A Comprehensive Overview in Communication Protocols for IEDs in Electric Power Systems

G. C. Lilli[*], L. S. Lessa[†], C. V. C. Grilo[‡] and A. J. Prado[§]
[1]Department of Electronic and Telecommunications Engineering, College of Engineering of São João
São Paulo State University, São João da Boa Vista, Brazil
[*]gustavo.lilli@unesp.br, [†]leonardo.s.lessa@unesp.br, [‡]caio.vinicius@unesp.br, [§]afonso.prado@unesp.br

***Abstract*—Substation automation is a crucial challenge in the modernization of electric power systems, aiming to improve operational efficiency, reliability, and safety. This paper provides a comprehensive overview of the communication protocols used in Intelligent Electronic Devices (IEDs) within power systems, with a focus on the IEC 61850 standard. The standard defines communication protocols for networks and substation systems, promoting interoperability between devices from different manufacturers. The analysis includes key protocols such as MMS, GOOSE, and SV, highlighting their advantages, disadvantages, and applications. The scope of the work aims to address important concepts, defining the entire structure of a network specified by the standard, and discussing recent technological advancements such as the complete digitalization of substations, which improves communication accuracy and speed, and the replacement of traditional analog measurement methods. Furthermore, it addresses the challenges faced in implementing these protocols, including the need for standardization and overcoming bandwidth limitations. This work contributes with a detailed analysis of the existing protocols, identifying gaps and areas for future research, with the goal of further enhancing substation automation and the efficiency of electric power systems.**

***Index Terms*—IEC 61850, Substation Automation, Communication Protocols, Intelligent Electronic Devices, Electrical System Protection**

I. Introdução

A transferência de dados e a comunicação autônoma entre equipamentos em sistemas de potência são desafios significativos, especialmente no que se refere à transmissão e operação em tempo real. Inicialmente, a coleta de informações sobre os equipamentos era realizada presencialmente por operadores, o que demandava tempo e esforço consideráveis. Com a introdução de canais de comunicação, por meio de linhas telefônicas, o processo foi simplificado [1]. Os primeiros Sistemas de Aquisição de Dados (DAS) automatizaram a coleta e o armazenamento, utilizando sensores para captar fenômenos físicos, conversores para transformar sinais analógicos em digitais e computadores para processar esses dados [2].

Embora revolucionária, essa tecnologia enfrentou limitações, como a largura de banda disponível. À medida que o uso do DAS se popularizou, a demanda por banda larga aumentou, tornando-a escassa. Isso exigiu ajustes nos protocolos de comunicação para operar eficientemente em canais de baixa largura de banda, tornando necessária a compactação e transmissão eficiente dos dados [3]. Os Dispositivos Eletrônicos Inteligentes (IEDs) integraram diversas funções, como medições, proteção e monitoramento em tempo real, além de utilizarem ondas de rádio como forma de comunicação, o que minimizou o problema da limitação da largura de banda.

No entanto, para que os IEDs operassem de forma eficiente, era crucial superar o desafio da padronização na coleta e transferência de dados. A *Utility Communication Architecture* (UCA) uniformizou a comunicação e a troca de informações entre sistemas diferentes, garantindo a interoperabilidade independentemente do fabricante. Contudo, ainda eram necessárias configurações e mapeamentos manuais de objetos, variáveis de sistemas de energia e números de registros de baixo nível. Essas limitações foram o foco do desenvolvimento de normas como a IEC 61850, que definiu redes e sistemas de comunicação em subestações [4].

O objetivo deste trabalho é apresentar uma revisão compreensiva dos principais protocolos de comunicação utilizados em Sistemas Elétricos de Potência (SEP), apresentando as vantagens e desvantagens desses protocolos. Além disso, o trabalho contribui com uma análise das lacunas que podem ser exploradas.

O restante do artigo está organizado da seguinte forma: a Seção II apresenta uma análise dos protocolos de comunicação utilizados por IEDs. Os avanços tecnológicos recentes são discutidos na Seção III, que inclui protocolos emergentes e um estudo de caso na Seção IV. Os desafios enfrentados na implementação desses protocolos e suas possíveis soluções são abordados na Seção V. Finalmente, a Seção VI apresenta as conclusões alcançadas a partir das análises realizadas neste trabalho.

II. Protocolos de Comunicação Atuais

Nesta seção, são apresentados os principais protocolos de comunicação da atualidade, destacando suas características e aplicações em SEPs. A Figura 1 ilustra, de forma prática, a hierarquia dos protocolos de comunicação que são utilizados na automação de uma subestação.

A. Manufacturing Message Specification (MMS)

O MMS é um protocolo de comunicação padronizado pela ISO 9506, utilizado para a troca de informações entre sistemas de automação e controle. Desenvolvido para suportar a comunicação em ambientes industriais, o MMS é projetado para fornecer uma interface de alto nível que permite a

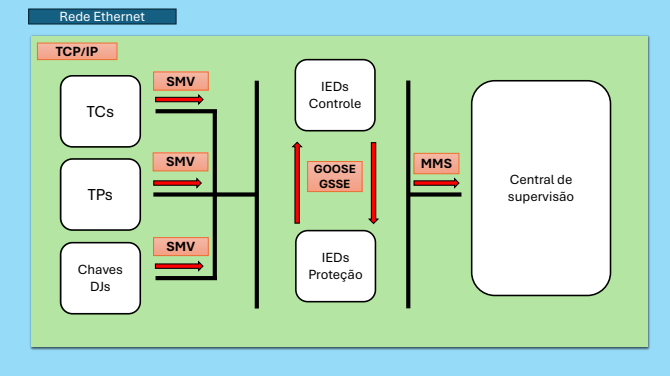


Fig. 1. Fluxograma dos Protocolos IEC 61850 no Sistema Elétrico de Potência.

integração entre diferentes dispositivos e sistemas, independentemente de seus fabricantes [5]–[7].

O MMS opera sobre a camada de aplicação do modelo *Open Systems Interconnection* (OSI) e é amplamente utilizado em sistemas *Supervisory Control and Data Acquisition* (SCADA) e na automação de subestações [8]. O protocolo oferece uma rica gama de serviços, incluindo leitura e escrita de dados, gerenciamento de arquivos, controle de dispositivos e reportes de eventos, facilitando a supervisão e o controle eficazes de equipamentos industriais.

A robustez e a flexibilidade do MMS são destacadas por sua capacidade de suportar uma significativa variedade de tipos de dados e operações de controle, tornando-o ideal para aplicações onde a confiabilidade e a eficiência são críticas. Com sua arquitetura baseada em objetos e suporte a comunicação em tempo real, o MMS é essencial para garantir a eficiência operacional em sistemas de automação industrial [9], [10].

B. Sampled Values (SV)

O SV refere-se a um protocolo de comunicação que permite a transmissão de valores de amostragem digitalizados de sinais analógicos, como tensões e correntes, em alta velocidade e precisão. O objetivo principal do SV é substituir os métodos tradicionais de medição analógica com uma abordagem mais eficiente e precisa, facilitando a digitalização total das subestações [7].

Os valores amostrados são transmitidos periodicamente em pacotes de dados através de uma rede *Ethernet*. Esses pacotes contêm informações sobre o tempo de amostragem e os valores medidos, permitindo que dispositivos, como relés de proteção e medidores, utilizem esses dados para monitoramento e controle em tempo real. A norma IEC 61850-9-2 especifica os requisitos para a transmissão de SV, garantindo a interoperabilidade entre equipamentos de diferentes fabricantes [11], [12].

A utilização de SV reduz a quantidade de cabos na infraestrutura, tem menor suscetibilidade a interferências eletromagnéticas e maior precisão nas medições. Além disso, a transmissão digital facilita a integração de sistemas de proteção, controle e monitoramento, melhorando a eficiência e a confiabilidade das operações da subestação [13].

C. Generic Object Oriented Substation Event (GOOSE)

O GOOSE é utilizado para facilitar a troca de mensagens de eventos entre IEDs em tempo real, promovendo uma resposta rápida e eficiente a mudanças no estado do sistema, como falhas ou alterações operacionais [12], [14].

O protocolo opera em uma rede *Ethernet*, utilizando pacotes *multicast* para transmitir mensagens de eventos para múltiplos dispositivos simultaneamente. Este método de comunicação é altamente eficiente, pois reduz a latência e permite a coordenação rápida entre equipamentos, como relés de proteção, disjuntores e controladores. O tempo de resposta é crucial para a proteção, garantindo que ações possam ser tomadas para mitigar problemas no sistema [6], [15], [16].

O GOOSE é projetado para ser altamente configurável, permitindo que os engenheiros definam quais eventos serão transmitidos e como serão interpretados pelos dispositivos. A flexibilidade do protocolo permite a implementação customizada de esquemas complexos de proteção e controle. Além disso, GOOSE suporta a redundância de rede e a reconfiguração dinâmica, aumentando a resiliência e a robustez da comunicação [7], [9].

A adoção do protocolo GOOSE tem como vantagens a simplificação da infraestrutura de comunicação, a redução de redes de cabos e a melhoria da interoperabilidade entre equipamentos de diferentes fabricantes. Além disso, ao possibilitar uma resposta rápida a eventos críticos, o GOOSE contribui significativamente para a estabilidade e a segurança do sistema. A implementação deste protocolo é fundamental na modernização das subestações, promovendo a transição para um sistema de energia mais inteligente e eficiente [10], [11].

D. Transmission Control Protocol/Internet Protocol (TCP/IP)

O TCP/IP é um conjunto de protocolos para a comunicação em redes de computadores, incluindo a Internet. Embora o TCP/IP não seja específico para sistemas de automação de subestações, ele desempenha um papel fundamental como infraestrutura de comunicação subjacente para a norma IEC 61850. O TCP/IP é empregado para garantir a operabilidade e a confiabilidade na troca de informações entre dispositivos [17].

Para a norma, o TCP/IP fornece os meios para transmitir os dados entre equipamentos de diferentes fabricantes, facilitando a comunicação entre dispositivos no mesmo nível hierárquico, como relés de proteção e sistemas de medição, e entre dispositivos de diferentes níveis hierárquicos, como dispositivos de comunicação. A camada de transporte TCP, com seu controle de fluxo e correção de erros, assegura que as mensagens críticas, como as de controle e proteção, sejam entregues de forma confiável e ordenada [18]. Isso é essencial para manter a integridade e a precisão das operações em subestações.

Além disso, o protocolo IP permite a integração de dispositivos em redes *Ethernet* padrão, beneficiando-se da infraestrutura de rede existente e de tecnologias adotadas. Essa

compatibilidade não só reduz os custos de implementação, mas também facilita a escalabilidade e a manutenção das redes de automação. A flexibilidade do TCP/IP permite a implementação de diferentes tipos de comunicação, como mensagens SV e GOOSE.

E. Sampled Measured Values (SMV)

O SMV, diferentemente do SV, é um conjunto de amostras que são enviadas como uma única mensagem. São utilizados para comunicação entre dispositivos em uma rede, enquanto o SV é utilizado para a comunicação interna dos dispositivos. Isso permite que múltiplos valores amostrados em um formato estruturado, tenham muitas vezes informações adicionais, como carimbos de tempo [7], [11]. Além disso, o uso de rede *Ethernet* visa reduzir a latência com que as amostras chegam ao destino, essencial para as aplicações de proteção e controle que requerem tempos de resposta extremamente rápidos [12].

Uma das principais vantagens do SMV é a redução da quantidade de cabos físicos necessários nas subestações. Tradicionalmente, as conexões físicas de fios de cobre eram utilizadas para transmitir sinais analógicos de sensores para dispositivos de proteção e medição. Com o SMV, essas conexões são substituídas por uma rede de comunicação digital, o que simplifica a instalação e manutenção [13].

F. Generic Substation Status Event (GSSE)

O GSSE é projetado para a comunicação rápida e eficiente de estados e eventos binários. O GSSE permite a troca de informações de status, como sinais de alarme e comandos entre IEDs de forma quase instantânea. Este protocolo é adequado para funções de proteção e controle em que o tempo de resposta seja crítico, como a coordenação de disjuntores e relés de proteção [19].

O funcionamento do GSSE baseia-se na transmissão de mensagens de status na rede *Ethernet*. Cada mensagem GSSE contém informações sobre o estado de vários sinais binários enviados de forma contínua e sinalizada quando ocorre uma mudança de estado. A alta prioridade dessas mensagens na rede de comunicação garante que elas sejam entregues com latência mínima [20].

As principais vantagens são a comunicação mútua entre equipamentos de diferentes fabricantes, assegurando que todos os dispositivos na subestação possam se comunicar de maneira padronizada e a flexibilidade de configuração ou reconfiguração via software, sem a necessidade de mudanças na estrutura física da rede [21].

III. Avanços Tecnológicos na IEC 61850

Protocolos legados, como *Distributed Network Protocol* (DNP3) e *Remote Terminal Unit* (Modbus RTU) do SCADA [22] [23], não padronizam a organização de dados nos dispositivos, exigindo configurações detalhadas manualmente e mapeamento de variáveis. Isso pode ser complexo e propenso a erros. A IEC 61850 soluciona essas limitações, oferecendo um modelo padronizado de comunicação e configurações automáticas.. A Figura 2 exemplifica todo o caminho que a informação percorre dentro de uma subestação automatizada, desde a captação dos sinais analógicos até a chegada dessa informação digitalizada na central de supervisão da subestação. Além disso, a Figura 2 denota as terminologias que serão abordadas nesta seção.

A. Funcionamento físico

Alguns dispositivos utilizam o *Substation Configuration Language* (SCL) para configurar seus objetos internos. O arquivo SCL descreve detalhadamente todos os objetos e suas propriedades [2]. Após a importação do SCL para o dispositivo e a conexão do mesmo na rede, os protocolos que compõem a norma, como o MMS, são capazes de se configurarem, alterando automaticamente todas as definições de objetos configurados de acordo com a SCL, incluindo dados de monitoramento. Essa automação permite que os dispositivos se configurem rapidamente e de forma confiável [24] [25].

Os protocolos de comunicação da IEC 61850 partem de um dispositivo físico (DF) que contenha o protocolo implementado em seu sistema, onde se conecta à rede e pode conter múltiplos dispositivos lógicos. Esse modelo permite que um único dispositivo físico atue como *proxy* ou *gateway* para múltiplos dispositivos, fornecendo uma representação padrão de um gerenciador de dados e garantindo interoperabilidade e eficiência na comunicação de dados entre diferentes dispositivos e sistemas [2].

B. Nós lógicos

Cada dispositivo lógico (DL) contém um ou mais nós lógicos (NL), que representam funções ou serviços específicos que o dispositivo pode realizar. Esses nós são definidos de acordo com modelos de dados abstratos especificados pela IEC 61850. Existem NL para diferentes funções, como controle automático, medição, supervisão, funções genéricas, interfacing/arquivamento, sistema, proteção, sensores, transformadores de instrumentos (CITs), equipamentos de manobra, transformadores de potencial e de corrente (TPs e TCs), sendo possível a criação de um NL para outros equipamentos. Cada NL é identificado por um *NL-Instance-ID*, que diferencia instâncias de nós lógicos com a mesma função dentro de um dispositivo [2], [7].

Cada NL contém um ou mais elementos de dados (ED), nomeados de acordo com o padrão e relacionados à função específica do equipamento. Por exemplo, um NL de disjuntor (XCBR) pode conter elementos de dados como *Pos*, que indica a posição do disjuntor (aberto ou fechado), e *OpCnt*, que conta o número de operações do disjuntor. Esses elementos de dados são estruturados, facilitando a interpretação e manipulação das informações [12], [14].

Para padronizar todas as definições dos objetos, são definidas Classes de Dados Comuns (CDC), que especificam tipos específicos de dados dentro de um NL. Cada CDC possui um nome, um conjunto de atributos com nomes e tipos definidos, e restrições funcionais que categorizam os atributos em grupos funcionais, como status, valor substituído, descrição

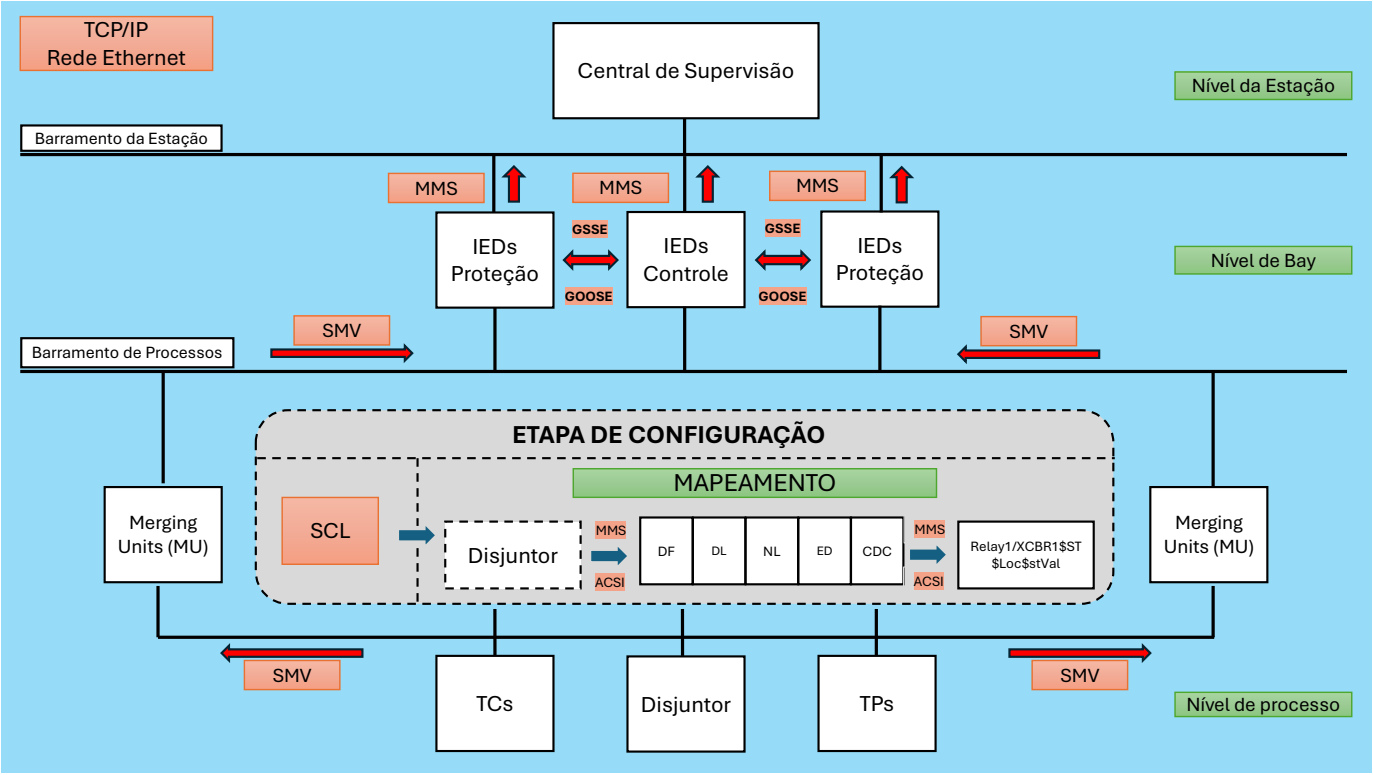


Fig. 2. Fluxograma do processo de atuação da IEC 61850 em um sistema elétrico de potência.

e definição estendida. Isso assegura a utilização de dados em diferentes dispositivos [2].

C. Mapeamento

Um dispositivo é inicialmente representado de forma abstrata, com uma descrição conceitual de seus componentes e funcionalidades. Essa representação abstrata é então mapeada para uma série específica de protocolos de comunicação como o MMS que utiliza TCP/IP e a rede Ethernet para a transmissão dos dados. O mapeamento envolve traduzir cada elemento de dados do modelo abstrato em um objeto variável MMS, garantindo uma referência única e clara para cada informação no contexto do protocolo MMS [9].

O processo de mapeamento dos modelos de objetos segue uma abordagem por camadas, começando com a correspondência entre os serviços definidos na Interface de Serviço de Comunicação Abstrata (ACSI), que trata de uma interface definida pela norma IEC 61850. A ACSI garante uma comunicação de alto nível, como leitura e escrita de dados, controle de dispositivos e gerenciamento de eventos, independentes das implementações físicas e dos protocolos de comunicação. A estrutura de dados baseada em objetos facilita a modelagem, gestão e manutenção de sistemas complexos, além de suportar serviços disponíveis no MMS, como leitura, escrita e controle. Em seguida, os modelos de objetos são associados a objetos específicos no MMS, permitindo uma implementação escalonada e estruturada. Essa abordagem garante que as funcionalidades abstratas e os serviços de alto nível definidos na ACSI sejam traduzidos de maneira eficaz para os serviços e objetos concretos no MMS, promovendo uma comunicação eficiente entre os sistemas [10].

A norma define perfis para várias camadas do conjunto de comunicação, facilitando a troca de informações entre diferentes dispositivos. Protocolos como SV e GOOSE garantem a entrega quase instantânea de dados, eliminando a necessidade de processamento por camadas intermediárias e acelerando a transmissão. A camada MMS, orientada à conexão, o que oferece flexibilidade na escolha do protocolo. Além disso, o GSSE utiliza serviços ISO/OSI sem conexão, transmitindo eventos de status de maneira eficiente sem estabelecer uma conexão permanente, adequado para comunicações rápidas e não críticas em tempo real.

Todos os dados são encapsulados em quadros Ethernet, que garantem a comunicação entre dispositivos de diferentes tipos e fabricantes. O Sampled Values, GOOSE, *TimeSync* e TCP/IP utilizam o tipo de dados *Ethertype* para identificar o protocolo de camada superior sendo transportado no quadro Ethernet. Mensagens ISO e GSSE, por outro lado, utilizam o tipo de dados "*802.3*", o padrão original para *Ethernet*, que especifica a transmissão de dados em redes locais.

D. Barramento de processos

Com o avanço dos dispositivos e da microeletrônica, as tecnologias passaram a utilizar sensores de corrente e tensão de baixa energia, com uma capacidade de digitalizar as quantidades básicas na fonte e transmitir os valores amostrados

resultantes de volta para a subestação. Além dos SV, a possibilidade de adquirir remotamente informações de status e definir controles de saída é altamente vantajosa. Por isso, a IEC 61850 atende a essa necessidade por meio da definição de serviços SMV e da estruturação de um barramento de processo [12]. A camada de Processo está relacionada à coleta de informações, como tensão, corrente e status dos transformadores e transdutores conectados à camada de proteção física do sistema elétrico. A coleta desses dados se dá por meio de duas abordagens diferentes: uma que especifica um link ponto-a-ponto unidirecional de *multidrop* que transporta um conjunto de dados fixo e outra que define um conjunto de dados configurável [2].

Os dados coletados pelos dispositivos de proteção são então digitalizados em unidade denominada *Merging Units* (MU). Essas unidades coletam os sinais analógicos medidos nos transformadores de corrente e transformadores de potencial e disponibilizam na rede, através do barramento de processos, que servirá de entrada para os IEDs. Atualmente, uma taxa básica de 80 amostras por ciclo do sistema de potência é utilizada para proteção e monitoramento da rede, enquanto uma taxa mais alta de 256 amostras por ciclo é usada para aplicações como qualidade de energia e obtenção de oscilografia da rede. A coleta e troca de dados em tempo real envolve dois tipos principais de conjuntos que são: conjuntos de dados pré-configurados e SMV.

O conjunto de dados pré-configurados inclui medições de tensão e corrente trifásicas para proteção e medição e tensão do barramento juntamente com duas palavras de status de 16 bits. Os valores analógicos são mapeados em registros de 16 bits. Já o SMV permite que os conjuntos de dados sejam definidos pelo usuário utilizando a SCL. Essa especificação sugere que o tamanho do dado seja de 32 bits com um fator de escala em que cada contagem corresponde a 1 mA. Isso permite a personalização dos dados de acordo com a necessidades para cada aplicação.

Ambas as especificações determinam o mapeamento diretamente para um transporte Ethernet. Dependendo da taxa de amostragem de dados, de 1 a 5 dispositivos podem ser mapeados em um único link *Ethernet* de 100 Mbps. Assim, é possível estabelecer fluxos de dados Ethernet de 100 Mbps e combiná-los em um único *switch Ethernet* com um *backbone* de 1 Gbps, permitindo que 50 ou mais conjuntos de dados sejam publicados para múltiplos assinantes [12].

E. Substation Configuration Language (SCL)

A SCL é uma linguagem de descrição projetada para simplificar a comunicação e padronização entre dispositivos. A SCL utiliza a notação *Extensible Markup Language* (XML) para descrever a estrutura, a comunicação e os dados funcionais nos sistemas de automação.

Um dos principais objetivos do SCL é fornecer uma visão completa e detalhada da configuração da subestação, desde a topologia física dos equipamentos até a configuração lógica dos dados e funções de controle. Isso inclui a descrição dos IEDs, suas capacidades de comunicação, a estrutura de dados, as conexões de rede e os links entre os dados e as funções de controle.

O SCL suporta várias definições de arquivos específicos, cada um com uma finalidade distinta no processo de configuração e operação. Por exemplo, o arquivo *System Specification Description* (SSD) descreve a especificação do sistema, o *Substation Configuration Description* (SCD) detalha a configuração da subestação completa, e o *Configured IED Description* (CID) fornece a configuração específica de um IED. Esses arquivos podem ser gerados e manipulados por ferramentas de software, permitindo uma configuração automatizada e verificável dos sistemas de automação. [2].

A sequência de aplicação do SCL pode ser descrita em três etapas:

- Especifica o sistema usando o arquivo SSD, onde é definida a topologia da subestação e as funções dos dispositivos, como relés e disjuntores;
- O arquivo SCD é criado para detalhar a configuração completa da subestação, incluindo parâmetros de comunicação dos dispositivos e suas conexões de rede;
- A CID é utilizada para programar os IEDs com suas configurações específicas, como endereços de rede e funções de proteção.

O SCL facilita a configuração inicial e a manutenção e atualização dos sistemas. Com uma documentação padronizada, qualquer alteração ou atualização no sistema pode ser implementada de maneira mais eficiente e com menos risco de erros. Isso inclui a adição de novos dispositivos, a reconfiguração de dispositivos existentes ou a atualização de firmware, tudo realizado de forma coerente e documentada.

IV. Estudo de caso

Nesta seção, é analisado de forma crítica o trabalho proposto por [26], intitulado "*Toward a Substation Automation System Based on IEC 61850*". Este estudo visa avaliar a latência na comunicação, consistência das informações que trafegam pela rede e a integração de ativos de plantas primárias de alta tensão, como transformadores de instrumentos, disjuntores e transformadores de potência, com diversos IEDs em um nível hierárquico. Além disso, o estudo aborda a necessidade de investigação detalhada do desempenho e viabilidade dos transformadores de instrumentos não convencionais para sua implementação em larga escala em subestações digitais, como sensores ópticos conectados.

A Figura 2, representa o diagrama de blocos típico do sistema automatizado de uma subestação utilizado pelos autores, no qual equipamentos da subestação, como transformadores e disjuntores, se comunicam com o barramento de processos. Os sinais analógicos são convertidos em digitais por unidades MUs e transmitidos para IEDs e dispositivos de controle no nível de *bay*. Pacotes digitais são, então, enviados para os IEDs da subestação no nível de estação, onde falhas, disparos e sinais de disponibilidade dos disjuntores são encaminhados para a sala de controle local, e, simultaneamente, para a sala de controle remoto.

Para os testes realizados, foram utilizados os protocolos de comunicação baseados na IEC 61850-9-2 e avaliados em uma arquitetura de barramento de processo utilizando o simulador OPNET. A avaliação do atraso de ponta-a-ponta é essencial para as redes, pois indica a latência na transmissão e recepção de quadros SV que viajam dos dispositivos de campo para os IEDs de proteção. A simulação considera um diagrama de linha única de uma subestação de zona de 132/22 kV com transformadores de instrumento não convencionais localizados no pátio de alta tensão e conectados aos IEDs via fibra óptica conforme mostrado na Figura 3.

Os resultados da simulação destacaram a latência e o atraso de ponta-a-ponta na transmissão de mensagens SV entre os dispositivos de campo e os IEDs de proteção. Esse estudo apontou que os MUs transmitiram dados SV de forma eficiente, com uma latência mínima de 122 µs e máxima de 138 µs, enquanto os IEDs processaram os dados SV e mensagens GOOSE com uma latência observada de 149 µs a 185 µs para mensagens GOOSE, devido ao maior tempo de processamento e enfileiramento. Dessa forma, a análise comparativa das mensagens SV e GOOSE mostrou que as mensagens SV apresentaram menor atraso durante a transmissão, o que é crítico para a proteção rápida e eficaz da subestação. As mensagens GOOSE, embora essenciais para eventos e comandos, apresentaram maior latência, destacando a necessidade de otimização adicional para garantir uma resposta rápida do sistema de proteção.

Embora tenham sido destacadas contribuições importantes pelos autores, ainda se faz necessárias mais investigações acerca da latência, pois ainda que a latência média esteja dentro das diretrizes, a variabilidade observada nas mensagens GOOSE sugere que há espaço para otimização. Impactos na coordenação e rápida atuação da proteção durante tráfego intenso ou situações de falha podem prejudicar a confiabilidade do sistema. A capacidade dos IEDs de processar grandes volumes de dados de forma eficiente é crítica. Sendo assim, são necessários maiores esforços e investigações acerca da capacidade de processamento, já que a capacidade atual apresentou um estrangulamento da informação.

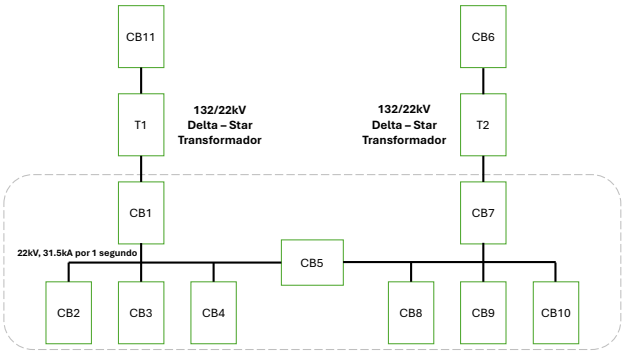


Fig. 3. Modelo de subestação utilizado em [26].

V. Desafios e Soluções

O avanço da tecnologia promoveu inúmeros benefícios para a automação dos sistemas elétricos, incluindo o monitoramento em tempo real e o controle dinâmico das redes elétricas. No entanto, essa integração tecnológica crescente também expôs os sistemas a uma avalanche de possibilidades de ciber-ameaças. Esta seção destaca algumas dessas ameaças à segurança tecnológica dos sistemas elétricos automatizados e também ressalta algumas estratégias para mitigar os ciber-ataques.

A. Desafios de segurança e estratégias de mitigação

Os desafios de segurança cibernética no sistema de automação de distribuição são significativos e multifacetados, refletindo a complexidade e a conectividade crescentes das redes de distribuição de energia. Alguns desafios e vulnerabilidades dessa automatização podem ser elencados de maneira a incitar a formação de um diagnóstico capaz de refletir sobre as formas de mitigar e evitar falhas de segurança.

1) **Protocolos de Comunicação não Seguros:** Os protocolos de comunicação industrial, como DNP 3.0 e IEC 61850, foram desenvolvidos antes do aumento da conscientização sobre segurança cibernética e, portanto, carecem de mecanismos de proteção robustos. Isso os torna vulneráveis a ataques de injeção de dados e modificações de pacotes, comprometendo a integridade e a confidencialidade das informações transmitidas.
2) **Dispositivos de Campo Expostos:** Dispositivos de controle, como Unidades Terminais Remotas (RTUs) e relés de proteção, são frequentemente instalados em locais acessíveis ao público. A falta de proteção física adequada permite que invasores obtenham acesso direto a esses dispositivos, comprometendo a segurança da rede de comunicação e do sistema todo.
3) **Malware e Vírus:** A invasão de malwares em sistemas de controle industrial tem sido uma crescente preocupação. Incidentes como os ataques à rede elétrica ucraniana ilustram como malwares sofisticados podem ser utilizados para interromper operações críticas, resultando em significativas interrupções no fornecimento de energia e danos econômicos [27].
4) **Senhas Padrão e Servidores Web Incorporados:** O uso de senhas padrão ou fracas para dispositivos de controle expõe o DAS a riscos elevados de invasão. Adicionalmente, a presença de servidores web incorporados em dispositivos de campo aumenta a vulnerabilidade a acessos não autorizados, permitindo que invasores executem comandos remotos e manipulem operações do sistema.
5) **Ataques Man-in-the-Middle (MitM):** Ataques MitM são particularmente perigosos porque permitem que os invasores interceptem e modifiquem comunicações entre partes confiáveis. Isso pode resultar na injeção de comandos falsos ou na repetição de mensagens de controle, causando falhas operacionais e comprometendo a segurança e a estabilidade da rede de distribuição.

6) **Mudança de Configuração:** Alterações não autorizadas nas configurações de dispositivos de proteção, como relés e reclosers, podem resultar em interrupções indesejadas ou falhas na proteção do sistema. Atacantes podem explorar essas vulnerabilidades para causar danos intencionais ou falhas operacionais durante situações de falha.

No entanto, ao implementar estratégias robustas de mitigação, é possível proteger esses sistemas contra ciberataques. Essas medidas são essenciais para garantir a resiliência e a confiabilidade das redes de distribuição de energia e podem ser ressaltadas em ordem de importância.

1) **Implementação de Protocolos de Comunicação Seguros:** A adoção de padrões de segurança como o IEC 62351, que fornece medidas de proteção para protocolos de comunicação industrial, é essencial para garantir a integridade e a confidencialidade das comunicações no DAS. Esses padrões ajudam a prevenir ataques de injeção de dados e modificações de pacotes.
2) **Proteção Física dos Dispositivos de Campo:** Garantir que dispositivos de controle estejam protegidos contra acesso físico não autorizado é fundamental. Medidas de segurança física, como cercas, câmeras de vigilância e alarmes, são necessárias para impedir que invasores comprometam diretamente os dispositivos de campo.
3) **Monitoramento e Resposta a Malware:** A implementação de sistemas robustos de detecção e resposta a intrusões (IDS/IPS) é crucial para identificar e mitigar ameaças de malware. Manter os sistemas atualizados com as últimas definições de malware, realizar varreduras regulares e simulações de ataque são práticas recomendadas para fortalecer a resiliência do sistema.
4) **Gestão de Senhas e Autenticação Forte:** Políticas de senhas fortes, incluindo a mudança regular de senhas e a utilização de autenticação multifator (MFA), são essenciais para proteger dispositivos críticos e sistemas de controle. A gestão adequada de senhas ajuda a prevenir acessos não autorizados e invasões.
5) **Criptografia e Assinatura Digital:** O uso de criptografia para proteger dados em trânsito e a implementação de assinaturas digitais para garantir a autenticidade das comunicações são medidas eficazes contra ataques MitM. Essas tecnologias ajudam a assegurar que os dados transmitidos permaneçam confidenciais e não sejam adulterados.
6) **Gerenciamento de Configuração:** Ferramentas de gestão de configuração e auditorias regulares são necessárias para garantir que todas as alterações de configuração sejam autorizadas e devidamente registradas. Implementar alertas para mudanças não autorizadas ajuda a detectar e responder rapidamente a possíveis compromissos de segurança.
7) **Treinamento e Conscientização:** Capacitar operadores e técnicos sobre práticas de segurança cibernética é fundamental para criar uma cultura de segurança. O treinamento contínuo e a conscientização sobre ameaças de engenharia social e a importância de seguir protocolos de segurança ajudam a prevenir ataques baseados em erro humano.

Por fim, os desafios de segurança cibernética são complexos e variados, refletindo a natureza cada vez mais interconectada das redes de informação e automatização dos sistemas de distribuição de energia. Os pontos discutidos nesta seção são essenciais para garantir a resiliência e a segurança das redes de distribuição de energia. Com essas medidas, pode-se proteger os sistemas contra ciberataques, assegurar a continuidade do fornecimento de energia e fortalecer a confiança no uso de tecnologias avançadas no setor elétrico.

B. Proposta para futuras direções de pesquisa

A implementação do protocolo IEC 61850 tem revolucionado a automação de subestações, proporcionando uma comunicação padronizada e interoperável entre dispositivos de diferentes fabricantes. No entanto, à medida que esta tecnologia avança, surgem desafios significativos que precisam ser abordados para garantir sua eficácia e confiabilidade em projetos de grande escala. Esta seção propõe algumas das direções de pesquisas futuras que serão abordadas com base nas lacunas que existem na literatura.

Um dos principais desafios enfrentados é a interoperabilidade entre dispositivos de diferentes fornecedores. Embora a IEC 61850 garanta a comunicação entre dispositivos de diferentes fabricantes, ela não garante a compatibilidade dos arquivos de configuração, o que pode causar problemas de integração, exigindo testes extensivos e ajustes manuais. Além disso, a implementação de redundância, essencial para a confiabilidade do sistema, pode impactar negativamente o tempo de resposta (atrasos de comunicação entre dispositivos), necessitando de uma avaliação cuidadosa para equilibrar ambos os aspectos.

A transmissão de mensagens GOOSE, crucial para a proteção e controle de subestações, também apresenta desafios. A seleção adequada dos switches de rede e a configuração de protocolos de comunicação, como o RSTP (*Rapid Spanning Tree Protocol*), são fundamentais para garantir a entrega rápida e confiável dessas mensagens. Além disso, a criação de ferramentas de integração e expansão eficientes é essencial para facilitar a configuração e gestão de redes complexas, reduzindo o tempo e os custos de engenharia.

Além disso, a análise de desempenho das mensagens GOOSE em cenários de falha e a avaliação das novas ferramentas de configuração do IEC 61850 são áreas que necessitam de investigação. Com a evolução do padrão IEC 61850, é crucial avaliar se as melhorias propostas realmente resolvem os problemas de integração encontrados pelos primeiros adotantes e identificar áreas que ainda precisam de desenvolvimento.

VI. Conclusão

O artigo abordou uma revisão geral sobre os principais protocolos de comunicação e esquema de digitação de

subestações. Uma das maiores preocupações apresentada pelo estudo reflete sobre a grande variedade de dispositivos e diferentes fabricantes e o quanto a não interoperabilidade entre esses dispositivos pode afetar o desempenho dos sistemas de proteção. A não interoperabilidade está diretamente ligada às questões de latência na transmissão e processamento da informação. Por isso a norma IEC 61850 surgiu como uma solução capaz de superar os desafios presentes na automação de subestações, uma vez que a norma integra protocolos de comunicação como SMV, GOOSE, GSSE, MMS e TCP/IP, visando assegurar a interoperabilidade e a comunicação rápida entre dispositivos em diferentes níveis hierárquicos da subestação.

A avaliação de um estudo de caso contribuiu com uma visão de aplicação, com o objetivo de analisar a latência de transmissão dos protocolos de comunicação, como GOOSE e SV, permitindo explorar lacunas e aplicações reais onde existem falhas no sistema.

Além disso, foram discutidos os desafios enfrentados pelo IEC 61850, especialmente no que tange à cibersegurança e à interoperabilidade. Apesar das melhorias significativas introduzidas pelo IEC 61850, a segurança cibernética e a compatibilidade entre dispositivos de diferentes fabricantes ainda requerem atenção contínua e o desenvolvimento de métodos eficazes para mitigar esses problemas.

AGRADECIMENTOS

Os autores gostariam de agradecer à Faculdade de Engenharia de São João (FESJ) da Universidade Estadual Paulista (UNESP) pelas facilidades oferecidas para realização deste trabalho.

REFERENCES

[1] M. S. Thomas, J. D. McDonald, Power system scada and smart grids (Dec. 2017). doi:10.1201/b18338.

[2] D. Baigent, M. Adamiak, R. Mackiewicz, G. Sisco, Iec 61850 communication networks and systems in substations: An overview for users, SISCO Systems (2004).

[3] M. Kr'ol, O. Ascigil, S. Rene, E. Rivière, M. Pigaglio, K. Peeroo, V. Stankovic, R. Sadre, F. Lange, Data availability sampling in ethereum: Analysis of p2p networking requirements, ArXiv abs/2306.11456 (2023). doi:10.48550/arXiv.2306.11456.

[4] K. Saadi, R. Abbou, On iec 61850 communication networks in smart grids system: Methodology of implementation and performances analysis on an experimental platform, International Journal of Energy Research 46 (2021) 103 – 89. doi:10.1002/er.6938.

[5] T. S. Ustun, S. S. Hussain, Iec 62351-4 security implementations for iec 61850 mms messages, IEEE Access 8 (2020) 123979–123985.

[6] S. S. Hussain, T. S. Ustun, A. Kalam, A review of iec 62351 security mechanisms for iec 61850 message exchanges, IEEE Transactions on Industrial Informatics 16 (9) (2019) 5643–5654.

[7] G. Ravikumar, B. Hyder, M. Govindarasu, Efficient modeling of iec-61850 logical nodes in ieds for scalability in cps security testbed, in: 2020 IEEE/PES Transmission and Distribution Conference and Exposition (T&D), IEEE, 2020, pp. 1–5.

[8] U. J. Otokwala, A. Petrovski, Ensemble common features technique for lightweight intrusion detection in industrial control system, in: 2023 IEEE 6th International Conference on Industrial Cyber-Physical Systems (ICPS), IEEE, 2023, pp. 1–6.

[9] Y. Zhang, Y. Zhang, X. Mu, X. Lei, F. Li, J. Zhou, L. Xu, Y. Gao, X. Liu, Development of iec 61850 and its application, in: Proceedings of the International Conference on Computer, Network Security and Communication Engineering (CNSCE), Bangkok, Thailand, 2017, pp. 26–27.

[10] Y. Ge, C. Sun, Y. Shan, T. Shan, D. Hu, Y. Zhu, Design of cloud-based conversion of modbus rtu to iec61850, in: 5th International Conference on Information Science, Electrical, and Automation Engineering (ISEAE 2023), Vol. 12748, SPIE, 2023, pp. 487–494.

[11] S. Kumar, A. Abu-Siada, N. Das, S. Islam, Review of the legacy and future of iec 61850 protocols encompassing substation automation system, Electronics 12 (15) (2023) 3345.

[12] N. Das, A. Haque, H. Zaman, S. Morsalin, S. Islam, Exploring the potential application of iec 61850 to enable energy interconnectivity in smart grid systems, IEEE Access (2024).

[13] S. M. Farooq, S. S. Hussain, T. S. Ustun, S-gosv: Framework for generating secure iec 61850 goose and sample value messages, Energies 12 (13) (2019) 2536.

[14] S. S. Hussain, S. M. Farooq, T. S. Ustun, A method for achieving confidentiality and integrity in iec 61850 goose messages, IEEE transactions on Power Delivery 35 (5) (2020) 2565–2567.

[15] M. F. Elrawy, E. Tekki, L. Hadjidemetriou, C. Laoudias, M. K. Michael, Protection and communication model of intelligent electronic devices to investigate security threats, in: 2023 IEEE Power & Energy Society Innovative Smart Grid Technologies Conference (ISGT), IEEE, 2023, pp. 1–5.

[16] H. T. Reda, B. Ray, P. Peidaee, A. Anwar, A. Mahmood, A. Kalam, N. Islam, Vulnerability and impact analysis of the iec 61850 goose protocol in the smart grid, Sensors 21 (4) (2021) 1554.

[17] S. Singh, Efficient data communication: Strategies for optimizing bandwidth utilization and minimizing latency in modern networks, Modern Data Networks 1.

[18] D. F. C. Solórzano, J. A. G. Chuñir, F. A. Q. Palomeque, Didactic integration for the monitoring of electric power systems using power monitoring expert with modbus tcp/ip and iec 61850 communication, in: 2023 5th Global Power, Energy and Communication Conference (GPECOM), IEEE, 2023, pp. 244–249.

[19] J. W. Konka, C. M. Arthur, F. J. Garcia, R. C. Atkinson, Traffic generation of iec 61850 sampled values, in: 2011 IEEE First International Workshop on Smart Grid Modeling and Simulation (SGMS), IEEE, 2011, pp. 43–48.

[20] V. Dehalwar, A. Kalam, M. L. Kolhe, A. Zayegh, Review of ieee 802.22 and iec 61850 for real-time communication in smart grid, in: 2015 International Conference on Computing and Network Communications (CoCoNet), IEEE, 2015, pp. 571–575.

[21] M. Strobel, N. Wiedermann, C. Eckert, Novel weaknesses in iec 62351 protected smart grid control systems, in: 2016 IEEE International Conference on Smart Grid Communications (SmartGridComm), IEEE, 2016, pp. 266–270.

[22] P. R. C. De Araújo, R. H. Filho, J. J. Rodrigues, J. P. Oliveira, S. A. Braga, Infrastructure for integration of legacy electrical equipment into a smart-grid using wireless sensor networks, Sensors 18 (5) (2018) 1312.

[23] P. R. C. Araújo, R. H. Filho, J. J. Rodrigues, J. P. Oliveira, S. A. Braga, Middleware for integration of legacy electrical equipment into smart grid infrastructure using wireless sensor networks, International Journal of Communication Systems 31 (1) (2018) e3380.

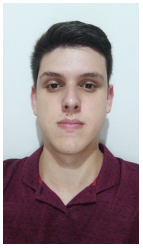
[24] L. Chen, H. Li, T. Charton, R. Zhang, Virtual digital substation test system and interoperability assessments. energies 2021, 14, 2337 (2021).

[25] E. Rencelj Ling, M. Ekstedt, Generating threat models and attack graphs based on the iec 61850 system configuration description language, in: Proceedings of the 2021 ACM Workshop on Secure and Trustworthy Cyber-Physical Systems, 2021, pp. 98–103.

[26] S. Kumar, A. Abu-Siada, N. Das, S. Islam, Toward a substation automation system based on iec 61850. electronics 2021, 10, 310 (2021).

[27] E. I. Sharing, Analysis of the cyber attack on the Ukrainian power grid, Tech. rep., Electr. Inf. Sharing Anal. Center, Washington, DC, USA (Mar. 2016).

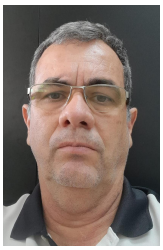
VII. BIOGRAPHIES



Gustavo da Costa Lilli é estudante de Engenharia Eletrônica e de Telecomunicações na Universidade Estadual Paulista (UNESP), onde iniciou os estudos em 2023. Tem desenvolvido pesquisas de iniciação científica nas áreas de comunicação e controle de sistemas, com foco em subestações de energia elétricas e protocolos de comunicação em sistemas de automação.

Leonardo da Silva Lessa possui graduação em Engenharia Elétrica pela Faculdade de Engenharia de Ilha Solteira (FEIS/UNESP) - Universidade Estadual Paulista (2017) e Mestrado em Engenharia Elétrica pela Faculdade de Engenharia de São João da Boa Vista (FESJ/UNESP) - Universidade Estadual Paulista (2020). Atualmente, é doutorando na Escola de Engenharia de São Carlos (EESC/USP) - Universidade de São Paulo. Seus principais interesses de pesquisa incluem transitórios eletromagnéticos, localização de faltas, modelagem de sistemas e algoritmos inteligentes aplicados a sistemas de distribuição com geração distribuída.

Caio Vinicius Colozzo Grilo possui graduação em Engenharia Eletrônica e de Telecomunicações pela Faculdade de Engenharia de São João (FESJ/UNESP) - Universidade Estadual Paulista (2021) e Mestrado em Engenharia Elétrica pela Escola de Engenharia de São Carlos (EESC/USP) - Universidade de São Paulo (2023). Atualmente, é doutorando na Escola de Engenharia de São Carlos (EESC/USP) - Universidade de São Paulo. Seus principais interesses de pesquisa incluem geração distribuída, transitórios eletromagnéticos, localização de faltas e algoritmos inteligentes aplicados a sistemas de distribuição com geração distribuída.



Afonso José do Prado obteve a graduação (1991) e o mestrado (1995) em Engenharia Elétrica pela Universidade Estadual Paulista Júlio de Mesquita Filho, UNESP. Obteve o doutorado em Engenharia Elétrica na Universidade Estadual de Campinas, UNICAMP, em 2002. Desde 2015, é docente da FESJ/UNESP em São João da Boa Vista.