, destacando sua importância para a interoperabilidade entre dispositivos eletrônicos inteligentes (IEDs) e a automação do sistema elétrico de potência. Inicialmente, aborda-se a evolução das subestações e os principais equipamentos envolvidos, como transformadores de corrente e potencial, disjuntores e chaves seccionadoras, além da transição dos relés eletromecânicos para relés digitais, que possibilitaram maior precisão e integração com sistemas de supervisão e controle. Em seguida, são explorados os protocolos de comunicação mais utilizados, como Fieldbus, Ethernet e TCP/IP, bem como os modelos OSI e suas camadas, fundamentais para entender a estrutura de transmissão de dados. O estudo aprofunda-se na norma IEC 61850, descrevendo sua arquitetura, modelo de dados orientado a objetos, linguagem de configuração SCL (*System Configuration Language*) baseada em XML (*Extensible Markup Language*), os principais serviços, como GOOSE (*Generic Object Oriented Substation Event*) e SVs (*Sampled Values*), que garantem baixa latência e alta confiabilidade na troca de informações críticas, e a topologia de redes para a redundância de comunicação entre os dispositivos e controle do tráfego de dados. Também são discutidos aspectos práticos da implementação, incluindo a simulação de mensagens GOOSE e SV por meio do emulador da SAMU (S*tand-Alone Merging Unit*), desenvolvido no Visual Studio 2022®, integrado à norma IEC 61850, e a análise do tráfego de pacotes utilizando o Wireshark®. Além disso, é apresentada a metodologia *Hardware-in-the-Loop* (HIL), que permite testar algoritmos de controle em condições realistas com baixo custo e alta fidelidade, reduzindo riscos e acelerando o desenvolvimento.

Palavras-chave: Automação em Subestações; IEC 61850; IEC 61850-8-1, IEC 61850-9-2; GOOSE; Modelo OSI; Protocolos de Comunicação; Sampled Values.

ABSTRACT

This work presents a study on data communication for measurement, control, and protection in digital substations using the IEC 61850 standard, highlighting its importance for interoperability among Intelligent Electronic Devices (IEDs) and the automation of the electric power system. Initially, it addresses the evolution of substations and the main equipment involved, such as current and voltage transformers, circuit breakers, and disconnect switches, as well as the transition from electromechanical relays to digital relays, which enabled greater accuracy and integration with supervision and control systems. Next, the most commonly used communication protocols are explored, such as Fieldbus, Ethernet, and TCP/IP, as well as the OSI models and their layers, which are fundamental for understanding the data transmission structure. The study delves into the IEC 61850 standard, describing its architecture, object-oriented data model, SCL configuration language based on XML (Extensible Markup Language), and the main services, such as GOOSE (Generic Object Oriented Substation Event) and SVs (Sampled Values), which ensure low latency and high reliability in the exchange of critical information, and the network topology for communication redundancy between devices and data traffic control. Practical aspects of implementation are also discussed, including the simulation of GOOSE and SV messages through the SAMU (Stand-Alone Merging Unit) program developed in Visual Studio, integrated with the IEC 61850 standard, and the analysis of packet traffic using Wireshark®. Furthermore, the Hardware-in-the-Loop (HIL) methodology is presented, which allows testing control algorithms under realistic conditions at low cost and high fidelity, reducing risks and accelerating development.

Keywords: Communication Protocols; GOOSE; IEC 61850; IEC 61850-8-1, IEC 61850-9-2; OSI Model; Sampled Values; Substation Automation.

LISTA DE FIGURAS

LISTA DE TABELAS

LISTA DE QUADROS

LISTA DE ABREVIATURAS E SIGLAS

ACSI	Abstract Communication Service Interface
APDU	Application Protocol Data Unit
APPID	Application Identification
ASDU	Application Service Data Unit
ASN.1	Abstract Syntax Notation One
BER	Basic Encoding Rules
CID	Configured IED Description
CLP	Controlador Lógico Programável
DA	Data Attribute
DANH	Doubly Attached Node for HSR
DANP	Doubly Attached Node for PRP
DO	Data Object
GOOSE	Generic Object Oriented Substation Event
GOOSE PDU	Generic Object Oriented Substation Event Protocol Data Unit
GPS	Global Positioning System
GSE	Generic Substation Event
GSSE	Generic Substation Status Event
HIL	Hardware-in-the-Loop
HSR	High-availability Seamless Redundancy
ICD	IED Configuration Description
IEC	International Electrotechnical Commission
IED	Intelligent Electronic Device
IEEE	Institute of Electrical and Electronics Engineers
IHM	Interface Homem-Máquina
IP	Internet Protocol
ISO	International Organization for Standardization
LAN	Local Area Network
LD	Logical Device
LN	Logical Node
LPDU	Link Protocol Data Unit
MAC	Media Access Control

MMI	Man-Machine Interface
MMS	Manufacturing Message Specification (ISO 9506)
MU	Merging Unit
OPC	OLE for Process Control
OSI	Open Systems Interconnection
PDU	Protocol Data Unit
PRP	Parallel Redundancy Protocol
SAMU	Stand-Alone Merging Unit
SAN	Single Attached Node
SAS	Sistema de Automação de Subestação
SCADA	Supervisory Control And Data Acquisition
SCD	System Configuration Description
SCL	substation automation System Configuration Language (IEC 61850-6)
SCSM	Specific Communication Service Mapping
SE	Subestação Elétrica
SEP	Sistema Elétrico de Potência
SNTP	Simple Network Time Protocol
SPCS	Sistema de Proteção, Controle e Supervisão
SSD	System Specification Description
SV	Sampled Value
SV PDU	Sampled Value Protocol Data Unit
TC	Transformador de Corrente
TCI	Tag Control Information
TCP	Transmission Control Protocol
TP	Transformador de Potencial
TPID	Tag Protocol Identifier
UDP	User Datagram Protocol)
UML	Unified Modeling Language
VLAN	Virtual Local Area Network
WAN	Wide Area Network
XML	Extensible Markup Language

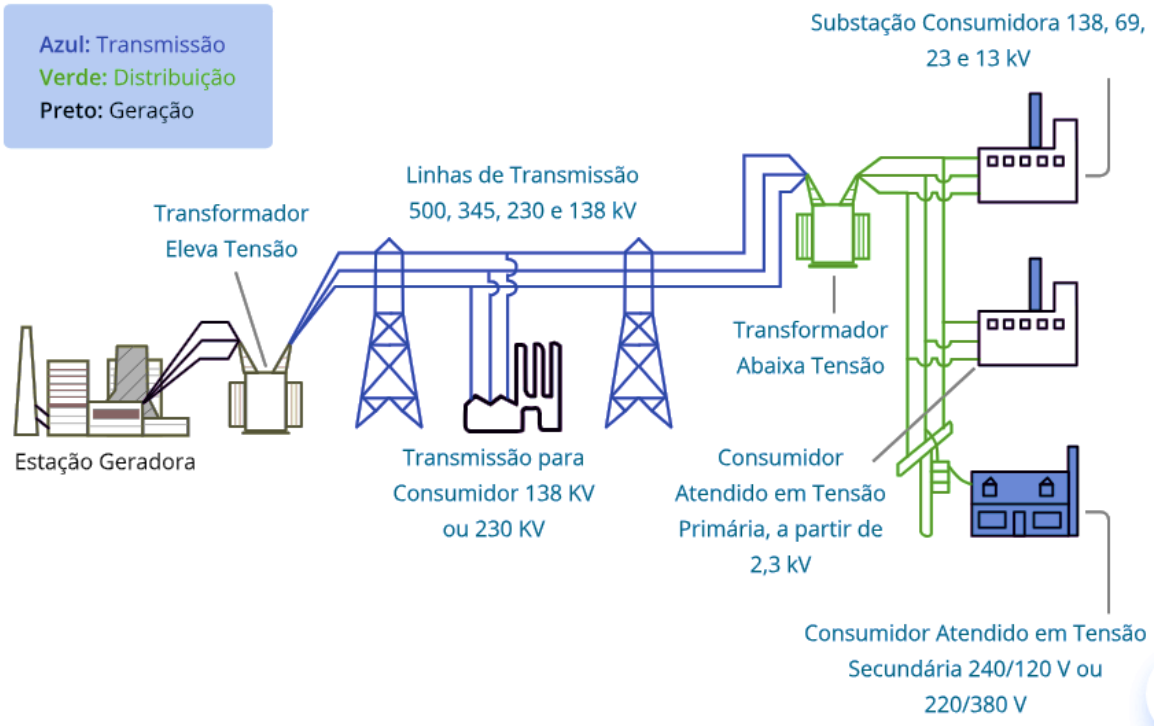
SUMÁRIO

1 INTRODUÇÃO

Nos últimos dez anos, a expansão do setor energético vem ganhando destaque de forma significante no Brasil. De acordo com o levantamento de dados feito pela Empresa de Pesquisa Energética (EPE), a capacidade instalada no país foi expandida em 4,6% no período entre 2023 e 2024, enquanto na geração de eletricidade houve um aumento de 6,1%, sendo que a maior parte corresponde à geração hidráulica (43,66%). Devido ao aumento do consumo de energia, tem-se como foco o aperfeiçoamento da transmissão de energia de forma mais sustentável possível. Dessa forma, visa-se a importância do desenvolvimento de soluções digitais para otimização do desempenho do setor energético, garantindo qualidade de transporte, agilidade na mitigação de falhas e, consequentemente, a diminuição de custos no comissionamento e manutenção de equipamentos.

Atualmente, o sistema elétrico de potência (SEP) é formado pela geração, transmissão e distribuição, conforme mostrado na Figura 1.

Figura 1 – Sistema Elétrico de Potência (SEP)



Fonte: ANEEL (s.d.)

- **Geração:** É responsável pela produção de energia elétrica, formado por centrais elétricas que convertem alguma forma de energia (cinética, calor, etc) em energia elétrica. Entre elas tem-se as usinas hidrelétricas, termelétricas, nucleares, eólicas e solares.

- **Transmissão:** Como o seu próprio nome já diz, é responsável pelo transporte de energia elétrica dos centros de geração até os de consumo. Geralmente, antes de a energia do sistema de geração chegar à subestação de transmissão, ela passa por uma subestação intermediária (elevadora), onde os transformadores elevam a tensão, consequentemente baixando a corrente, para diminuição de perdas no meio do caminho devido à resistência elétrica nos condutores.

- **Distribuição:** Realiza a distribuição da energia elétrica recebida do sistema de transmissão aos consumidores finais. Note que na Figura 1, antes da distribuição, a energia passa por transformadores que reduzem a tensão, controlando o fluxo de potência de acordo com a necessidade dos consumidores.

No passado, o controle e o monitoramento das subestações elétricas eram realizados manualmente por operadores. Além disso, utilizavam-se sistemas convencionais com relés eletromecânicos e cabeamento físico extenso, o que resultava em baixa flexibilidade, dificuldade de integração com outros sistemas, altos custos de manutenção e demora na atuação em caso de falhas no sistema elétrico.

A automação das subestações começou a ganhar espaço com o desenvolvimento dos dispositivos eletrônicos inteligentes (IEDs), baseados em tecnologia de microprocessadores, permitindo a inclusão de mais funções e variáveis para controle e proteção. No entanto, como cada fabricante adotava protocolos de comunicação próprios, a interoperabilidade entre IEDs era limitada, obrigando o uso de dispositivos de um único fabricante ou a reconfiguração completa da subestação.

Para resolver esse problema, foi criada, em 2003, a norma IEC 61850, que padroniza a comunicação no processo de digitalização das subestações elétricas, tornando-a mais eficiente, segura e interoperável.

A norma IEC 61850 estabelece uma arquitetura hierárquica composta por três níveis — *station*, *bay* e *process* — que organiza as funções de supervisão, controle e proteção de forma padronizada. Para garantir interoperabilidade entre dispositivos, ela utiliza a linguagem SCL (*Substation Configuration Language*), baseada em XML (*Extensible Markup Language*), para modelagem de dados orientada a objetos, permitindo descrever de maneira estruturada a configuração da subestação, os IEDs e suas funcionalidades. Além disso, a norma define serviços essenciais como GOOSE (*Generic Object Oriented Substation Event*), SVs (*Sampled Values*) e MMS (*Manufacturing Message Specification*), que utilizam a comunicação digital via rede Ethernet, assegurando comunicação rápida em tempo real e confiável entre os equipamentos, reduzindo significativamente a necessidade de cabeamento físico e aumentando a eficiência operacional.

1.1 OBJETIVOS

Este trabalho tem como objetivo estudar a comunicação de dados de medição, controle e proteção em subestações digitais baseada na norma IEC 61850, abordando sua arquitetura, modelo de dados, serviços de comunicação, redundância de redes e aplicação prática. Para isso, são explorados conceitos fundamentais, como a evolução da automação nas subestações, protocolos de rede, modelos OSI e TCP/IP, arquiteturas de rede, além da implementação de simulações com o emulador SAMU (*Stand-Alone Merging Unit*), desenvolvido no Visual Studio 2022, e análise de tráfego de mensagens via Wireshark®. Também é apresentada a metodologia *Hardware-in-the-Loop* (HIL), que permite testar algoritmos de controle em condições realistas com baixo custo e alta fidelidade, contribuindo para a modernização do setor elétrico e para o desenvolvimento sustentável.

1.2 ORGANIZAÇÃO DO TRABALHO

Este documento está estruturado da seguinte forma:

No capítulo 1 é apresentada a introdução, que contém o contexto da importância deste trabalho e os principais objetivos.

No capítulo 2 são abordados os conceitos teóricos do funcionamento das subestações elétricas, a evolução e arquitetura dos sistemas de automação (SAS), os principais protocolos de comunicação e os modelos OSI e TCP/IP, que organizam as funções de rede em camadas lógicas.

No capítulo 3 é introduzida a norma IEC 61850, descrevendo os conceitos gerais, sua arquitetura, a modelagem de dados orientada a objetos, os serviços de comunicação (MMS, GOOSE e SVs) e mecanismos de redundância de rede para garantir confiabilidade.

No capítulo 4 é abordado o estudo prático por meio da simulação com o emulador SAMU, baseado na metodologia *Hardware-in-the-Loop*, para testar a transmissão dos *Sampled Values* conforme IEC 61850-9-2. Este tópico inclui análise do tráfego de dados com Wireshark® e decodificação do frame savPDU.

No capítulo 5, por fim, é apresentada a conclusão do trabalho, contendo as considerações finais de tudo que foi aprendido no processo de pesquisa e no estudo prático.

2 CONCEITOS TEÓRICOS

Para facilitar a compreensão da comunicação de dados de medição, controle e proteção conforme a norma IEC 61850, este capítulo apresenta os conceitos teóricos fundamentais. Serão abordados subestações elétricas, a evolução e arquitetura dos sistemas de automação (SAS), os principais protocolos de comunicação e os modelos OSI e TCP/IP, que organizam as funções de rede em camadas lógicas.

2.1 SUBESTAÇÕES ELÉTRICAS

Pode-se definir uma subestação (SE) como sendo um conjunto de equipamentos de manobras e/ou transformação e ainda eventualmente de compensação de reativos usado para transferir o fluxo de energia no sistema elétrico de potência (SEP) e possibilitar a sua diversificação por meio de rotas alternativas, possuindo dispositivos de proteção capazes de identificar os diferentes tipos de faltas que ocorrem no sistema e isolar os trechos onde estas falhas ocorrem para realizar a devida manutenção nos equipamentos, servindo assim o sistema elétrico da melhor forma possível.

Segundo Frontin (2013), a implementação de uma subestação ocorre quando há necessidade de expansão do sistema elétrico para atendimento de uma determinada região, a uma cidade ou a uma planta industrial. Ao realizar os estudos de planejamento específicos, define-se então a configuração de barra da futura subestação, as principais características de seus equipamentos do pátio de manobras e do seu sistema de proteção e controle.

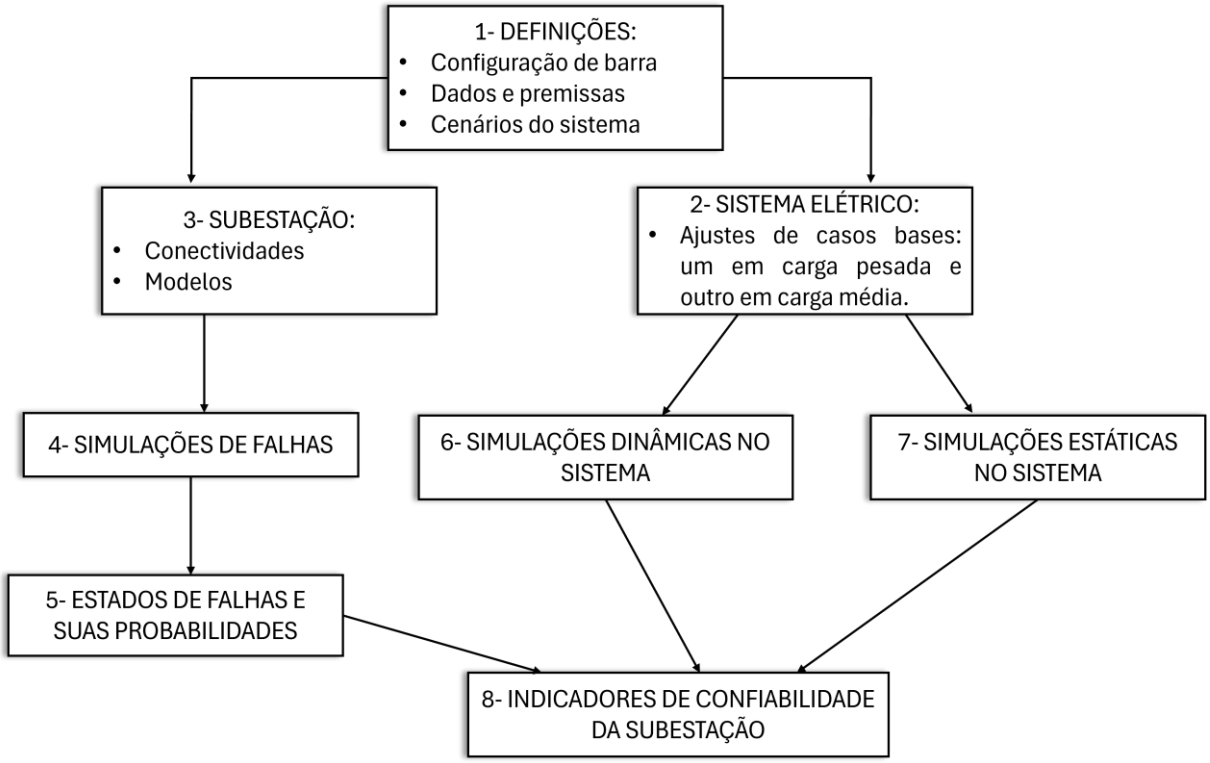
Além disso, no projeto de uma subestação, deve-se considerar aspectos como confiabilidade do sistema elétrico, o que depende da configuração das barras; facilidade de manutenção e expansão, garantidas por um arranjo físico bem planejado; resistência dos equipamentos às exigências operacionais; e atuação segura e eficaz dos sistemas de comando e proteção.

De acordo com o NERC (*North American Electric Reability Corporation*), citado por Frontin (2013), o conceito de confiabilidade vai muito além da avaliação quantitativa dos parâmetros tradicionais, tais como a probabilidade de perda de energia, frequência de falha, expectativa de energia não suprida etc, ela implementa também a segurança, caracterizada pela capacidade do sistema elétrico em resistir

aos distúrbios súbitos, e a adequação, que, por sua vez, caracteriza-se a capacidade do sistema elétrico em oferecer redundância razoável no atendimento às cargas.

No fluxograma da Figura 2 são apresentadas as principais etapas do processo como é feita essa avaliação.

Figura 2 – Fluxograma Etapas do Processo



Fonte: Adaptada de FRONTIN (2013)

2.1.1 Tipos de subestações

Como foi dito anteriormente, uma subestação pode ser configurada atendendo diferentes funções, dependendo do seu propósito e onde ela será instalada. O Quadro 1 apresenta os tipos de subestações e suas principais funções.

Quadro 1 - Tipos de subestações e suas respectivas funções

SE de manobra	Permite realizar manobras no sistema, inserindo ou retirando partes do serviço no mesmo nível de tensão.
SE Elevadora	Encontra-se na saída das usinas geradoras; tem como objetivo de elevar a tensão para níveis de transmissão e subtransmissão (transporte econômico de energia) para minimizar perdas de energia em longas distâncias.
SE Abaixadora	Encontra-se na periferia das cidades; faz o trabalho de diminuir os níveis de tensão para reduzir o risco de eventuais acidentes

	e inconveniências para a população como: rádio interferência (RIV), campos magnéticos intensos e faixas de passagem muito largas. Elas alimentam as SEs de distribuição.
SE de Distribuição	Tem como objetivo diminuir a tensão para o nível de distribuição primária (13,8kV – 34,5kV). Pode pertencer à concessionária ou aos grandes consumidores. Portanto, está mais próxima ao consumidor final.
SE de Regulação de Tensão	Regula a tensão através do emprego de equipamentos de compensação, tais como reatores, capacitores, compensadores estáticos etc.
SE Conversora	É associada aos sistemas de transmissão em corrente contínua HVDC. Tem-se SE Retificadora (CA para CC) e SE Inversora (CC para CA).

Fonte: Produção do próprio autor (descrição baseada em materiais internos da Siemens)

Nessas subestações, existem três formas de operação:

- **Subestações com operador:** exige presença humana e alto nível de treinamento, e o uso de computadores na supervisão e operação local só se justifica para instalações de maior porte.

- **Subestações Semiautomáticas:** possuem computadores locais ou intertravamentos eletromecânicos para impedir operações indevidas por parte do operador local; portanto, consistem em sistemas automáticos com intervenção humana.

- **Subestações automatizadas:** são supervisionadas remotamente por meio de computadores e SCADA (*Supervisory Control and Data Acquisiton*).

2.1.2 Principais equipamentos encontrados em subestações

Comumente, uma subestação tradicional é composta por para-raios, transformador de corrente (TC), transformador de potencial (TP), disjuntores, chaves seccionadoras e transformador de potência, como mostrada na Figura 3.

Figura 3 – Visão geral de uma subestação

1 - Para-raios; 2 - Transformador de potencial; 3 - Transformador de corrente;
4 - Disjuntor tripolar; 5 - Chave seccionadora; 6 - Transformador de potência

Fonte: MAMEDE (2016)

- **Para-raios:** Os para-raios são instalados próximos à entrada de linha da subestação para proteger os equipamentos contra sobretensões, como as causadas por descargas atmosféricas. Quando ocorre uma sobretensão, eles desviam a corrente para o aterramento e limitam a tensão aplicada aos equipamentos.

- **Transformador de Corrente (TC):** É um equipamento que faz transformação da corrente, onde o lado secundário costuma sair uma corrente em uma escala bem menor para que os equipamentos consigam fazer medição e proteção de forma segura.

- **Transformador de Potencial (TP):** Assim como o TC, o TP faz a transformação em relação à tensão, reduzindo a tensão a níveis seguros para que consiga ser conectado aos relés e medidores para fazer a proteção e medição.

- **Disjuntores:** São equipamentos de manobra encontrados nos pátios das subestações, compondo a proteção do sistema. Eles são capazes de conduzir

ou interromper o fluxo de energia na subestação. Quando é detectada uma sobretensão, ocorre abertura do circuito dos disjuntores, fazendo com que interrompa o trecho de energia onde há falha, isolando assim o sistema elétrico.

- **Chave Seccionadora:** São equipamentos também de manobra encontrados nos pátios da subestação. Diferentes dos disjuntores, eles somente fazem abertura ou fechamento quando não há corrente, ou seja, a carga deve ser nula. Eles isolam o trecho do sistema a partir da distância do seccionamento. Além disso, as chaves seccionadoras costumam se encontrar ao lado dos disjuntores, estes, por sua vez, não podem ser vistos a olho nu o *status* de abertura e fechamento em campo, visto que a unidade interruptora é encobrida pelo invólucro de porcelana. Portanto, a chave seccionadora garante que o circuito esteja totalmente aberto/fechado ou isolado.

- **Transformador de Potência:** Diferente do TP, este transformador comumente se encontra logo na entrada ou saída de linha. Esse equipamento serve para controlar o fluxo de potência, elevando ou reduzindo a tensão (subestação elevadora e subestação abaixadora) durante a transmissão e distribuição, respectivamente, diminuindo as perdas de energia e sendo distribuída conforme a demanda.

2.2 AUTOMAÇÃO NAS SUBESTAÇÕES ELÉTRICAS

No passado, as subestações convencionais dependiam de dispositivos eletromecânicos para atuar na proteção, comando e supervisão, exigindo a presença contínua de profissionais no local para operar os equipamentos de forma manual. Além disso, essas instalações operavam de forma isolada, sem qualquer integração ou troca de informações entre si (REIS, 2023).

Essa limitação estava diretamente relacionada à tecnologia disponível na época, baseada em relés eletromecânicos ou eletrônicos, que realizavam apenas uma função por equipamento e operavam de forma analógica. A monitoração desses relés era restrita a contatos auxiliares, indicando posições aberta ou fechada, e, para converter sinais analógicos em digitais, era necessário o uso de transdutores adicionais, aumentando a complexidade e os custos do sistema (MAMEDE, 2016).

Ademais, nos sistemas convencionais na década de 50, a comunicação entre os diferentes níveis da subestação era restrita a informações essenciais e ocorria exclusivamente por meio do cabeamento metálico. Cada ponto de sinal exigia um cabo de cobre único ligando o equipamento ao dispositivo de controle ou proteção, resultando em grande quantidade de cabos e borneiras nos painéis, tornando também uma manutenção difícil (MENDES; JARDINI, 2009).

No entanto, devido ao crescimento do consumo de energia ao longo do tempo, surgiu a necessidade de evoluir os sistemas de automação de subestações (SAS) para atender ao mercado de forma mais eficiente, acompanhando simultaneamente os avanços das tecnologias associadas, principalmente computadores e dispositivos inteligentes baseados em microprocessadores.

Um exemplo de tecnologia baseada em microprocessadores é o CLP, em inglês PLC (*Programmable Logic Controller*), desenvolvido por General Motor em 1968 para automação de processos na indústria. No passado, os painéis eletromecânicos para controle lógico demonstravam dificuldades nas utilizações e ajustes da lógica, fazendo com que os programadores levassem mais tempo e, consequentemente, gastassem mais dinheiro para alteração das linhas de produção. O CLP é um aparelho eletrônico digital que utiliza uma memória reprogramável para armazenar internamente instruções e para implementar funções específicas tais como lógicas, sequenciamento, temporização, contagem e aritmética, controlando por meio de módulos de entradas e saídas vários tipos de máquinas ou processos (ZANCAN, 2011).

No final dos anos 1980, muitos fabricantes de medidores, relés, controladores, registradores e entre outros dispositivos passaram a incorporar microprocessadores em seus projetos. O maior avanço na automação das subestações ocorreu na década de 1990, com o surgimento dos IEDs (*Intelligent Electronic Devices*), que passaram a concentrar diversas funções de proteção, controle e medição em um único dispositivo, marcando o início da digitalização das subestações. Dessa forma, os medidores podem fornecer dados de faltas e de qualidade de energia; relés podem fornecer dados de medição, assim como dados de registros de faltas e sequência de eventos, por exemplo. Além disso, por concentrar informações em um único dispositivo e estar localizado próximo ao processo controlado, os IEDs reduziram significativamente a necessidade de cabeamento (MENDES; JARDINI, 2009).

Os IEDs mais comuns são os relés de proteção, os controladores lógicos programáveis (CLP) e os controladores de potência. No entanto, os CLPs estão mais associados à automação industrial e não diretamente no sistema elétrico, portanto, para esse trabalho relacionado aos sistemas de medição, controle e proteção da SAS (Sistema de Automação de Subestação), serão intercambiados os termos IEDs com os relés de proteção. A Figura 4 mostra um relé de proteção (IED) da Siemens.

Figura 4 – Relé de Proteção (IED) da Siemens

Fonte: MESH ENGENHARIA (s.d.)

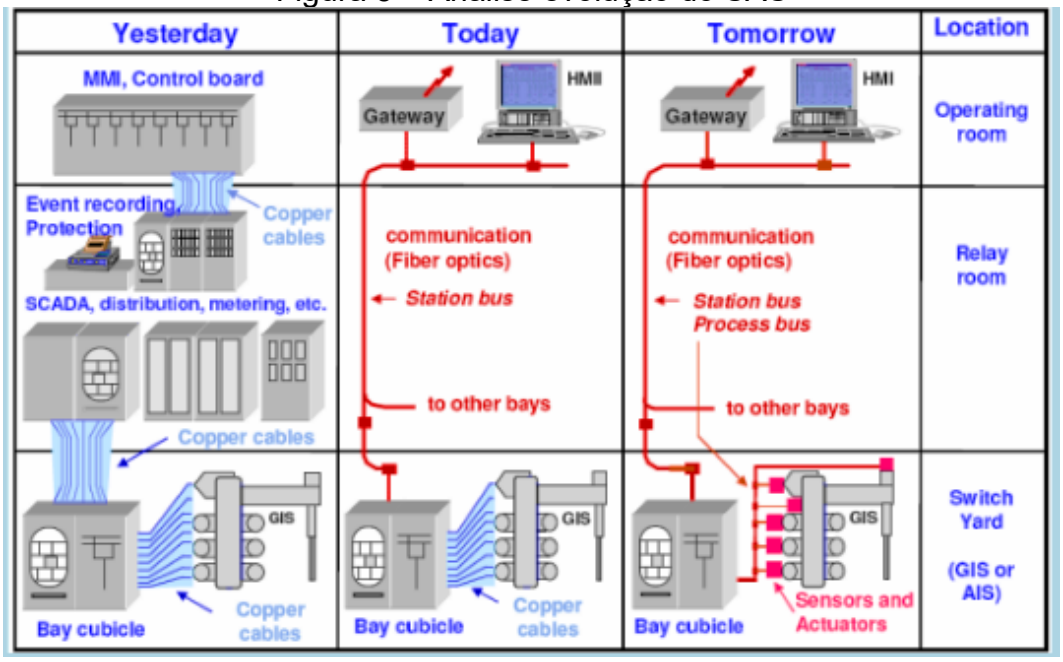
No nível de estação, os antigos painéis sinóticos (MMI) foram substituídos por Interfaces Humano-Máquina (IHMs), que se tornaram comuns nessa década, trazendo mais informações visuais em tela sobre o status do sistema de potência e seus equipamentos (primários e secundários) usados, formando uma rede robusta de sistemas de Aquisição de Dados e Controle Supervisório (SCADA). Esse sistema é composto por um software que faz interface do sistema de automação da subestação com o operador. A principal atribuição do sistema supervisório em subestações elétricas consiste em efetuar o controle e a supervisão unificada dos equipamentos de nível primário, bem como o acompanhamento dos sistemas de apoio (secundários). De modo geral, tais sistemas estão localizados em instalações externas à subestação, denominadas Centros de Operações do Sistema (COS) (SOUZA, 2016).

Além disso, com o grande aumento da quantidade de informações, também foram integrados os *gateways*, que funcionam como uma porta para o controle do tráfego de dados que chegam de outros locais da rede, bem como a tradução de protocolos, funcionando como um meio intermediário entre diferentes redes.

Somente após a metade da primeira década dos anos 2000, as subestações passaram a ser totalmente digitais. Nas subestações atuais modernas, os dispositivos digitais, como atuadores e sensores, foram incorporados também ao nível de processo — o mais baixo da subestação — onde estão os equipamentos de manobra e medição, como disjuntores, seccionadoras, TCs e TPs. Nesse nível, o cabeamento de cobre convencional foi substituído por redes de comunicação de dados, geralmente em fibra óptica (MENDES; JARDINI, 2009).

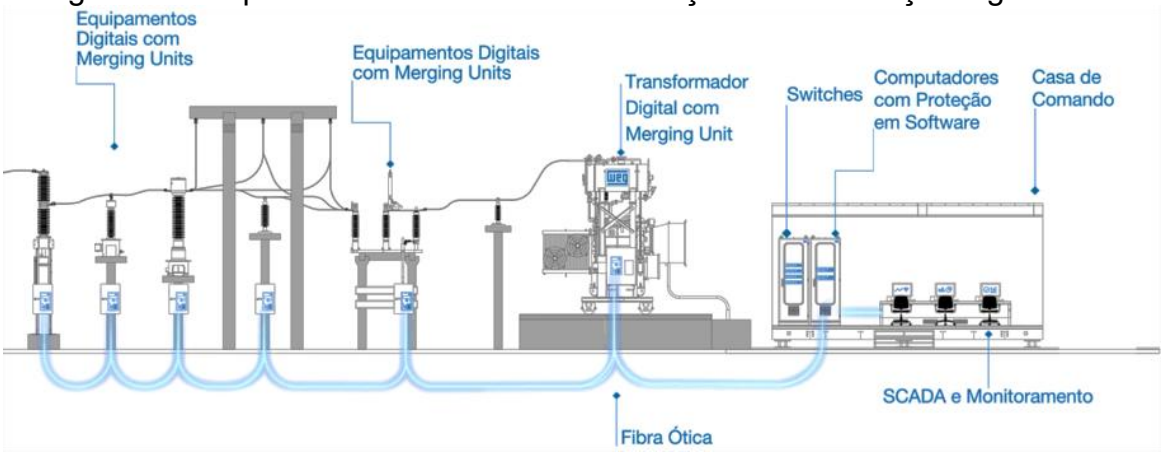
A Figura 5 apresenta uma comparação entre as subestações convencionais (*Yesterday*), as subestações digitais a partir da década 90 (*Today*) e as subestações 100% digitais depois dos anos 2000 (*Tomorrow*), reforçando como essa nova configuração do sistema elétrico fez com que a configuração se tornasse mais simples, reduzindo a quantidade de cabos de cobre usados para comunicação dos equipamentos em diferentes locais. Enquanto isso, a Figura 6 apresenta a vista frontal da subestação digitalizada com mais detalhes.

Figura 5 – Análise evolução do SAS



Fonte: SIEMENS (2010)

Figura 6 – Esquema do sistema de comunicação da subestação digitalizada



Fonte: WEG (s.d.)

Portanto, essa integração dos computadores com os IEDs nas subestações de automação possibilitaram a maior aquisição de dados, diminuição da ocorrência de erros, melhoria no diagnóstico do sistema e rápida atuação no caso de falhas, avanço no desempenho, testes, operação, manutenção, flexibilidade e maior confiabilidade devido à integração das funções de supervisão, controle, automação, proteção e monitoramento no sistema como um todo, não mais atuando de forma independente (MENDES; JARDINI, 2009).

Isso reforça a importância de um projeto bem elaborado de SPCS (Sistema de Proteção, Controle e Supervisão) para evitar danos permanentes aos equipamentos do sistema elétrico e, consequentemente, a necessidade de substituição, considerando que um transformador de alta tensão, por exemplo, pode custar milhares ou até milhões de reais, e sua troca pode levar vários meses até a entrega de um novo equipamento pelo fabricante, caso não haja peças sobressalentes disponíveis no local (METRUM, 2023).

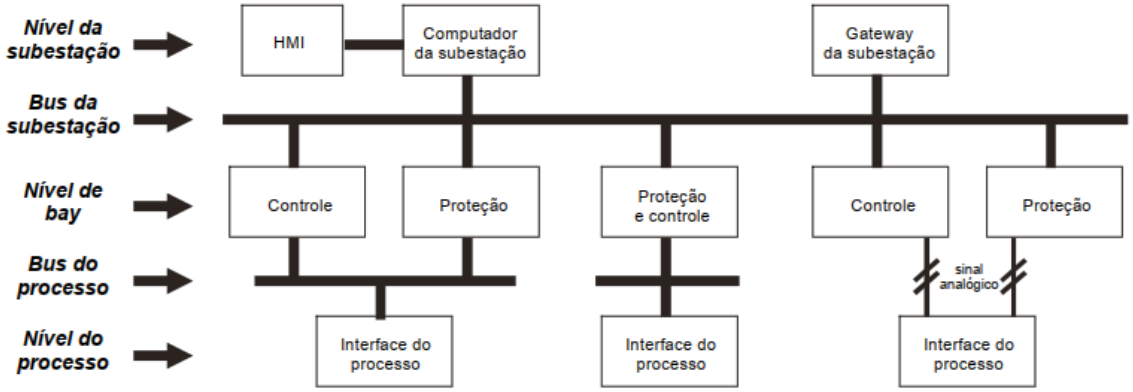
2.2.1 Arquitetura do Sistema de Automação de Subestações (SAS)

Um dos principais desafios na digitalização das subestações consiste em assegurar uma comunicação eficiente entre equipamentos localizados em diferentes pontos, garantindo a confiabilidade do sistema e a coordenação adequada das funções executadas por múltiplas aplicações em diversos dispositivos, de modo que a atuação ocorra de forma rápida e precisa diante de falhas. Dessa forma, antes de tudo, deve-se definir claramente a arquitetura da subestação elétrica, indicando como

serão disponibilizados cada equipamento em diferentes níveis, os quais são divididos entre os níveis da subestação, de *bay* e do processo, como mostra a Figura 7.

Além disso, a interligação entre os níveis é feita pelos barramentos “bus da subestação” e “bus de processo”, de forma digital, ou seja, se dá pela comunicação serial com o protocolo implementado ou convencional (sinais analógicos para disparo da bobina do disjuntor, e sinais analógicos dos valores de medição de corrente e tensão vindos dos TCs e TPs convencionais), permitindo a maior eficiência na troca de informações (IGARASHI, 2008).

Figura 7 – Arquitetura Comunicação Serial Dividida em Níveis na Subestação



Fonte: IGARASHI (2008)

- **Nível da Subestação:** Esse nível corresponde à sala de supervisão e controle remoto, onde computadores robustos do sistema SCADA realizam a supervisão e a aquisição de dados da subestação, coletando informações dos dispositivos de controle e proteção do nível *bay* e permitindo a interação dos operadores por meio das IHMs (Interface Homem-Máquina). Caso ocorra alguma anormalidade, os equipamentos do nível de subestação enviam comando para que os dispositivos nos níveis abaixo atuem para proteger ou eliminar a falha. Nesse nível ainda contam com o *gateway*, o qual atua como porta de entrada para controle do fluxo de recebimento dos dados.

- **Nível de *Bay*:** Nessa seção se concentram os relés de proteção, medidores de energia e oscilógrafos, onde fazem o monitoramento, controle e proteção dos equipamentos de pátio da subestação e enviam informações para a sala de supervisão e controle remoto. Caso haja alguma anormalidade, eles

respondem comandos da sala e atuam enviando sinais para que os equipamentos do nível de processo interrompam a energização no sistema, isolando assim o trecho com falha.

- **Nível de Processo:** Encontram-se os equipamentos de pátio como transformadores de medição (TPs e TCs, que podem ser convencionais ou com interface em fibra óptica) e disjuntores e chaves seccionadoras, responsáveis pela transmissão ou interrupção de energia elétrica caso ocorra uma falha no sistema. Ainda nesse nível de processo, estão localizadas as *Merging Units* (MUs), que digitalizam sinais de corrente e tensão (valores analógicos) antes de chegarem aos IEDs, detalhada no capítulo 3.

2.3 PROTOCOLOS DE COMUNICAÇÃO

No contexto deste trabalho, os protocolos de comunicação são responsáveis por estabelecer a forma como os equipamentos trocam informações no ambiente do *Hub*, definindo um conjunto de regras e procedimentos que regulam essa troca de dados entre os IEDs e outros dispositivos do sistema elétrico.

Atualmente há três modelos de protocolos de comunicação bastante usados nas aplicações industriais: Field Bus, Ethernet e Wireless.

No modelo Field Bus, as informações são transmitidas através de um barramento de comunicação compartilhado. Ele funciona como dois fios de cabos de cobre trançados, enviando assim informações bit a bit de forma linear. Devido a esse tipo de transmissão, possui uma característica mais lenta no envio de mensagens, porém isso permite a diminuição de ruídos, mais robustez e mais segura em relação aos ataques cibernéticos (EATON, 2025).

Alguns protocolos que usam essas conexões de par trançado do Field Bus são: Modbus RTU, Profibus e Can Bus.

O modelo Ethernet, por sua vez, em vez de transmitir bits de informação um por vez, como os quadros ou pacotes padronizados, pode conter até 12.000 bits cada. Isso é possível devido à sua característica que dentro de um cabo e do conhecido conector RJ45 há oito condutores de sinal, que tradicionalmente estão em quatro pares trançados, como mostrada na Figura 8.

Figura 8 – Cabo Ethernet com Conector RJ45

Fonte: EATON (2025)

Curiosamente, para velocidades abaixo de gigabit, apenas dois desses pares são realmente usados. Em aplicações mais modernas, cabos de fibra óptica podem ser usados no lugar dos pares trançados, oferecendo velocidades ainda maiores e imunidade a ruídos. Esse tipo de densidade de informações é adequado para criar redes nas quais muitos dispositivos podem se comunicar entre si, seja em uma rede local (LAN) ou em rede de longa distância (WAN). Dessa forma, possui velocidade com várias ordens de magnitude mais rápidas que o Field Bus, tornando-a favorável para comunicação de superlonga distância e, na aplicação de subestações, a coleta de medidores e qualidade de energia e CLP (EATON, 2025).

Os protocolos Ethernet mais comuns em sistemas de comunicação industrial são: Modbus TCP/IP (ou TCP, de forma abreviada), PROFINET e ETHERNET/IP.

É importante ressaltar que o Modbus RTU e Modbus TCP são parentes, trabalham exatamente com os mesmos princípios operacionais de protocolo. No entanto, com a transmissão ETHERNET, o TCP pode enviar significantemente mais dados de forma muito mais rápida.

O Modbus RTU é adequado para conexões de dispositivo para dispositivo, como um relé para cadeia de disjuntores. Já o modelo Modbus TCP é muito mais útil para extrair muitos dados de diversos dispositivos, tornando-se mais adequado para conectar dispositivos de nível superior com CLP, medidores ou em outros CLPs. Ademais, o TCP é conhecido como protocolo *half duplex*, ou seja, todos os dispositivos conectados podem tanto transmitir quanto receber. Contudo, é importante salientar que eles não conseguem fazer as duas coisas ao mesmo tempo.

O Profinet é uma conectividade mais aprimorada da ETHERNET, e é *full-duplex*, ou seja, todos os dispositivos conectados podem transmitir e receber simultaneamente. Portanto, isso ajuda na melhoria significativa da velocidade e precisão do sistema, tornando possível gerenciar topologias de redes complexas com vários controladores interligados entre si.

O Ethernet/IP possui aplicação e desempenho bastante semelhantes ao Profinet, porém o seu uso é mais comum na América do Norte e se destaca na flexibilidade e acessibilidade, tendo muitos componentes disponíveis no mercado.

Por último, os protocolos Wireless estão associados às comunicações sem fio, reservadas para o monitoramento remoto e limitadas a aplicações de baixa potência e menos críticas.

2.4 MODELO OSI

O Modelo de Referência OSI (ISO/IEC 7498-1) surgiu na década de 80 para padronizar a comunicação entre os sistemas abertos. Esse modelo conceitual é dividido em 7 camadas, o que auxilia o entendimento da comunicação entre os sistemas, onde cada camada possui uma função específica.

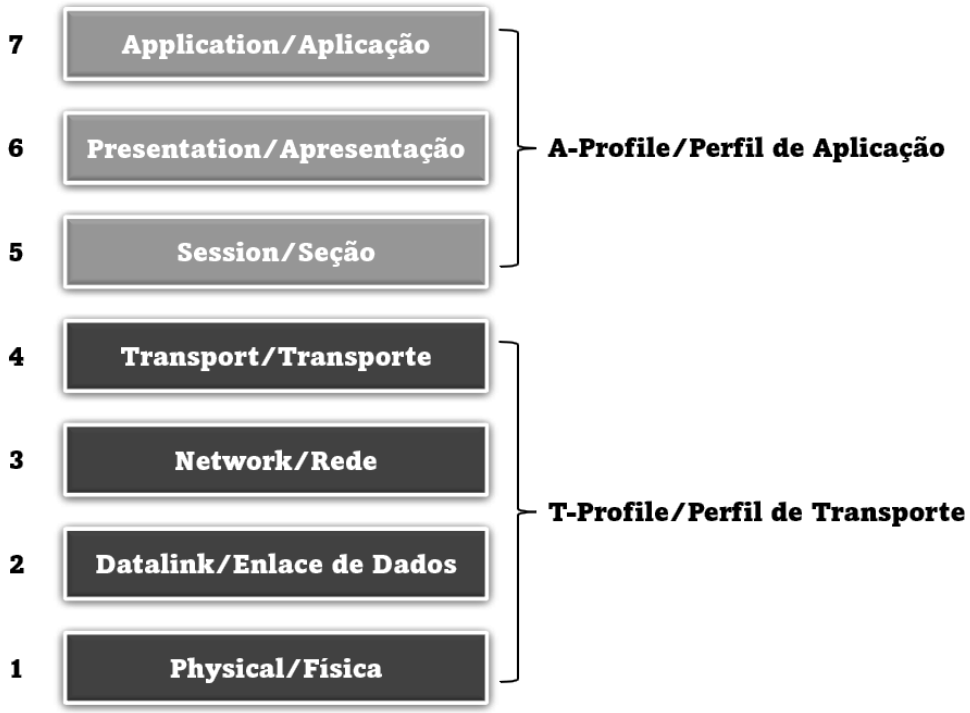
Durante a transmissão, cada camada recebe os dados da camada superior, adiciona informações de controle e os encaminha para a camada inferior (nesse processo, ele inicia na camada de aplicação para a camada física). No processo de recepção, cada camada obtém os dados da camada inferior, remove as informações de controle e os repassa para a camada superior, onde começa na camada física e termina na camada de aplicação.

A Figura 9 descreve como um pacote de dados, que passa por encapsulamento, viaja de uma camada para outra, onde a mensagem sai do meio físico e chega do outro lado, onde ocorre o desempacotamento da mensagem. As três camadas mais acima representam o perfil de aplicação, enquanto o restante das camadas mais abaixo representa o perfil de transporte.

1) **Camada Física:** Lida com os equipamentos e meios de transmissão, garantindo que os bits consigam trafegar pelo meio físico que está conectado dois equipamentos. Os bits são convertidos em sinais elétricos ou ópticos, que são enviados por conexão guiada ou não guiada.

2) **Camada de Enlace de Dados:** Lida com a transmissão dos quadros de dados (*frames*) da rede. Para isso, faz-se o endereçamento físico, que, por sua vez, é definido pelo MAC (*Media Access Control*), garantindo assim a correta ordem de entrega dos dados (nó a nó) para que a mensagem seja entregue de forma confiável. Dessa forma, evita-se que receptores lentos não sejam atropelados por transmissores rápidos, tendo como controle de fluxo baseado em *feedback*. Tem-se como exemplo de dispositivos que operam nessa camada os *bridges* e *switches*.

Figura 9 – Modelo de Referência OSI e os perfis de Aplicação e Transporte



Fonte: Produção do próprio autor

3) **Camada de Rede:** Faz o endereçamento lógico e estabelecimento de dados. Responsável pelo roteamento de dados, determinando o melhor caminho para que os dados viajem de um ponto para o outro.

4) **Camada de Transporte:** Faz o controle do fluxo e integridade da informação e segmentação de dados, verificando o tráfego de informações que estão indo e vindo.

5) **Camada de Seção:** É responsável por estabelecer, gerenciar e encerrar sessões de interação entre dois dispositivos no sistema.

6) **Camada de Apresentação:** Faz a conversão dos dados recebidos em um formato que possa ser lido pela camada de aplicação (tradução). A codificação e decodificação dos dados feita nessa camada depende do protocolo da camada de aplicação que está enviando ou recebendo dados. Essa camada também cuida da criptografia e descriptografia, usadas para proteger os dados.

7) **Camada de Aplicação:** Envia dados quando uma comunicação estiver ocorrendo de um ponto para o outro, é onde vai receber dados quando uma comunicação estiver recebendo informação. Essa camada faz interface com as aplicações da máquina. Alguns exemplos são http (web), https (web com criptografia), FTP (transferência de arquivos) e SMTP (e-mail).

2.5 MODELO TCP/IP

O modelo TCP/IP, utilizado na Ethernet, surgiu na década de 1970 a partir de pesquisas do Departamento de Defesa dos Estados Unidos. Desenvolvido por Vinton Cerf e Robert Kahn, esse conjunto de protocolos tinha como objetivo criar uma rede de comunicação ampla, descentralizada e resiliente a falhas e ataques. A ARPANET, rede criada para interligar centros de pesquisa e instalações militares, foi a primeira a implementar o protocolo TCP/IP. Graças à sua flexibilidade e capacidade de integrar diferentes redes, o modelo tornou-se o padrão para a comunicação na Internet (TECNOBLOG, 2024).

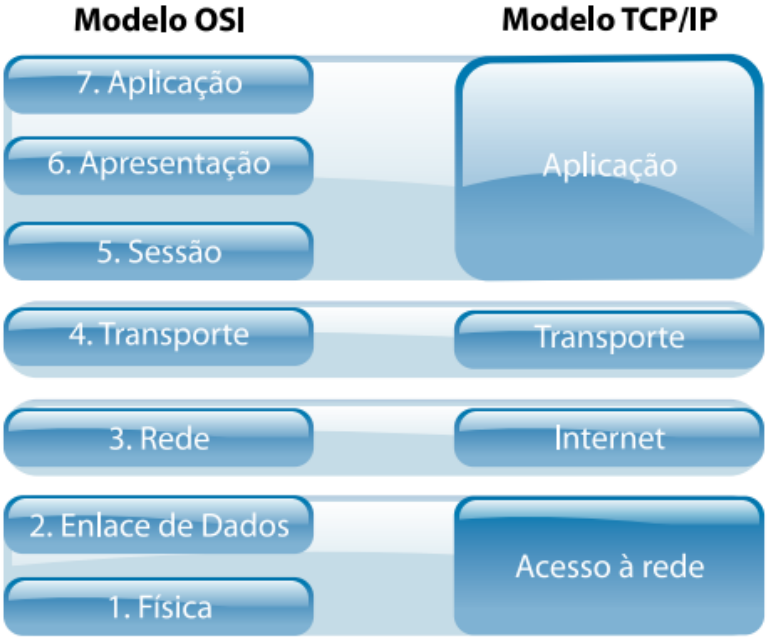
O sistema TCP/IP é semelhante ao modelo OSI. Enquanto o OSI é um modelo teórico pré-estabelecido, o TCP/IP é o modelo prático de como são transferidas as informações entre as camadas, tendo uma diferença que sua arquitetura é organizada por 4 camadas em vez de 7, como mostra a Figura 10.

Na camada de aplicação, residem os protocolos que possibilitam a comunicação entre as aplicações dos usuários, onde os mais conhecidos são: http (ou https, este fornece criptografia dos dados) para serviços Web, FTP para transferência de arquivos e SMTP para e-mails (MAIA, 2013).

Na camada de transporte temos os dois tipos: TCP (*Transmission Control Prototocol*) e UDP (*User Datagram Protocol*); o primeiro garante a entrega confiável e ordenada dos dados, estabelecendo conexões entre os dispositivos e retransmitindo pacotes perdidos, enquanto o segundo é usado para envio de dados com ampla velocidade sem verificação de entrega ou retransmissão de pacotes perdidos.

Na camada de internet (ou rede) se encontra o IP (*Internet Protocol*), responsável por endereçar os pacotes e encaminhá-los pela rede, determinando a melhor rota para cada destino.

Figura 10 – Camadas do modelo TCP/IP



Fonte: Cisco Networking Academy (2011) *apud* SENAI (2012)

Por fim, a camada de acesso à rede (ou enlace) faz o enquadramento, detecção e tratamento de erros, controle de fluxo e de acesso ao meio físico, usando os protocolos como Ethernet e Wi-Fi (MAIA, 2013; TECNOBLOG, 2024).

Resumindo, o Protocolo de Controle de Transmissão (TCP) é responsável por garantir que os dados cheguem ao destino de forma correta e completa, enquanto o Protocolo de Internet (IP) tem a função de endereçar os dispositivos na rede para a entrega dos dados.

3 NORMA IEC 61850

Nas últimas décadas, o aumento do consumo de energia elétrica e a necessidade de expansão contínua das subestações trouxeram à tona a demanda por aprimoramento dos sistemas de potência. Nesse contexto, destacou-se a importância do monitoramento em tempo real, essencial para identificar rapidamente falhas no sistema e garantir ações eficazes de controle e proteção.

Como resposta a essa necessidade, surgiram os IEDs (*Intelligent Electronic Devices*, baseados em tecnologia de microprocessadores, capazes de executar múltiplas funções de monitoramento, controle e proteção. Entretanto, a diversidade de protocolos de comunicação utilizados pelos diferentes fabricantes dificultava a interoperabilidade entre os IEDs. Essa limitação obrigava os clientes a adquirirem equipamentos de um único fabricante ou realizar reconfigurações físicas complexas na infraestrutura da subestação, implicando custos elevados, maior tempo de implementação e desafios adicionais para a expansão do sistema elétrico.

Foi então, em 2003, que surgiu oficialmente a norma IEC 61850, estabelecendo um modelo de referência para comunicação padronizada entre dispositivos inteligentes, com o objetivo de garantir interoperabilidade e promover avanços na automação de subestações elétricas.

Para alcançar esse objetivo, a norma IEC 61850 define um modelo de comunicação baseado em conceitos abstratos, chamado ACSI (*Abstract Communication Service Interface*). Esse modelo permite mapear objetos e serviços para diferentes protocolos que atendam às necessidades de dados e funções, sem obrigar o uso de um protocolo específico em cada camada.

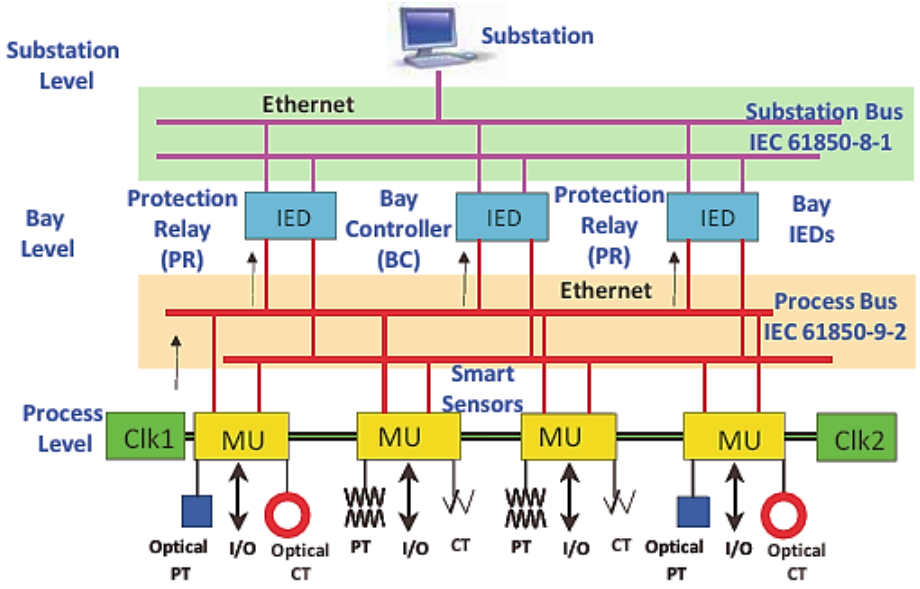
Além disso, a interoperatividade ocorre por meio da definição padronizada de nomes de objetos, conforme estabelecido pela IEC 61850, apresentados dentro do contexto do sistema elétrico. Essa padronização permite que os engenheiros interpretem rapidamente o significado dos dados, sem a necessidade de mapear números de registradores para grandezas como tensão ou corrente. Dessa forma, os nomes dos dados nos IEDs não são atribuídos pelo fabricante nem configurados pelo usuário, mas seguem um modelo normativo.

A norma também estabelece diretrizes que impactam diretamente o projeto e a construção futura de sistemas elétricos. Isso se deve ao fato de a IEC 61850 adotar uma representação clara e padronizada de todos os dispositivos, suas respectivas

funções e a configuração da subestação como um todo, utilizando uma linguagem padronizada chamada SCL, baseada em XML (MACKIEWICZ, 2006).

Em adicional, a norma garante maior segurança e rápida atuação em falhas, pois permite definir prioridades no envio das mensagens, controlando o fluxo de dados e possibilitando a troca de informações críticas entre os IEDs de forma ágil por meio dos serviços GOOSE, utilizados para mudança de eventos como abertura de disjuntores, trabalhando em conjunto com os SVs, destinados à transmissão de valores medidos nos equipamentos no barramento de processo, conforme as normas IEC 61850-8-1 e IEC 61850-9-2, respectivamente. Por fim, não menos importante na norma, destaca-se o serviço MMS (*Manufacturing Message Specification*), responsável pela comunicação entre equipamentos do nível *bay* e da subestação, como IEDs e sistemas SCADA, permitindo supervisão e controle remotos, monitoramento em tempo real e transferência de arquivos. A Figura 11 mostra o esquema de um Sistema de Automação de Subestações usando a norma IEC 61850.

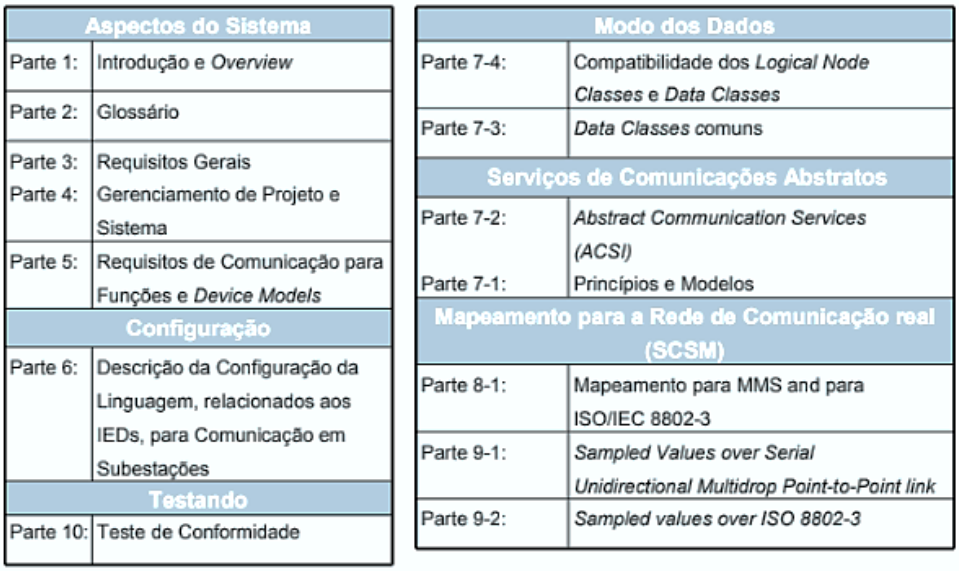
Figura 11 – Esquema de um SAS baseado no IEC 61850



Fonte: SONG; LEE; FITZPATRICK; ZHANG (2017)

Atualmente a norma IEC 61850 é dividida em 14 partes, onde são subdivididas por documentos que apresentam os aspectos do sistema, configuração, modelo de dados, serviços de comunicações abstratos, mapeamento para a rede de comunicação real (SCSM) e, por fim, os testes de conformidade, assim como é mostrada na Figura 12.

Figura 12 – Estrutura da IEC 61850



Aspectos do Sistema	
Parte 1:	Introdução e *Overview*
Parte 2:	Glossário
Parte 3:	Requisitos Gerais
Parte 4:	Gerenciamento de Projeto e Sistema
Parte 5:	Requisitos de Comunicação para Funções e *Device Models*
Configuração	
Parte 6:	Descrição da Configuração da Linguagem, relacionados aos IEDs, para Comunicação em Subestações
Testando	
Parte 10:	Teste de Conformidade

Modo dos Dados	
Parte 7-4:	Compatibilidade dos *Logical Node Classes* e *Data Classes*
Parte 7-3:	*Data Classes* comuns
Serviços de Comunicações Abstratos	
Parte 7-2:	*Abstract Communication Services (ACSI)*
Parte 7-1:	Princípios e Modelos
Mapeamento para a Rede de Comunicação real (SCSM)	
Parte 8-1:	Mapeamento para MMS and para ISO/IEC 8802-3
Parte 9-1:	*Sampled Values over Serial Unidirectional Multidrop Point-to-Point link*
Parte 9-2:	*Sampled values over ISO 8802-3*

Fonte: SIEMENS (2010)

3.1 LINGUAGEM DE PROGRAMAÇÃO PARA A NORMA IEC 61850

Para que os IEDs consigam se comunicar entre si no sistema de proteção, controle e supervisão de subestações, foi definida na IEC 61850-6 uma linguagem padrão de configuração dos equipamentos chamada SCL (*Substation Configuration Language*) baseada em XML (*Extensible Markup Language*).

Com essa linguagem, torna-se possível descrever as funções e características de um IED de forma legível por máquinas e importá-las de forma válida para as ferramentas de engenharia. Ademais, a SCL permite a descrição da configuração dos equipamentos na subestação de acordo com o seu diagrama unifilar, assim como as funções atribuídas aos IEDs e como eles se comunicam entre si.

De acordo com a norma IEC 61850-6, essa linguagem utiliza quatro arquivos para realizar a descrição formal dos modelos: *System Specification Description* (SSD), *System Configuration Description* (SCD), *IED Capability Description* (ICD) e *Configurated IED Description* (CID).

- SSD: É o arquivo que descreve o sistema completo da subestação, bem como seu diagrama unifilar e suas funcionalidades. Além disso, também engloba o SCD e ICD.

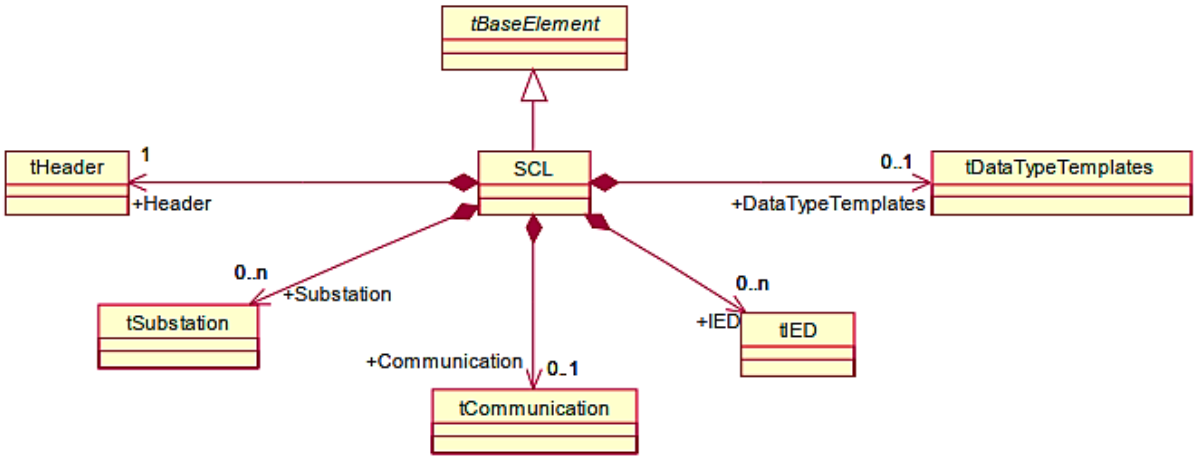
- SCD: Inclui informações de todos os IEDs presentes, uma seção de configuração da comunicação e uma seção de descrição da subestação. Quando um novo projeto é criado, o arquivo SCD é gerado e importado para o configurador IEC 61850 (SOUZA, 2021).

- ICD: Detalha as capacidades específicas de um IED, o que inclui informações sobre o modelo e suporte a serviços.

- CID: É a configuração aplicada ao IED real, que carrega informações do seu endereço de comunicação na rede, nomes e funções, garantindo que esse dispositivo opere conforme o projeto definido no SCD.

Enquanto o XML é uma metalinguagem utilizada para definir gramáticas e estruturar dados de forma hierárquica e semântica, a linguagem SCL incorpora também conceitos da UML (*Unified Modeling Language*), que é uma linguagem visual de modelagem orientada a objetos. Essa combinação permite criar uma representação lógica da subestação e de seus dispositivos antes da implementação. Na Figura 13 são mostrados os principais componentes necessários para a modelagem da subestação e seus respectivos equipamentos presentes usando o diagrama UML.

Figura 13 – Visualização do diagrama UML no esquema SCL



Fonte: IEC 61850-6 (2004)

O bloco SCL é o elemento central do modelo. Ele representa o arquivo XML no qual descreve toda a configuração da subestação, incluindo os dispositivos, comunicação e modelo de dados.

O tBaseElement representa uma classe genérica que serve como base todos os outros elementos do modelo SCL, garantindo a interoperabilidade, validação da XML e permite adicionar atributos sem quebrar a estrutura principal.

O bloco tHeader é o cabeçalho que contém informações gerais do arquivo, como a versão, data, nome dos projetos etc. Isso permite rastreabilidade e escolha da convenção de nomes para comunicação, principalmente na conexão de IEDs de diferentes fabricantes.

O bloco tSubstation representa a modelagem funcional da subestação, que inclui níveis de tensão (VoltageLevel), *bays* e seus equipamentos primários (disjuntores, transformadores, seccionadoras), conexões topológicas (ConnectivityNode) e Associação dos LogicalNodes (LNode) aos equipamentos. Ademais, pode haver mais de uma subestação dentro do arquivo SCL, principalmente em projetos com múltiplas subestações.

O bloco tIED descreve cada dispositivo eletrônico inteligente presente na subestação, o que inclui os pontos de acesso à rede (*AccessPoint*), *Logical Devices* (LDevice) e *Logical Nodes* (LN), assim como os serviços suportados, como GOOSE, SV e relatórios.

O bloco tCommunication define a configuração da rede da comunicação, como sub-redes (*station bus* e *process bus*), endereços e protocolos utilizados, atributos para roteadores e sincronização de tempo. Portanto, ele detalha como os IEDs se conectam e trocam dados.

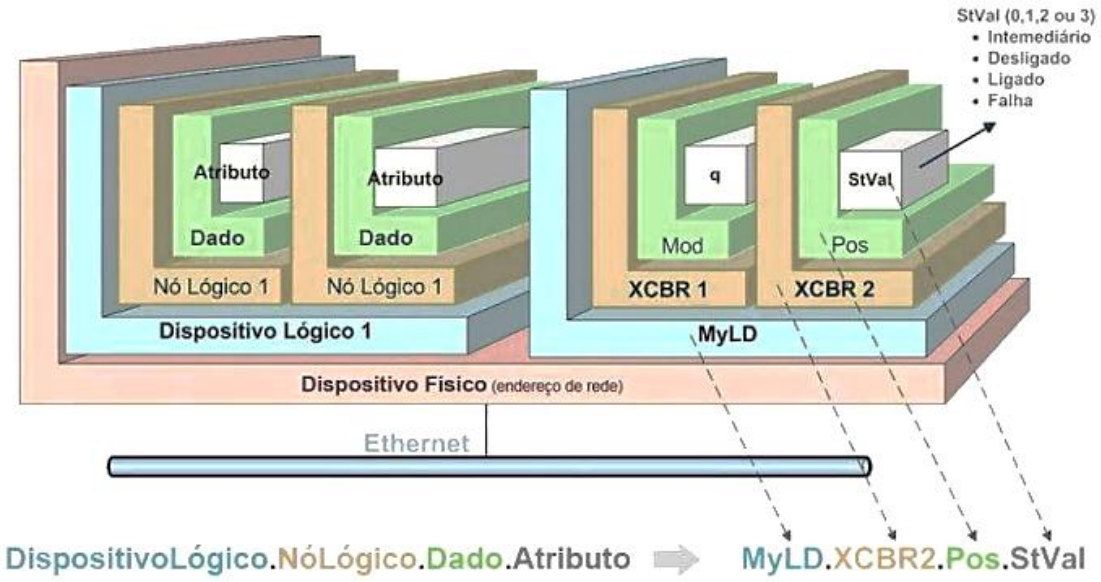
O bloco tDataTypeTemplate faz a definição dos tipos de dados usados pelos *Logical Nodes* e *Data Objects*, logo ele descreve o LNodeType, DOType e DAType, garantindo assim a consistência e reutilização dos modelos de dados.

3.2 MODELO DE DADOS

A norma IEC 61850 utiliza um modelo de dados orientado a objetos para a representação dos dispositivos IEDs e suas respectivas funcionalidades, onde a sua estrutura hierárquica de dados é dividida em: dispositivo físico (*physical device*),

dispositivo lógico (*logical device*), nós lógicos (*logical nodes*), objeto de dados (*data object*) e atributos de dados (*data attributes*), conforme a Figura 14.

Figura 14 – Estrutura Hierárquica dos Dados



Fonte: SEL (2023) *apud* REIS (2023)

Physical Device:

O *Physical Device* representa o próprio dispositivo físico real na subestação, normalmente um IED. Dentro dele existem um ou mais *Logical Devices*, que agrupam funções lógicas (como proteção, medição ou controle). Um dispositivo físico pode alojar mais de um dispositivo lógico, pois nele pode coletar dados de mais de um equipamento.

Logical Device (LD):

O *Logical Device* (LD), ou dispositivo lógico, é um agrupamento lógico dentro do IED que organiza funções relacionadas. Dentro dele existem *Logical Nodes* (LN), que representam funções específicas, como proteção, medição ou controle.

Logical Node (LN):

O nó lógico (*Logical Node*) é definido como um mecanismo que permite modelar a subestação em um formato padrão. Quando é feita essa padronização, permite-se alcançar a interoperabilidade entre os dispositivos e também nos permite alcançar essa natureza descritiva da IEC 61850, onde pode-se descrever como a subestação é construída a partir do IED. Existem funções que são definidas como nós lógicos. O

nó lógico é a menor unidade funcional em que ocorre a troca de dados e está alojado dentro de um dispositivo físico e um dispositivo lógico. Eles são representados pelas iniciais das letras conforme o Quadro 2.

Quadro 2 – Grupos de Nós Lógicos

Inicial	Grupo	Número de nós lógicos
L	Nós lógicos no sistema	3
P	Proteção	28
R	Nós lógicos relacionados à proteção	10
C	Controle	5
G	Genéricos	3
I	Interfaceamento e arquivamento	4
A	Controle automático	4
M	Medição	8
S	Sensoreamento e monitoração	8
X	Chaveamento	2
T	Transformadores de instrumentação	2
Y	Transformadores de potência	4
Z	Equipamentos adicionais do sistema de potência	15
	Número total de nós lógicos	92

Fonte: KIRRMANN (2004) *apud* SOUZA (2023)

Todos esses 92 nós lógicos são representados por um acrônimo de quatro letras, dentre os mais comuns tem-se:

- XCBR: Disjuntor
- PDIF: Proteção Diferencial
- YPTR: Transformador de Potência

Data Objects (DO)

Eles descrevem estados ou parâmetros (por exemplo: posição do disjuntor, “POS”), e esses objetos são detalhados por *Data Attributes*, que indicam valores, qualidade e tempo. Essa estrutura padronizada permite que qualquer sistema IEC 61850 entenda e troque informações sobre o status e comandos dos equipamentos da subestação.

Data Attributes (DA)

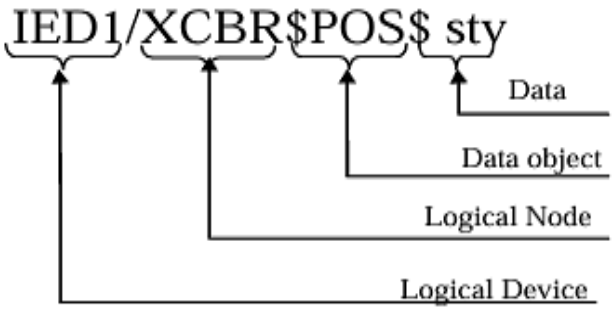
O Atributo de Dados (*Data Attribute*) é um detalhe dentro do *Data Object* que mostra informações específicas sobre aquele ponto. Os mais usados são:

- stVal: valor do status (ex.: TRUE = disjuntor fechado);
- q: qualidade do ponto (ex.: GOOD, BAD);
- t: *timestamp*, que indica o momento em que o valor foi atualizado. Esses atributos ajudam a entender não só o valor, mas também se ele é confiável e quando foi medido.

Com essa padronização na estrutura dos dados, outros dispositivos podem saber interpretar isso e compreender que essa é a posição do disjuntor.

Além disso, os objetos devem ser descritos seguindo a ordem *Logical Device*, *Logical Node*, *Data Objet* e *Data Attribute*, separados com "/" entre o *Logical Device* e o *Logical Node*, e "$" entre o *Data Object* e o *Data Attribute*, conforme indicado na figura 15.

Figura 15 – Estrutura Nomeação dos Objetos na IEC 61850



Fonte: FERNANDES; BORKAR; GOHIL (2014)

Portanto, o conceito de nós lógicos (LN) é a espinha dorsal do IEC 61850. Seguir essa hierarquia é fundamental para padronizar nomes e estruturas, permitindo que diferentes fornecedores implementem funções de forma consistente. Essa padronização garante interoperabilidade entre dispositivos e ferramentas, além de simplificar a identificação e configuração pelos engenheiros.

3.3 TIPOS DE MENSAGENS NA COMUNICAÇÃO DE SUBESTAÇÕES

Na comunicação das subestações, a velocidade de recebimento de mensagens e sua classe de performance são definidas pela classificação do tipo de mensagens de acordo com o nível de prioridade, informadas no Quadro 3.

Quadro 3 – Classificação tipos de mensagens

Tipo	Classe	Serviços
1	Mensagens Rápidas	GOOSE-GSEE
1A	Trip	GOOSE-GSEE
2	Mensagens de velocidade média	CLIENTE/SERVIDOR (MMS)
3	Mensagens de velocidade baixa	CIENTE/SERVIDOR (MMS)
4	Mensagens de dados brutos	SAMPLED VALUES
5	Funções de transferência de arquivos	CLIENTE/SERVIDOR (MMS)
6	Mensagens de sincronização do tempo	SYNC TIME

Fonte: IEC 61850-8-1 (Adaptada pelo autor)

Na Figura 16 é apresentado com mais detalhes o tempo de transmissão de cada tipo de mensagem.

As mensagens do Tipo 1 e Tipo 1A são mapeadas para *Ethertypes* distintos para otimizar a decodificação das mensagens recebidas. Possuem velocidade alta para realizar *trips* a partir das mensagens GOOSE para proteger contra a falha o mais rápido possível, como comando para abertura de disjuntor em um curto-circuito.

Mensagens dos Tipos 2, 3 e 5 requerem serviços orientados a mensagens (MMS), onde não possuem muita urgência na atuação, como a transferência de arquivos.

Mensagens do tipo 4 se tratam valores amostrais (SVs) de medidas analógicas, como tensão e corrente, com velocidade de transmissão mínima de até 3ms. Assim como as mensagens do tipo 1A e 1B, são mensagens rápidas por estar relacionadas à proteção do sistema em caso de falhas (MACHADO, 2023).

Mensagens do Tipo 6 são as mensagens de sincronização do tempo (TimeSync), as quais têm a função de garantir que todos os dispositivos da subestação, como IEDs e *Merging Units*, estejam sincronizados em hora e data para garantir a coerência dos dados recebidos dos dispositivos. Geralmente, todos esses dispositivos possuem um relógio interno para garantir que o horário dos equipamentos esteja sincronizado, evitando assim disparos incorretos, por exemplo. Essa sincronização é feita através do receptor *Global Positioning System* (GPS) conectado à rede Ethernet em conjunto com o protocolo *Simple Network Time Protocol* (SNTP).

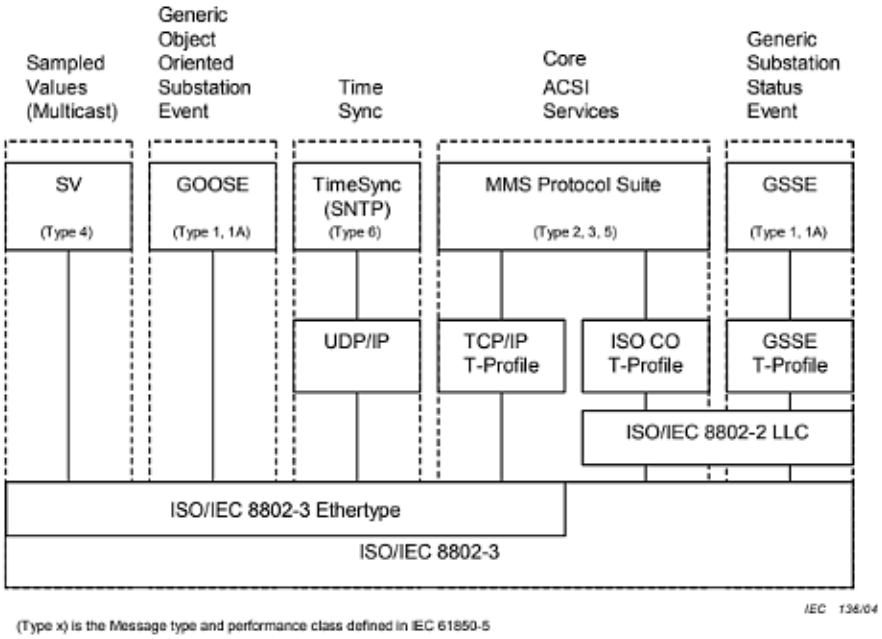
Figura 16 – Tempo de transmissão de acordo com a aplicação das mensagens

Type	Applications	Performance Class	Requirements (Transmission Time)
1A	Fast Messages (Trip)	P1	10 ms
		P2/P3	3 ms
1B	Fast Messages (Other)	P1	100 ms
		P2/P3	20 ms
2	Medium Speed		100 ms
3	Low Speed		500 ms
4	Raw Data	P1	10 ms
		P2/P3	3 ms
5	File Transfer		≥1000 ms
6	Time Synchronization		(Accuracy)

Fonte: HOU D (2010) *apud* SOUZA (2021)

A Figura 17 permite visualizar de forma resumida a classificação de mensagens na transmissão de acordo com a IEC 61850-8-1.

Figura 17 – Classificação dos tipos de mensagens



Fonte: IEC 61850-8-1 (2004)

3.4 SERVIÇOS DE COMUNICAÇÃO IEC 61850

Após compreender a classificação dos tipos de mensagens, neste capítulo serão apresentados com mais detalhes os principais serviços de comunicação (GOOSE, SVs e MMS) definidos pela norma IEC 61850, destacando como ocorre a troca de informações entre diferentes dispositivos e o fluxo de mensagens entre diferentes níveis da subestação.

3.4.1 Cliente/Servidor e MMS

A comunicação no modelo Cliente/Servidor consiste em uma interação onde um programa (cliente) envia solicitações a outro programa (servidor), que processa essas requisições e retorna as respostas. No contexto deste trabalho, o cliente é geralmente um sistema supervisório (SCADA), responsável por solicitar dados ou enviar comandos, enquanto o servidor é o IED, que fornece informações ou executa ações.

Essa arquitetura é amplamente usada para supervisão remota de subestações, controle de equipamentos de campo, monitoramento de variáveis em tempo real, troca de dados com sistemas de engenharia e bancos de dados históricos e integração com sistemas de gestão de energia (CONPROVE, 2025).

Esse modelo utiliza o protocolo MMS (*Manufacturing Message Specification*), definido pela norma IEC 61850-8-1, garantindo interoperabilidade, confiabilidade e

segurança na troca de informações. O tráfego MMS permite que clientes, como SCADA, servidores OPC ou gateways, acessem verticalmente todos os objetos dos IEDs. Essa comunicação ocorre tanto pelo *station bus* quanto pelo *process bus*, embora alguns IEDs do *process bus* não suportem MMS.

Por operar na camada de rede (camada 3 do modelo OSI), o MMS utiliza endereços IP e pode atravessar roteadores. Em um modo de operação, o cliente MMS envia uma solicitação para um dado específico ao servidor MMS do IED, identificado pelo seu endereço IP, e recebe a resposta correspondente. Em outro modo, o cliente pode configurar o servidor para enviar notificações espontâneas quando ocorrerem eventos.

Normalmente, os dados não são perdidos por passar por todas as camadas do modelo TCP/IP, diferente dos dados da GOOSE e SV, desde que telegramas com erros possam ser reenviados novamente, como mostrado na Figura 18.

Figura 18 – Pilha de Comunicação e Mapeamento na IEC 61850

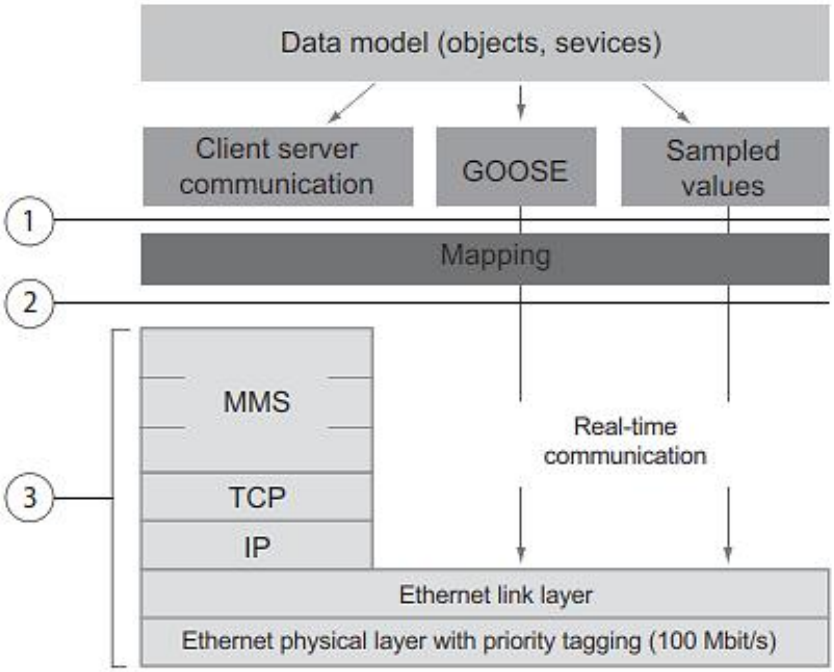


Figure 3: Communication stacks and mapping used in IEC 61850

1 Abstract communication services interface (ACSI)
2 Stack interface
3 ISO/OSI stack

Fonte: ABB (2023)

É de suma importância esclarecer que, apesar de ser um mecanismo cômodo, o tempo gasto não é adequado para comunicações de tempo crítico, logo o modelo Cliente/Servidor só é usado em serviços que não exigem tanta urgência.

A norma IEC 61850 ainda define um método de comunicação eficiente chamado "*reporting*". Em vez de o servidor enviar constantemente novos dados ao cliente, ele é configurado para transmitir os dados apenas quando ocorrerem alterações relevantes, como uma mudança no valor da medida ou na qualidade do sinal. Os *reports* são transmitidos pelo objeto *control block*, que é acionado logo após uma ocorrência de *trigger*, e podem ser do tipo *buffered* ou *unbuffered* (SOUZA, 2021).

O *buffered report* corresponde à memória de armazenamento dos eventos ocorridos durante a perda de comunicação com o sistema supervisório. Assim, quando a conexão é restabelecida, o relé envia automaticamente todos esses eventos ao supervisório. Já o *unbuffered report* corresponde a uma memória volátil, ou seja, caso ocorra perda de comunicação entre o relé e o sistema supervisório, os eventos gerados durante esse período não serão armazenados pelo relé. Assim, se houver atuação de pontos enquanto a supervisão estiver indisponível, o supervisório não terá registro dessas ocorrências.

3.4.2 GOOSE

As mensagens GOOSE são utilizadas para comunicação rápida entre IEDs, transmitindo principalmente sinais binários simples ou duplos para funções de proteção e controle, podendo incluir valores analógicos em alguns casos.

Essas mensagens fazem parte do grupo GSE (*Generic Substation Events*), que engloba serviços destinados à troca de eventos, sinais de controle e, eventualmente, sinais analógicos entre os IEDs. Dentro desse grupo, as mensagens GOOSE se destacam por sua flexibilidade e estrutura orientada a objetos, diferindo das mensagens GSSE (*Generic Substation Status Event*), que são mais antigas, possuem estrutura fixa e transmitem apenas sinais digitais, sem permitir a configuração de conjuntos de dados (*data sets*), o que limita a sua adaptabilidade (Adaptado de HOU D, 2010 *apud* SOUZA, 2021).

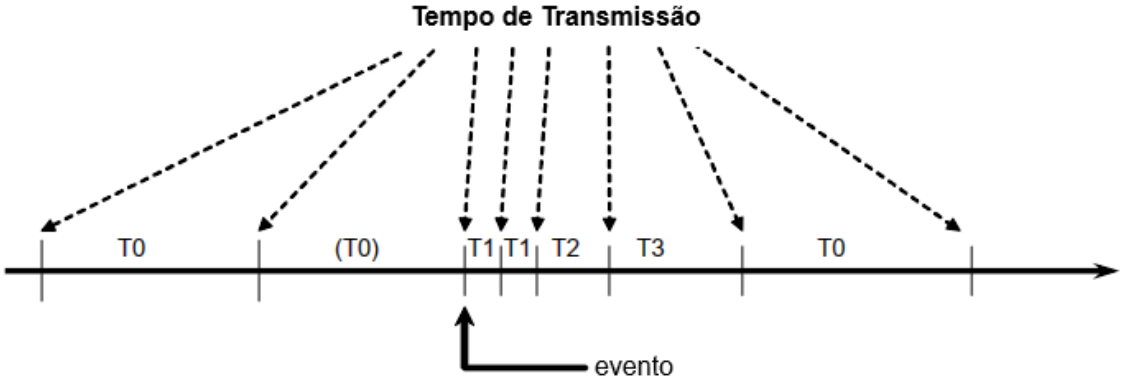
Definidas pela norma IEC 61850-8-1, essas mensagens são trocadas de forma “horizontal”, ou seja, entre os IEDs no barramento da subestação, sendo aplicadas especialmente para sinais de status, disparo (*trip*) e intertravamentos, onde são eventos mais críticos que necessitam de atuação rápida para proteger a subestação.

As mensagens GOOSE realizam comunicação direta entre IEDs no formato *peer-to-peer*, dispensando a necessidade de um servidor central ou controlador mestre. Nesse mecanismo, um IED atua como publicador, enviando mensagens via *multicast* Ethernet, enquanto os demais dispositivos assinantes monitoram e respondem às informações relevantes. Cada IED deve ser capaz de lidar com perda de pacotes, atrasos, entrega fora de ordem e falhas de conectividade, o que exige uma lógica robusta para contornar essas situações.

A IEC 61850-8-1 também especifica um esquema de retransmissão para atingir um nível confiável de entrega de mensagens, conforme mostrado na Figura 19.

Quando ocorre alguma anormalidade nas variáveis definidas, como religamento de um disjuntor, a informação de evento é transmitida e repetida no menor tempo (T1). O tempo de retransmissão aumenta gradualmente de T2 para T3 e eventualmente se estabiliza em um tempo de retransmissão estável T0. Esse tempo de retransmissão estável é reduzido quando o próximo novo evento acontece.

Figura 19 – Esquema de retransmissão de mensagens GOOSE



T0	retransmissão em condições estáveis (nenhum evento por muito tempo).
(T0)	retransmissão em condições estáveis pode ser encurtada por um evento.
T1	menor tempo de retransmissão após o evento.
T2, T3	tempos de retransmissão até atingir o tempo de condições estáveis.

Fonte: Adaptada da IEC 61850-8-1 (2004)

Enquanto em um mecanismo tradicional pode levar entre 8 e 20 ms para iniciar a abertura de um equipamento, no GOOSE leva menos de 3 ms, tornando-o mais seguro e rápido na atuação de falhas. Se o dispositivo não receber a mensagem após uma mudança de evento, pode indicar falha de monitoramento, como equipamento está offline ou com fios cortados ou desconectados (SMITH, 2020).

3.4.3 Sampled Values (SV)

As mensagens de valores amostrados (*Sampled Values*) transmitem valores analógicos das unidades de medição (transformadores de instrumento) para os IEDs, e suas características de funcionamento estão especificadas nas normas IEC 61850-9-1 e IEC 61850-9-2.

O tráfego de mensagens SVs normalmente percorre o barramento de processo, mas também pode passar pelo barramento da estação, por exemplo, em aplicações como proteção de barramento ou medição fasorial.

Assim como a GOOSE, as mensagens SVs não passam pelas camadas de transporte e rede do TCP/IP, ou seja, dispensam o processo de confirmação de recebimento da mensagem, fazendo com que a velocidade de transmissão seja extremamente rápida. Além disso, essas mensagens têm o modo de transmissão via Ethernet M*ulticast* através do mecanismo *publisher*/*subscriber*.

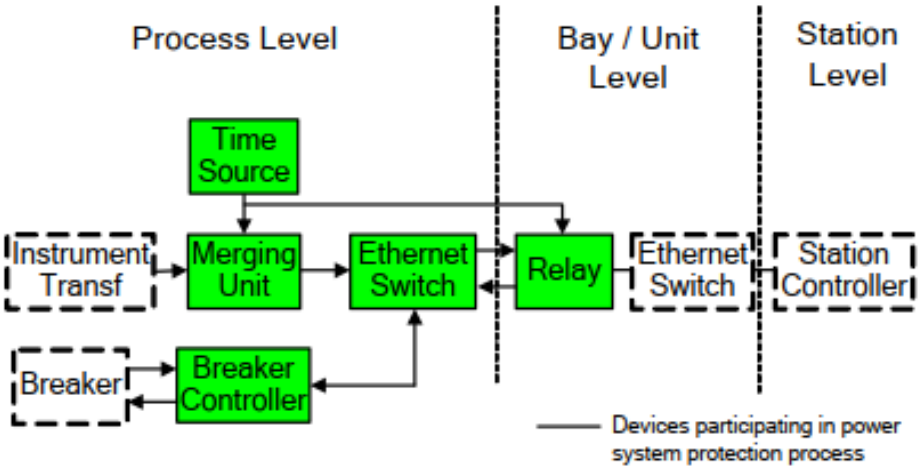
No entanto, diferente das mensagens GOOSE, as mensagens SVs são transmitidas sempre de forma contínua, em intervalos regulares.

Conforme a UCA 61850-9-2, mencionada no documento IEC/TR 61850-90-4, uma mensagem SV é enviada a cada 250 microssegundos, o que equivale a 4000 mensagens por segundo. Para redes de 60 Hz, o período é de 208,3 microssegundos, resultando em aproximadamente 4800 mensagens por segundo.

3.4.3.1 Merging Unit (MU)

Merging Unit, ou unidade de mesclagem, é um dispositivo que se encontra na interface entre transformadores de instrumentos (convencionais ou não convencionais) no nível de processo e IEDs no nível de *bay*. Sua principal função é digitalizar sinais de corrente e tensão dos secundários dos TCs e TPs, ou seja, faz a leitura e conversão analógica/digital dos valores desses sinais, em seguida processa esses dados e publica na rede em um quadro ETHERNET padronizado de acordo com as normas IE 61850-9-2 e IEC 61869-9 usando SVs, mostrada na Figura 20.

Figura 20 – Esquema de conexão da *Merging Unit* com os equipamentos



Fonte: SKENDZIC; ENDER; ZWEIGLE (2007)

Vale ressaltar que as MUs produzidas de diferentes fabricantes podem não interoperar, mesmo que estejam em conformidade com os padrões IEC 61860-9-2. Sendo assim, a melhor forma de alcançar a interoperatividade é por meio dos testes de interoperatividade de MUs, onde são analisados (CONPROVE, [s.d.]):

- **Linearidade:** avalia-se na MU a resposta linearmente em amplitude e angulo de acordo com a variação dos sinais analógicos injetados.
- **Resposta em frequência:** verifica os erros de amplitude e angulo na saída da MU quando os sinais de tensão e corrente contém harmônicos. A resposta da MU a cada ordem harmônica deve ser analisada individualmente.
- **Precisão de amplitude e ângulo:** examina a precisão dos valores de corrente e tensão na saída da MU na frequência fundamental, com base em um sinal estático na entrada durante um período prolongado (teste de longa duração).
- **Monitoramento de erros:** este monitoramento tem como objetivo avaliar a saúde da rede, verificando se não há mensagens SV perdidas, corrompidas ou amostras duplicadas ou atrasadas.
- **Monitoramento estatística de tempo:** serve para analisar os tempos envolvidos na transmissão e no processamento das mensagens SV na *Merging Unit*. Ele verifica se o intervalo entre os quadros está de acordo com a taxa de amostragem configurada e se a soma do tempo de digitalização da amostra com o tempo de envio pela rede fica abaixo de 5 ms, conforme

estabelecido na IEC 61850-5 (item 11.2.4, edição 2) e na IEC 61850-9 (item 6-902-2, edição 1).

- **Monitoramento de sincronização:** garante que as amostras fiquem sempre sincronizadas e com boa qualidade. Para isso, é verificado o sinal de sincronização presente no quadro SV.

3.4.4 Sistema Publicador e Assinante

Analogia: Quando nos inscrevemos em um canal no Youtube, isso nos permite que recebamos notificações de atualizações do canal sempre que há conteúdo novo.

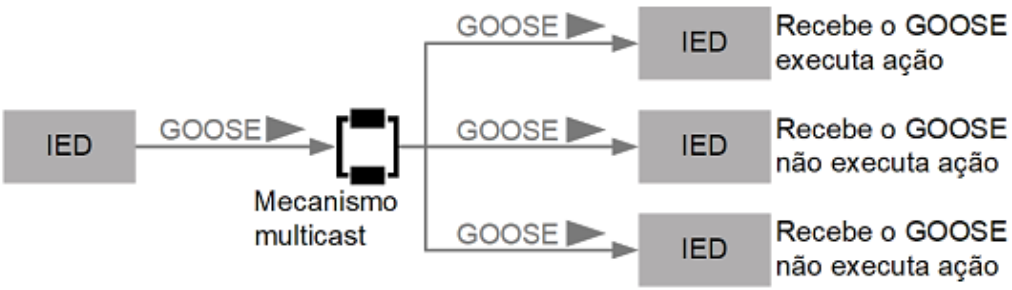
O sistema *publicador*/*assinante* é essencial para gerenciar o tráfego de dados na rede, permitindo que os IEDs processem informações de forma eficiente. Nesse modelo, o IED publicador envia os dados, enquanto o assinante recebe apenas as informações relevantes para sua função, descartando conteúdos desnecessários.

Um exemplo disso é quando um IED detecta uma falta em sua zona de proteção, em seguida ele publica uma mensagem GOOSE que contém o sinal de disparo e informações relevantes. O IED assinante, ao receber essa mensagem, interpreta que a falta está fora de sua área e bloqueia sua própria atuação, evitando um desligamento em cascata. Dessa forma, esse mecanismo de comunicação entre dois IEDs garante seletividade e evita desligamentos desnecessários.

Sempre que os novos eventos são gerados na aplicação local do IED, eles são mapeados no conjunto de dados (*Datasets*) e envelopados nas mensagens GOOSE para publicação (SILVEIRA; FRANCO, 2021).

Na Figura 21 é apresentado o esquema de transmissão da GOOSE para vários IEDs, também chamado de *Multicast*.

Figura 21 – Esquema Sistema Publisher/Subscriber na GOOSE



Fonte: SILVEIRA; FRANCO (2021)

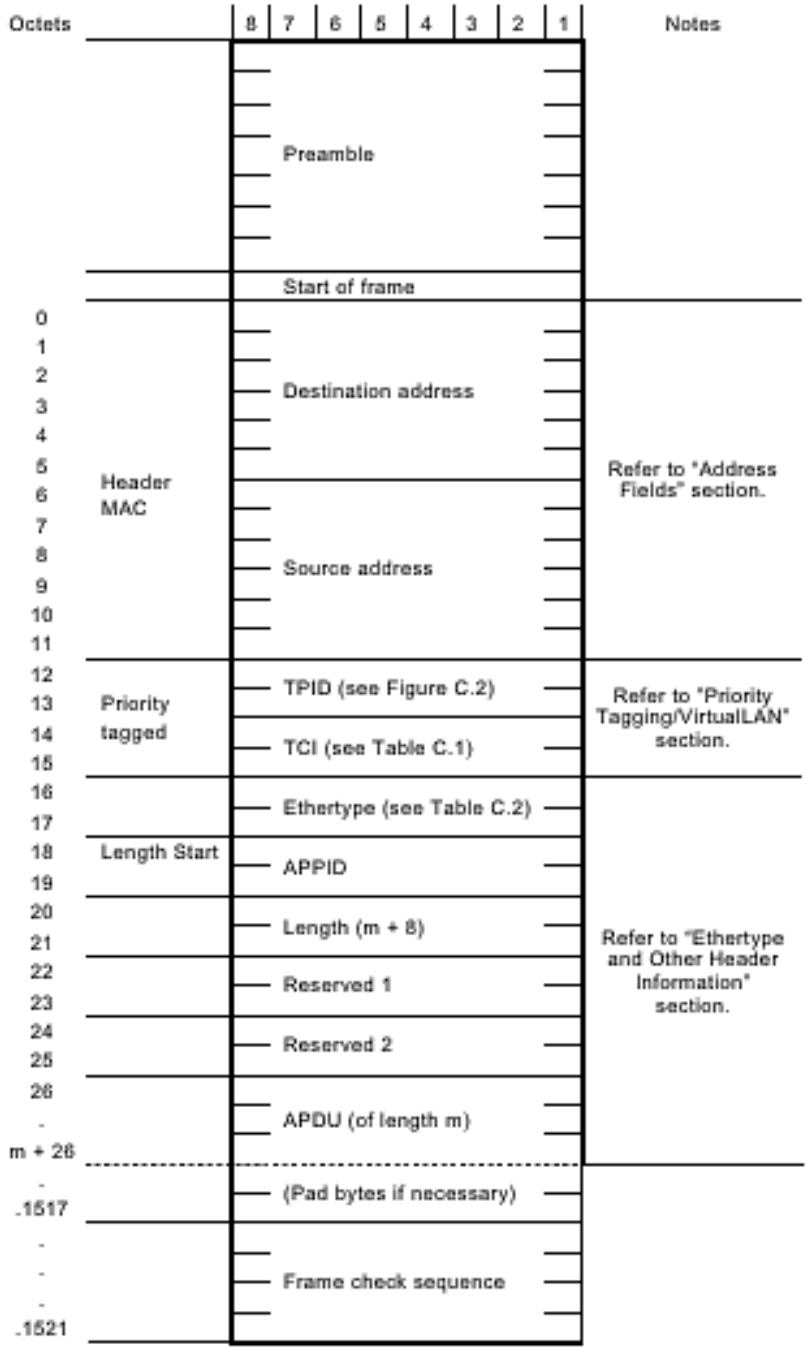
Além da GOOSE, como mencionado anteriormente, os SVs também utilizam o mecanismo de transmissão *multicast*. Quando um conjunto de valores amostrados de corrente e tensão é gerado por uma *Merging Unit*, ele pode ser enviado para vários IEDs. Dessa forma, todos os dispositivos assinantes precisam receber os dados simultaneamente para interpretar de forma consistente e sincronizada as medições usadas para proteção e controle.

Esse controle de dados é feito através dos endereços MAC (*Media Access Control*) únicos para cada IED. As mensagens GOOSE quando são publicadas, elas são transmitidas via Ethernet, entrando diretamente na camada de enlace (camada 2 do modelo OSI), para garantir a baixa latência e alta confiabilidade para o envio prioritário de mensagens, sem passar pelas camadas de transporte e rede do TCP/IP, onde este último faz a confirmação de entrega das mensagens.

Por esse motivo, as mensagens GOOSE utilizam classificadores *Ethertype* no intervalo hexadecimal 0x0000 a 0x3FFF e dependem de um esquema de retransmissão para garantir confiabilidade na entrega dos dados. As mensagens SVs, por sua vez, são mapeadas dentro da transmissão Ethernet usando classificadores *Ethertypes* no range 0x4000 a 0x7FFF em hexadecimal.

O esquema de envio de mensagens do GOOSE é definido pela ISO/IEC 8802-3 para Redes Locais Virtuais Interligadas, encontrada no anexo C da norma IEC 61850-8-1, indicada na Figura 22. Essa estrutura também é válida para as mensagens SVs, que é semelhante e se encontra no Anexo A da IEC 61850-9-2, mudando apenas os valores de bit para identificação das mensagens através de um range de octetos diferentes que serão explicados nas páginas seguintes.

Figura 22 – Estrutura do *frame* do GOOSE/SVs



Fonte: IEC 81850-8-1 (2004)

1. **Preamble:** É formado por 7 bytes iguais, onde cada byte do preâmbulo segue um padrão específico alternando entre uns e zeros (10101010), semelhante ao *frame* Ethernet. Tem como função avisar os dispositivos receptores para que se preparem para receber um novo *frame*.

2. **Start of frame:** É o último byte que aparece logo após o preâmbulo e antes do início do *frame*. Ele se diferencia por ter o último bit distinto do padrão usado nos bytes do preâmbulo e sempre apresenta a sequência “10101011”.
3. **Destination Address:** É o endereço físico dos *subscribers* na rede Ethernet. Tal endereçamento tem os bits mais significativos sempre constante para indicar que se trata de uma mensagem *multicast*. De acordo com a norma IEC 61850-8-1, os três primeiros octetos do endereço devem ser 01-0C-0D. O quarto octeto indica o tipo de mensagem transmitida, podendo assumir o valor 01 para GOOSE, 02 para GSSE ou 04 para SV. Já os quinto e sexto octetos são utilizados para definir um identificador único para a mensagem específica que está sendo enviada, os quais têm o range de 00-00 a 01-FF, conforme indicado na Figura 23.

Figura 23 – Range do endereço MAC

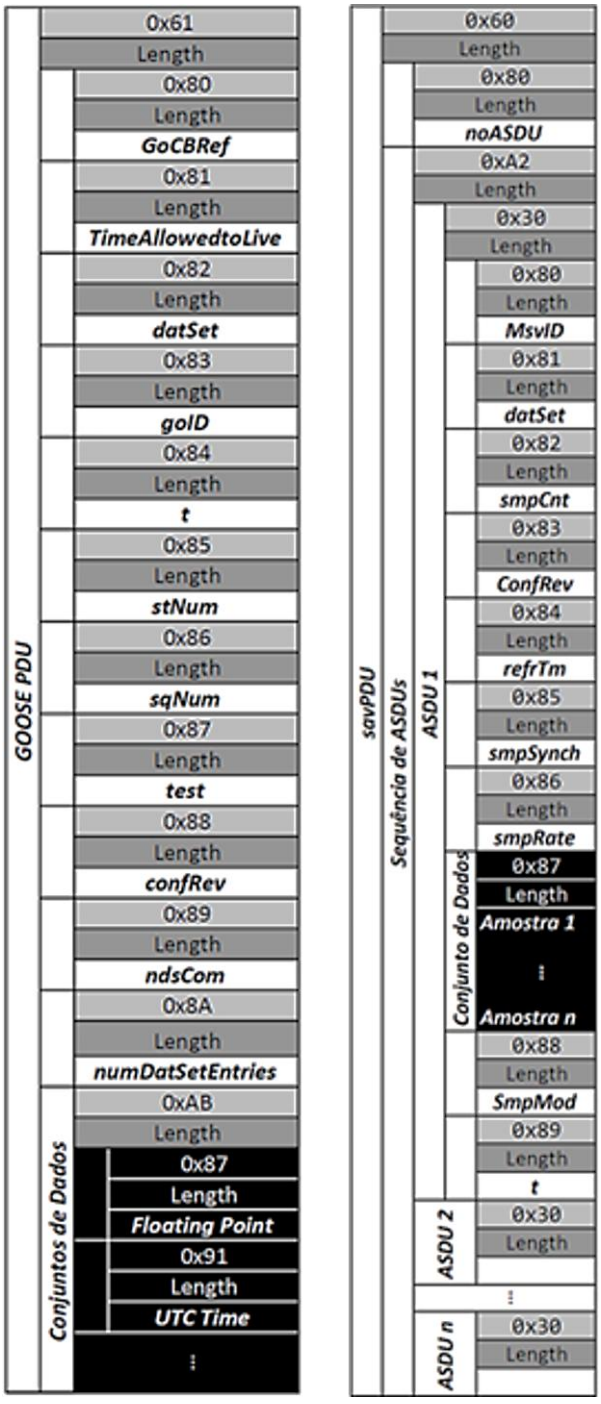
Service	Recommended address range assignments	
	Starting address (hexadecimal)	Ending address (hexadecimal)
GOOSE	01-0C-CD-01-00-00	01-0C-CD-01-01-FF
GSSE	01-0C-CD-02-00-00	01-0C-CD-02-01-FF
Multicast sampled values	01-0C-CD-04-00-00	01-0C-CD-04-01-FF

Fonte: IEC 61850-8-1 (2004)

4. **Source Address:** Consiste no endereço físico do dispositivo que publica a mensagem na rede.
5. **TPID (Tag Protocol Identifier):** Refere-se à prioridade da seção de tagging/virtual LAN. De acordo com o IEEE 802.1Q, e explicado na IEC 61850, este campo é usado para separar o tempo crítico e tráfico de barramento de alta prioridade para aplicações relevantes de proteção da baixa prioridade do barramento de carga. Para isso, seu valor configurado deve ser 0x8100.
6. **TCI (Tag Control Information):** Assim como o TCI, refere-se à prioridade da seção de tagging/virtual LAN. A prioridade do usuário deve ser configurada nesse campo para separar mensagens importantes (como SVs e GOOSE usadas para proteção rápida) das mensagens menos importantes que ocupam a rede.

7. **Ethertype:** Este campo identifica se as mensagens são do tipo GOOSE, GSE Management ou SVs dentro do padrão de *frame* ethernet, onde os valores *Ethertype* em hexadecimal são 88-B8, 88-B9 e 88-BA, respectivamente.
8. **APPID (Application Identifier):** Faz a identificação do *frame* na rede. Para mensagens SVs, ele seleciona mensagens de valores analógicos amostrados que estão reservados a partir de 0x4000 a 0x7FFF. Já para GOOSE é 0x0000 a 0x3FFF.
9. **Length:** Indica o número total de bytes da mensagem.
10. **Reserved (1 e 2):** Esses dois campos são reservados para futura padronização das aplicações e, de acordo com a IEC 61850, ela deve vir configurada como 0 por padrão.
11. **APDU (Application Protocol Data Unit):** A sigla no português significa “Unidade de Dados do Protocolo de Aplicação”; essa camada contém informações de parametrização e endereçamento da mensagem a ser enviada, como a informação do *data set* em que a mensagem está sendo publicada. Além disso, os dados devem ser codificados de acordo com a *Abstract Syntax Notation One* / *Basic Encoding Rule* (ASN.1/BER). Na Figura 24 são apresentadas as estruturas APDU do GOOSE e do SV.

Figura 24 – Estrutura APDU do GOOSE e do SV



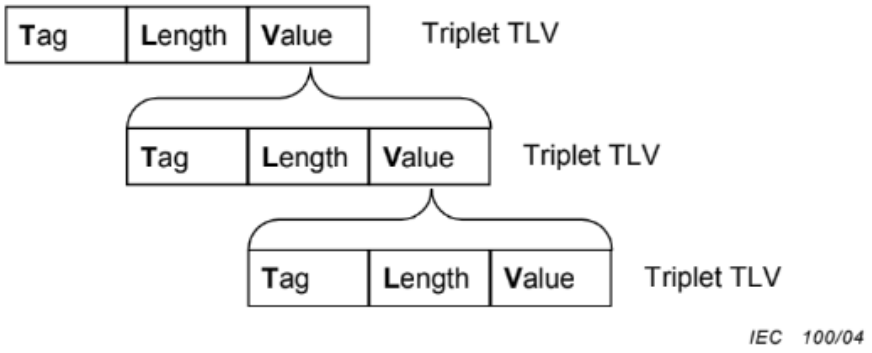
Fonte: LEITE; REIZ (2021)

12. **Pad bytes if necessary:** Bytes de preenchimento para que a estrutura APDU atenda o tamanho mínimo exigido pelo protocolo.
13. **Frame check sequence:** Como o próprio nome já diz, é a checagem sequencial dos *frames* se não há erros nos dados enviados pelos remetentes ou corrompidos.

3.4.5 ASN.1. Basic Encoding Rules (BER)

Para que seja possível a codificação e decodificação da GOOSE e dos SVs na APDU, tem-se o ASN.1 *Basic Encoding Rules* (BER), especificado na ISO/IEC 8825-1. Esse modelo da OSI trabalha com o trio T-L-V, no inglês a sigla é *Type*, *Length* e *Value*, que indica o tipo de mensagem, comprimento e valor. Ou então o T pode significar *Tag* em vez *Type*, como mostrado na Figura 25.

Figura 25 – Formato do BER (*Basic Encoding Rules*)



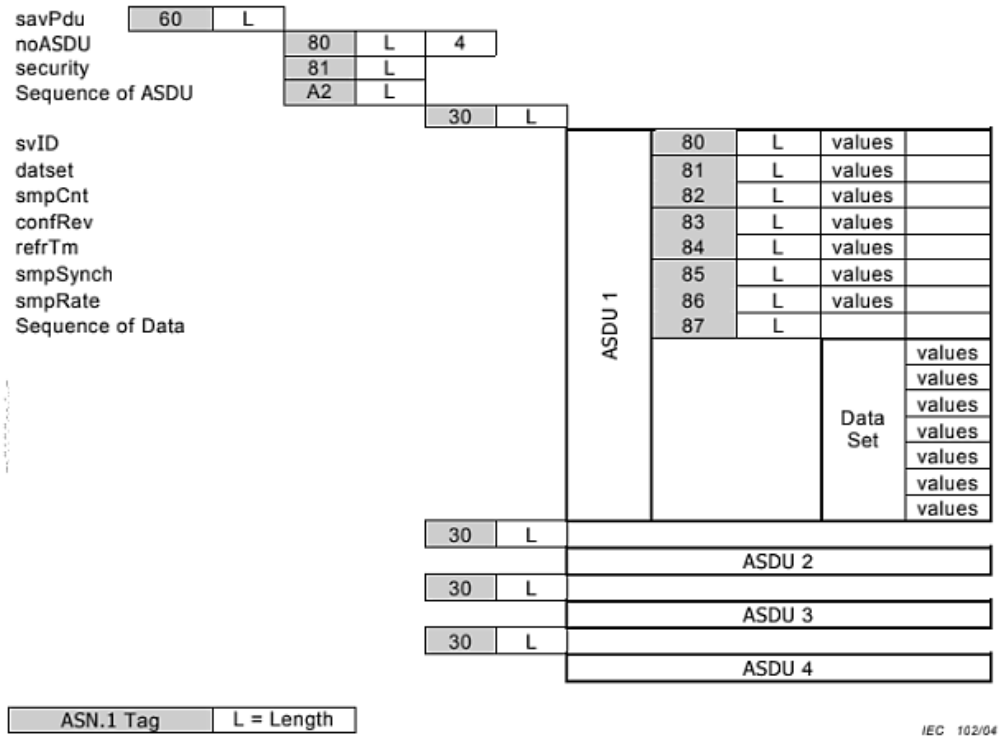
Fonte: IEC 61850-9-2 (2004)

Conforme as Figuras 24 e 26, o *framework* da APDU do *Sampled Value* (SV PDU) para o início da parametrização e endereçamento da mensagem a ser enviada, como a informação do *data set* em que a mensagem está sendo publicada, deve estar codificada com a tag 0x60 e a parte do seu valor savPDU contém a seguinte sequência de dados (LEITE; REIZ, 2021):

a) noASDU: indica o número de ASDUs que será concatenado em uma APDU;

b) Sequence of ASDUs: indica a sequência completa de ASDUs (*Application Service Data Units*) associada com o SV PDU. Na Figura 26, por exemplo, tem 4 ASDUs.

Figura 26 – Exemplo do ASN.1 no APDU de Sampled Values



Fonte: IEC 61850-9-2 (2004)

Cada ASDU é codificada com a tag de 0x30 associando os seguintes dados:

i. *MsvID:* faz a identificação da ASDU;

ii. *datSet:* representa a referência do conjunto de dados (*DataSets*);

iii. *smpCnt:* indica o valor da contagem de amostras ao ser incrementado a cada nova amostragem;

iv. *ConfRev:* indica a contagem da mudança de configuração;

v. *refrTm:* este campo não é obrigatório e contém o instante de atualização do registro do SV;

vi. smpSynch: indica a condição em que as amostras são sincronizadas;

vii. *smpRate:* indica o valor da taxa de amostragem;

viii. *Sample:* listagem dos dados que serão enviados pelo SV PDU;

ix. *SmpMod:* este campo é facultativo e indica o modo de amostragem;

x. t: campo facultativo que contém a estampa de tempo de transmissão do pacote.

As mensagens GOOSE seguem uma estrutura semelhante no *framework* APDU, ou seja, também são codificadas usando a estrutura T-L-V, todavia com a *Tag* iniciando-se com 0x61, que contém a seguinte sequência de dados:

i. *GoCBRef:* é a referência para o bloco de controle que está controlando a mensagem GOOSE;
ii. *TimeAllowedtoLive*: avisa o receptor o máximo tempo de espera até ocorrer a próxima retransmissão;
iii. *datSet:* contém o valor de referência do conjunto de dados (*DataSets*);
iv. *goID:* identifica e diferencia a mensagem GOOSE das outras;
v. *t:* estampa de tempo da mensagem GOOSE;
vi. *stNum*: contém o contador que incrementa toda vez que ocorre mudança do dado GOOSE;
vii. *sqNum*: contador que registra o número de mensagens GOOSE enviadas sob o mesmo estado (retransmissão);
viii. *test*: indica se o dispositivo enviando a mensagem GOOSE está em modo teste;
ix. *ConfRev*: indica a contagem da mudança de configuração;
x. *ndsCom*: *Needs Comissioning*, indica se GOOSE precisa ainda ser configurada;
xi. *numDatSetEntries*: indica o número de membros do conjunto de dados (*DataSets*);
xii. *allData*: o conjunto de dados (*DataSets*) que estão sendo transmitidos na mensagem GOOSE.

Basicamente, o APDU é responsável por encapsular várias ASDUs, permitindo assim o envio de múltiplos conjuntos de amostras em um único quadro.

3.5 TOPOLOGIA DE REDES

Nas redes de comunicações, é essencial definir como seus dispositivos são conectados entre si para garantir a troca de informações entre os equipamentos de maneira eficaz e evitar perda de comunicação.

Uma rede é composta por nós, os quais representam os pontos de conexão, e pelos links que os conectam. No contexto de uma rede de área local (LAN), cada computador representa um nó. Enquanto isso, os links são os meios de transmissão utilizados para enviar informações entre os nós, que podem ser cabos coaxiais, de pares trançados ou de fibra óptica (IBM, 2024).

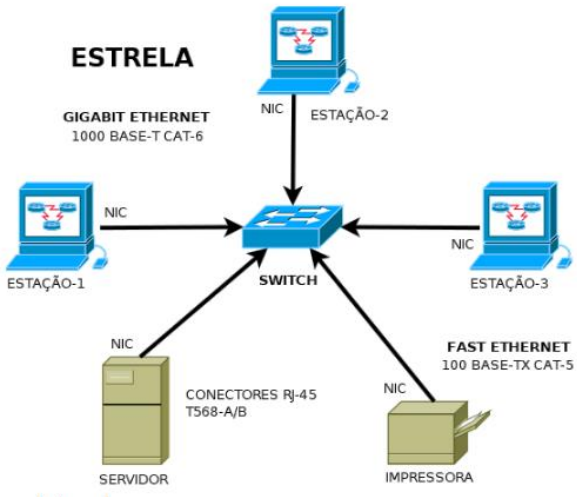
Além disso, na troca de mensagens, fazem-se necessários alguns equipamentos de conectividade para estabelecer a comunicação entre os dois pontos e controle do tráfego de dados, como placa de rede (NIC), repetidores, *hubs*, pontes, *switches*, roteadores e *gateways*, e seu uso varia bastante de acordo com o objetivo final do projeto (FERNANDÉZ, 2019).

Os principais tipos de topologia são: Estrela, Barramento, Anel, Árvore, Malha (*Mesh*) e Híbrida.

3.5.1 Topologia Estrela

Na topologia em estrela, todos os dispositivos são conectados a um nó central, o qual funciona como um controle supervisor do sistema. Quando o nó central é um *hub* (repetidor de múltiplas portas), ele simplesmente replica os sinais recebidos e os transmite para todos os dispositivos conectados, sem qualquer filtragem. Por outro lado, se o nó central for um *switch* (comutador), a transmissão ocorre de forma seletiva, direcionando os dados apenas ao destino correto, o que reduz o tráfego desnecessário na rede (FERNÁNDEZ, 2019). Na Figura 27 é mostrada a representação topologia estrela.

Figura 27 – Representação Topologia Estrela

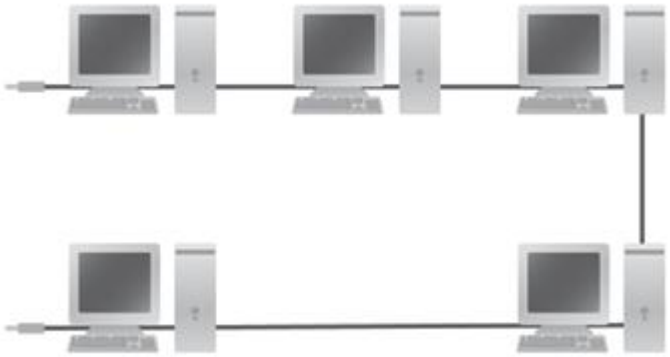


Fonte: SECBITREZ (2018)

3.5.2 Topologia Barramento

Em uma rede em barramento, todos os nós são conectados a um único cabo, semelhante a paradas de ônibus ao longo de uma mesma rota. A transmissão de dados percorre essa linha central, tornando a topologia simples, econômica e fácil de configurar, além de permitir a adição de novos nós com facilidade. A Figura 28 representa a topologia barramento.

Figura 28 – Representação Topologia Barramento



Fonte: ALENCAR (2010)

Infelizmente, essa estrutura apresenta desvantagens: como todos os dispositivos dependem do mesmo link central, qualquer falha nesse ponto compromete toda a rede. Adicionalmente, a sua segurança é menor em comparação com outras topologias, devido ao compartilhamento do mesmo link na transmissão. Outro fator que compromete o desempenho é a quantidade de nós conectados: quanto maior o número de dispositivos compartilhando o cabo central, mais lenta se torna a rede (IBM, 2024).

3.5.3 Topologia Anel

Em uma rede em anel, os nós e links estão dispostos de forma circular, de modo que cada nó possua exatamente dois vizinhos. Nessa disposição, os repetidores são usados para garantir que os dados consigam percorrer todo o anel, alcançando os nós mais distantes. Normalmente, o fluxo de dados ocorre em uma única direção, o que faz com que a falha em um único nó possa derrubar a rede inteira. Na Figura 29 é mostrada a representação da topologia anel.

Figura 29 – Representação Topologia Anel

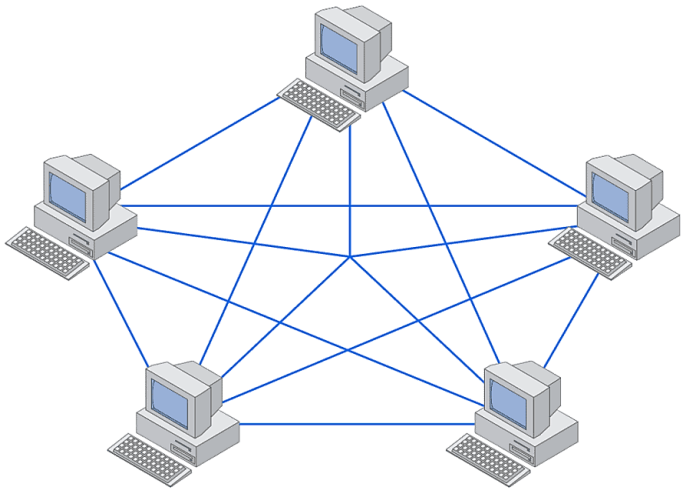
Fonte: ALENCAR (2010)

Para proteger contra esse tipo de falha, são usadas redes em anel duplo. Esse tipo de rede possui dois anéis concêntricos, nos quais os dados trafegam em direções opostas. O segundo anel atua como redundância em caso de falha no primeiro (esse tipo de rede é amplamente usado para suportar infraestruturas críticas).

3.5.4 Topologia Malha (*Mesh*)

Nessa configuração, cada dispositivo está conectado a pelo menos outro nó na rede. Na malha completa, todos os nós possuem conexões diretas entre si, ou seja, cada nó está conectado a todos os outros, enquanto na malha parcial apenas alguns nós são interligados diretamente, exigindo que outros utilizem nós intermediários para alcançar o destino. É mostrada na Figura 30 a representação da topologia do tipo malha.

Figura 30 – Representação Topologia Malha



Fonte: A3A ENGENHARIA DE SISTEMAS (s.d.)

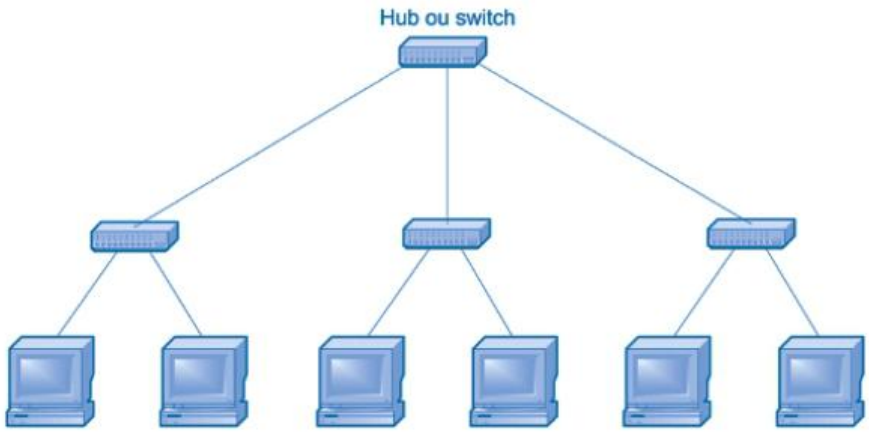
Por permitir uma comunicação direta entre os nós, sem o uso de um *hub* central, esse tipo de arranjo costuma ser muito rápida. A internet é um exemplo de aplicação, onde cada computador representa um nó em uma rede fornecida por diferentes provedores de serviços de internet, que também estão interconectados entre si. Além disso, uma outra vantagem é que as redes em malha são mais resilientes que os vários outros modelos, pois seu funcionamento não é comprometido mesmo que um nó ou conexão falhe.

Contudo, esse tipo de topologia apresenta um custo elevado de implementação devido à grande quantidade de cabos e conexões usados. Adicionalmente, a complexidade na instalação e manutenção de múltiplos caminhos também geram custos mais altos em comparação com as outras topologias (IBM, 2024).

3.5.5 Topologia Árvore

A topologia em árvore é uma combinação das redes em barramento e em estrela, onde existe um nó central que conecta os demais, mas, em vez de ramificações simples a partir desse ponto, há várias redes em estrela interligadas. Esse formato permite conectar um número maior de dispositivos a um centro de dados, favorecendo o fluxo de informações. Na figura 31 é mostrada a representação da topologia árvore.

Figura 31 – Representação Topologia Árvore



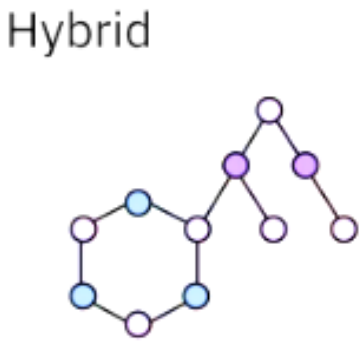
Fonte: MAIA (2013)

No entanto, a topologia em árvore compartilha as mesmas desvantagens das redes em barramento e em estrela: a vulnerabilidade a um único ponto de falha. Se a conexão central for interrompida, toda a rede fica inoperante.

3.5.6 Topologia Híbrida

A topologia híbrida é um tipo de rede que utiliza uma combinação de topologias de forma a atender às suas necessidades de comunicação, velocidade, eficiência e segurança. A Figura 32 apresenta um exemplo de topologia híbrida, combinando a topologia em anel com a topologia em árvore.

Figura 32 – Representação Topologia Híbrida



Fonte: IBM (2024)

Contudo, projetar uma arquitetura de rede personalizada pode exigir mais cabos e dispositivos de rede, aumentando assim os custos de manutenção (IBM, 2024).

3.6 PROTOCOLOS DE REDUNDÂNCIA NA REDE

É fundamental que os IEDs e os *switches* estejam interligados de forma eficiente, garantindo baixa latência e evitando a perda de pacotes em caso de falhas na rede. Essa configuração assegura a transmissão correta das mensagens GOOSE e SV, essenciais para a proteção e o controle nos barramentos da subestação e do processo. Para atender a esses requisitos, a norma IEC 61850 define protocolos de redundância que permitem continuidade operacional quase instantânea. Entre eles, destacam-se o HSR (*High-availability Seamless Redundancy*) e o PRP (*Parallel Redundancy Protocol*), baseados nas topologias de rede apresentadas anteriormente.

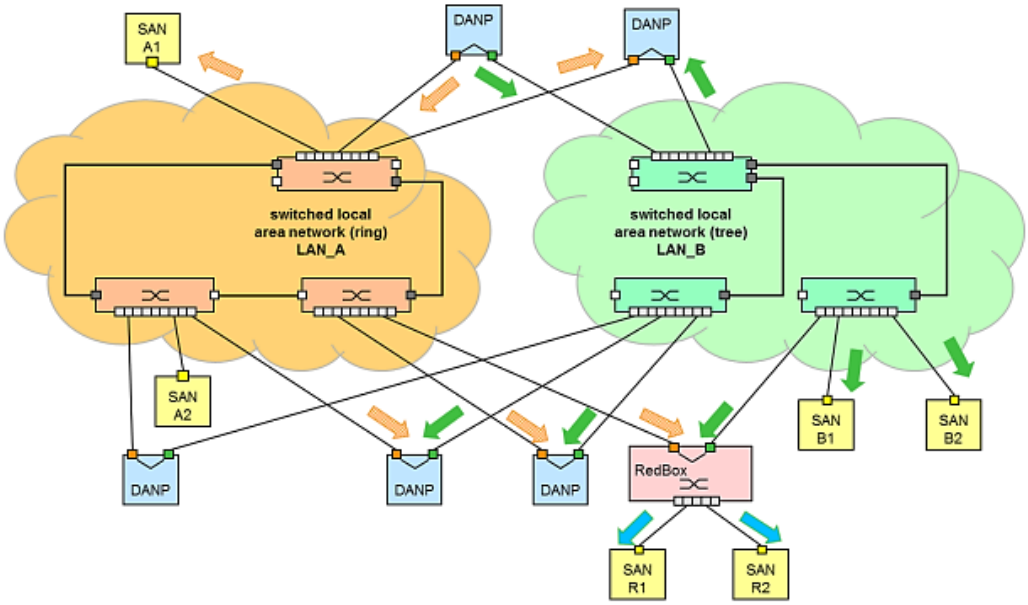
3.6.1 **PRP (*Parallel Redundancy Protocol*)**

Especificado na cláusula 4 da IEC 62439-3:2012, é um protocolo de redundância de camada 2 com o propósito de garantir que a comunicação continue funcionando mesmo se um cabo (enlace) ou um equipamento intermediário (ponte) falhar.

Ele faz isso enviando cada mensagem duas vezes, por duas redes separadas que funcionam em paralelo, LAN A e LAN B, baseada na topologia de estrela-dupla.

Para isso, o dispositivo DANP (*Doubly Attached Node for PRP*) envia o mesmo pacote nas duas redes, e cada pacote tem um código extra (trailer) para indicar que é duplicado. Dessa forma, o dispositivo que recebe descarta o pacote duplicado e usa só o primeiro. Se uma rede falhar, a outra continua funcionando sem interrupção. Nessa imagem também está o SAN (*Singly Attached Node*), é um dispositivo comum (como um laptop ou impressora) que tem apenas uma porta de rede. Ele funciona normalmente, mas não tem redundância. Portanto, o RedBox (*Redundancy Box*) faz o papel de conectar os dispositivos que não têm PRP (como SAN) às duas redes redundantes. A Figura 33 mostra esse modelo de protocolo de redundância.

Figura 33 – Modelo PRP (*Parallel Redundancy Protocol*)



Fonte: IEC 61850-90-4 (2013)

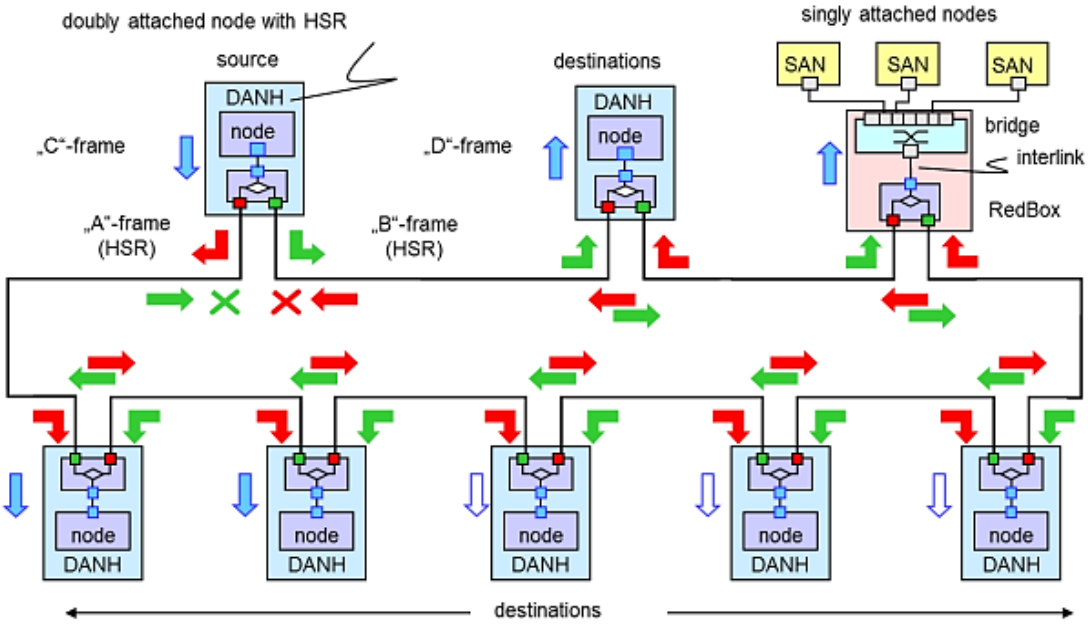
3.6.2 **HSR (*High-availability Seamless Redundancy*)**

Especificado na cláusula 5 da IEC 62439-3:12, o modelo HSR é um jeito de garantir que a rede continue funcionando mesmo se um cabo ou equipamento falhar. Por meio da ligação em anel entre os dispositivos, cada equipamento DANH (*Doubly Attached Node for HSR*) tem duas portas e manda a mesma informação (*frame*) pelos dois lados ao mesmo tempo. Assim, se um caminho parar de funcionar, o outro continua sem interrupção.

Dentro do equipamento, essas duas portas funcionam como se fossem uma só para os programas, então quem está usando a rede nem percebe que existe essa redundância. Outra vantagem é que o HSR não precisa de *switches* dedicados, o que ajuda a economizar.

Como os pacotes HSR têm uma marca especial que os dispositivos comuns não entendem, para ligar equipamentos simples como o SAN, é preciso usar um *RedBox*. A Figura 34 mostra o modelo HSR para redundância de redes.

Figura 34 – Modelo HSR (*High-availability Seamless Redundancy*)



Fonte: IEC 61850-90-4 (2013)

Vale ressaltar que redes HSR e PRP podem trabalhar juntas como uma topologia de rede mista. Para isso, um dispositivo HSR usa duas interfaces para se conectar ao anel HSR e uma terceira interface para se ligar à LAN A ou LAN B da rede PRP. Quando o dispositivo HSR envia dados pelo anel, ele identifica para qual rede

PRP o tráfego deve ir usando a etiqueta correta. Depois, os dispositivos HSR encaminham esse tráfego para a LAN A ou LAN B. O dispositivo PRP recebe os dados e processa conforme as regras do PRP. Um único anel HSR pode marcar e gerenciar tráfego para até sete redes PRP conectadas (MACHADO, 2023 *apud* SCHNEIDER ELECTRIC; MEDEIROS, 2020).

4 ESTUDO PRÁTICO

Para esse estudo prático da norma IEC 61850 aplicada às subestações digitais, o experimento foi feito em três etapas: funcionamento da simulação *Hardware-in-the-Loop* (HIL), a transmissão de dados pelo emulador SAMU, desenvolvido no Visual Studio 2022, e análise e interpretação da captura de pacotes no software Wireshark® juntamente com os conceitos vistos nos capítulos anteriores.

4.1 HARDWARE-IN-THE-LOOP

Com o passar dos anos, a automação avançada de distribuição foi se tornando cada vez mais relevante no setor elétrico. Para isso, foi necessário o desenvolvimento de novas metodologias e ferramentas computacionais que fossem capazes de simular as redes de distribuição em tempo real, juntamente com as técnicas de HIL, reduzindo assim os tempos de projeto e teste com baixo custo (LEITE; REIZ, 2021).

O HIL é usado para validar a integração de algoritmos de controle com componentes de hardware reais. Ao conectar o hardware do controlador real a uma planta simulada em tempo real, o teste HIL fornece um ambiente de alta fidelidade para testar o sistema em condições e cenários realistas. Com essa simulação, torna-se capaz de testar algoritmos de controle em componentes de hardware antes mesmo que todo o hardware físico esteja disponível. Isso faz com que mitigue risco de danos a equipamentos caros, permitindo que engenheiros testem cenários e casos extremos em um ambiente virtual controlado. Assim, esse método não só acelera o desenvolvimento, mas também comprova que o sistema projetado é robusto e pronto para operar no mundo real sem comprometer um hardware valioso.

O teste HIL consiste nas seguintes etapas: modelagem da planta, simulação em tempo real, conexão com o controlador, aquisição de dados e feedback e testes e validação do sistema (MATHWORKS, [s.d.]).

Além disso, com as simulações de transitórios de redes elétricas, é possível fazer o estudo de sobretensão, coordenação de sistemas de proteção e isolamento, qualidade de energia e entre outros.

Trabalhando com o modelo HIL, é possível reduzir o custo de cabeamento de cobre complexo e extenso, assim como obter flexibilidade na comunicação de sinais, pois o protocolo IEC 61850-9-2 propõe uma rede de comunicação via Ethernet entre os equipamentos no nível de processo e os IEDs (dispositivos eletrônicos inteligentes)

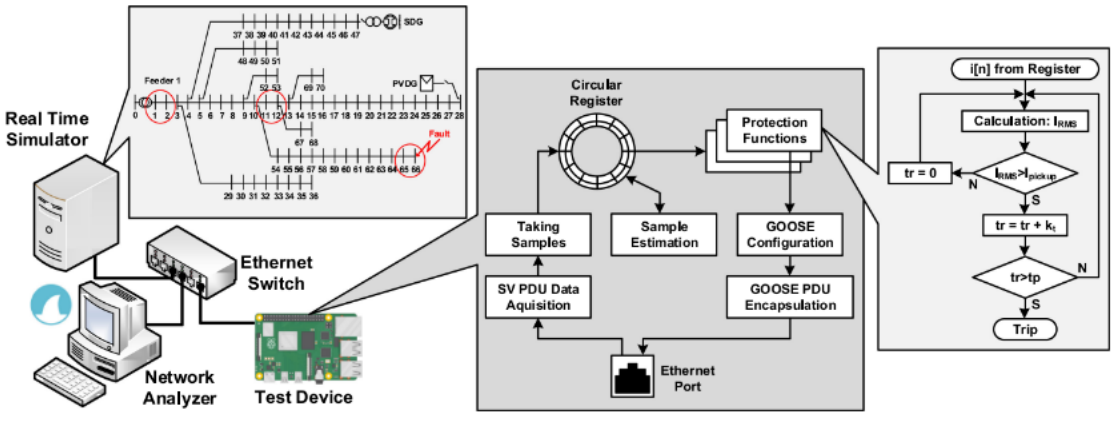
de controle e proteção no nível *bay*. Portanto, a rede local baseada em Ethernet poderá permitir a troca de mensagens críticas no tempo como eventos genéricos orientados (GOOSE) e valores de amostras brutas (SV) dentro do tempo permitido.

Dessa forma, este trabalho consiste em uma metodologia que utiliza uma simulação híbrida, junto com os conceitos do HIL, na qual os cálculos de fluxo de potência utilizando modelos fasoriais são combinados com o modelo transitório para resposta em tempo discreto.

O modelo transitório é simples o suficiente para gerar valores discretos de corrente e tensão com tempo de processamento abaixo do período de amostragem, definido pelo protocolo de comunicação. A norma IEC 61850-9-2 é codificada para coletar os valores amostrais do modelo transitório, enquanto a norma IEC 61850-8-1 permite eventos de comutação para modificar a topologia da rede no modelo fasorial (LEITE; REIZ, 2021).

A Figura 35 representa um esquema detalhado da estrutura experimental a ser utilizada. O nó de comunicação (Ethernet Switch) conecta o simulador em tempo real com o dispositivo testado. Em seguida, o fluxo de dados é monitorado por um analisador de rede, o Wireshark®. Com isso, o diagrama funcional do dispositivo testado é usado para demonstrar seus principais recursos lógicos, tais como o bloco de aquisição do SV PDU e encapsulamento do GOOSE PDU para comunicação via Ethernet. Por fim, as amostras obtidas dos valores de tensão e corrente são armazenadas em um registrador circular que fornece os dados de entrada para as funções de proteção e medição.

Figura 35 – Esquema *Hardware-In-The-Loop*



Fonte: LEITE; REIZ (2021)

4.2 PROGRAMA SAMU

Considerando a ausência de uma *Merging Unit* física e visando a redução de custos, foi utilizado neste trabalho o recurso lógico SAMU, desenvolvido no Visual Studio 2022, para simular a operação de troca de dados de amostras de corrente e tensão (*Sampled Values*) dessa unidade, utilizando o protocolo de comunicação IEC 61850-9-2.

A configuração desse emulador foi baseada no *Harmonized* CIM (*Common Information Model*), que consiste no modelo padronizado para representar dados de sistemas elétricos, e na SCL (*Substation Configuration Language*), este último contém a linguagem usada para descrever a configuração dos dispositivos IEC 61850, ou seja, o próprio arquivo XML. Nele contém informações sobre a configuração da subestação, os IEDs, AccessPoint, Servidor do IEC 61850, Nós Lógicos (LN) e suas classes (LNClass), *Data Objects* (DO), *Data Attributes* (DA), *Common Data Classes* (CDC), *Control Blocks* (GOOSE e Sampled Values), *Datasets* e seus respectivos valores medidos/configurados.

Quando esse emulador é executado, ele coleta fasores de tensão e corrente (representação em magnitude e ângulo) gerados pelo EDSIM (Simulador das Redes de Distribuição de Energia) e os converte em valores discretos instantâneos (amostras no tempo) e codificados em um quadro de bytes para transmissão. Em seguida, o quadro de dados é enviado via comunicação serial para um dispositivo chamado EDGE, este, por sua vez, contém a função lógica MMXU, que é o bloco lógico que coleta esses dados de medição essenciais para o monitoramento e controle do sistema elétrico.

Neste trabalho em específico, trabalha-se com a coleta de dados referentes a três equipamentos, o transformador de corrente, o transformador potencial e o disjuntor, que são descritos como TCTR, TVTR e XCBR, onde são medidos os valores de corrente e de tensão (ambos nas fases A, B, C e N) via SV (9-2LE) nos dois primeiros equipamentos, enquanto no último é analisado o controle de posição aberto ou fechado via GOOSE. Além disso, nosso dispositivo lógico (LD) é o MUuu.

No código do arquivo XML, cada objeto é identificado pelo ID (*Substation*, IED, *LogicalDevice*, *LogicalNode*, *DataSet*, *MeasurementValue*, etc.), onde sua estrutura hierárquica foi dividida da seguinte forma:

Quadro 4 – Visão Geral dos Objetos no arquivo XML do SAMU

ID	Identificação Objetos	Descrição
_ID_0000	Substation	É a identificação da subestação onde são coletados todos os dados dos equipamentos.
_ID_1001	IED	Objeto identificado como VD01.
_ID_1005	IEC61850Server	Aqui é onde se faz a configuração de quais funções serão ativadas para enviar para o cliente.
_ID_1006	LogicalDevice	É o dispositivo lógico IED, identificado como MUnn.
_ID_1016 a _ID_1019	LogicalNodes (TCTR)	É aqui onde inicia o comando da coleta de dados de medição das correntes do TC nas fases A, B, C e N, indicadas como InnATCTR1, InnBTCTR2, InnCTCTR3 e InnNTCTR4, respectivamente.
_ID_1080 a _ID_1083	LogicalNodes (TVTR)	É aqui onde inicia o comando da coleta de dados de medição das tensões do TP nas fases A, B, C e N, indicadas como InnATVTR1, InnBTVTR2, InnCTVTR3 e InnNTVTR4, respectivamente.
_ID_1106:	LogicalNodes (XCBR)	É aqui onde inicia o comando da coleta de dados no XCBR, identificado como InnXCBR1.
_ID_1044, _ID_1142, _ID_1143:	DataSets	Aqui se tem um grupo de pontos de dados (Data Objects) sendo transmitidos juntos em uma única mensagem. MUnn/LLN0.PhsMeas1 MUnn/LLN0.CbrST1 e MUnn/LLN0.CbrCO1
_ID_1023, _ID_1051, _ID_1055, _ID_1059, _ID_1032, _ID_1063, _ID_1067, _ID_1071	Measurement Values	MUnn/TCTR1.Amp.instMag[MX] (_ID_1023) indica os valores de medição, onde o MUnn é um Logical Device, TCTR1 é o Logical Nodes, Amp.instMag é o objeto de dados que representa a magnitude instantânea da corrente e MX sendo o grupo funcional de medição. Existem outros com mesma estrutura.

Fonte: Produção do próprio autor

Note que o Quadro 4 apresenta uma visão macro do código a respeito da identificação dos objetos, visando o entendimento de quais principais objetos estão

sendo trabalhados, pois dentro das linhas de código dos _ID_s, há outras informações que descrevem quais tipos de informações estão sendo coletadas.

4.3 WIRESHARK

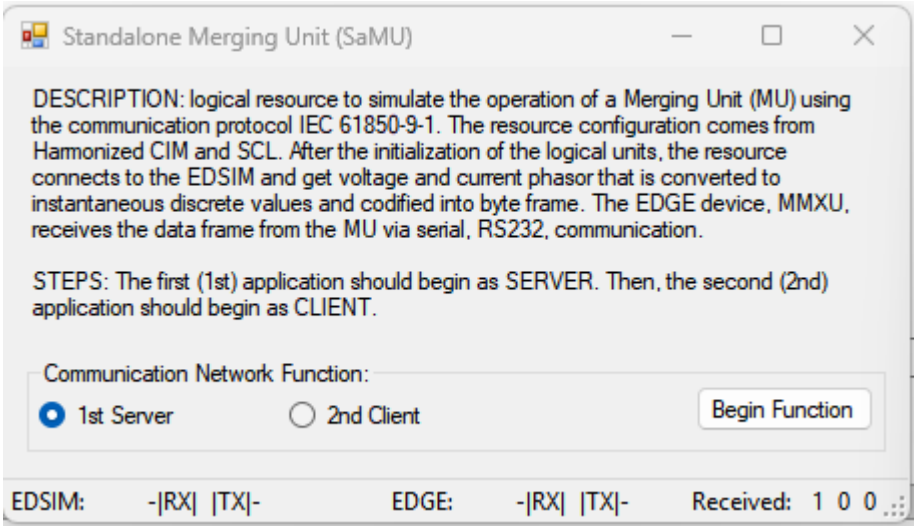
O Wireshark® é uma ferramenta para análise de protocolos que fazem a captura e análise de dados em interfaces de redes cabeadas ou sem fio.

Ele pode ser configurado para identificar o tipo específico de pacote, como no caso das mensagens GOOSE e SVs, e, com isso, filtrar este pacote de dados para análise. Os valores dos *frames* são coletados após o início da transmissão do emulador SAMU, onde são analisados os valores de tensão e corrente dos transformadores, o protocolo utilizado na comunicação e a estrutura savPDU no geral. Para o caso da GOOSE, o Wireshark® é comumente usado para fazer análise dos tempos de atraso das mensagens em relação ao tempo em que o relé de origem envia a mensagem e o dispositivo de destino o recebe.

4.4 FASE DE SIMULAÇÃO

Inicialmente, o programa SAMU foi aberto e configurado para atuar como Servidor. Nessa função, ele é responsável por transmitir os pacotes de dados conforme os parâmetros definidos no arquivo XML integrado à norma IEC 61850. Essa etapa garante que os dados de medição e controle sejam disponibilizados para os dispositivos clientes, conforme a Figura 36.

Figura 36 – Programa SAMU como Cliente/Servidor



Fonte: Produção do próprio autor

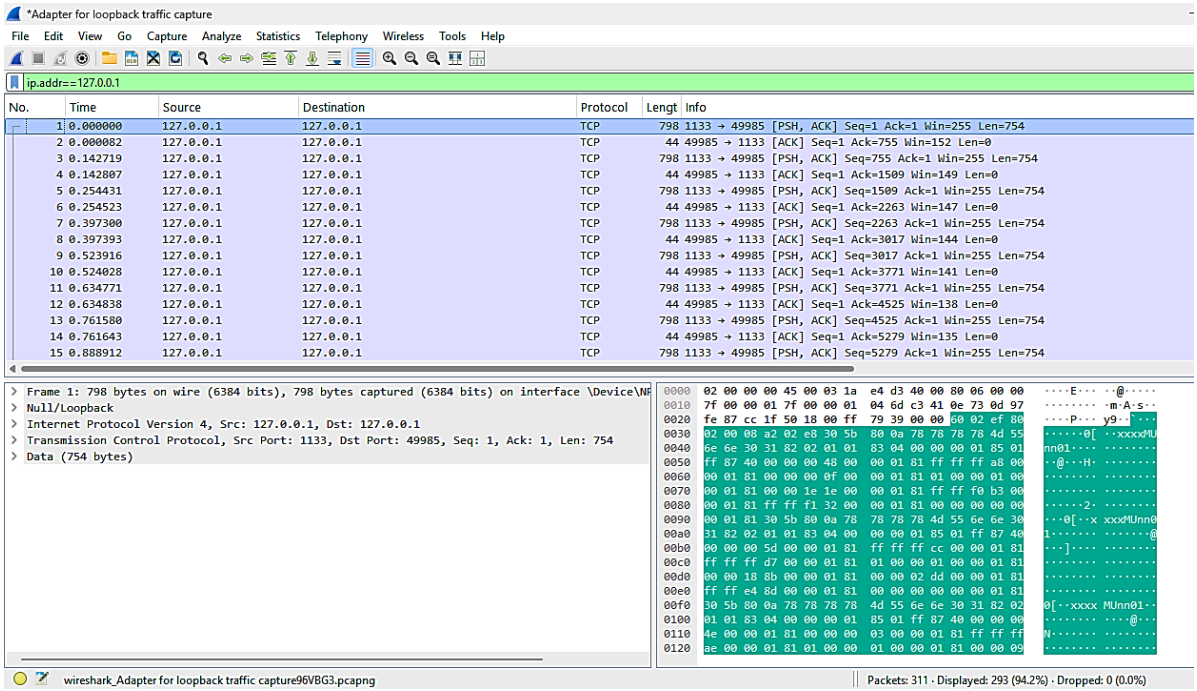
Em seguida, o mesmo programa foi aberto em uma segunda instância, mas configurado para operar como Cliente. Nessa função, ele recebe os pacotes de dados enviados pelo servidor, simulando o comportamento de um sistema supervisório ou outro IED que consome as informações transmitidas.

Essa configuração cliente-servidor permite validar a comunicação bidirecional conforme a norma IEC 61850, garantindo que os dados encapsulados nos protocolos GOOSE e *Sampled Values* possam ser transmitidos e recebidos corretamente em um ambiente controlado.

Após o início da transmissão pelo programa SAMU, o Wireshark® foi aberto para dar início à captura dos pacotes de dados enviados pela SAMU, para monitorar e verificar a recepção dos pacotes de dados (*frames*) enviados pelo SAMU.

Enquanto o SAMU ainda está sendo executado tanto como servidor e cliente, na janela de aplicação do Wireshark® pode-se observar diversas linhas percorrendo a tela, montando o *frame* savPDU, conforme mostrada na Figura 37.

Figura 37 – Captura de pacotes no Wireshark



Fonte: Produção do próprio autor

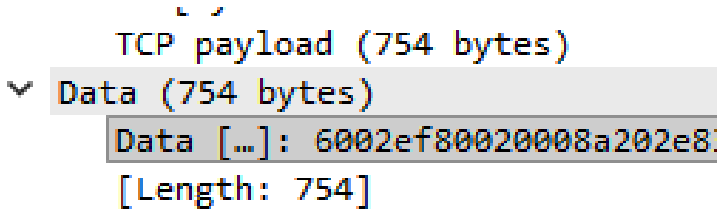
Para verificar os *frames* que contém as informações da SAMU, filtrou-se o IP Host Local (127.0.0.1) da máquina usada no processo de *loopback*, também indicada na Figura 37, que é um endereço de IP especial amplamente usado para testar a funcionalidade da pilha de protocolos de rede em um dispositivo. A simulação foi feita

no 127.0.0.1 porque durante o experimento prático realizado de forma online, não foi possível conectar o dispositivo computacional com o servidor EDSIM, localizado em rede externa e fora do domínio, para transmissão de dados do SAMU. Vale ressaltar que nessa simulação, usando o endereço de *loopback*, os pacotes de dados não são transmitidos pela rede física, e sim processados internamente pelo sistema operacional. Além disso, esse endereço de *loopback* não pode ser roteado na internet, ou seja, qualquer pacote enviado para esse endereço não sai do dispositivo.

Nessa captura de pacotes, pode-se confirmar que o IP *local host* da máquina usada, 127.0.0.1, realmente está atuando tanto na transmissão dos pacotes de dados quanto no recebimento (*Source*/*Destination*), visto que foi configurada anteriormente no programa SAMU que o equipamento é tanto cliente quanto servidor. Além disso, consegue-se visualizar que a porta usada para transmissão dos dados (Port src) é a porta 1133, enquanto a porta de destino que recebe os dados (Port dst) é a 49985.

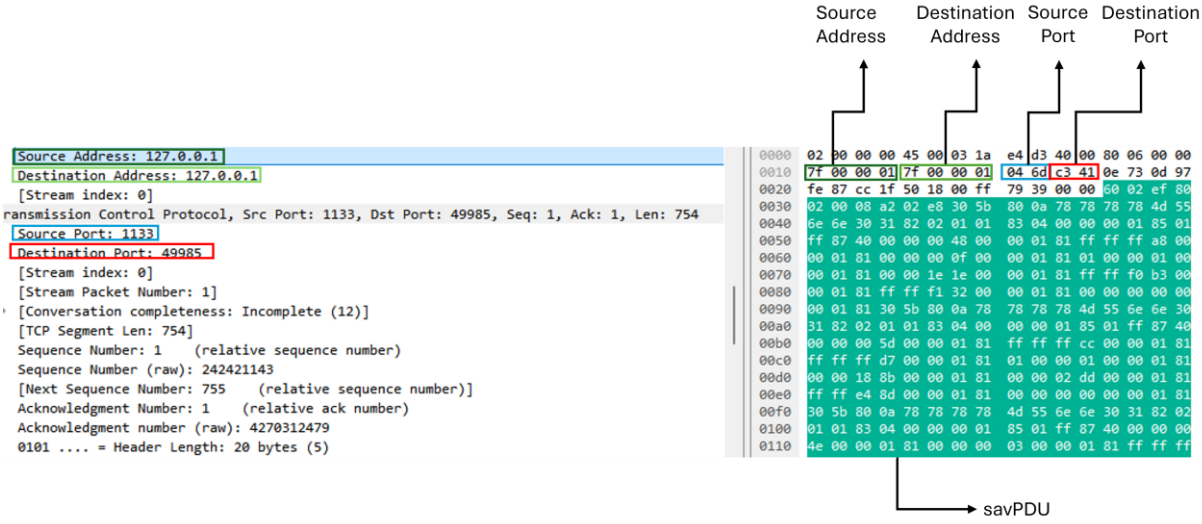
Além disso, no painel inferior à esquerda que contém todas as informações da captura de pacotes é possível verificar o tamanho total do *frame*, indicando 798 bytes. Nesses 798 bytes, o tamanho (*length*) do savPDU (*payload*) encapsulado pelo protocolo TCP é de 754 bytes, enquanto o restante dos bytes foi usado para indicar o cabeçalho do protocolo utilizado, o endereço de destino (*destination*) e origem (*source*), a porta de destino (*source port*) e a porta de origem (*source port*), o tempo de vida do pacote até ocorrer uma nova transmissão (*Time to Live/ TimeAllowedtoLive*) e entre outras informações. Na Figura 38, é mostrado o TCP responsável por encapsular os dados e transferir os pacotes, enquanto na Figura 39 são mostrados mais detalhes em relação à transferência desses pacotes e o conteúdo do *frame* em bytes.

Figura 38 – Imagem detalhada do TCP Payload



Fonte: Produção do próprio autor

Figura 39 – Relação dos bytes com a descrição do *frame*



Fonte: Produção do próprio autor

Enquanto no campo de informações inferior à esquerda do Wireshark® indica claramente as informações em valor decimal, a janela de aplicação mostra a captura do tráfego em hexadecimal.

Fazendo a conversão de alguns dados do cabeçalho, pode-se confirmar as seguintes informações:

Tabela 1 – Conversão dos bytes dos endereços e portas de destino/origem

Descrição	Decimal	Hexadecimal
Source Address	127.0.0.1	7f 00 00 01
Destination Address	127.0.0.1	7f 00 00 01
Src Port	1133	04 6d
Dst Port	49985	c3 41

Fonte: Produção do próprio autor

Outra informação interessante de notar é que a alternância entre 798 (PSH, ACK) e 44 (ACK) no comprimento do quadro indica que no primeiro o *frame* contém tanto dados *payload* quanto confirmação do recebimento, indicando a transmissão contínua dos dados e a confirmação simultânea, enquanto o ACK é um pacote sem dados, apenas de confirmação. Esse esquema de comunicação é usado para quando o remetente deseja garantir que a aplicação no destino processe os dados sem atraso (muito importante para mensagens críticas como GOOSE).

Na etapa seguinte, foi feita a identificação e decodificação dos bytes capturados que contém no quadro savPDU. Para isso, todos os bytes foram comparados com a estrutura ASN.1 no *framework* APDU, conforme foi visto anteriormente na Figura 26. As Tabelas 2, 3 e 4 apresentam a separação do cabeçalho, comprimento dos dados e valores, e seus respectivos campos da APDU.

Tabela 2 – Decodificação dos *frames* capturados

Hexadecimal	Comprimento	IEC 61850-9-2
60 02 ef	02 ef	savPdu
80 02 00 08	02 00	noASDU
a2 02 e8	02 e8	asdu
30 5b	5b	Sequence of ASDU

Fonte: Produção do próprio autor

Tabela 3 – Cabeçalho do ASDU

Hexadecimal	Comprimento	Valores	IEC 61850-9-2
80 0a 78 78 78 4d 55 6e 6e 30 31	0a	78 78 78 4d 55 6e 6e 30 31	svID
82 02 01 01	02	01 01	smpCnt
83 04 00 00 00 01	04	00 00 00 01	confRev
85 01 ff	01	Ff	smpSynch
87 40	40	Vide Tabela (4)	Sequence of Data

Fonte: Produção do próprio autor

Tabela 4 – Valores do cabeçalho do Sequence of Data ASDU1

Conjunto de dados	Hexadecimal	Binário
TCTR1.Amp.instMag	00 00 00 48	00000000 00000000 00000000 01001000
TCTR1.Amp.q	00 00 01 81	00000000 00000000 00000001 10000001
TCTR2.Amp.instMag	ff ff ff a8	11111111 11111111 11111111 10101000
TCTR2.Amp.q	00 00 01 81	00000000 00000000 00000001 10000001
TCTR3.Amp.instMag	00 00 00 0f	00000000 00000000

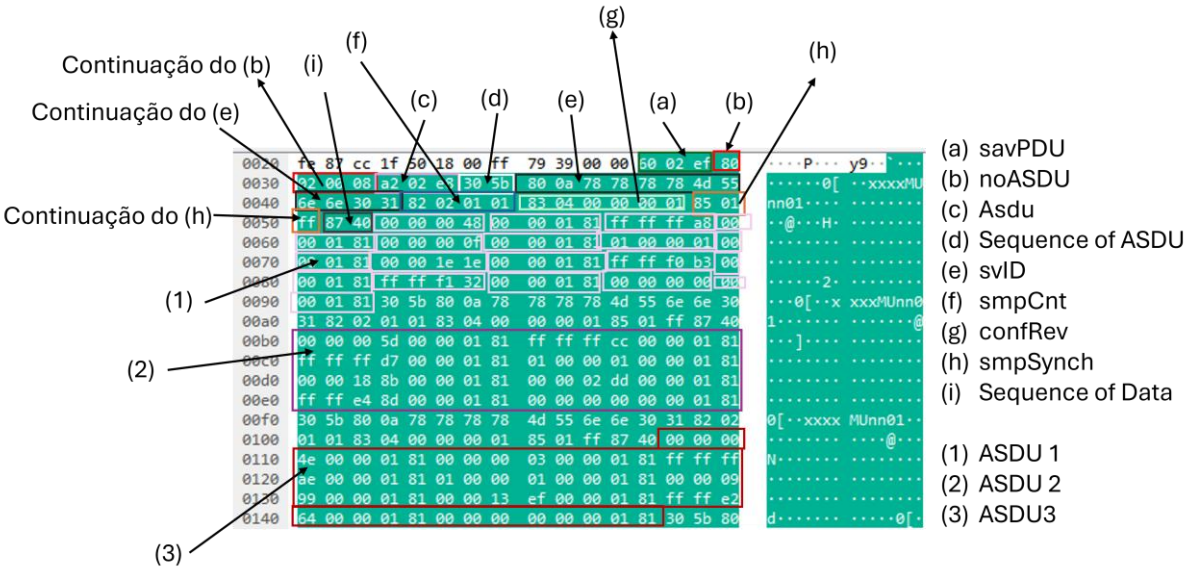
		00000000 00001111
TCTR3.Amp.q	00 00 01 81	00000000 00000000 00000001 10000001
TCTR4.Amp.instMag	01 00 00 01	00000001 00000000 00000000 00000001
TCTR4.Amp.q	00 00 01 81	00000000 00000000 00000001 10000001
TVTR1.Amp.instMag	00 00 1e 1e	00000000 00000000 00011110 00011110
TVTR1.Amp.q	00 00 01 81	00000000 00000000 00000001 10000001
TVTR2.Amp.instMag	ff ff f0 b3	11111111 11111111 11110000 10110011
TVTR2.Amp.q	00 00 01 81	00000000 00000000 00000001 10000001
TVTR3.Amp.instMag	ff ff f1 32	11111111 11111111 11110001 00110010
TVTR3.Amp.q	00 00 01 81	00000000 00000000 00000001 10000001
TVTR4.Amp.instMag	00 00 00 00	00000000 00000000 00000000 00000000
TVTR4.Amp.q	00 00 01 81	00000000 00000000 00000001 10000001

Fonte: Produção do próprio autor

Infelizmente, não foi possível realizar a conversão dos valores de tensão e corrente em magnitude instantânea para valor decimal, pois dependem da norma

IEC 60044-8, um documento à parte fora do escopo do presente trabalho. É mostrada na Figura 40, de forma mais detalhada, onde cada dado do savPDU se encontra no Wireshark®.

Figura 40 – Detalhes da identificação dos campos dos dados do savPDU



Fonte: Produção do próprio autor

Além disso, é possível notar que o ciclo da ASDU que coleta os valores de corrente e tensão se repete, pois o número de ASDUs concatenados equivale a 8, conforme indicada na Tabela 2, na segunda linha da primeira coluna, destacada em azul. Na Figura 40, no print, somente foi possível destacar 3, mas rolando nas linhas para baixo, aparece o restante dos dados que totaliza as 8 ASDUs.

Durante a simulação, não foi possível a coleta de mensagens GOOSE, pois o código XML que descreve a SAMU, no bloco *ClientServices*, referente aos serviços de GOOSE, assim como GSSE, e *Report*, não está habilitada no servidor IEC 61850 para ser utilizado pelos clientes. Isso pode ser identificado no bloco do código abaixo indicando “false”.

```
!-- IEC 61850 Server -->
<cim:IEC61850Server rdf:ID="_ID_1005">
   <cim:IdentifiedObject.aliasName/>
   <cim:IdentifiedObject.description/>
   <cim:IdentifiedObject.mRID/>
   <cim:IdentifiedObject.name/>
```

<cim:IEC61850Server.IEC61850ClientServices.goose>false</cim:IEC61850Server.IEC61850ClientServices.goose>
<cim:IEC61850Server.IEC61850ClientServices.gsse>false</cim:IEC61850Server.IEC61850ClientServices.gsse>
<cim:IEC61850Server.IEC61850ClientServices.bufReport>false</cim:IEC61850Server.IEC61850ClientServices.bufReport>
<cim:IEC61850Server.IEC61850ClientServices.unbufReport>false</cim:IEC61850Server.IEC61850ClientServices.unbufReport>
<cim:IEC61850Server.IEC61850ClientServices.readLog>false</cim:IEC61850Server.IEC61850ClientServices.readLog>

Portanto, esse dispositivo não aceita requisições ou não fornece funcionalidades relacionadas aos serviços GOOSE. Para ativá-lo, seria necessário alterar a configuração do IED ou do arquivo SCL (*System Configuration Language*) para “true” e garantir suporte no *firmware* do dispositivo.

Além disso, esse programa SAMU não possui uma interface que permite simular a alteração dos valores de estado para avaliar o comportamento de envio das mensagens GOOSE, visto que elas trabalham com uma mudança de evento, como sinal de disparo ou abertura de um disjuntor. No entanto, devido às mensagens GOOSE terem uma estrutura *frame* semelhante à das *Sampled Values*, logo o estudo se torna válido, com o pequeno detalhe que o *frame* da GOOSE começa com 0x61, em vez de 0x60.

5 CONCLUSÃO

Após realizar o trabalho, constatou-se que a digitalização das subestações, aliada à norma IEC 61850, é essencial para garantir interoperabilidade entre dispositivos e aumentar a confiabilidade do sistema elétrico. Ao longo do trabalho, foram abordados conceitos fundamentais como arquitetura SAS, protocolos de comunicação, modelo OSI, serviços definidos pela IEC 61850 e a topologia e redundância de redes, permitindo compreender a estrutura de troca de informações em ambientes críticos.

No estudo prático, a simulação com o emulador SAMU e a análise via Wireshark® confirmaram a conformidade das mensagens *Sampled Values* com a estrutura T-L-V e codificação BER, validando a viabilidade da comunicação baseada em Ethernet para substituir cabeamento físico e otimizar a operação. Essa abordagem mostrou potencial para reduzir complexidade, aumentar flexibilidade e atender aos requisitos de tempo real exigidos pela norma.

Embora não tenha sido possível estudar de forma experimental o comportamento das mensagens GOOSE devido à ausência de interface para simular a mudança de eventos no SAMU, verificou-se que sua estrutura *frame* APDU segue princípios semelhantes aos das SVs, indicando potencial para aplicações futuras.

Portanto, esse trabalho contribui para o estudo e modernização do setor elétrico, alinhando-se às tendências de automação, reforçando a relevância da IEC 61850 para a segurança, interoperatividade e confiabilidade nas subestações.

REFERÊNCIAS

A3A ENGENHARIA DE SISTEMAS. **Topologia de Rede:** tipos e aplicações em Redes de Telecomunicações. Disponível em: < https://a3aengenharia.com.br/conteudo/artigos-tecnicos/topologia-de-rede/>. Acesso em: 15 nov. 2025.

ABB. **REX640 IEC 61850 Engineering Guide**. 2023. Disponível em: <https://library.e.abb.com/public/2f6ec5cba04b4481975e930b8b075318/REX640_iec61850eng_759116_ENc.pdf?x-sign=7uEhJILNrugM38zqglyWjoopFBlRXOsD%2BCNEwY%2Bky6rIBIGqpcFGvVXTHJAc7Lu0>. Acesso em: 20 ago. 2025.

ALENCAR, Márcio Aurélio dos Santos. **Fundamentos de redes de computadores**. Manaus: Universidade Federal do Amazonas; CETAM, 2010. 47 p.

ANEEL. **Curso EAD: Fundamentos do Setor Elétrico**. Disponível em: <https://ead.aneel.gov.br/ava-aneel-ws/instituicao/aid/conteudo/modulo/12/mod4/uni1/slide05.html>. Acesso em: 10 nov. 2025.

CONPROVE. **Cliente – Servidor IEC 61850:** Comunicação MMS para Supervisão e Controle no Setor Elétrico. Disponível em <https://conprove.com/cliente-servidor-iec-61850-comunicacao-mms-para-supervisao-e-controle-no-setor-eletrico/?srsltid=AfmBOop6jD5HiLEzo2RzrjvWQMkZC-xQbZPkCapvvP-aw-E7IunI0BN9>. Acesso em: 02 out. 2025.

CONPROVE. **Merging Units Testing**. Disponível em:<https://conprove.com/en/power-system-communication-testing/merging-units-testing/?srsltid=AfmBOoqkE4zcpvWfvPT9DoMRa98AISu7tv5zvQM2PIx3tUMBDGwnw1KQ>. Acesso em: 21 set. 2025.

EATON. **Industrial communication protocols explained** | Eaton PSEC [S.l.]:

YouTube, 2025. 1 vídeo (12 min). Disponível em: <www.youtube.com.>. Acesso em: 04 ago. 2025.

FERNANDES C.; BORKAR S.; GOHIL J. **Testing of Goose Protocol of IEC61850 Standard in Protection IED**. *International Journal of Computer Applications*, 2014. ISSN 0975-8887.

FERNÁNDEZ M. P. **Rede de Computadores**. 2. ed. Fortaleza, CE: EduECE, 2015.

FRONTIN S.O. **Equipamentos de Alta Tensão:** Prospecção e Hierarquização de Inovações Tecnológicas. Brasília 2013. 1. ed.

IBM. **O que é topologia de rede?** Disponível em: <https://www.ibm.com/br-pt/think/topics/network-topology>. Acesso em: 18 nov. 2025.

IEC 61850-6. **Communication networks and systems in substations – Part-6: Configuration description language for communication in electrical substations related to IEDs**. 1. ed. 2004.

IEC 61850-7-4. **Communication networks and systems in substations – Part-7-4: Basic Communication Structure for Substation and feeder equipment – Compatible Logical Node Classes and Data Classes**. 1. ed. 2003.

IEC 61850-8-1. **Communication networks and systems in substations – Part-8-1: Specific Communication Service Mapping (SCSM) - Mappings to MMS (ISO 9506-1 and ISO 9506-2) and to ISO/IEC 8802-3**. 1. ed. 2004.

IEC 61850-9-2. **Communication networks and systems in substations – Part-9-2: Specific Communication Service Mapping (SCSM) - Sampled Values over ISO/IEC 8802-3. 1**. ed. 2004.

IEC/TR 61850-90-4. **Technical Report. Communication networks and systems for power utility automation – Part 90-4: Network engineering guidelines**. 1. ed. 2013

JARDINI J.A.; MENDES M. F. **História da Automação Elétrica e Estado da Arte**. THE 8th LATIN-AMERICAN CONGRESS ON ELECTRICITY GENERATION AND TRANSMISSION - CLAGTEE 2009.

LEITE J.B.; REIZ C. **Hardware-In-the-Loop Simulation to Test Advanced Automation Devices in Power Distribution Networks**. IEEE TRANSACTIONS ON POWER DELIVERY,VOL.36, NO.4, ago 2021.

MACHADO H. A. **Análise de impacto e desempenho do barramento de processos em uma subestação à luz da norma IEC 61850** / Hugo Araújo Machado. -- Ilha Solteira: [s.n.], 2023.

MACKIEWICZ. R.E. **Overview of IEC 61850 and Benefits**. IEEE Explore, 2006.

MAIA L. P. **Arquitetura de redes de computadores**. 2. ed. Rio de Janeiro: LTC, 2013. ISBN 978-85-216-2435-6.

MAMEDE F. J. **Instalações elétricas industriais**. 9. ed. Rio de Janeiro: LTC, 2016.

MATHWORKS. **What Is Hardware-in-the-Loop (HIL)?** Disponível em: <https://www.mathworks.com/discovery/hardware-in-the-loop-hil.html>. Acesso em: 06 out. 2025.

MESH ENGENHARIA. **IED's em Subestações**. Disponível em: <https://meshengenharia.com/2023/05/30/ieds-em-subestacoes/>. Acesso em: 16 nov. 2025.

METRUM. **A importância dos Sistemas de Proteção e Controle e dos IED**. Disponível em: <https://memt.com.br/a-importancia-dos-sistemas-de-protecao-e-controle-e-dos-ied/> Acesso em: 05 set. 2025.

REIS A. N. **Análise da Norma IEC 61850 Em Sistemas de Automação de Subestações e Proteção de Sistemas Elétricos**. CEFET-MG, 2023.

SECBITREZ. **Topologia de Redes**. Disponível em: <https://secbitrez.wordpress.com/2018/10/01/topologias-de-redes/>. Acesso em: 15 nov. 2025.

SENAI. Departamento Nacional. **Arquitetura de redes / Serviço Nacional de Aprendizagem Industrial**. Departamento Nacional, Serviço Nacional de Aprendizagem Industrial. Departamento Regional de Santa Catarina. Brasília : SENAI/DN, 2012. 183 p. il. (Série Tecnologia da informação - Hardware).

SIEMENS. **IEC 61850 Parte 1 – Introdução – Rev C**.pdf. 2010.

SILVEIRA M. G; FRANCO P. H. **Segurança Cibernética em Redes IEC 61850: Como Mitigar Vulnerabilidades Das Mensagens GOOSE**. Schweitzer Engineering Laboratories, Inc., 2021. Disponível em:< https://selinc.com/api/download/134469/?lang=pt>. Acesso em: 12 nov. 2025.

SKENDZIC, V.; ENDER, I.; ZWEIGLE, G. **IEC 61850-9-2 Process Bus and Its Impact on Power System Protection and Control Reliability**. Washington: Schweitzer Engineering Laboratories, Inc., 2007.

SMITH, T. **IEC 61850 in the Modern Substation**. YouTube, 2025. Disponível em: <https://www.youtube.com/watch?v=p3gf-ErGcBs>. Acesso em: 02 ago. 2025.

SONG E.Y; LEE K.B; FITZPATRICK G.J.; ZHANG Y. **Interoperability Test for IEC 61850-9-2 Standard-based Merging Units**. IEEE Explore, 2017.

SOUZA, A. M. **Estudo e aplicação da norma IEC61850 em automação de subestações**. Universidade Estadual Paulista (Unesp), 2021.

TECNOBLOG. **O que é TCP/IP? Saiba como funcionam os protocolos de comunicação da internet**. Disponível em: < https://tecnoblog.net/responde/o-que-e-tcp-ip/>. Acesso em: 20 ago. 2025.

WEG. **Sistema de Proteção, Controle e Supervisão de Subestações (SPCS) e Telecomunicações**. Disponível em <https://www.weg.net/catalog/weg/BR/pt/Gera%C3%A7%C3%A3o%2C-Transmiss%C3%A3o-e-Distribui%C3%A7%C3%A3o/Subesta%C3%A7%C3%B5es/Sistemas-de-Prote%C3%A7%C3%A3o%2C-Controle-e-Supervis%C3%A3o-de-Subesta%C3%A7%C3%B5es-%26-Telecomunica%C3%A7%C3%B5es/Sistema-de-Prote%C3%A7%C3%A3o%2C-Controle-e-Supervis%C3%A3o-de-Subesta%C3%A7%C3%B5es-%28SPCS%29-e-Telecomunica%C3%A7%C3%B5es/p/MKT_WTD_SPCS>. Acesso em: 10 out. 2025.

ZANCAN M.D. **Controladores Programáveis**. Universidade Federal de Santa Maria: Colégio Técnico Industrial de Santa Maria, 2011.