ISSN 1678-0817 Qualis B2
Revista Científica de Alto Impacto.

ISSN 1678-0817 Qualis B2
Revista Científica de Alto Impacto.

EFICIÊNCIA COM SEGURANÇA: INTEGRAÇÃO DO IEC 61850 COM O IEC 62351 PARA MITIGAR RISCOS DE ATAQUES CIBERNÉTICOS EM SUBESTAÇÕES DIGITAIS

Ciências Exatas e da Terra, Edição 126 SET/23 SUMÁRIO, Engenharia Elétrica / 25/09/2023

EFFICIENCY WITH SECURITY: IEC 61850 INTEGRATION WITH IEC 62351 TO MITIGATE CYBERSECURITY ATTACK RISKS IN SUBSTATIONS

REGISTRO DOI: 10.5281/zenodo.8376843

Lucas Matheus Matos Pacheco Ziles
Rian Lima Silva
Iuri de Paula Jordão Gomes
Roniel Brito de Souza
Joana Luísa Alves Fraga
Alex Dayne Melo Conde
Nathalia Martins da Silva Reis Pimentel

Resumo: A automação de subestações elétricas desempenha um papel crítico na modernização e eficiência dos sistemas de energia elétrica. No entanto, a crescente dependência do protocolo IEC 61850 para comunicação e controle pode criar vulnerabilidades significativas à segurança cibernética. Este artigo explora a importância do IEC 61850 no monitoramento de subestações além de destacar a necessidade de integração com o IEC 62351 como uma medida crucial para mitigar os riscos de ataque cibernético.

Palavras-chave: Automação, modernização, controle, vulnerabilidade, ataque cibernético.

Abstract: Substation automation plays a critical role in the modernization and efficiency of electrical power systems. However, the increasing reliance on the IEC 61850 protocol for communication and control can create significant cybersecurity vulnerabilities. This article explores the importance of IEC 61850 in substation monitoring while highlighting the need for integration with IEC 62351 as a crucial measure to mitigate cyberattack risks.

Keywords: Automation, modernization, control, vulnerability, cyberattack.

INTRODUÇÃO

“A subestação desempenha um papel vital na transferência de eletricidade, realizando a conversão do nível de voltagem de alto para baixo e vice-versa por meio de transformadores de potência, além de executar operações de comutação e proteção” (AFTAB, 2020). Portanto, desenvolver métodos para a automação de subestações é de suma importância, uma vez que impacta consideravelmente nos custos de operação, qualidade da energia e capacidade de resposta a falhas, oferecendo recursos e funcionalidades únicas que não seriam viáveis com sistemas legados.

Aftab (2020) completa destacando que “Por meio de um protocolo de comunicação padrão, as concessionárias podem instalar dispositivos de diferentes fabricantes que podem cooperar prontamente no ambiente da concessionária. Após pesquisas deliberadas e inúmeras reuniões, a agência de padronização IEC TC 57 propôs o padrão IEC 61850 para automação de subestações.”

O protocolo IEC 61850 funciona como um meio de comunicação que permite a troca eficiente de informações entre sistemas de energia elétrica, sendo otimizado para uso de bytes e adaptado para funcionar sobre TCP/IP-Ethernet, tirando proveito das tecnologias de rede modernas.

No entanto, a crescente preocupação com a segurança cibernética se tornou evidente. A possibilidade de monitorar e controlar irrestritamente todos os dispositivos levanta sérias preocupações quanto a ataques cibernéticos.

Conforme observado por Hussain (2019), “A cibersegurança não era realmente um tópico de pesquisa proeminente, uma vez que os protocolos de comunicação para o sistema de energia eram considerados altamente especializados e distintos. Assim, a abordagem de ‘segurança pela obscuridade’ era considerada suficiente. Além disso, os dados trocados nessas comunicações, como medições de tensão de uma linha de energia, não eram considerados tão valiosos quanto informações financeiras.”

Em resposta a esses desafios, foi desenvolvida a série de padrões IEC 62351, projetada especificamente para abordar questões de segurança cibernética nos padrões de comunicação de energia. Esses padrões fornecem medidas e soluções abrangentes de segurança de ponta a ponta para proteger contra possíveis ataques. Este artigo abordará a funcionalidade desses protocolos, sua integração e as expectativas futuras em relação a essa tecnologia.

REVISÃO BIBLIOGRÁFICA

Aftab (2020) informa que “As subestações são componentes essenciais das redes elétricas inteligentes, onde o sistema de comunicação é integrado. No entanto, alcançar um sistema de comunicação de subestação padrão que possa operar com os princípios de plug- and-play (PnP) não é uma tarefa trivial. Considerando a natureza ciberfísica dos equipamentos do sistema de energia, a integração requer mais diligência para uma operação segura. Além disso, existem muitos tipos diferentes de equipamentos de subestação fabricados por inúmeros fornecedores. Alcançar uma linguagem comum e interoperabilidade entre eles é uma tarefa difícil.

O padrão IEC 61850 tem avançado na direção desse objetivo, sua estrutura orientada a objetos o torna versátil, enquanto blocos de modelagem bem definidos garantem compatibilidade. O trabalho recente tem se concentrado na modelagem baseada em IEC 61850 de equipamentos de subestação, no desenvolvimento de formatos de troca de mensagens para funcionalidades de subestação, bem como na investigação do desempenho de diferentes tecnologias de comunicação quando são usadas para implementar modelos baseados em IEC 61850.”

A complexidade de lidar com equipamentos de diferentes fornecedores é mencionada como um obstáculo. O avanço do padrão IEC 61850 é reconhecido como uma abordagem promissora para superar esses desafios, com ênfase na modelagem, formatos de troca de mensagens e investigação de tecnologias de comunicação.

Em resumo, a norma IEC61850 é um padrão internacional para comunicação em subestações elétricas. Ela define um conjunto de regras e protocolos para garantir a interoperabilidade entre os diferentes dispositivos presentes em uma subestação digital de alta tensão.

Essa norma é fundamental para o funcionamento das subestações digitais de alta tensão, pois permite que diferentes fabricantes possam desenvolver equipamentos compatíveis e interconectados, garantindo a eficiência e confiabilidade do sistema como um todo.

> *"Esta norma (IEC 61850) foi publicada em 2004, mas vem sendo desenvolvida desde a década de 1990 envolvendo grandes entidades de pesquisas mundiais, como o Electric Power Research Institute (EPRI), Ingeneering Eletrothecnical Comitê (IEC), Centro de Pesquisas de Energia Elétrica (Cepel), só para citar alguns. A norma tem grande aceitação nas Américas, Europa e Ásia e já esta se firmando como um padrão mundial, o que justifica uma real avaliação pelas empresas sobre a pertinência da sua utilização." (SOUZA, 2016).*

O fato de a norma ter obtido uma ampla aceitação nas Américas, Europa e Ásia e estar se consolidando como um padrão global implica na sua importância e relevância no cenário da automação de subestações elétricas, sugerindo que as empresas devem considerar seriamente a adoção dessa norma.

A automação de subestações foi possível graças ao desenvolvimento dos IEDs – Dispositivos Eletrônicos Inteligentes – que são evoluções dos tradicionais relés de proteção. São unidades multifuncionais, microprocessadas, para a proteção, controle, medição e monitoramento de sistemas elétricos, permitindo ainda a concepção de lógicas de bloqueio e de intertravamentos.

Kreutz (2014) conta que "Os IEDs possuem diferentes tipos de interface com o usuário, sendo a comunicação remota a mais importante delas. Normalmente os dados processados pelos IEDs são lidos por um sistema SCADA e apresentados ao usuário via uma IHM. Em um ambiente de rede ethernet TCP/IP, um IED pode ser pensado como um servidor, possuindo uma interface de comunicação que possui um endereço IP, acessível através de uma rede por um cliente externo. O servidor pode então aceitar uma conexão de um ou mais clientes externos, autenticar esta conexão, sincronizar seu relógio com o cliente, e transferir informações entre ele o cliente.

A função da norma IEC 61850 em relação às IEDs é fornecer uma linguagem de configuração padronizada, facilitando a configuração integrada do sistema e padronizando as informações relativas aos IEDs. Além disso, a norma também fornece redundância a falhas em qualquer ponto do sistema, permitindo a utilização direta de dispositivos de diferentes fabricantes em uma única rede. A adoção da norma também garante com que a instalação não sofra obsolência, possibilitando expansões futuras de forma mais rápida e com menores custos, além de permitir o uso de lógicas de seletividade mais eficientes, reduzindo o desgaste dos equipamentos do sistema.

Souza (2016) acrescenta que "O padrão IEC 61850 toma como base o princípio de orientação a objetos, de forma a trabalhar com modelamento orientado a informação e não ao dispositivo nem ao protocolo. Esses modelos definem os formatos dos dados, identificadores, comportamento e controles."

Para compreender seu funcionamento é necessário saber que protocolo IEC 61850 dispõe da adoção de alguns dispositivos para auxiliar nas suas funções de controle e monitoramento, como por exemplo Merging Units e o emprego de distintos mensageiros como sampled values e mensagens goose.

Segundo Pena (2018) “É sabido que a automação do barramento de processo em uma subestação está pautada na digitalização dos valores de tensão e corrente nos secundários dos TP’s e TC’s. Nesse sentido, como forma de amostrar os valores de corrente e tensão, a norma IEC 61850 prevê a utilização do dispositivo conhecido como Merging Unit e definido pela sigla MU.” Em resumo, o dispositivo converte sinais analógicos em sinais digitais, adotando o uso de sensores, para transmissão dos dados coletados para as IEDs na sala de controle da subestação. Para isso, o MU é composto por um circuito elétrico para leitura dos valores analógicos, um conversor analógico-digital para amostragem dos sinais e um processador para padronização dos dados digitais de acordo com a norma IEC 61850. Para compensar o atraso no processamento interno, é comum utilizar um sincronizador de tempo externo, como o GPS. Além disso, as Merging Units também possibilitam a redução do cabeamento necessário na subestação, uma vez que os sinais digitais podem ser transmitidos por meio de cabos de fibra óptica ou redes Ethernet. Isso resulta em uma redução significativa nos custos de instalação e manutenção da subestação.

Ingram (2013) relata que “A IEC 61850-5 especifica limites de tempo para a entrega de mensagens, incluindo GOOSE (Generic Object Oriented Substation Event) e sampled values. Os requisitos para uma mensagem dependem do tipo de mensagem e da classe de desempenho da aplicação. “

Sampled values são fluxos contínuos de dados que contêm números inteiros de 32 bits representando valores amostrados de um barramento de processo, ou seja, são valores de tensão e corrente que são amostrados em alta frequência e transmitidos digitalmente para a unidade de controle da subestação. Esses valores são usados para monitorar e controlar o sistema elétrico em tempo real, permitindo uma resposta mais rápida a eventos como falhas na rede ou sobrecargas.

As mensagens GOOSE são mensagens periódicas em uma taxa baixa (mensagens de “batimento cardíaco”) ou esporádicas em uma taxa alta (geralmente, três mensagens enviadas em alguns milissegundos). As mensagens GOOSE são tipicamente comandos do SAS (por exemplo, abrir ou fechar um interruptor, disparar ou fechar um disjuntor, ou controles de mudança de tap de transformador) ou atualizações de status da planta de alta tensão (por exemplo, indicações digitais, valores analógicos transmitidas e confirmações de comando). Essas mensagens são baseadas em objetos genéricos, que podem ser definidos pelo usuário de acordo com as necessidades específicas da aplicação. Além disso, elas são transmitidas através de redes Ethernet, o que simplifica a infraestrutura de comunicação e permite maior flexibilidade na configuração da rede.

Quando foi desenvolvido o protocolo IEC 61850, não havia a necessidade percebida de implementar medidas de segurança cibernética, pois seu principal propósito era estabelecer uma padronização para a interligação de dispositivos elétricos de diferentes fabricantes. No entanto, com o avanço das ameaças cibernéticas, tornou-se claro que a segurança da informação era uma preocupação crucial. Portanto, o protocolo IEC 62351 surgiu como um complemento necessário, centrado nas questões de segurança, a fim de evitar o vazamento de dados e proteger os sistemas contra possíveis ataques cibernéticos.

“Geralmente, os canais de comunicação usados para a comunicação do sistema de energia são de banda estreita, com restrições de largura de banda, portanto, as medidas de segurança resultantes incluem sobrecargas adicionais, como trocas de chaves, assinaturas digitais etc. Além disso, os equipamentos de comunicação de energia, como controladores, têm poder de processamento e memória limitados, tornando assim medidas de segurança, como criptografia, muito difíceis.” (HUSSAIN, 2019).

O IEC 62351 é uma série de padrões desenvolvidos para abordar questões de segurança cibernética nos padrões de comunicação de energia. Ele fornece medidas e soluções de segurança de ponta a ponta para possíveis ataques. O IEC 62351 consiste em 16 partes que abrangem desde a introdução às questões de segurança até a geração, distribuição, revogação e manipulação de certificados de chave pública e chaves criptográficas. Ele também define modelos de objetos de gerenciamento de rede e sistema (NSM) para determinar a segurança e a confiabilidade da rede. Esses modelos ajudam na detecção de intrusão, monitoramento da saúde e condição dos IEDs (Intelligent Electronic Devices). Além disso, o IEC 62351 fornece orientações sobre tópicos de segurança a serem abordados em padrões e especificações. Em resumo, o IEC 62351 é um conjunto de padrões que visa garantir a segurança e a confiabilidade das comunicações de energia, fornecendo diretrizes e soluções para proteger contra possíveis ataques cibernéticos.

Hussain (2019) completa dizendo que “Os quatro requisitos básicos de segurança em qualquer sistema para prevenir as quatro ameaças básicas de segurança são:

1. Confidencialidade – prevenção de acesso não autorizado a informações;
2. Integridade – prevenção de qualquer modificação ou roubo de informações;
3. Disponibilidade – prevenção da negação de serviço e disponibilidade de informações para usuários autorizados;
4. Não repúdio – prevenção da negação de uma ação que ocorreu ou da reivindicação de uma ação que não ocorreu.”

Esses requisitos – confidencialidade, integridade, disponibilidade e não repúdio – desempenham um papel crucial na proteção das informações e na garantia de que os sistemas permaneçam seguros e confiáveis. Eles formam a base sólida sobre a qual as estratégias de segurança são construídas, ajudando a prevenir ameaças potenciais e a manter a integridade dos dados e serviços.

METODOLOGIA

A metodologia deste artigo será baseada em uma revisão sistemática da literatura, com o objetivo de explorar e sintetizar as informações relevantes relacionadas ao IEC 61850, sua importância, vantagens, vulnerabilidades e a integração com o IEC 62351. As estapas seguidas foram:

1. Levantamento bibliográfico: fora realizado um levantamento de artigos cientificos sobre a IEC 61850 no Google Schoolar, com o auxílio do SCI-HUB para ter acesso aos conteúdos na integra.
2. Tradução: Por ter pouco conteúdo publicado em português, foi adotado do ChatGPT da OpenAI para fazer a tradução dos artigos de forma rápida e sem perder coesão e coerência.
3. Filtragem do material de interesse: Foi realizado a leitura de uma seleção de artigos sobre o tema, da qual extraiu informações de apenas alguns.
4. Analise e síntese do conteúdo: Síntese das informações coletadas para criar uma visão abrangente sobre o IEC 61850, sua relação com a segurança cibernética e as perspectivas futuras com a integração do IEC 62351.

RESULTADOS E DISCUSSÃO

A revisão da literatura revelou a importância fundamental do protocolo IEC 61850 na automação de subestações elétricas, destacando seus benefícios em termos de eficiência e interoperabilidade. Esse protocolo permite a integração de dispositivos de diferentes fabricantes, proporcionando uma padronização para o setor elétrico. No entanto, tornou-se evidente que o IEC 61850 não considerou inicialmente as questões de segurança cibernética, uma vez que seu desenvolvimento ocorreu em uma época em que a segurança da informação não era uma prioridade.

Com o aumento das ameaças cibernéticas e a dependência crescente do IEC 61850, tornou-se crucial abordar as vulnerabilidades inerentes a esse protocolo. A série de padrões IEC 62351 foi desenvolvida especificamente para atender a essas preocupações, fornecendo medidas abrangentes de segurança cibernética para proteger os sistemas de energia contra possíveis ataques.

A análise desses padrões IEC 62351 mostrou que eles abrangem várias áreas, desde a geração e distribuição de certificados de chave pública até a detecção de intrusões e monitoramento da saúde dos dispositivos eletrônicos inteligentes (IEDs). Esses padrões fornecem uma estrutura sólida para a implementação de medidas de segurança cibernética em sistemas de energia.

Além disso, foi ressaltada a importância dos quatro requisitos básicos de segurança: confidencialidade, integridade, disponibilidade e não repúdio. Esses requisitos são essenciais para prevenir as quatro ameaças básicas de segurança e formam a base para o desenvolvimento de estratégias de segurança eficazes.

Portanto, a integração do IEC 61850 com o IEC 62351 surge como uma medida crucial para mitigar os riscos de ataques cibernéticos em subestações elétricas. Essa integração permite que os sistemas de energia aproveitem os benefícios do IEC 61850 enquanto implementam medidas sólidas de segurança cibernética de acordo com os padrões do IEC 62351.

CONCLUSÃO

A automação de subestações elétricas é essencial para modernizar o setor de energia elétrica. As subestações digitais de alta tensão oferecem várias vantagens em relação às subestações convencionais, incluindo maior eficiência energética, controle mais preciso do fluxo de energia e redução das perdas por dissipação de calor. Além disso, proporcionam maior segurança devido à menor propensão a falhas e erros humanos, e facilitam a manutenção e o diagnóstico de problemas por meio do monitoramento remoto em tempo real.

Dentre os recursos que as subestações digitais possuem, vale destacar:

Merging Units (MU): Convertem sinais analógicos de tensão e corrente em sinais digitais para transmissão às IEDs, integrando informações na automação de subestações.

Sampled Values: Permitem a transmissão contínua de valores amostrados de tensão e corrente para monitoramento e controle em tempo real do sistema elétrico.

Mensagens GOOSE (Generic Object Oriented Substation Event): Contêm comandos do SAS (Sistema de Automação de Subestações) e atualizações de status da planta de alta tensão, simplificando a comunicação e oferecendo flexibilidade na configuração da rede.

No entanto, a crescente dependência do protocolo IEC 61850 levanta preocupações sobre a segurança cibernética. Para contornar essa questão, o IEC 61850, inicialmente criado sem um foco específico em segurança cibernética, precisou ser complementado pelo IEC 62351 para proteger os sistemas elétricos contra possíveis ataques hackers. A implementação do IEC 62351, no entanto, apresenta desafios significativos, principalmente em relação ao custo, dada a possibilidade de substituir muitos dispositivos antigos que não suportam os novos protocolos.

Os ataques cibernéticos em subestações podem ter consequências graves para a segurança do sistema elétrico, afetando desde o fornecimento de energia até a integridade física das pessoas envolvidas. Entre os principais riscos estão a possibilidade de desligamento remoto de equipamentos, a manipulação de dados de medição e controle, além da exposição de informações sensíveis do sistema.

Essa integração é crucial para garantir que a automação das subestações continue eficiente e segura. Afinal, a segurança da informação é tão importante quanto a eficiência na automação elétrica. Portanto, a união desses padrões é a chave para um setor elétrico moderno, eficiente e protegido contra os ataques cibernéticos em constante evolução. No futuro, podemos esperar que, após uma integração bem-sucedida desses protocolos, a utilização de inteligência artificial e machine learning também se torne uma tendência, possibilitando a previsão de falhas e a otimização do desempenho do sistema.

REFERÊNCIAS

Aftab, M. A., Hussain, S. M. S., Ali, I., & Ustun, T. S. (2020). IEC 61850 based substation automation system: A survey. International Journal of Electrical Power & Energy Systems, 120, 106008. doi:10.1016/j.ijepes.2020.106008

Albarakati, A., Robillard, C., Karanfil, M., Kassouf, M., Debbabi, M., Youssef, A., ... Hadjidj, R.

(2021). Security Monitoring of IEC 61850 Substations Using IEC 62351-7 Network and System Management. IEEE Transactions on Industrial Informatics, 1–1. doi:10.1109/tii.2021.3082079

Hussain, S. M. S., Ustun, T. S., & Kalam, A. (2019). A Review of IEC 62351 Security

Mechanisms for IEC 61850 Message Exchanges. IEEE Transactions on Industrial Informatics, 1–1. doi:10.1109/tii.2019.2956734

Ingram, D. M. E., Schaub, P., Taylor, R. R., & Campbell, D. A. (2013). Performance Analysis of IEC 61850 Sampled Value Process Bus Networks. IEEE Transactions on Industrial Informatics, 9(3), 1445–1454. doi:10.1109/tii.2012.2228874

PENA, D. **MERGING UNIT – UMA BREVE ABORDAGEM.** 4 de setembro de 2018. Linkedin:

Dayane Pena – Engenheira Eletricista | Mec Nc. Disponível em: <https://www.linkedin.com/pulse/merging-unit-uma-breve-abordagem-dayane- pena/?originalSubdomain=pt>. Acesso em 6 de setembro de 2023,

SOUZA, E. H N. **AUTOMAÇÃO DE SUBESTAÇÕES COM PROTOCOLO IEC-61850: estudo de caso**. Monografia de especialização UTFPR, Curitiba, 2016. Disponível em: <http://riut.utfpr.edu.br/jspui/bitstream/1/17088/1/CT_CEAUT_2015_10.pdf>. Acesso em 6 de setembro de 2023.

← Post anterior

RevistaFT

A RevistaFT têm 28 anos. É uma **Revista Científica Eletrônica Multidisciplinar Indexada de Alto Impacto e Qualis "B2" em 2023.** Periodicidade mensal e de acesso livre. Leia gratuitamente todos os artigos e publique o seu também clicando aqui.

Contato

Queremos te ouvir.
WhatsApp RJ: (21) 98159-7352
WhatsApp SP: (11) 98597-3405
e-Mail:
contato@revistaft.com.br

Conselho Editorial

Editores Fundadores:
Dr. Oston de Lacerda Mendes.
Dr. João Marcelo Gigliotti.
Editor Científico:
Dr. Oston de Lacerda Mendes

ISSN: 1678-0817

CNPJ: 48.728.404/0001-22

CAPES – Coordenação de Aperfeiçoamento de Pessoal de Nível Superior (CAPES), fundação do Ministério da Educação (MEC), desempenha papel fundamental na expansão e consolidação da pós-graduação stricto sensu (mestrado e doutorado) em todos os estados da Federação.

Orientadoras:

Dra. Hevellyn Andrade Monteiro

Dra. Chimene Kuhn Nobre

Revisores:

Lista atualizada periodicamente em revistaft.com.br/expediente

Venha fazer parte de nosso time de revisores também!

Rua José Linhares, 134 - Leblon | Rio de Janeiro-RJ | Brasil