

LEONARDO GALO ASSIS CARDOSO FUMIÃ

Estudo da norma IEC 61850 - *Communication Network and System in Substations*

Trabalho de conclusão de curso apresentado ao Departamento de Engenharia Elétrica do Centro de Ciências Exatas e Tecnológicas da Universidade Federal de Viçosa, para a obtenção dos créditos da disciplina ELT 402 – Projeto de Engenharia II - e cumprimento do requisito parcial para obtenção do grau de Bacharel em Engenharia Elétrica.

Aprovada em 07 de julho de 2026.

COMISSÃO EXAMINADORA

Documento assinado digitalmente
 JOSE CARLOS DA COSTA CAMPOS
Data: 08/07/2026 10:23:27-0300
Verifique em <https://validar.iti.gov.br>

Prof. Dr. José Carlos da Costa Campos - Orientador
Universidade Federal de Viçosa

Documento assinado digitalmente
 JOSE TARCISIO DE RESENDE
Data: 08/07/2026 11:17:13-0300
Verifique em <https://validar.iti.gov.br>

Prof. Dr. José Tarcísio de Resende - Membro
Universidade Federal de Viçosa

Documento assinado digitalmente
 DIOGO XAVIER SCHMITT
Data: 08/07/2026 14:17:48-0300
Verifique em <https://validar.iti.gov.br>

Diogo Xavier Schmitt - Membro
WEG

Estudo da norma IEC61850 - *Communication Network and System in Substations*

Leonardo Galo Assis Cardoso Fumiã; José Carlos da Costa Campos

Departamento de Engenharia Elétrica,

Universidade Federal de Viçosa, Viçosa - MG Email: leonardo.g.cardoso@ufv.br; josec.campos@ufv.br

Resumo—An overview of the application of the IEC 61850 standard in power substations, highlighting its importance for interoperability among IEDs, standardization of communication, and the evolution of conventional substations toward digital architectures. The article covers the main components of a substation, the role of protection relays, the MMS, GOOSE, and Sampled Values protocols, as well as the standard's applications in automation, protection, supervision, and process buses. It also discusses cybersecurity aspects in digital substations, particularly as they relate to IEC 62351, IEC 62443, and the protection of critical communications.

Resumo—Este artigo apresenta uma revisão sobre a aplicação da norma IEC 61850 em subestações de energia, destacando sua importância para a interoperabilidade entre IEDs, padronização da comunicação e evolução das subestações convencionais para arquiteturas digitais. São abordados os principais elementos de uma subestação, o papel dos relés de proteção, os protocolos MMS, GOOSE e Sampled Values, além das aplicações da norma em automação, proteção, supervisão e barramento de processo. Também são discutidos aspectos de cibersegurança em subestações digitais, especialmente relacionados à IEC 62351, IEC 62443 e proteção das comunicações críticas.

Palavras-chave: IEC 61850; subestações digitais; relés de proteção; GOOSE; Sampled Values; cibersegurança.

I. INTRODUÇÃO

Com a crescente demanda por energia elétrica, que nos últimos anos tem sido impulsionada principalmente pelo aumento da frota de carros elétricos e pela disparada do uso de inteligência artificial generativa, que demanda de grandes estruturas de data centers para o seu funcionamento/manutenção. Estima-se que somente nos Estados Unidos a energia destinada a exclusivamente para IA poderá chegar a 326 terawatts-hora por ano, energia essa que seria suficiente para abastecer 22% dos lares americanos [1]. Estima-se ainda que até 2030 o consumo mundial de energia por data centers para uso em IA deve chegar ao patamar de 945 TWh representando cerca de 3% de todo o consumo de energia do globo [2].

Toda essa demanda por energia exigirá uma grande robustez do sistema elétrico de potência para viabilizar uma entrega de energia constante e de qualidade [3], [4], mas acima de tudo que este sistema seja capaz de suportar a demanda, mas também que esteja protegido na ocorrência de algum distúrbio em algum ponto do sistema. Além do aumento da demanda por energia elétrica, é observado um grande aumento na geração distribuída, em que o principal protagonista é a geração de energia através de módulos fotovoltaicos que tem ganhado destaque,

principalmente pelo apelo ecológico e payback de curto prazo proporcionando um retorno financeiro convidativo [5]. Apesar de todas as vantagens associadas, a geração de energia elétrica nos chamados micro grids pode causar problemas no sistema elétrico de energia devido a picos de geração de energia injetando no sistema uma quantidade de energia maior do que a demandada [6]–[8], podendo gerar sobretensões em momentos onde a demanda é menor do que a potência no sistema e também acima da capacidade do sistema o que pode causar apagões no sistema. O uso de equipamentos inteligentes no sistema de proteção do sistema elétrico de energia é de extrema importância, para evitar apagões e danos aos equipamentos conectados ao SE [9]–[11].

Na Figura 1, pode-se notar a complexidade do SE, que conta com geração distribuída, diferentes fontes de geração e estações de recarga de veículos além das tradicionais cargas presentes no SE. A Figura 1 apresenta ainda a evolução das subestações convencionais para as subestações digitais, o que apresenta também novos desafios ao setor.

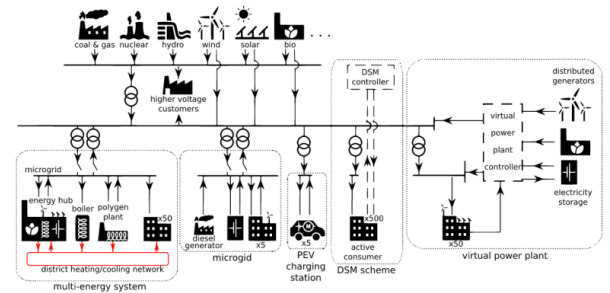


Figura 1. Arquitetura conceitual de uma rede elétrica inteligente com integração de recursos energéticos distribuídos. [12]

Considerando a relevância da energia elétrica para a sociedade e para os processos produtivos, os sistemas de transmissão e distribuição devem ser projetados com elevado grau de robustez e confiabilidade. Nesse sentido a coordenação e a seletividade dos dispositivos de proteção são fundamentais para garantir que, diante de distúrbios elétricos, os equipamentos de proteção do sistema atuem localmente, desconectando apenas a região de ocorrência do distúrbio e que o tempo de atuação seja rápido o suficiente para evitar que os equipamentos conectados a rede sofram danos, minimizando impactos sobre o restante

do sistema [9], [11], [13].

Tratando-se de proteção do sistema de energia, um dos elementos mais importantes para garantir a proteção, seletividade e robustez do sistema é o relé de proteção, conhecido também como o “cérebro” do sistema de proteção em subestações por concentrar o monitoramento de eventos caóticos para o sistema e ser responsável pela execução da lógica de proteção [9], [14], [15]. O relé de proteção é então um equipamento crítico dentro do SE. Dada a sua importância na transmissão e distribuição de energia, é imprescindível que este equipamento atenda a certos padrões de segurança e de operabilidade. Então já que o relé de proteção coordenará a proteção do sistema ele deverá se comunicar com os demais dispositivos de forma eficiente [16]–[18]. Porém, é natural dentro dos sistemas de energia que tenhamos dispositivos de fabricantes diferentes o que pode dificultar a integração destes dispositivos, uma vez que cada fabricante terá protocolos proprietários, que por serem produzidos por marcas distintas certamente terão padrões de comunicação diferentes um dos outros com lógicas de programação completamente distintas, portanto para realizar uma integração destes dispositivos seria necessário um conhecimento profundo do funcionamento e construção lógica dos *firmwares* de todos os equipamentos.

Com o intuito de padronizar e garantir a interoperabilidade de equipamentos de diferentes fabricantes a *International Electrotechnical Commission* (IEC) desenvolveu a norma IEC 61850, que tem como principal objetivo padronizar a comunicação e definir os protocolos e nós lógicos utilizados nos Sistemas de Energia, fornecendo um mesmo padrão de comunicação o que garante a interoperabilidade entre os *Intelligent Electronic Device* (IED’s).

II. SUBESTAÇÕES DE ENERGIA

As subestações de energia elétrica são instalações fundamentais nos sistemas elétricos de potência, pois realizam a interligação entre diferentes níveis de tensão, permitem o seccionamento de circuitos, viabilizam o controle do fluxo de energia e concentram funções de proteção, supervisão, controle e automação. As subestações podem estar associadas aos sistemas de geração, transmissão, subtransmissão ou distribuição, sendo projetada de acordo com sua função no sistema: Ajuste de tensão, arranjo de barramento, potência instalada e requisitos de confiabilidade operacional [9], [15].

O funcionamento básico de uma subestação consiste em receber energia elétrica por meio de linhas ou alimentadores, adequar seus níveis de tensão quando necessário, controlar sua distribuição entre diferentes circuitos e proteger os equipamentos contra condições anormais de operação. Para isso, a subestação é composta por equipamentos primários, diretamente conectados ao circuito de potência, e equipamentos secundários, responsáveis pelas funções de medição, proteção, controle, supervisão e comunicação [9], [14].

A. Equipamentos Primários

Os equipamentos primários incluem as linhas de entrada e saída, barramentos, disjuntores, chaves seccionadoras, transformadores de potência, transformadores para instrumentos, para-raios, bancos de capacitores, reatores e o sistema de aterramento. As linhas ou alimentadores são responsáveis pela conexão da subestação ao restante do sistema elétrico, permitindo a entrada ou saída de energia. Os barramentos constituem pontos comuns de conexão entre os circuitos, possibilitando diferentes configurações operativas e permitindo flexibilidade para manobras, manutenção e contingências. Dependendo da importância da subestação, podem ser utilizados arranjos como barra simples, barra dupla, barra principal e transferência, anel ou disjuntor e meio [9].

Os disjuntores são os principais equipamentos de manobra sob carga e sob condição de falta. Sua função é interromper correntes normais de operação e correntes de curto-circuito, sempre que comandados pelo sistema de proteção ou pelo sistema de controle. Em uma condição anormal de operação, o disjuntor deve atuar rapidamente para isolar o trecho afetado, evitando a propagação do distúrbio e reduzindo os danos térmicos, mecânicos e dielétricos aos equipamentos conectados ao sistema. As chaves seccionadoras, por sua vez, são utilizadas para isolar trechos do circuito, normalmente sem capacidade de interrupção de corrente de carga ou de curto-circuito, sendo aplicadas principalmente em procedimentos de manutenção e recomposição operacional [11], [15].

O transformador de potência é um dos principais componentes da subestação, pois permite a elevação ou redução do nível de tensão entre diferentes partes do sistema elétrico. Em subestações elevadoras, localizadas próximas às usinas geradoras, os transformadores elevam a tensão para reduzir perdas na transmissão. Em subestações abaidadoras, presentes nos sistemas de transmissão e distribuição, os transformadores reduzem a tensão para níveis adequados ao atendimento das cargas. Devido ao seu elevado custo e importância operacional, o transformador de potência é normalmente protegido por funções específicas, como proteção diferencial, proteção de sobrecorrente, proteção de sobretemperatura, proteção contra sobrepressão e proteção de gás em transformadores imersos em óleo [9], [15].

Os transformadores para instrumentos são responsáveis por adequar as grandezas elétricas do sistema de potência aos níveis compatíveis com os equipamentos de medição, proteção e controle. Os transformadores de corrente, conhecidos como TC’s, fornecem ao sistema secundário correntes proporcionais às correntes primárias, enquanto os transformadores de potencial, ou TP’s, fornecem tensões proporcionais às tensões do sistema. Esses equipamentos permitem que os relés de proteção e os medidores operem com sinais padronizados e isolados eletricamente do circuito de alta tensão [9], [14].

Além desses elementos, as subestações contam com para-raios, responsáveis pela proteção contra sobretensões transitórias originadas por descargas atmosféricas ou manobras; bancos de capacitores, utilizados para compensação de potência reativa e melhoria do perfil de tensão; reatores, aplicados no controle de sobretensões e limitação de correntes; e sistemas de aterramento, que garantem referência de potencial, segurança às pessoas e caminho adequado para correntes de falta à terra [9].

Os equipamentos secundários são responsáveis por transformar a subestação em um sistema supervisionado, controlável e protegido. Entre eles estão os painéis de proteção e controle, relés de proteção, medidores, registradores, unidades terminais remotas, sistemas supervisórios, fontes auxiliares em corrente contínua e alternada, bancos de baterias, carregadores, redes de comunicação e interfaces homem-máquina. Esses sistemas recebem informações dos equipamentos primários, processam os sinais, executam lógicas de controle e proteção e enviam comandos aos dispositivos de manobra [14], [17].

Na proteção do sistema elétrico, o relé de proteção ocupa posição de destaque, pois é o dispositivo responsável por monitorar continuamente as grandezas elétricas, identificar condições anormais e comandar a atuação dos disjuntores quando necessário. Por essa razão, o relé é frequentemente tratado como o elemento central, do sistema de proteção de uma subestação. Sua operação baseia-se na aquisição de sinais provenientes dos TC's e TP's, no processamento desses sinais por meio de algoritmos de proteção e na comparação dos valores medidos com parâmetros previamente ajustados [14], [15].

III. O RELÉ DE PROTEÇÃO

O relé de proteção merece destaque, uma vez que dentro das subestações este é o principal ator na proteção dos sistemas. Quando ocorre um distúrbio, como curto-circuito, sobrecorrente, subtensão, sobretensão, falta à terra, perda de sincronismo ou desequilíbrio de corrente, o relé avalia a condição do sistema e decide se a atuação é necessária. Caso os critérios de operação sejam atendidos, o relé envia um comando de abertura ao disjuntor (Comando de trip) correspondente, isolando a região defeituosa. Essa atuação deve respeitar os princípios de seletividade, sensibilidade, confiabilidade e rapidez. A seletividade garante que apenas o trecho afetado seja desconectado; a sensibilidade assegura que o relé seja capaz de detectar faltas dentro de sua zona de proteção; a confiabilidade está associada à atuação correta quando requerida e à não atuação indevida; e a rapidez reduz o tempo de exposição dos equipamentos às correntes de falta [9], [11]. Vale destacar que a definição dos limites de atuação serão determinadas a partir do estudo de proteção de cada sistema que deverá ser feito pelo projetista responsável. A Figura 2 exemplifica como o relé de proteção se relaciona com os demais equipamentos dentro do circuito de proteção de uma subestação de média tensão.

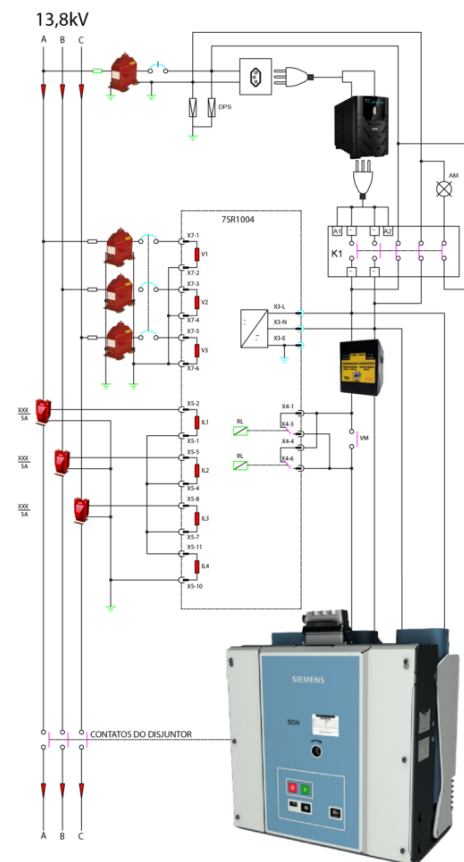


Figura 2. Esquema do sistema de proteção em média tensão. [19]

Os relés modernos, baseados em tecnologia digital e microprocessada, são classificados como Dispositivos Eletrônicos Inteligentes, ou IED's. Diferentemente dos relés eletromecânicos tradicionais, esses equipamentos podem concentrar diversas funções em uma única unidade, como proteção, medição, controle, supervisão, oscilografia, registro de eventos, autodiagnóstico e comunicação com outros dispositivos da subestação. Assim, um único relé de proteção pode executar funções de sobrecorrente, distância, diferencial, religamento automático, falha de disjuntor, supervisão de circuitos de corrente e tensão, além de disponibilizar informações ao sistema supervisório [16], [20].

Com os avanços tecnológicos do mundo moderno, os sistemas tem se tornado cada vez mais conectados e automatizados, nas subestações não é diferente. Com sistemas cada vez mais complexos, a necessidade por sistemas mais robustos e confiáveis, cresce a cada dia, aumentando também a necessidade por sistemas mais automatizados. Com isso a comunicação entre os dispositivos da subestação tornou-se um requisito essencial para a automação moderna. Em arquiteturas convencionais, muitos sinais de intertravamento, comando e supervisão são transmitidos

por cabos de cobre ponto a ponto. Já em subestações digitais, parte significativa dessas informações pode ser transmitida por redes de comunicação, reduzindo cabeamento, ampliando a flexibilidade de engenharia e facilitando a integração com sistemas supervisórios. Neste cenário, surge a necessidade de uma padronização na comunicação entre os IEC's, uma vez que cada fabricante utiliza protocolos proprietário, então a norma IEC 61850 *Communication Network and System in Substations* surge para estabelecer essa padronização [21]–[24].

IV. NORMA IEC 61850 (*Communication Network and System in Substations*)

A IEC 61850 (*Communication Network and System in Substations*) contribui diretamente para o funcionamento das subestações digitais ao padronizar a representação das funções do sistema elétrico por meio de nós lógicos. Isto é, funções associadas a disjuntores, chaves seccionadoras, medições, proteção de sobrecorrente, proteção diferencial e intertravamentos são descritas por modelos padronizados. Além disso, a norma define serviços de comunicação como MMS, GOOSE e Sampled Values. O MMS é utilizado principalmente para supervisão e controle em comunicação cliente-servidor; as mensagens GOOSE são aplicadas em eventos rápidos, como comandos de trip, bloqueios e intertravamentos; e os Sampled Values são utilizados para transmissão de amostras digitalizadas de corrente e tensão, especialmente em arquiteturas com barramento de processo [17], [22].

A norma trata do projeto de digitalização de subestações de energia de forma ampla, descrevendo os requisitos de gerenciamento de sistema e projetos, ferramentas de suporte, ciclo de vida dos IED's (Intelligent electronic devices), define protocolos de comunicação, e ainda toda a estrutura responsável pela comunicação e automação do sistema.

A. Definições

A norma IEC 61850 (*Communication Network and System in Substations*) apresenta conceitos importantes para a modelagem de informação:

- Dispositivo Eletrônico inteligente: Equipamentos que possuam processadores integrados com capacidade de se comunicarem com fontes externas.
- Nó Lógico (LN): Esta é a menor entidade funcional que pode trocar informações. Os LN's agrupam dados com significado semântico alto, como o XCBBR para um disjuntor ou PDIS para proteção de distância;
- Dispositivo Lógico (LD): Uma entidade virtual que agrega vários Nós Lógicos relacionados, sendo sempre implementada dentro de um único IED;
- Interface de Serviço de Comunicação Abstrata (ACSI): Fornece modelos de informação e métodos de modelagem independentes da pilha de protocolos de comunicação utilizada;

- Interoperabilidade: A capacidade de dois ou mais IED's de um ou vários fabricantes trocarem informações e as utilizarem para a execução correta de funções;
- Classes de Dados Comuns (CDC): Estruturas que definem o tipo e a semântica dos atributos de dados (ex: status, medições), promovendo a consistência em todas as definições.
- Processo de Engenharia: Envolve papéis como o engenheiro de requisitos (define o escopo), o projetista (define a arquitetura) e o integrador do sistema (constrói e comissiona o sistema);
- Ferramentas de Engenharia: Ferramentas de especificação, configuração e documentação que utilizam a Linguagem de Descrição de Configuração (SCL) para trocar dados de forma compatível entre fabricantes;
- Classes de Desempenho: Mensagens são categorizadas por tipos, como Mensagens Rápidas (Tipo 1) para funções de proteção, que exigem tempos de transferência extremamente curtos;
- Integridade e Confiabilidade: Define classes de integridade de dados para minimizar erros residuais causados por interferências eletromagnéticas, sendo a Classe 3 a mais alta para mensagens de segurança;
- Merging Units (MU): São IED's que realizam a conversão dos sinais medidos através dos TC's e TP's e faz a comunicação desses dados com os sistemas supervisórios, a Figura 3 apresenta um diagrama de funcionamento de uma merging unit;

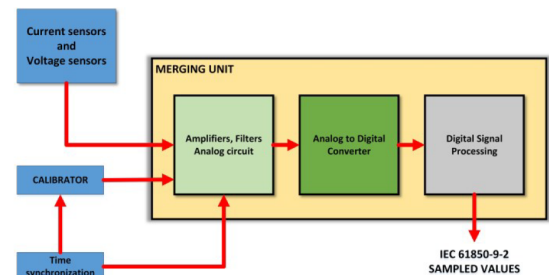


Figura 3. Merging Unit. Fonte [25]

- Process Bus (Barramento de Processo): A norma define este barramento digital para conectar os equipamentos de pátio (nível de processo) aos dispositivos de proteção e controle (nível de baía), eliminando a necessidade de fiação de cobre extensa, a Figura 4 mostra a comunicação através do barramento de processos.

1) *Hierarquias*: A norma IEC61850-5 apresenta a definição de diferentes níveis hierárquicos dentro das subestações de energia: nível de estação, que pode ser entendido como, o sistema supervisório, nível de bay que é onde se encontra cada módulo da subestação e nível de processo onde de fato estão os equipamentos como TC's, TP's, disjuntores, transformadores e demais equipamentos.

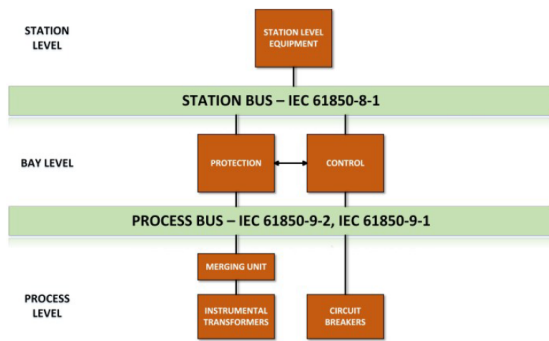


Figura 4. Comunicação pelos barramentos de processos. [25]

Então a comunicação entre os diferentes dispositivos presentes nas SE's pode acontecer verticalmente e horizontalmente. Dizemos que a comunicação se deu de forma vertical quando ela acontece de uma hierarquia para outra e ela se dá horizontalmente quando acontece dentro da mesma hierarquia. A Figura 5 exemplifica o sentido das comunicações dentro e através das hierarquias dentro das subestações.

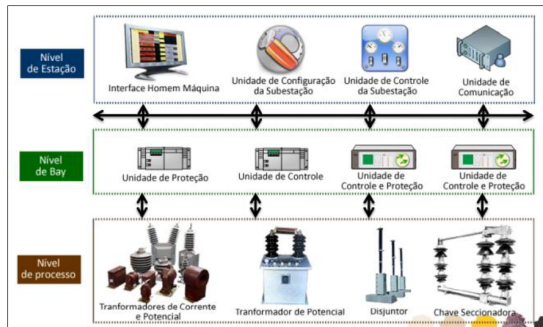


Figura 5. Hierarquias nas subestações automatizadas e seus equipamentos. [26]

Para que a comunicação entre as hierarquias se dê de forma efetiva e na velocidade e qualidade necessária que a aplicação necessita, a norma define padrões de envio de mensagens, que são eles MMS (Manufacturing Message Specification), GOOSE (Generic Object Oriented Substation Event) e SV (Sampled Values), em que cada um dos três padrões será mais adequado para uma troca específica de informação de acordo com cada aplicação.

B. Protocolos de comunicação

1) *Manufacturing Message Specification - MMS*: São mensagens destinadas a um endereço específico de rede que por utilizar o modelo de referência ISO/OSI, tornam a informação carregada pela mensagem muito confiável. Este mecanismo é mais adequado para aplicações em que o tempo de resposta pode ser mais lento, este pode ser utilizado por exemplo na comunicação com o sistema supervisorio

2) *Generic Object Oriented Substation Event - GOOSE e Sampled Values*: As mensagens GOOSE e SV, são transmitidas em alta velocidade, tipo raw Ethernet multicast, as mensagens GOOSE carregam a informação de atuação das proteções e mudanças de estado digital, essas mensagens no entanto não possuem mecanismos para verificação de erros, portanto vários pacotes são gerados até que se tenha a confirmação do recebimento. Já o protocolo SV transporta as leituras analógicas digitalizadas da subestação.

3) Aplicações:

- As mensagens GOOSE são utilizadas para envio rápido de eventos entre IEDs, principalmente em aplicações de proteção, intertravamento, bloqueio, alarme e comando de trip. A IEC 61850-7-1 define o serviço GSE/GOOSE como um mecanismo de distribuição rápida e confiável de dados em todo o sistema, permitindo troca peer-to-peer de informações de estado binário entre IEDs; a mensagem GOOSE transporta dados organizados em um DataSet. Ou seja as mensagens GOOSE é orientada a eventos. Isso significa que ela é enviada imediatamente quando ocorre uma alteração em algum dado do DataSet, como uma partida de proteção, um trip, um bloqueio ou uma mudança de posição de disjuntor. Como a GOOSE é mapeada diretamente na camada Ethernet, ela não utiliza TCP/IP para confirmação de entrega. A confiabilidade é obtida por retransmissões sucessivas, quando ocorre uma mudança de estado, a mensagem é enviada rapidamente várias vezes, depois, o intervalo entre retransmissões aumenta gradualmente até atingir um intervalo estável. Esse mecanismo permite velocidade na primeira atuação e supervisão contínua da comunicação. Na prática, em uma aplicação de proteção, um relé pode publicar uma mensagem GOOSE com o sinal de trip. Os IEDs assinantes recebem esse sinal e podem comandar disjuntores, bloquear religamento, iniciar oscilografia ou executar intertravamentos.
- As mensagens Sampled Values — SV são utilizadas para transportar amostras digitalizadas de grandezas analógicas, principalmente correntes e tensões provenientes de TCs e TP's, normalmente digitalizadas por uma Merging Unit. A IEC 61850-7-1 define a transmissão de valores amostrados como transferência rápida e cíclica de amostras, por exemplo, de transformadores de instrumentos. Enquanto a GOOSE é orientada a eventos, a SV é cíclica e contínua. Ela transmite amostras em alta frequência para que os relés de proteção possam reconstruir as formas de onda de corrente e tensão. A mensagem SV é usada no barramento de processo, substituindo ou reduzindo o cabeamento analógico entre TC's, TP's e relés. Em uma subestação digital, os sinais de corrente e tensão são convertidos para o formato digital por Merging Units e enviados pela rede Ethernet aos IEDs de proteção e medição. A IEC 61850-9-2 também estabelece que os dispositivos emissores de Sampled Values

devem permitir configuração de VID e prioridade, enquanto os dispositivos receptores devem ser capazes de receber mensagens com diferentes valores de VID e prioridade, inclusive mensagens sem informação IEEE 802.1Q.

Pode-se concluir então que a mensagem GOOSE é projetada para transmitir eventos discretos de alta prioridade, como comandos de abertura, bloqueios e permissivos de proteção. Sua confiabilidade é baseada em multicast, prioridade Ethernet, repetição de mensagens e controle por stNum, sqNum e timeAllowedToLive. Já a mensagem Sampled Values é projetada para transmitir continuamente amostras digitais de corrente e tensão. Sua estrutura é baseada em savPdu, ASDU, svID, smpCnt, confRev, smpSynch, smpRate e sequência de dados. Ela é essencial para o barramento de processo em subestações digitais, permitindo que relés recebam grandezas elétricas pela rede em vez de sinais analógicos por cabos convencionais.

Em conjunto, GOOSE e Sampled Values permitem que a subestação digital reduza cabeamento, aumente a interoperabilidade entre IEDs e viabilize funções rápidas de proteção, controle e automação.

4) *Aplicabilidade da norma:* É possível verificar um amplo campo de aplicação da norma uma vez que as definições apresentadas por ela são abrangentes e que os sistemas de comunicação para que os dispositivos eletrônicos operem em conjunto de maneira coordenada, que é o grande foco da norma. Embora tenha sido inicialmente concebida para aplicações em subestações, sua utilização foi progressivamente ampliada para diferentes ambientes do sistema elétrico de potência, incluindo geração, transmissão, distribuição, usinas hidrelétricas, geração distribuída, microgrids e subestações digitais. Sua principal contribuição está na definição de uma arquitetura comum de comunicação entre Dispositivos Eletrônicos Inteligentes, ou IEDs, permitindo interoperabilidade entre equipamentos de diferentes fabricantes por meio de modelos de dados, nós lógicos, serviços de comunicação e linguagem de configuração padronizados [21], [22], [24].

Uma das principais aplicações da IEC 61850 ocorre na automação de subestações. Nesse contexto, a norma permite integrar relés de proteção, controladores de bay, medidores, unidades de aquisição, sistemas supervisórios, gateways e interfaces homem-máquina em uma arquitetura comum de comunicação. A norma estrutura as funções da subestação em dispositivos físicos, dispositivos lógicos, nós lógicos, objetos de dados e atributos de dados, permitindo que funções como proteção, controle, medição, supervisão e intertravamento sejam representadas de forma padronizada. Dessa maneira, a subestação deixa de depender exclusivamente de sinais cabeados ponto a ponto e passa a utilizar uma rede de comunicação capaz de transportar informações operacionais, comandos, alarmes e eventos entre os diferentes IED's [16], [22], [23].

No campo da proteção de sistemas elétricos, a IEC 61850 é aplicada na troca rápida de informações entre

relés e demais dispositivos da subestação. Por meio das mensagens GOOSE, é possível transmitir sinais de trip, bloqueio, intertravamento, permissivos, falha de disjuntor e outras informações críticas com elevada velocidade. Essas mensagens utilizam o modelo publicador/assinante, no qual um IED publica uma informação na rede e os demais dispositivos interessados recebem essa informação para execução de suas lógicas locais. Essa aplicação é particularmente relevante em esquemas de proteção distribuída, nos quais a atuação correta depende da comunicação rápida entre dispositivos instalados em diferentes posições da subestação [16], [17], [20].

Outra aplicação relevante está relacionada ao controle e intertravamento de equipamentos primários. A IEC 61850 permite representar chaves seccionadoras, disjuntores, transformadores, bancos de capacitores e demais equipamentos por meio de nós lógicos específicos. Com isso, comandos de abertura, fechamento, bloqueio, supervisão de posição e permissivos operacionais podem ser integrados aos sistemas de automação. Essa estrutura reduz ambiguidades de engenharia e facilita a implementação de lógicas de controle, uma vez que os dados possuem semântica padronizada. Por exemplo, a posição de um disjuntor pode ser representada por um objeto de dado associado ao nó lógico correspondente, permitindo que diferentes dispositivos interpretem corretamente o mesmo sinal [23], [27].

A norma também possui aplicação direta na medição e supervisão de grandezas elétricas. Por meio de nós lógicos de medição, como aqueles associados a correntes, tensões, potências, frequência e qualidade de energia, os IED's podem disponibilizar informações ao sistema supervisório e a outros dispositivos da subestação. Essas informações podem ser utilizadas para operação em tempo real, registro de eventos, análise pós-falta, diagnóstico de equipamentos e manutenção preditiva. Dessa forma, a IEC 61850 contribui para uma supervisão mais integrada e detalhada do estado operativo do sistema elétrico [22], [23].

Nas subestações digitais, uma das aplicações mais importantes da IEC 61850 está no barramento de processo. Nesse tipo de arquitetura, os sinais analógicos provenientes de transformadores de corrente e transformadores de potencial podem ser digitalizados por merging units, apresentada na Figura 3 e transmitidos pela rede de comunicação por meio de mensagens Sampled Values. Essa abordagem permite reduzir a quantidade de cabeamento metálico entre o pátio da subestação e os painéis de proteção e controle, além de facilitar a distribuição das amostras de corrente e tensão para múltiplos IED's. Com isso, os relés passam a receber grandezas elétricas em formato digital, viabilizando arquiteturas mais flexíveis, compactas e integradas [17], [28].

Além das aplicações em subestações convencionais e digitais, a IEC 61850 também é utilizada na integração com sistemas supervisórios e centros de controle. Por meio de serviços de comunicação mapeados, como o MMS, os dados

dos IED's podem ser acessados por sistemas SCADA, gateways e plataformas de supervisão. Essa aplicação permite monitorar estados, medições, alarmes, eventos, registros e comandos de operação de forma padronizada. A utilização de modelos comuns facilita a engenharia, reduz a dependência de protocolos proprietários e favorece a expansão futura do sistema [22], [24].

Quando se fala em automação, controle e proteção de subestações de energia, a norma tem um papel fundamental podendo ser utilizada em todos os níveis destes três processos, seja na coleta de informações no nível de processo até o nível gerencial, portanto a norma pode ser aplicada em projetos de automação de subestações a norma é ainda aplicável no monitoramento e controle de usina hidrelétricas, com uma parte dedicada a tratar especificamente das centrais hidrelétricas a IEC 61850-7-4-10.

A linguagem SCL (*Substation Configuration Language*), constitui outra aplicação essencial da norma. Ela permite descrever formalmente a configuração dos IEDs, suas capacidades, seus datasets, blocos de controle, mensagens GOOSE, mensagens Sampled Values e a estrutura da subestação. Arquivos como ICD, CID, SCD e SSD permitem a troca de informações entre ferramentas de engenharia de diferentes fabricantes, contribuindo para reduzir erros de configuração e melhorar o processo de comissionamento. Essa característica é fundamental para projetos multivendor, nos quais equipamentos de diferentes fabricantes precisam operar de forma integrada dentro de uma mesma arquitetura de automação [21], [22], [29], [30].

Outra área de aplicação da IEC 61850 está relacionada à automação de usinas e recursos energéticos distribuídos. Extensões da norma foram desenvolvidas para contemplar aplicações específicas, como usinas hidrelétricas, geração eólica, sistemas fotovoltaicos, armazenamento de energia e geração distribuída. Nessas aplicações, a norma fornece modelos de dados específicos para representar equipamentos, funções de controle, medições e estados operacionais associados a esses recursos. Essa expansão é relevante porque o sistema elétrico moderno tem se tornado mais descentralizado, com maior presença de fontes renováveis e dispositivos conectados às redes de distribuição [24], [31].

Em microgrids, a IEC 61850 pode ser aplicada para coordenar dispositivos de proteção, inversores, unidades de geração distribuída, sistemas de armazenamento, cargas controláveis e controladores centrais. Como esses sistemas podem operar tanto conectados à rede principal quanto em modo ilhado, a comunicação entre dispositivos torna-se essencial para a correta alteração dos ajustes de proteção, controle de fluxo de potência, supervisão de tensão e frequência e gerenciamento da operação local. Nesse cenário, a padronização dos dados e dos serviços de comunicação contribui para a implementação de estratégias de proteção adaptativa e automação distribuída [18], [24].

A norma também é aplicada em atividades de comissionamento, testes e manutenção de sistemas de proteção e

automação. Recursos como mensagens simuladas, controle de qualidade dos dados, revisão de configuração, supervisão da comunicação e registros de eventos permitem verificar o comportamento dos IED's antes da entrada em operação. Além disso, os testes de conformidade e interoperabilidade são fundamentais para garantir que os dispositivos implementem corretamente os modelos e serviços definidos pela norma. Dessa forma, a IEC 61850 não se limita à operação do sistema, mas também contribui para as etapas de projeto, engenharia, validação, expansão e manutenção das instalações [17], [29], [30].

Conclui-se então que a IEC 61850 abrange aplicações de automação de subestações, proteção distribuída, intertravamento, controle de equipamentos primários, supervisão, medição, barramento de processo, integração com sistemas SCADA, configuração de IED's, interoperabilidade multivendor, automação de fontes renováveis e operação de microgrids. Ao estabelecer modelos de dados e serviços de comunicação padronizados, a norma viabiliza a evolução das subestações convencionais para arquiteturas digitais, aumentando a flexibilidade, a confiabilidade e a capacidade de integração dos sistemas elétricos de energia.

V. CYBERSEGURANÇA EM SUBESTAÇÕES DIGITAIS

A evolução das subestações de energia elétrica para arquiteturas digitais trouxe ganhos significativos em automação, supervisão, interoperabilidade e redução de cabeamento. Entretanto, a intensificação do uso de redes Ethernet, protocolos de comunicação padronizados, dispositivos eletrônicos inteligentes e integração com sistemas supervisórios também ampliou a superfície de exposição a ameaças cibernéticas. Nesse contexto, a cybersegurança passa a ser um requisito essencial para garantir a confiabilidade, a disponibilidade e a integridade dos sistemas de proteção, controle e automação de subestações [32], [33].

Em subestações convencionais, grande parte das funções de proteção e controle era implementada por meio de sinais cabeados ponto a ponto, com menor dependência de redes de comunicação digitais. Nas subestações modernas, por outro lado, mensagens críticas como GOOSE, Sampled Values, MMS e comandos de supervisão trafegam por redes de comunicação internas, conectando relés de proteção, controladores de bay, merging units, gateways, sistemas SCADA e interfaces homem-máquina. Essa digitalização melhora a flexibilidade operacional, mas também cria novos vetores de ataque, como acesso não autorizado, interceptação de tráfego, alteração de mensagens, negação de serviço, inserção de comandos indevidos e comprometimento de dispositivos de proteção [17], [22], [28].

Para garantir a cybersegurança nas subestações deve-se considerar os três princípios fundamentais da segurança da informação: confidencialidade, integridade e disponibilidade. A confidencialidade está relacionada à proteção contra acesso indevido a informações sensíveis, como topologia da subestação, ajustes de proteção, registros de eventos e configurações dos IED's. A integridade garante que

mensagens, comandos, arquivos de configuração e dados de medição não sejam alterados de forma indevida. Já a disponibilidade assegura que os serviços de proteção, controle, supervisão e comunicação permaneçam operacionais mesmo diante de falhas, ataques ou tentativas de indisponibilização da rede [34], [35].

No ambiente de subestações, a disponibilidade possui relevância especial, pois os sistemas de proteção devem atuar em tempos reduzidos para isolar faltas e evitar danos aos equipamentos. Ataques de negação de serviço, congestionamento de rede ou degradação de desempenho podem comprometer a transmissão de mensagens críticas e afetar diretamente a seletividade e a rapidez da proteção. Da mesma forma, a alteração maliciosa de mensagens GOOSE pode causar abertura indevida de disjuntores, bloqueio de funções de proteção ou falha na atuação durante um defeito real. Em arquiteturas com barramento de processos, a manipulação ou atraso de mensagens *Sampled Values* pode comprometer a correta medição de correntes e tensões pelos relés de proteção [28], [36].

As mensagens GOOSE, amplamente utilizadas em aplicações de proteção e intertravamento, apresentam características específicas de segurança. Por serem transmitidas diretamente sobre Ethernet, utilizando comunicação multicast e com requisitos rigorosos de tempo, sua proteção exige mecanismos que não comprometam o desempenho da aplicação. Uma ameaça relevante é a injeção de mensagens falsas na rede, na qual um atacante poderia simular um IED legítimo e publicar sinais de *trip*, bloqueio ou permissivo. Outra possibilidade é a repetição de mensagens antigas, conhecida como *replay attack*, em que uma mensagem válida é capturada e reenviada posteriormente para provocar uma atuação indevida. Por esse motivo, mecanismos de autenticação, verificação de integridade, controle de sequência, segregação de rede e monitoração contínua são fundamentais em aplicações baseadas em GOOSE [32], [36].

As mensagens *Sampled Values* também exigem atenção especial. Como transportam amostras digitalizadas de corrente e tensão utilizadas pelos relés de proteção, qualquer alteração, perda, atraso ou falsificação dessas informações pode afetar o cálculo fasorial, a estimação de grandezas elétricas e a decisão de atuação das funções de proteção. Em um cenário de ataque, a manipulação dos valores amostrados poderia levar o relé a interpretar uma condição normal como falta, ou uma condição de falta como operação normal. Portanto, a proteção do barramento de processo deve envolver sincronização temporal confiável, controle de acesso à rede, validação de origem das mensagens, redundância de comunicação e monitoramento de anomalias no tráfego [28], [35], [36].

A série IEC 62351 (*Power systems management and associated information exchange — Data and communications security*) foi desenvolvida para tratar aspectos de segurança em protocolos de comunicação, incluindo aqueles associados à IEC 61850. Essa série aborda mecanismos

como autenticação, criptografia, controle de acesso, gestão de chaves, segurança para MMS, segurança para GOOSE e *Sampled Values*, além de diretrizes para monitoramento e gestão da segurança. Em particular, a IEC 62351-6 trata de mecanismos de segurança aplicáveis às mensagens GOOSE e *Sampled Values*, buscando preservar integridade e autenticidade das mensagens sem comprometer os requisitos de desempenho das aplicações de proteção [32], [36].

Além das normas específicas para sistemas elétricos, a cybergsegurança de subestações também pode ser orientada por normas e guias voltados a sistemas de automação industrial, como a série IEC 62443 e o guia NIST SP 800-82. Esses documentos recomendam a adoção de uma abordagem baseada em defesa em profundidade, na qual diferentes camadas de proteção são implementadas simultaneamente. Essa estratégia inclui segmentação de redes, zonas e conduítes de segurança, controle de acesso baseado em funções, autenticação forte, registro de eventos, gestão de vulnerabilidades, atualização controlada de *firmware*, *hardening* de dispositivos, cópias de segurança, resposta a incidentes e monitoramento contínuo [34], [35].

Em uma subestação digital, a segmentação de rede é uma das medidas mais importantes. A rede deve ser organizada de forma a separar o tráfego de proteção, controle, supervisão, engenharia e acesso remoto. Aplicações de tempo crítico, como GOOSE e *Sampled Values*, devem trafegar em redes ou VLANs adequadamente configuradas, com prioridade de comunicação e controle rigoroso dos dispositivos autorizados. *Firewalls* industriais, *switches* gerenciáveis, listas de controle de acesso e sistemas de detecção de intrusão podem ser utilizados para limitar a comunicação apenas aos fluxos necessários, reduzindo a possibilidade de propagação de ataques dentro da instalação [34], [35].

Outro aspecto crítico está relacionado à gestão de acessos. IED's, relés de proteção, *gateways* e sistemas supervisórios devem possuir controle de usuários, senhas robustas, autenticação adequada e perfis de acesso compatíveis com as responsabilidades de cada operador, engenheiro ou mantenedor. O acesso remoto, quando necessário, deve ser realizado por canais seguros, com autenticação multifator, criptografia e registro das atividades executadas. A ausência de controle adequado pode permitir alterações indevidas em ajustes de proteção, modificações em arquivos de configuração ou execução de comandos operacionais não autorizados [33], [35].

A gestão de configuração também é essencial para a segurança das subestações. Arquivos SCL, como ICD, CID, SCD e SSD, descrevem a estrutura dos IED's, *datasets*, blocos de controle, mensagens GOOSE, *Sampled Values* e demais parâmetros de comunicação. Alterações indevidas nesses arquivos podem modificar a lógica de funcionamento da subestação, causando perda de comunicação, atuação incorreta da proteção ou falhas de interoperabilidade. Dessa forma, esses arquivos devem ser protegidos contra alterações não autorizadas, versionados, validados

e armazenados em repositórios seguros [22], [32].

A cybersegurança também deve ser considerada durante todo o ciclo de vida da subestação, desde a etapa de projeto até a operação e manutenção. Durante o projeto, devem ser definidos requisitos de segurança, arquitetura de rede, zonas de segurança, políticas de acesso, requisitos de conformidade e critérios de testes. Durante o comissionamento, devem ser verificadas as configurações dos IED's, a segmentação da rede, a integridade dos arquivos de configuração, os fluxos de comunicação e a resposta dos sistemas diante de falhas simuladas. Na operação, é necessário manter monitoramento contínuo, análise de logs, atualização de inventário, gestão de vulnerabilidades e planos de resposta a incidentes [33]–[35].

Portanto, a cybersegurança em subestações digitais não deve ser tratada apenas como uma camada adicional de proteção, mas como um requisito estrutural do sistema de automação. A adoção de normas como IEC 62351, IEC 62443 e guias como o NIST SP 800-82 contribui para estabelecer mecanismos de proteção compatíveis com os requisitos de confiabilidade e tempo real dos sistemas elétricos. Em especial, nas arquiteturas baseadas na IEC 61850, a proteção das mensagens GOOSE, *Sampled Values*, MMS e dos arquivos de configuração é fundamental para preservar a interoperabilidade, a seletividade da proteção, a continuidade operacional e a segurança dos equipamentos conectados ao sistema elétrico.

VI. CONCLUSÃO

Feito um estudo aprofundado da operação de subestações de energia e também da Norma IEC 61850, torna-se evidente que a interoperabilidade entre os equipamentos utilizados dentro de uma subestação é essencial para evolução do setor elétrico, principalmente quando se considera a complexidade do sistema, o que exige cada vez mais o uso de tecnologias para tornar as subestações mais robustas e confiáveis. Além disso com a expansão do conceito de subestações digitais, as SE's tornam-se cada vez mais suscetíveis a ataques cibernéticos, portanto a adequação das SE's também à norma IEC 62351, principalmente a parte IEC 62351-6 que trata mais objetivamente das mensagens GOOSE e *Sample Value*, definidas na IEC 61850, se torna imprescindível para garantir o maior nível de confiabilidade do sistema elétrico de energia.

REFERÊNCIAS

- [1] J. O'Donnell, "A história que você ainda não conhece sobre a pegada energética da IA", MIT Technology Review Brasil, acesso em: 22 out. 2025, jun 2025, URL: <https://mittechreview.com.br/impacto-energetico-ia-inteligencia-artificial-data-centers/>.
- [2] International Energy Agency, *Energy and AI*, IEA, Paris, 2025, URL: <https://www.iea.org/reports/energy-and-ai>, licence: CC BY 4.0.
- [3] International Energy Agency, *Electricity Grids and Secure Energy Transitions*, International Energy Agency, Paris, 2023, URL: <https://www.iea.org/reports/electricity-grids-and-secure-energy-transitions>, acesso em: 28 jun. 2026.
- [4] International Energy Agency, *Energy and AI*, International Energy Agency, Paris, 2025, URL: <https://www.iea.org/reports/energy-and-ai>, acesso em: 28 jun. 2026.
- [5] C. D. Iweh, S. Gyamfi, E. Tanyi, E. Effah-Donyina, "Distributed Generation and Renewable Energy Integration into the Grid: Prerequisites, Push Factors, Practical Options, Issues and Merits", *Energies*, vol. 14, no. 17, p. 5375, 2021, doi:10.3390/en14175375, URL: <https://www.mdpi.com/1996-1073/14/17/5375>, acesso em: 28 jun. 2026.
- [6] E.-C. Liu, J. Bebic, *Distribution System Voltage Performance Analysis for High-Penetration Photovoltaics*, National Renewable Energy Laboratory, Golden, 2008, URL: <https://www.nrel.gov/docs/fy08osti/42298.pdf>, acesso em: 28 jun. 2026.
- [7] R. Seguin, J. Woyak, D. Costyk, J. Hambrick, B. Mather, *High-Penetration PV Integration Handbook for Distribution Engineers*, National Renewable Energy Laboratory, Golden, 2016, URL: <https://www.nrel.gov/docs/fy16osti/63114.pdf>, acesso em: 28 jun. 2026.
- [8] A. S. Akinyemi, et al., "Analysis of voltage rise phenomena in electrical power network with high concentration of renewable distributed generation", *Scientific Reports*, vol. 12, 2022, URL: <https://www.nature.com/articles/s41598-022-11771-x>, acesso em: 28 jun. 2026.
- [9] A. C. d. R. Duarte, *Equipamentos de geração e transmissão: introdução à proteção de sistemas elétricos de potência: conceitos e critérios*, Artliber, São Paulo, 2018.
- [10] L. Comassetto, D. P. Bernardon, L. N. Canha, A. d. R. Abaide, "Automatic coordination of protection devices in distribution system", *Electric Power Systems Research*, vol. 78, no. 7, pp. 1210–1216, 2008.
- [11] Institute of Electrical and Electronics Engineers, *IEEE Std 242-2001: IEEE Recommended Practice for Protection and Coordination of Industrial and Commercial Power Systems*, Institute of Electrical and Electronics Engineers, New York, 2001.
- [12] S. Howell, et al., "Towards the Next Generation of Smart Grids: Semantic and Holonic Multi-Agent Management of Distributed Energy Resources", *Renewable and Sustainable Energy Reviews*, vol. 77, pp. 193–214, sep 2017.
- [13] Institute of Electrical and Electronics Engineers, *IEEE Std C37.230-2007: IEEE Guide for Protective Relay Applications to Distribution Lines*, Institute of Electrical and Electronics Engineers, New York, 2007.
- [14] S. H. Horowitz, A. G. Phadke, *Power System Relaying*, 4 ed., John Wiley & Sons, Chichester, 2014.
- [15] J. L. Blackburn, T. J. Domin, *Protective Relaying: Principles and Applications*, 4 ed., CRC Press, Boca Raton, 2014.
- [16] D. Hou, D. Dolezilek, "IEC 61850: What It Can and Cannot Offer to Traditional Protection Schemes", in *Proceedings of the 35th Annual Western Protective Relay Conference*, Spokane, 2008, URL: https://cdn.selinc.com/assets/Literature/Publications/Technical%20Papers/6335-IEC61850_DH-DD-20080912.Web.pdf, acesso em: 28 jun. 2026.
- [17] IEEE Power System Relaying and Control Committee, *Application Testing of IEC 61850 Based Systems*, IEEE Power & Energy Society, 2019, URL: <https://www.pes-psrc.org/kb/report/053.pdf>, acesso em: 28 jun. 2026.
- [18] S. Sanati, M. Azzouz, A. Awad, "An Adaptive Overcurrent Protection for Solar-Based DC Microgrids Using IEC 61850", *arXiv preprint arXiv:230701940*, 2023, URL: <https://arxiv.org/abs/2307.01940>, acesso em: 28 jun. 2026.
- [19] M. Engenharia, *Relé secundário: Proteção BT vs proteção MT*, Mesh Engenharia, 2026, URL: <https://meshengenharia.com/2023/06/01/rele-secundario-protecao-bt-vs-protecao-mt/>, acesso em: 30 jun. 2026.
- [20] CIGRÉ Working Group B5.36, *Applications of IEC 61850 Standard to Protection Schemes*, CIGRÉ, Paris, 2011.
- [21] International Electrotechnical Commission, *IEC 61850: Communication Networks and Systems for Power Utility Automation*, International Electrotechnical Commission, Geneva, 2011.
- [22] International Electrotechnical Commission, *IEC 61850-7-1: Communication Networks and Systems for Power Utility Automation – Part 7-1: Basic Communication Structure – Principles and Models*, International Electrotechnical Commission, Geneva, 2011.

- [23] International Electrotechnical Commission, *IEC 61850-7-4: Communication Networks and Systems for Power Utility Automation – Part 7-4: Basic Communication Structure – Compatible Logical Node Classes and Data Object Classes*, International Electrotechnical Commission, Geneva, 2010.
- [24] S. Kumar, *et al.*, “Review of the Legacy and Future of IEC 61850 Protocols Encompassing Substation Automation System”, *Electronics*, vol. 12, no. 15, p. 3345, 2023, doi:10.3390/electronics12153345, URL: <https://www.mdpi.com/2079-9292/12/15/3345>, acesso em: 28 jun. 2026.
- [25] T. Bajanek, “Overcurrent Protection Relay Model Using IEC 61850-9-2 Sampled Values”, in *Proceedings of the 2014 15th International Scientific Conference on Electric Power Engineering (EPE)*, pp. 101–106, IEEE, Brno-Bystrc, Czech Republic, 2014, doi:10.1109/EPE.2014.6839480.
- [26] G. F. Barbosa, *Proteção e automação de subestações: um estudo dos padrões IEC 61850 e CPC*, Instituto Federal de Educação, Ciência e Tecnologia do Triângulo Mineiro, Campus Paracatu, Paracatu, MG, 2021, trabalho de Conclusão de Curso, Bacharelado em Engenharia Elétrica.
- [27] ABB, *Special Report IEC 61850*, ABB Review, 2010, URL: https://library.e.abb.com/public/a56430e1e7c06fdcf12577a00043ab8b/3BSE063756_en_ABB_Review_Special_Report_IEC_61850.pdf, acesso em: 28 jun. 2026.
- [28] International Electrotechnical Commission, *IEC 61850-9-2: Communication Networks and Systems for Power Utility Automation – Part 9-2: Specific Communication Service Mapping – Sampled Values over ISO/IEC 8802-3*, International Electrotechnical Commission, Geneva, 2011.
- [29] J. C. Tan, C. H. Lee, P. A. Crossley, “Testing IEC 61850 Based Multi-Vendor Substation Automation Systems for Interoperability”, in *IEEE PES Power Systems Conference and Exposition*, IEEE, 2009.
- [30] M. Daboul, *et al.*, “Interoperability Testing for IEC 61850 Based Substation Automation System”, in *IEEE Conference Proceedings*, IEEE, 2018.
- [31] International Electrotechnical Commission, *IEC 61850-7-410: Communication Networks and Systems for Power Utility Automation – Part 7-410: Basic Communication Structure – Hydroelectric Power Plants – Communication for Monitoring and Control*, International Electrotechnical Commission, Geneva, 2012.
- [32] International Electrotechnical Commission, *IEC 62351: Power Systems Management and Associated Information Exchange – Data and Communications Security*, International Electrotechnical Commission, Geneva, 2023.
- [33] North American Electric Reliability Corporation, *Critical Infrastructure Protection Standards*, North American Electric Reliability Corporation, Atlanta, 2024, URL: <https://www.nerc.com/pa/Stand/Pages/CIPStandards.aspx>, acesso em: 28 jun. 2026.
- [34] International Electrotechnical Commission, *IEC 62443: Industrial Communication Networks – Network and System Security*, International Electrotechnical Commission, Geneva, 2018.
- [35] K. Stouffer, V. Pillitteri, S. Lightman, M. Abrams, A. Hahn, *Guide to Industrial Control Systems Security*, National Institute of Standards and Technology, Gaithersburg, 2015, URL: <https://doi.org/10.6028/NIST.SP.800-82r2>, acesso em: 28 jun. 2026.
- [36] International Electrotechnical Commission, *IEC 62351-6: Power Systems Management and Associated Information Exchange – Data and Communications Security – Part 6: Security for IEC 61850*, International Electrotechnical Commission, Geneva, 2020.