UNIVERSIDADE FEDERAL DO CEARÁ

CENTRO DE TECNOLOGIA

DEPARTAMENTO DE ENGENHARIA ELÉTRICA

CURSO DE GRADUAÇÃO EM ENGENHARIA ELÉTRICA

MARCUS VINICIUS SOARES REBOUÇAS

DESENVOLVIMENTO DE UM SISTEMA SUPERVISÓRIO SCADA-LTS PARA MONITORAMENTO E COMANDO DE IEDS EM USINA FOTOVOLTAICA COM ACESSO REMOTO

FORTALEZA

2025

MARCUS VINICIUS SOARES REBOUÇAS

DESENVOLVIMENTO DE UM SISTEMA SUPERVISÓRIO SCADA-LTS PARA MONITORAMENTO E COMANDO DE IEDS EM USINA FOTOVOLTAICA COM ACESSO REMOTO

Trabalho de Conclusão de Curso apresentado ao Curso de Graduação em Engenharia Elétrica do Centro de Tecnologia da Universidade Federal do Ceará, como requisito parcial à obtenção do grau de bacharel em Engenharia Elétrica.

Orientador: Prof. Dr. Lucas Silveira Melo

FORTALEZA

2025

Dados Internacionais de Catalogação na Publicação
Universidade Federal do Ceará
Sistema de Bibliotecas
Gerada automaticamente pelo módulo Catalog, mediante os dados fornecidos pelo(a) autor(a)

R241d Rebouças, Marcus Vinicius Soares.
Desenvolvimento de um sistema supervisório SCADA-LTS para monitoramento e comando de IEDs em usina fotovoltaica com acesso remoto / Marcus Vinicius Soares Rebouças. – 2026.
83 f. : il. color.

Trabalho de Conclusão de Curso (graduação) – Universidade Federal do Ceará, Centro de Tecnologia, Curso de Engenharia Elétrica, Fortaleza, 2026.
Orientação: Prof. Dr. Lucas Silveira Melo.

1. Micro e minigeração distribuída. 2. Sistema SCADA. 3. Supervisão remota. 4. Código aberto. 5. Proteção elétrica. I. Título.

CDD 621.3

MARCUS VINICIUS SOARES REBOUÇAS

DESENVOLVIMENTO DE UM SISTEMA SUPERVISÓRIO SCADA-LTS PARA MONITORAMENTO E COMANDO DE IEDS EM USINA FOTOVOLTAICA COM ACESSO REMOTO

Trabalho de Conclusão de Curso apresentado ao Curso de Graduação em Engenharia Elétrica do Centro de Tecnologia da Universidade Federal do Ceará, como requisito parcial à obtenção do grau de bacharel em Engenharia Elétrica.

Aprovada em:

BANCA EXAMINADORA

Prof. Dr. Lucas Silveira Melo (Orientador)
Universidade Federal do Ceará (UFC)

Prof. Dr. Raimundo Furtado Sampaio
Universidade Federal do Ceará (UFC)

Francisco Petrucio Andrade da Silva
Engenheiro Eletricista, Especialista em Engenharia Clínica

À memória do meu querido avô, que foi um grande exemplo de vida, bondade e determinação. Mesmo ausente fisicamente, sua influência e seus ensinamentos seguem vivos em meu coração e foram essenciais para que eu chegasse até aqui.

AGRADECIMENTOS

Gostaria de expressar, primeiramente, minha profunda gratidão aos meus pais e a toda a minha família, cujo apoio incondicional foi essencial ao longo de toda a minha trajetória acadêmica. A presença constante, o amor, a paciência e a compreensão de vocês foram o alicerce que me permitiu seguir em frente, mesmo nos momentos mais difíceis. Sem o incentivo e a confiança de todos vocês, certamente eu não teria chegado até aqui.

Agradeço, de forma especial, a todos que me apoiaram ao longo dessa jornada acadêmica e que foram fundamentais para que eu alcançasse meus objetivos. Em particular, registro minha gratidão aos professores que contribuíram para o meu crescimento profissional e pessoal, com destaque ao Professor Dr. Lucas Silveira Melo, que acreditou no meu potencial, ofereceu orientação constante e foi peça-chave no desenvolvimento deste trabalho. Seu apoio e suas contribuições foram cruciais para a realização deste projeto com dedicação e êxito.

Aos meus amigos de Campina Grande, que estiveram comigo no início dessa caminhada e foram essenciais para que eu me encontrasse dentro dessa graduação, deixo meu sincero agradecimento. Em especial, Marcos Henrique e Lucas Viana, que sempre estiveram ao meu lado durante o período em que estive lá. A companhia, o apoio e a amizade de vocês tornaram os primeiros desafios dessa trajetória muito mais leves.

Aos meus colegas da UFC, João Pedro e Rubens Costa, com quem compartilhei grande parte da graduação, trabalhando, estudando e trocando conhecimentos ao longo do curso, agradeço pela parceria e colaboração. A convivência e o apoio mútuo foram fundamentais para manter o foco e superar as dificuldades, possibilitando a conquista dos objetivos ao longo dessa jornada.

Por fim, agradeço aos meus primos Ivo Gabriel e Gabriel Marques, que sempre se fizeram presentes quando precisei, oferecendo apoio e força nos momentos mais desafiadores. O carinho e a amizade de vocês foram extremamente importantes em diversas etapas da minha caminhada.

RESUMO

Atualmente, com o crescimento da micro e da minigeração distribuída, observa-se que o acompanhamento presencial das usinas não ocorre de forma diária, e os intervalos de manutenção tendem a ser cada vez mais longos. Como consequência, muitas dessas instalações permanecem desacompanhadas por períodos prolongados, o que pode resultar na não detecção imediata de falhas operacionais. Essa condição pode ocasionar perdas de geração de energia e, consequentemente, prejuízos financeiros aos proprietários das usinas. Diante desse cenário, torna-se evidente a necessidade de uma forma eficiente de supervisão remota dessas instalações.

Nesse contexto, os sistemas de supervisão e controle, especialmente os sistemas SCADA (Supervisory Control and Data Acquisition), destacam-se como uma das soluções mais amplamente utilizadas em diversos setores industriais. Atualmente, os sistemas SCADA estão cada vez mais presentes em áreas como a indústria, a manutenção de instalações críticas, hospitais e, principalmente, na proteção de sistemas elétricos. Esses sistemas desempenham um papel fundamental na supervisão contínua e na segurança das instalações, permitindo o monitoramento em tempo real, o registro de eventos e a adequada coordenação entre relés de proteção e disjuntores.

Dessa forma, este trabalho tem como objetivo demonstrar a implementação de um sistema SCADA baseado em software de código aberto (open source), propondo uma solução de baixo custo, flexível e escalável. Adicionalmente, será incorporado o uso de uma Rede Privada Virtual (VPN), possibilitando o acesso remoto seguro ao sistema de supervisão, o que amplia sua aplicabilidade e viabilidade em ambientes reais de operação. Conclui-se que o objetivo deste trabalho foi plenamente alcançado, uma vez que foi desenvolvido e validado um sistema supervisório específico para uma usina fotovoltaica utilizando soluções de baixo custo e software de código aberto. A implementação de um SCADA dedicado ao relé de proteção mostrou-se eficaz durante os testes realizados, tanto em ambiente de bancada quanto com o auxílio de maleta de testes, atendendo satisfatoriamente às demandas de monitoramento, supervisão e acesso remoto seguro. O sistema possibilita que usuários autorizados sejam notificados sobre eventos operacionais, acessem o relé remotamente e visualizem registros e ocorrências fornecidos pelo próprio equipamento. Apesar das limitações inerentes ao SCADA-LTS, especialmente no que se refere à interface gráfica e à necessidade de conhecimentos em HTML e JavaScript, os resultados demonstram que a ferramenta é adequada para a aplicação proposta.

Palavras-chave: Micro e minigeração distribuída. Sistema SCADA. Supervisão remota. Código

aberto. Proteção elétrica. VPN. Automação. Baixo custo.

ABSTRACT

Currently, with the growth of micro and mini distributed generation, it is observed that on-site monitoring of power plants does not occur on a daily basis, and maintenance intervals tend to become increasingly longer. As a result, many of these installations remain unattended for extended periods, which may lead to the delayed detection of operational faults. This condition can cause losses in energy generation and, consequently, financial losses for plant owners. In this context, the need for an efficient method of remote supervision of these installations becomes evident. Within this scenario, supervision and control systems, especially SCADA (Supervisory Control and Data Acquisition) systems, stand out as one of the most widely used solutions across various industrial sectors. Currently, SCADA systems are increasingly present in areas such as industry, maintenance of critical facilities, hospitals, and, most notably, in the protection of electrical power systems. These systems play a fundamental role in continuous supervision and operational safety, enabling real-time monitoring, event logging, and proper coordination between protection relays and circuit breakers. Thus, this work aims to demonstrate the implementation of a SCADA system based on open-source software, proposing a low-cost, flexible, and scalable solution. Additionally, the use of a Virtual Private Network (VPN) is incorporated, enabling secure remote access to the supervision system, thereby expanding its applicability and feasibility in real operating environments. It is concluded that the objective of this work was fully achieved, as a supervisory system specifically designed for a photovoltaic power plant was developed and validated using low-cost solutions and open-source software. The implementation of a SCADA system dedicated to the protection relay proved to be effective during the tests performed, both in a laboratory environment and with the support of a relay test set, satisfactorily meeting the requirements for monitoring, supervision, and secure remote access. The system allows authorized users to be notified of operational events, remotely access the relay, and view records and events provided by the device itself. Despite the inherent limitations of SCADA-LTS, particularly regarding the graphical interface and the need for knowledge of HTML and JavaScript, the results demonstrate that the tool is suitable for the proposed application.

Keywords: Distributed microgeneration and minigeneration. SCADA system. Remote supervision. Open-source. Electrical protection. VPN. Automation. Low cost.

LISTA DE FIGURAS

LISTA DE TABELAS

SUMÁRIO

1 INTRODUÇÃO

1.1 Justificativa e Motivação

Nos últimos anos, os sistemas de supervisão e controle tornaram-se cada vez mais presentes em diversos setores industriais e de infraestrutura, tais como automação de processos, manutenção de equipamentos, hospitais, transporte, saneamento e sistemas de geração e distribuição de energia elétrica. Tais sistemas permitem a aquisição e processamento de dados em tempo real, além de oferecerem interfaces de visualização e controle que contribuem diretamente para a eficiência operacional e a segurança das operações. Dentre as soluções existentes, os sistemas SCADA (Supervisory Control and Data Acquisition) destacam-se por integrar comunicação remota, aquisição de dados contínua e controle de processos complexos, possibilitando a tomada de decisão em tempo hábil e a otimização de recursos em processos distribuídos geograficamente (PROMETHEUS GROUP, 2026).

No setor elétrico, a supervisão adequada das instalações é essencial para assegurar a proteção de equipamentos, a continuidade do fornecimento de energia e a integridade de operadores e usuários, especialmente em redes de geração, transmissão e distribuição. Os sistemas SCADA permitem a leitura de parâmetros elétricos em tempo real, a visualização do estado de dispositivos como disjuntores e relés, e o acionamento remoto de elementos de controle, integrando dispositivos inteligentes (IEDs) e garantindo respostas rápidas a eventos operacionais. Essa capacidade de monitoramento e controle aprimora a confiabilidade do sistema elétrico, reduzindo o tempo de resposta a falhas e mitigando impactos adversos sobre a infraestrutura crítica (PROMETHEUS GROUP, 2026).

Contudo, soluções SCADA comerciais geralmente envolvem altos custos de aquisição, licenciamento e manutenção, além de dependência de fornecedores específicos, o que pode limitar sua aplicação em projetos de menor escala, instituições públicas ou sistemas educacionais. Em contraste, abordagens baseadas em software de código aberto têm demonstrado potencial para reduzir custos de licenciamento e permitir maior flexibilidade e personalização, oferecendo uma alternativa viável para aplicações que necessitam de soluções robustas com orçamento restrito (AGHENTA; IQBAL, 2019).

1.2 Objetivos

1.2.1 Objetivos Principal

O objetivo deste trabalho é apresentar o desenvolvimento de um sistema SCADA aplicado a um IED em uma usina fotovoltaica, com acesso remoto.

1.2.2 Objetivos Específicos

Este trabalho propõe o desenvolvimento de um sistema SCADA baseado em ferramentas de código aberto (open source), com ênfase na supervisão de sistemas de proteção elétrica. A proposta contempla, ainda, a incorporação de uma Rede Privada Virtual (VPN – Virtual Private Network), a qual possibilita o acesso remoto seguro ao sistema supervisório, ampliando sua aplicabilidade e oferecendo maior flexibilidade às atividades de operação e manutenção, mesmo em ambientes geograficamente distantes.

O estudo apresenta a implementação das data sources, data points e eventos, evidenciando as vantagens proporcionadas pela integração dessas funcionalidades no contexto da proteção e da supervisão de uma usina fotovoltaica. Nesse sentido, o presente trabalho tem como objetivos o desenvolvimento de um sistema supervisório de baixo custo e fácil acesso, o estabelecimento da comunicação entre o software supervisório e o IED (Intelligent Electronic Device), a implementação de mecanismos para a geração de relatórios operacionais, bem como a viabilização do acesso e do monitoramento remoto da usina fotovoltaica.

Essas etapas visam assegurar uma supervisão eficiente, segura e acessível, contribuindo de forma significativa para o aprimoramento da operação, do monitoramento e da proteção do sistema fotovoltaico.

Por fim, demonstrar a viabilidade técnica e econômica dessa solução, destacando sua aplicabilidade em ambientes reais, como usinas, subestações, escolas técnicas ou sistemas isolados, contribuindo para a democratização do acesso à automação e à supervisão industrial no setor elétrico.

1.3 Estrutura do trabalho

A organização deste trabalho foi estruturada em cinco capítulos, além das referências e apêndices. O Capítulo 1 apresenta a introdução, abordando a contextualização do tema, os

objetivos e a descrição da estrutura geral. No Capítulo 2, é desenvolvida a fundamentação teórica, reunindo os conceitos essenciais sobre sistemas fotovoltaicos, relés de proteção IED, sistemas supervisórios SCADA e o uso do Tailscale para comunicação remota segura. O Capítulo 3 descreve os materiais e métodos utilizados no desenvolvimento do sistema proposto, detalhando os equipamentos, softwares e procedimentos de implementação. O Capítulo 4 apresenta e discute os resultados obtidos a partir dos testes de integração entre o SCADA LTS, o IED e o Tailscale. Por fim, o Capítulo 5 reúne as conclusões, destacando as contribuições alcançadas, as limitações encontradas e as sugestões para trabalhos futuros.

2 FUNDAMENTAÇÃO TEÓRICA

2.1 Energia Solar Fotovoltaica

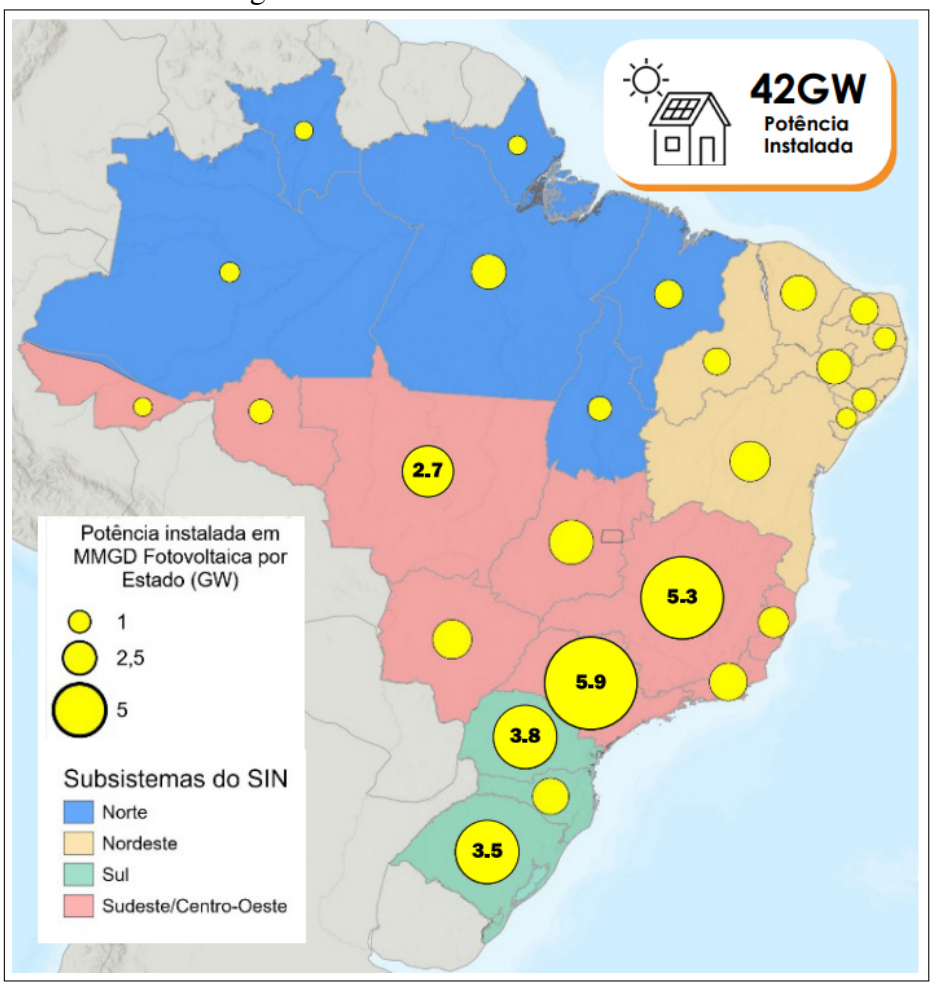
A matriz energética brasileira distingue-se da de grande parte dos países por sua elevada participação de fontes renováveis, e a energia solar fotovoltaica tem conquistado uma parcela cada vez mais relevante dentro desse contexto. Segundo a Associação Brasileira de Energia Solar Fotovoltaica (Absolar), a capacidade instalada operacional de energia solar no Brasil ultrapassou 55 GW (AGENCIA BRASIL, 2025).

No que se refere à geração distribuída, destaca-se o fato de que residências correspondem a 69,2% das unidades consumidoras com sistemas solares próprios, seguidas por estabelecimentos comerciais (18,4%) e propriedades rurais (9,9%). Entre os estados brasileiros, Minas Gerais lidera o ranking com mais de 900 mil imóveis com geração solar própria, seguida por São Paulo e Rio Grande do Sul, conforme dados da Absolar (AGENCIA BRASIL, 2025).

Alguns dos fatores que impulsionam esse crescimento da geração fotovoltaica no Brasil incluem a economia na conta de energia, a sustentabilidade dessa fonte e a manutenção relativamente baixa, especialmente considerando o abundante recurso solar no território nacional. No entanto, apesar dessas vantagens, há importantes desafios operacionais a serem superados: a geração distribuída sofre com restrições nas redes de distribuição, especialmente no que tange ao fluxo de potência, o que exige medidas rigorosas de supervisão e proteção das usinas fotovoltaicas. Portanto, reforça-se a necessidade de um acompanhamento técnico robusto por meio de sistemas de supervisão e proteção (como SCADA e IED), visando mitigar os riscos associados à injeção de potência e garantir a estabilidade, a confiabilidade e a segurança operacional das instalações fotovoltaicas (CALIXTO *et al.*, 2025).

Na Figura 1, observa-se a potência instalada no país e sua distribuição por subsistema, destacando-se que a maior concentração encontra-se nas regiões Sudeste/Centro-Oeste e Sul.

Figura 1 – Potência instalada MMGD



Fonte: EMPRESA DE PESQUISA ENERGETICA (2025)

2.1.1 Micro e minigeração distribuída

No projeto realizado o escopo está direcionado a usinas fotovoltaicas conectadas ao sistema elétrico em média tensão, especificamente no nível de 13,8 kV, as quais, no contexto da concessionária do estado do Ceará, enquadram-se majoritariamente nas categorias de micro e minigeração distribuída (ENEL DISTRIBUICAO CEARA, 2024).

De acordo com a regulamentação da Agência Nacional de Energia Elétrica (ANEEL), a microgeração distribuída corresponde a centrais geradoras com potência instalada menor ou igual a 75 kW, enquanto a minigeração distribuída abrange centrais com potência instalada superior a 75 kW e menor ou igual a 5 MW, independentemente da fonte energética utilizada, desde que atendidos os critérios técnicos e regulatórios aplicáveis (ENEL DISTRIBUICAO CEARA, 2024).

No âmbito da concessionária do Estado do Ceará, as usinas enquadradas como

minigeração distribuída, com potência instalada superior a 75 kW, são, de modo geral, conectadas ao sistema de distribuição em média tensão, tipicamente no nível de 13,8 kV. Para essa classe de tensão, a concessionária estabelece limites operacionais específicos de potência instalada, os quais, a depender dos critérios de conexão adotados e da capacidade da rede local, podem atingir valores da ordem de 2,5 MW (ENEL DISTRIBUICAO CEARA, 2024).

2.2 Sistemas de Proteção em Usinas Fotovoltaicas

2.2.1 Requisitos normativos de proteção para micro e minigeração distribuída

A correta implementação das funções de proteção em relés requer que o projetista compreenda os princípios de funcionamento de cada função e avalie de forma criteriosa o contexto elétrico no qual o equipamento será aplicado. Nesse sentido, a definição das funções de proteção deve estar alinhada às características da instalação, aos requisitos operacionais do sistema elétrico e aos critérios de segurança, seletividade e confiabilidade estabelecidos pelas normas técnicas vigentes, de modo a assegurar a adequada atuação do sistema de proteção em condições normais e de falta (AGÊNCIA NACIONAL DE ENERGIA ELÉTRICA, 2023).

No caso de usinas fotovoltaicas conectadas em média tensão, particularmente aquelas operando em 13,8 kV e enquadradas nas categorias de micro e minigeração distribuída, torna-se essencial a observância dos critérios técnicos estabelecidos pela concessionária local. Neste trabalho, adota-se como referência a Especificação Técnica nº 0005 da Enel Distribuição Ceará, a qual define os requisitos mínimos de proteção e medição para a conexão dessas instalações ao sistema elétrico de distribuição (ENEL DISTRIBUICAO CEARA, 2024).

De acordo com essa especificação, especialmente no ponto de comum conexão(PCC) ou na barra de alimentação da subestação, torna-se necessária a disponibilização das grandezas elétricas de corrente e tensão para fins de proteção, medição e supervisão. Para esse fim, são usualmente empregados transformadores de corrente (TCs) e transformadores de potencial (TPs), responsáveis por adequar os níveis dessas grandezas aos valores compatíveis com os relés de proteção. Esses dispositivos possibilitam o correto processamento das lógicas de proteção, a supervisão do sistema e a atuação segura dos dispositivos de interrupção (ENEL DISTRIBUICAO CEARA, 2024; HEITOR THOMAZ, 2018).

Nesse contexto, os requisitos mínimos de proteção requeridos para esse tipo de instalação podem ser visualizados na Figura 2.

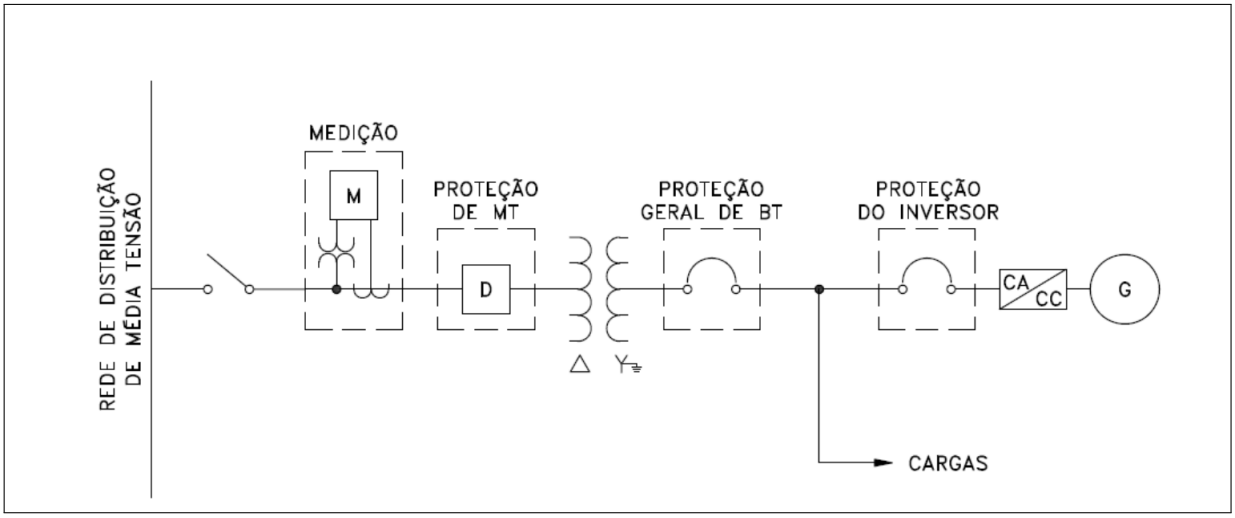
Figura 2 – Requisitos Mínimos em Função da Potência Instalada - Microgeração ou Minigeração

Elemento		Potência Instalada		
		Menor ou igual a 75 kW	Maior que 75 kW e menor ou igual a 500 kW	Maior que 500 kW e menor ou igual a 5 MW
Acoplamento [1]		Não	Sim	Sim
Seccionamento [2]		Sim (Disjuntor termomagnético)	Sim (Chave seccionadora acessível)	Sim (Chave seccionadora acessível)
Interrupção [3][4]		Sim	Sim	Sim
Proteção [5]		Sim	Sim	Sim
Medição [6]		Sistema de Medição Bidirecional	Medidor 4 Quadrantes	Medidor 4 Quadrantes
Função Proteção	**Cód. ANSI**			
Sub e Sobretensão	27 / 59 / 59N	Sim	Sim	Sim
Sub e Sobrefrequência	81O/ 81U	Sim	Sim	Sim
Contra desequilíbrio de corrente entre fases	46	Sim [7][14]	Sim	Sim
Contra reversão e desequilíbrio de tensão	47	Sim [7][14]	Sim	Sim
Contra curto-circuito	50/50N	Sim [7]	Sim	Sim
Seletiva contra curto-circuito	51/51N	Sim [7]	Sim	Sim
Perda de rede (proteção anti-ilhamento) [8][9]	78 [11]	Sim	Sim	Sim
Verificação de sincronismo	25	Sim	Sim	Sim
Espera de tempo de reconexão [10]	62	Sim	Sim	Sim
Direcional Contra Curto-Circuito [11]	67/67N	Não	Sim	Sim
Direcional de Potência	32	Não	Sim	Sim

Fonte: ENEL DISTRIBUICAO CEARA (2024)

Na Figura 3 é apresentado o diagrama unifilar típico de conexão do acessante à rede de média tensão da Enel.

Figura 3 – Diagrama Unifilar Conexão do acessante à Rede de Média Tensão da Enel



Fonte: ENEL DISTRIBUICAO CEARA (2023)

2.2.2 Relés IED: conceitos, funções e comunicação

Com o advento da eletrônica digital e dos microprocessadores, os relés eletromecânicos começaram a ser gradualmente substituídos por relés mais modernos, capazes de executar suas funções com maior eficiência. Esses novos dispositivos são conhecidos como relés digitais

ou numéricos, também chamados de Dispositivos Eletrônicos Inteligentes(IED) de proteção, e possuem a capacidade de receber dados de tensões e correntes do sistema, convertendo-os em valores digitais para análise e processamento (KINDERMANN, 1999).

Atualmente, os relés IED evoluíram significativamente, sendo capazes de realizar diversos testes e funções automáticas, inclusive de autoverificação de seu próprio funcionamento. Eles conseguem detectar diferentes tipos de falhas no sistema de proteção, como sobrecorrente, subtensão, sobrecarga, entre outros. Esses relés modernos oferecem ainda a vantagem de auxiliar a equipe técnica, simplificando tarefas de operação e manutenção, além de possuírem funcionalidades que não podem ser replicadas por relés eletromecânicos, como registro de eventos, comunicação com sistemas supervisórios e integração via protocolos digitais, para ilustrar a Figura 4 mostra alguns dos reles da fabricante utilizada no trabalho (INDÚSTRIA AUTOMÁTICA, 2015).

Figura 4 – Relés IED SEL

Fonte: SCHWEITZER ENGINEERING LABORATORIES (2025)

No que se refere aos aspectos de comunicação, os IEDs modernos fazem uso predominante de protocolos digitais padronizados, dentre os quais se destaca o Modbus, amplamente empregado em sistemas de automação elétrica e que será abordado com maior detalhamento na seção subsequente. Por meio desse protocolo, torna-se possível a integração dos relés de proteção a sistemas SCADA, plataformas supervisórias e demais arquiteturas de automação, viabilizando a troca bidirecional de dados em tempo real. Ademais, a utilização do Modbus permite a configuração remota de parâmetros operacionais, o monitoramento contínuo de grandezas elétricas e a detecção e sinalização ágil de eventos e alarmes. Essa abordagem de comunicação digital contribui de forma significativa para o aumento da eficiência operacional, a melhoria da confiabilidade do sistema elétrico e o reforço da segurança das operações, consolidando os IEDs como elementos fundamentais na gestão moderna de subestações e unidades de geração de energia (MODBUS ORGANIZATION, 2012; SCHWEITZER ENGINEERING LABORATORIES, 2019).

2.2.3 Protocolos de comunicação (Modbus)

O protocolo Modbus é um dos mais utilizados na comunicação entre sistemas supervisórios e dispositivos de campo. Desenvolvido originalmente pela empresa Modicon — atualmente Schneider Electric —, o Modbus tornou-se amplamente empregado em diversos setores industriais ao longo de várias décadas, devido à sua simplicidade, confiabilidade e ampla compatibilidade. Seu principal objetivo é permitir a troca eficiente e segura de dados entre dispositivos como sensores, controladores lógicos programáveis (CLPs) e sistemas SCADA, integrando todos os elementos de automação e controle de processos. De acordo com a MODBUS Organization (2012), o Modbus é um protocolo de mensagens da camada de aplicação, situado no nível 7 do modelo OSI, amplamente utilizado desde 1979 como padrão de fato para comunicação serial industrial. O protocolo possibilita a comunicação do tipo cliente-servidor entre dispositivos conectados a diferentes tipos de redes e barramentos, sendo atualmente acessível em redes TCP/IP por meio da porta reservada 502.

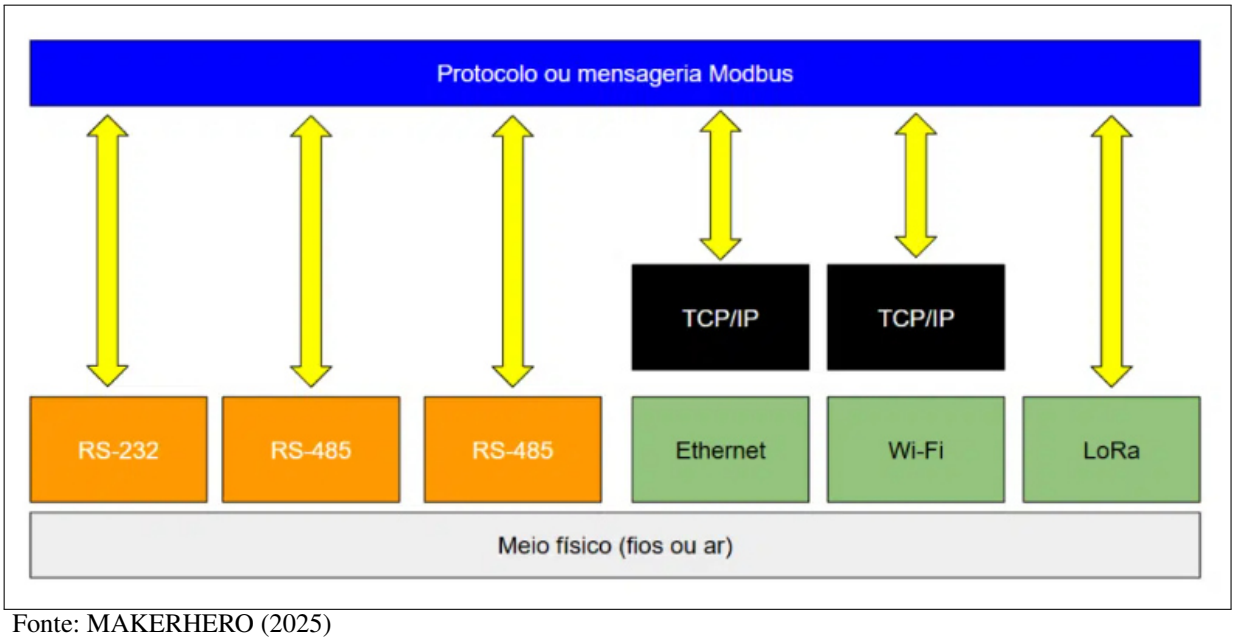
Nas sua versão tradicional, o Modbus RTU, o protocolo adota o modelo de comunicação mestre–escravo, no qual o dispositivo mestre é responsável por iniciar todas as trocas de dados, enquanto os escravos apenas respondem às solicitações. Essa estrutura garante uma comunicação determinística, organizada e confiável, evitando colisões e assegurando a integridade das informações transmitidas. O Modbus opera em redes seriais privadas, baseando-se no princípio

de requisição e resposta, o que o torna adequado para aplicações que exigem simplicidade e robustez operacional. O Modbus RTU, utiliza comunicação serial por meio dos padrões RS-232 ou RS-485, sendo amplamente aplicado em sistemas de automação industrial de pequeno e médio porte. Essa versão se destaca por permitir transmissões a longas distâncias — podendo alcançar até aproximadamente 1 quilômetro, dependendo do meio físico — e por sua facilidade de implementação e baixo custo (MAKERHERO, 2025).

Já o Modbus TCP/IP representa uma evolução do protocolo, adaptado para redes Ethernet e Wi-Fi. Nessa versão, adota-se o modelo cliente–servidor, substituindo a nomenclatura mestre–escravo, embora o princípio de operação permaneça o mesmo. Essa adaptação possibilita maior velocidade de comunicação, integração com sistemas modernos de rede e escalabilidade, tornando o protocolo ideal para aplicações que requerem alta confiabilidade, desempenho e conectividade, como em subestações elétricas, usinas fotovoltaicas e sistemas SCADA distribuídos (MAKERHERO, 2025).

Na Figura 5 é ilustrada a utilização do protocolo MODBUS (em azul) com interfaces de comunicação cabeadas (em laranja) e sem fio (em verde) para interfacear as mensagens MODBUS com o meio físico (em cinza).

Figura 5 – Organização em camadas



Fonte: MAKERHERO (2025)

2.3 Sistemas Supervisórios (SCADA)

Os sistemas SCADA exercem papel central na automação e supervisão de sistemas elétricos, ao possibilitarem que centros de controle remotos tenham acesso, em tempo real, a informações críticas provenientes de equipamentos de campo distribuídos ao longo do sistema de potência. Os autores ressaltam que o canal de comunicação entre esses dispositivos deve apresentar elevada robustez, de modo a assegurar a transmissão confiável de dados como grandezas elétricas, estados operacionais e posições de disjuntores, contribuindo para a estabilidade, a segurança e a confiabilidade do sistema. Ademais, os autores estabelecem uma analogia entre a comunicação em sistemas SCADA e o sistema nervoso de um organismo, uma vez que essa infraestrutura é responsável pelo transporte contínuo de sinais e informações entre o campo e o centro de controle, viabilizando respostas rápidas e eficazes para a manutenção da operação segura e estável do sistema elétrico (THOMAS; MCDONALD, 2015).

Os sistemas SCADA são amplamente utilizados em diversos setores, como geração de energia, indústria, hospitais, petróleo e gás. Por meio da coleta de dados de sensores e equipamentos conectados a uma rede, o sistema é capaz de processar, registrar e tratar as informações de forma eficiente. Essa estrutura permite a criação de eventos e alarmes, proporcionando maior controle sobre os processos monitorados, aumento da eficiência operacional, redução de riscos de acidentes e suporte à tomada de decisão. Além disso, o SCADA possibilita a comunicação em tempo real com dispositivos de campo, como motores, sensores e válvulas, registrando qualquer alteração em seu estado de operação. O sistema também permite a intervenção tanto manual quanto automatizada, de acordo com a lógica configurada no software supervisório (TOTVS, 2023).

2.3.1 Conceito e arquitetura de um SCADA

As principais funcionalidades do sistema SCADA são a aquisição, supervisão e controle, esses três pilares são essenciais para garantir o funcionamento seguro, eficiente e automatizado de diferentes tipos de instalações, como usinas, subestações e sistemas de produção. A aquisição de dados consiste na coleta contínua de informações provenientes de sensores, medidores, controladores e dispositivos eletrônicos distribuídos no campo. Esses dados podem incluir grandezas elétricas, como tensão, corrente, potência, frequência e estado de chaves, além de variáveis de processo, como temperatura, pressão e vazão. A aquisição é feita de forma

automática e em tempo real, utilizando protocolos de comunicação específicos, permitindo que o sistema registre e armazene as informações em bancos de dados para análise posterior. A supervisão é a etapa em que os dados coletados são apresentados ao operador por meio de interfaces gráficas (IHM), painéis e telas de monitoramento. Essa visualização permite acompanhar o estado do sistema em tempo real, identificar falhas, gerar alarmes e emitir relatórios de desempenho. A supervisão facilita a tomada de decisões rápidas e assertivas, garantindo maior confiabilidade operacional e segurança do processo. Já o controle é responsável por executar ações corretivas ou de comando sobre os equipamentos monitorados. Essas ações podem ser realizadas de forma manual, pelo operador através do sistema supervisório, ou automática, por meio de rotinas e lógicas programadas no software. O controle remoto de dispositivos, como disjuntores, válvulas e motores, permite otimizar a operação, reduzir o tempo de resposta a falhas e aumentar a eficiência global do sistema (IBERDROLA, 2023).

2.3.2 SCADA LTS: características, vantagens e aplicações

O SCADA LTS é uma solução *open-source* e multiplataforma que possibilita o desenvolvimento de sistemas supervisórios personalizados. A plataforma oferece todos os recursos presentes em softwares SCADA comerciais, incluindo suporte a diversos protocolos de comunicação, aquisição de dados, criação de interfaces homem-máquina (IHM), além de funcionalidades para alarmes, eventos e geração de relatórios (SCADA-LTS, 2025).

Desenvolvido em Java, o SCADA LTS garante ampla compatibilidade e pode ser executado em diferentes arquiteturas de sistema, como Windows, macOS e Linux. O servidor pode ser distribuído no formato .WAR, permitindo implantação em servidores web multiplataforma, ou por meio de um instalador para Windows, facilitando a instalação e configuração. A interface do usuário é totalmente baseada em navegador web, dispensando softwares clientes dedicados, o que simplifica o acesso e a manutenção do sistema. Além disso, o SCADA LTS oferece suporte a APIs SOAP e REST, permitindo integração personalizada com outros sistemas e aplicações externas, aumentando sua flexibilidade e interoperabilidade em ambientes industriais (SCADA-LTS, 2025).

Entre suas principais vantagens em relação a soluções comerciais, destaca-se o acesso total ao código-fonte, que possibilita personalização, transparência e ausência de custos de licença, tornando-o uma alternativa de baixo custo para projetos acadêmicos e industriais. Diferentemente de muitos softwares comerciais, o SCADA LTS não impõe limites ao número de

data points nem ao número de usuários, permitindo escalabilidade total conforme a necessidade do sistema. Sua natureza multiplataforma garante compatibilidade com diferentes sistemas operacionais, enquanto a interface web intuitiva e responsiva facilita o acesso remoto e a manutenção. O sistema ainda suporta diversos protocolos de comunicação, como Modbus TCP/IP, DNP3 e ASCII Serial, permitindo integração com uma ampla gama de dispositivos e controladores. Além disso, sua escalabilidade e flexibilidade permitem utilização tanto em pequenos sistemas de monitoramento quanto em grandes plantas industriais (SCADA-LTS, 2025).

O SCADA-LTS pode ser aplicado em diversos setores que demandam supervisão e controle de processos em tempo real. No contexto da geração e distribuição de energia elétrica, a plataforma pode ser utilizada para o monitoramento de subestações, usinas fotovoltaicas e sistemas de armazenamento de energia, permitindo a aquisição, visualização e registro de dados operacionais. Em ambientes industriais, o SCADA-LTS é adequado ao acompanhamento de processos produtivos, à automação de linhas de fabricação e à supervisão de equipamentos críticos. A plataforma também pode ser empregada em sistemas de saneamento, como no monitoramento de estações de tratamento de água e esgoto, bem como em aplicações de automação predial, abrangendo o controle de climatização, iluminação e sistemas de segurança. Além disso, sua arquitetura aberta possibilita a integração com outros sistemas corporativos, bancos de dados e plataformas de análise, o que contribui para a centralização das informações, o aumento da eficiência operacional e a melhoria da confiabilidade e da segurança das operações, consolidando o SCADA-LTS como uma solução versátil para aplicações modernas de automação (SCADABR, 2017; IBERDROLA, 2023).

2.3.3 Conteinerização e virtualização leve em sistemas SCADA

O Docker, abordagem que proporciona maior padronização, portabilidade e facilidade de configuração do ambiente de execução. Os contêineres Docker constituem uma tecnologia de virtualização leve que permite empacotar aplicações juntamente com todas as suas dependências, assegurando portabilidade, reprodutibilidade e isolamento do ambiente de execução. Diferentemente das máquinas virtuais tradicionais, os contêineres não requerem a virtualização de um sistema operacional completo, uma vez que compartilham o núcleo do sistema operacional hospedeiro. Essa característica resulta em menor sobrecarga computacional e maior eficiência na utilização dos recursos do sistema (DOCKER, 2026).

2.4 Acesso Remoto e Cibersegurança

A literatura especializada destaca que a evolução dos sistemas de automação, impulsionada pela popularização de redes digitais baseadas em LAN e WAN, introduziu novos desafios de segurança que antes eram praticamente inexistentes. Thomas e McDonald ressaltam que os sistemas anteriores operavam em arquiteturas simples do tipo mestre–escravo, utilizando canais de comunicação dedicados e restritos, o que reduzia significativamente a exposição a ataques cibernéticos. Com a integração dos sistemas de automação às redes corporativas e o aumento do fluxo de dados em larga escala, as concessionárias passaram a enfrentar um cenário mais vulnerável e suscetível a ameaças externas e internas (THOMAS; MCDONALD, 2015).

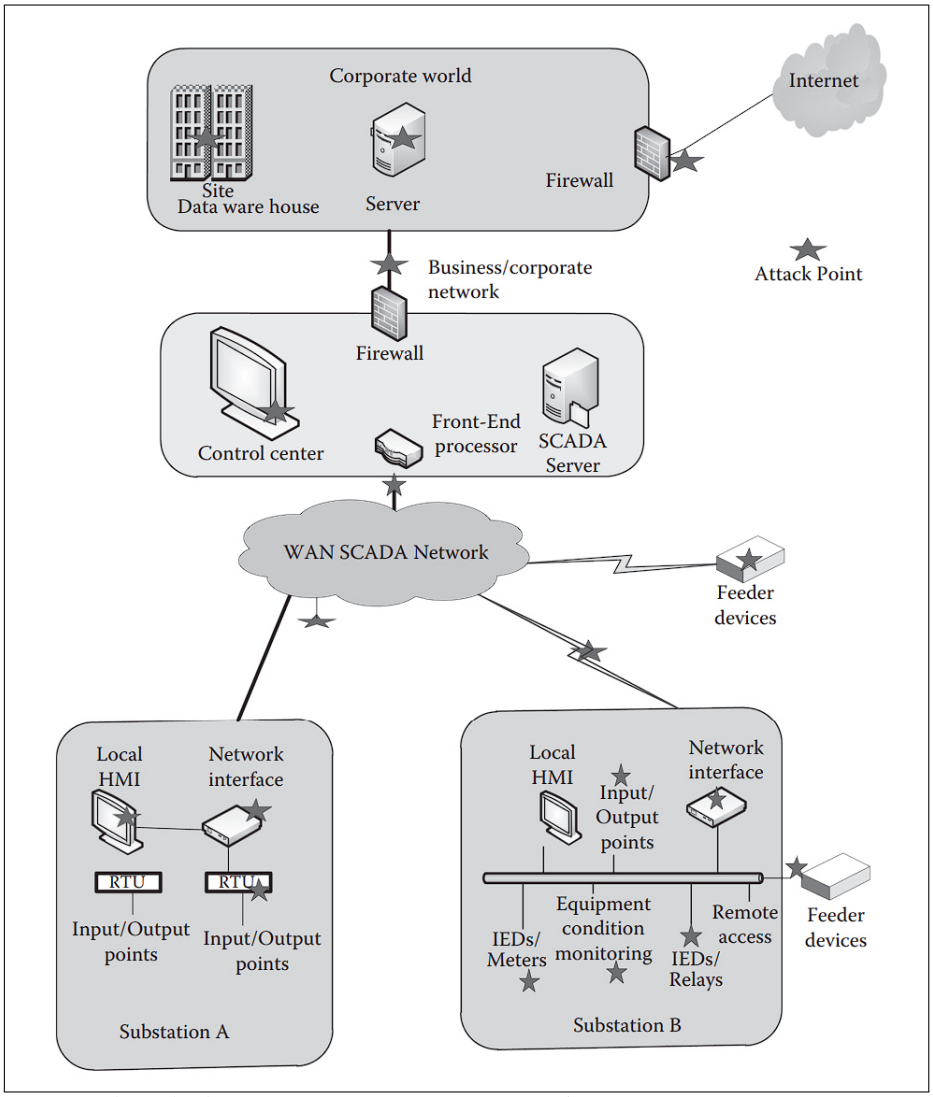
Segundo Thomas and McDonald (2015), a adoção de sistemas de controle digital baseados em redes LAN e WAN, intensificada nas últimas décadas no contexto da automação de sistemas de potência, introduziu novos desafios relacionados à segurança da informação. Os autores explicam que, nos sistemas mais antigos, caracterizados por arquiteturas simples do tipo mestre-escravo e por canais de comunicação dedicados, as questões de segurança eram relativamente limitadas. Contudo, com a expansão das redes corporativas e a integração dos sistemas de automação às redes WAN empresariais, as concessionárias passaram a se tornar significativamente mais vulneráveis a ameaças cibernéticas.

2.4.1 Riscos em sistemas industriais conectados

A segurança cibernética em sistemas SCADA enfrenta uma ampla gama de ameaças, entre elas violações de autorização, espionagem de tráfego (eavesdropping), interceptação ou alteração de mensagens, falsificação de identidade, ataques de repetição e negação de serviço. Tais vulnerabilidades podem ser exploradas tanto por agentes externos quanto internos, especialmente em arquiteturas que utilizam linhas de comunicação desprotegidas — como enlaces SCADA tradicionais ou conexões discadas presentes em determinados IEDs. De forma similar, redes corporativas mal segmentadas permitem que usuários não autorizados ou até mesmo funcionários e fornecedores obtenham acesso indevido a dados sensíveis, ampliando significativamente o risco de comprometimento do sistema. Os autores destacam que ataques desse tipo podem afetar profundamente a operação de sistemas elétricos de potência, especialmente devido à fragilidade histórica das comunicações industriais diante de ameaças modernas (THOMAS; MCDONALD, 2015).

Na Figura 6, são apresentados os principais pontos de vulnerabilidade que podem comprometer o sistema SCADA, constituindo potenciais vetores de ataque ou falhas operacionais.

Figura 6 – Pontos de ameaça à segurança em uma rede SCADA



Fonte: Adaptado de THOMAS; McDONALD (2015, p.129).

Como pode ser observado na Figura, a simples adoção de múltiplos firewalls não é suficiente para eliminar os riscos de segurança em sistemas SCADA, uma vez que os ataques podem se originar em diferentes pontos da arquitetura. A integração do SCADA com redes corporativas e com a Internet rompe o isolamento que historicamente conferia maior segurança a esses sistemas, ampliando significativamente a superfície de ataque. Ademais, elementos do nível de campo, como IEDs, RTUs e interfaces locais, também se configuram como potenciais vetores de vulnerabilidade, especialmente quando operam com protocolos ou mecanismos de

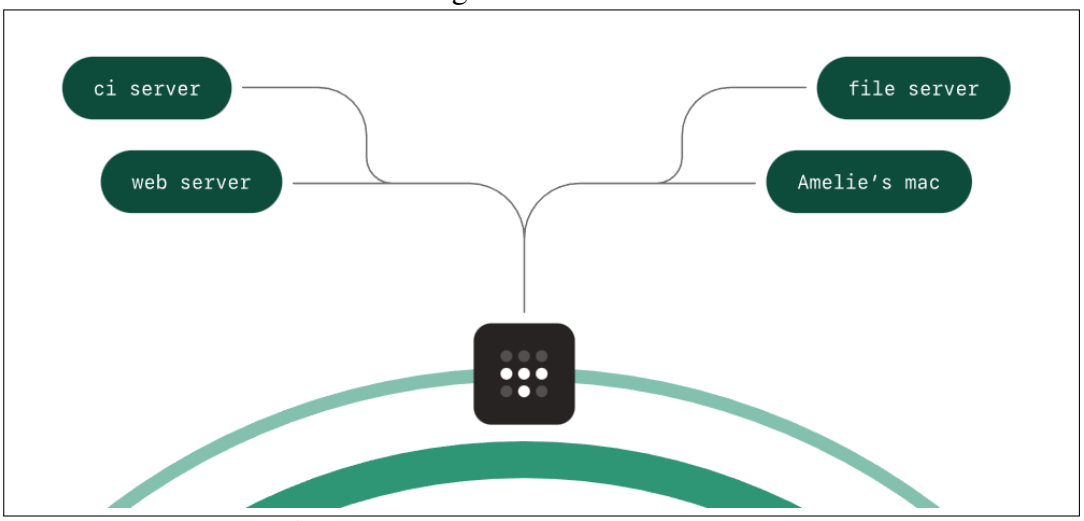
autenticação limitados. Esse cenário evidencia que, na conjuntura atual dos sistemas supervisórios, a segurança não pode ser tratada apenas por meio de barreiras perimetrais, tornando-se necessário a adoção de estratégias mais abrangentes e integradas de cibersegurança (THOMAS; MCDONALD, 2015).

Diante desse cenário, fica claro que a segurança em sistemas SCADA não pode ser tratada apenas como a instalação de firewalls ou outros mecanismos pontuais de proteção. A crescente integração entre redes corporativas e ambientes operacionais, somada ao uso de tecnologias de comunicação cada vez mais abertas, exige uma abordagem mais cuidadosa e abrangente. Torna-se necessário considerar aspectos como a segmentação adequada das redes, o controle de acessos, a proteção das comunicações e o uso de soluções seguras para acesso remoto. Dessa forma, a segurança passa a ser um elemento essencial no projeto e na operação de sistemas supervisórios, contribuindo para reduzir vulnerabilidades e aumentar a confiabilidade das instalações frente às ameaças atuais.

2.4.2 Ferramentas modernas de acesso remoto seguro (Tailscale e RustDesk)

O Tailscale é uma solução de acesso remoto seguro baseada no conceito de VPN definida por software, destacando-se por sua facilidade de uso e por dispensar configurações complexas típicas de VPNs tradicionais. A ferramenta permite a criação de uma rede virtual privada, como visto na Figura 7 formada apenas por dispositivos autorizados, funcionando como uma malha própria de comunicação. Após a instalação do aplicativo e a autenticação do usuário, o dispositivo é automaticamente integrado à *Tailnet* — o agrupamento lógico de dispositivos da plataforma — passando a se comunicar de forma direta e criptografada com os demais nós. Dessa forma, o Tailscale oferece uma alternativa gratuita, prática e segura para acesso remoto, podendo ser útil em aplicações industriais ou de supervisão onde a simplicidade operacional e a segurança são requisitos fundamentais. Vale destacar que, embora o Tailscale seja uma solução paga, ele oferece diversas funcionalidades gratuitas que foram suficientes para atender às necessidades deste projeto (TAILSCALE, 2025).

Figura 7 – Tailnet



Fonte: TAILSCALE (2025)

O RustDesk é um software de acesso remoto gratuito e *open-source* que permite a visualização e o controle de outro computador ou dispositivo a distância, desde que ambos estejam conectados à internet e executando o aplicativo. A ferramenta possibilita a operação remota completa, incluindo o uso de teclado e mouse, e apresenta ampla compatibilidade, estando disponível para Windows, Linux, Android, iOS e outras plataformas. Um dos principais diferenciais do RustDesk é o uso de criptografia de ponta a ponta (E2E), assegurando que os dados transmitidos entre os dispositivos não possam ser facilmente interceptados. Além disso, o software prioriza a comunicação direta entre os clientes, buscando estabelecer conexões ponto a ponto (P2P) sempre que possível, o que contribui para maior desempenho e menor latência (RUSTDESK, 2025).

Dessa forma, o presente capítulo apresentou a fundamentação teórica necessária para a compreensão dos sistemas envolvidos no desenvolvimento do trabalho, abordando os conceitos de geração fotovoltaica, sistemas de proteção, dispositivos eletrônicos inteligentes, protocolos de comunicação, sistemas supervisórios e aspectos relacionados à cibersegurança. Também foram discutidas arquiteturas modernas de infraestrutura, como a conteinerização por meio do Docker e o uso de ferramentas de acesso remoto seguro, exemplificadas pelo Tailscale e pelo RustDesk, destacando-se sua relevância na operação de sistemas SCADA contemporâneos. Esses conceitos fornecem a base técnica que sustenta as escolhas metodológicas adotadas no capítulo seguinte, no qual é apresentada a implementação do sistema de supervisão e monitoramento proposto.

3 METODOLOGIA E DESENVOLVIMENTO DO SISTEMA SCADA

3.1 Arquitetura geral do sistema proposto

Para arquitetura do projeto se propõe a utilização do SCADA-LTS, uma plataforma supervisória *open-source*, como alternativa de baixo custo para a supervisão e o monitoramento do PCC aplicado a uma usina fotovoltaica. A comunicação entre o SCADA e o IED é estabelecida por meio do protocolo Modbus TCP/IP, possibilitando a aquisição das grandezas analogicas e digitais em tempo real e o acompanhamento de eventos. Para a execução do SCADA-LTS, optou-se pelo uso do Windows Subsystem for Linux (WSL), uma vez que a plataforma apresenta maior estabilidade quando operada em ambiente Linux.

Adicionalmente, o sistema incorpora acesso remoto por meio do Tailscale, com o objetivo de garantir uma conexão segura, estável e criptografada ao supervisório, ampliando a flexibilidade operacional e permitindo intervenções remotas com maior confiabilidade. De forma complementar, utiliza-se o RustDesk como ferramenta de acesso remoto à estação de supervisão, possibilitando o gerenciamento do sistema mesmo fora da rede local e assegurando maior disponibilidade e continuidade operacional.

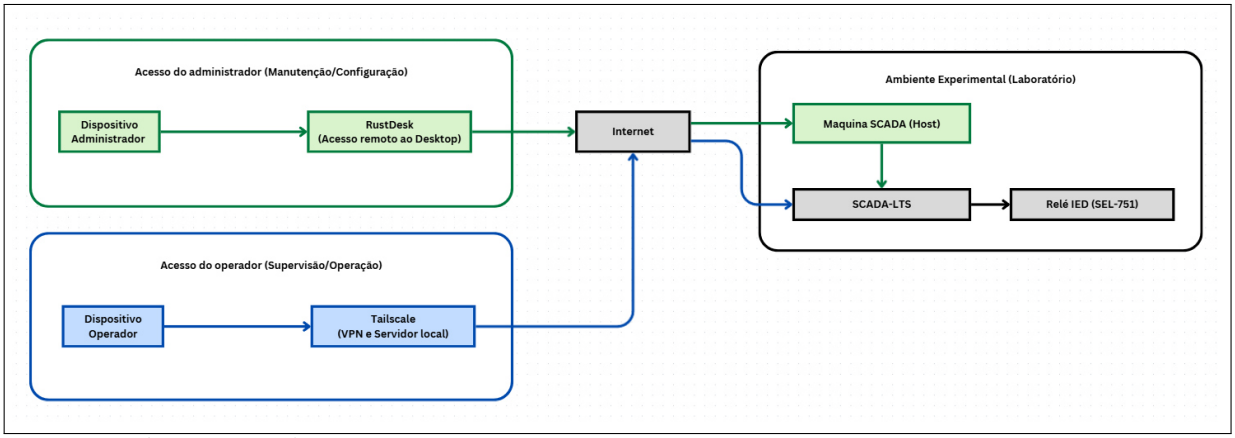
Ressalta-se, entretanto, que a solução proposta mostra-se mais adequada ao uso por administradores do sistema. Tal adequação decorre do fato de que o RustDesk fornece acesso integral à interface do computador hospedeiro, o que possibilita ao operador um controle irrestrito sobre a máquina, em desacordo com os princípios do modelo de segurança Zero Trust. Nesse paradigma, preconiza-se a concessão apenas do acesso estritamente necessário à execução das tarefas requeridas — neste caso, limitado exclusivamente à interface do sistema supervisório.

Adicionalmente, em razão da utilização do WSL para a execução do SCADA-LTS em ambiente Linux, não foi possível empregar de forma direta o acesso por endereço IP fornecido pelo Tailscale. Em um cenário ideal, o uso do endereço IP do dispositivo que hospeda o SCADA-LTS seria suficiente para permitir o acesso ao sistema supervisório a partir de qualquer máquina na *tailnet*, garantindo maior aderência aos princípios de segmentação de rede e de controle refinado de permissões.

Com o objetivo de viabilizar o acesso ao sistema sem a necessidade de concessão de acesso integral à máquina que executa o SCADA-LTS, requisito particularmente relevante para operadores, foi empregada uma funcionalidade do Tailscale que possibilita a criação de servidores locais. Essa abordagem consiste na criação de um servidor para encaminhar a porta

na qual o SCADA-LTS está em execução, permitindo o acesso por meio de um link gerado automaticamente. Tal funcionalidade pode ser restrita a dispositivos pertencentes à *tailnet* por meio do comando tailscale serve, ou, alternativamente, disponibilizada a usuários externos utilizando o comando tailscale funnel. A Figura 8 apresenta um diagrama esquemático que sintetiza a arquitetura e o fluxo geral da solução desenvolvida.

Figura 8 – Diagrama do projeto



Fonte: Próprio Autor(2025)

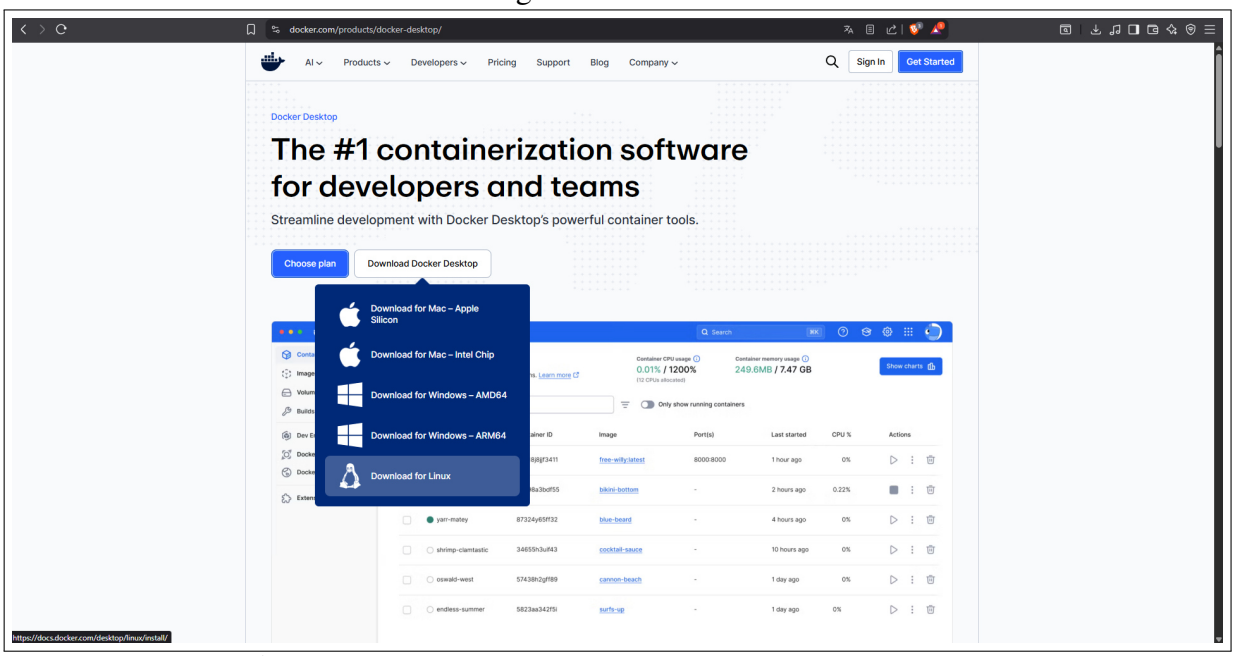
3.2 Equipamentos e softwares utilizados

3.2.1 SCADA LTS

O SCADA-LTS consiste em uma solução multiplataforma e de código aberto, desenvolvida para permitir a criação de sistemas supervisórios (SCADA – Supervisory Control and Data Acquisition) baseados em ambiente web. A plataforma oferece recursos para monitoramento, tratamento e controle de processos industriais e de energia, possibilitando sua integração com diversos dispositivos e protocolos utilizados em automação.

No contexto deste trabalho, o uso de contêineres Docker possibilitou a execução dos principais componentes do SCADA-LTS, incluindo o banco de dados e a interface gráfica do sistema, de forma integrada e isolada, garantindo maior estabilidade e facilidade de manutenção da aplicação. A ferramenta Docker foi obtida diretamente no site oficial do projeto, conforme ilustrado na Figura 9, sendo instalada a versão compatível com o sistema operacional Linux, utilizado neste trabalho.

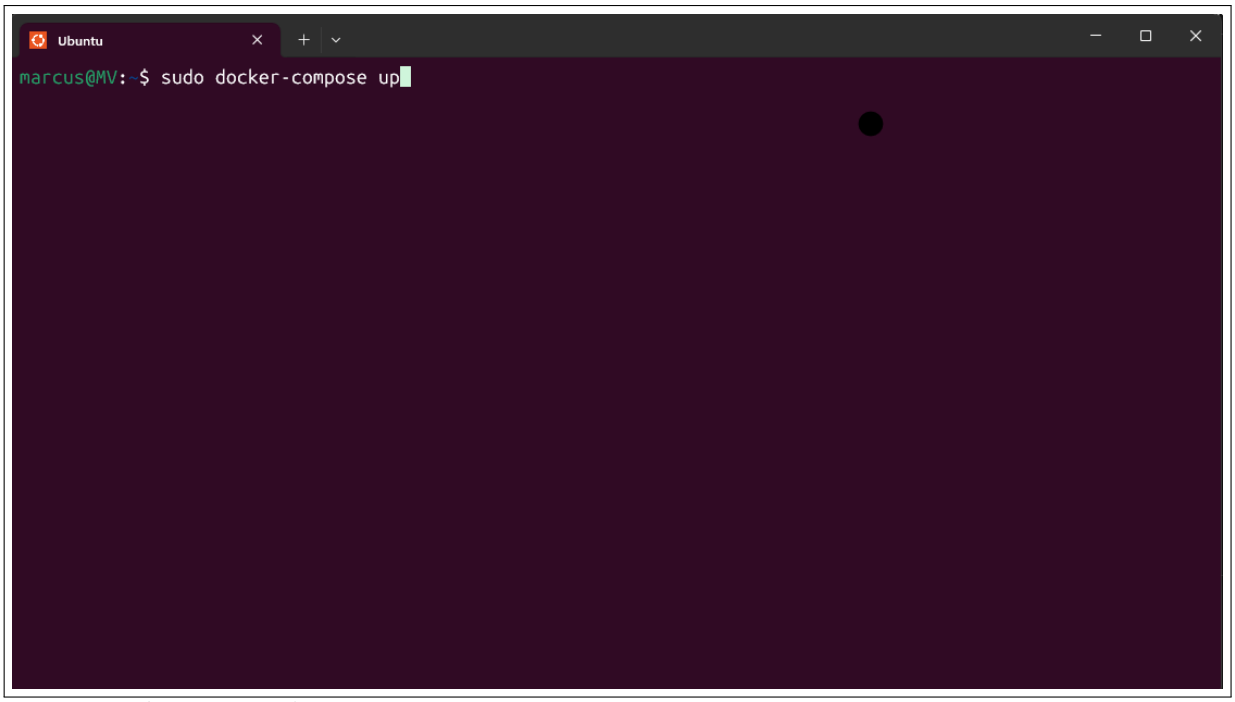
Figura 9 – Docker



Fonte: DOCKER (2025)

Após a instalação, a inicialização do ambiente SCADA-LTS é realizada por meio do terminal do Ubuntu, utilizando o comando, como mostrado na Figura 10:

Figura 10 – Comando docker-compose up



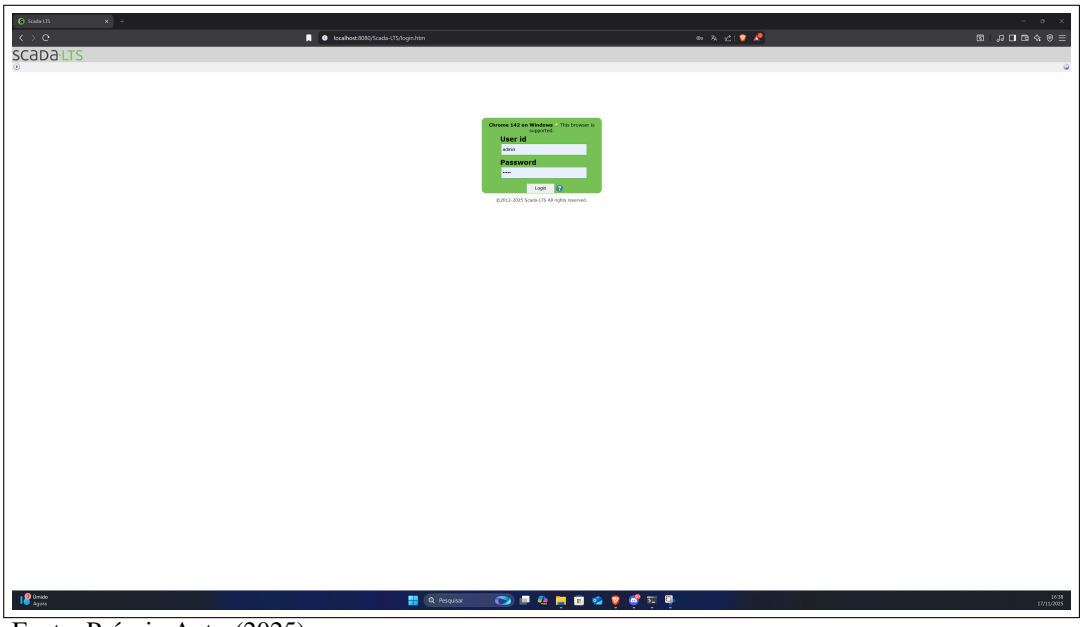
Fonte: Próprio Autor(2025)

Após a autenticação do usuário, os contêineres necessários são automaticamente inicializados, permitindo a disponibilização do ambiente SCADA-LTS para acesso via browser. Con-

cluída essa etapa, o sistema pode ser acessado por meio do endereço http://localhost:8080/Scada-LTS.

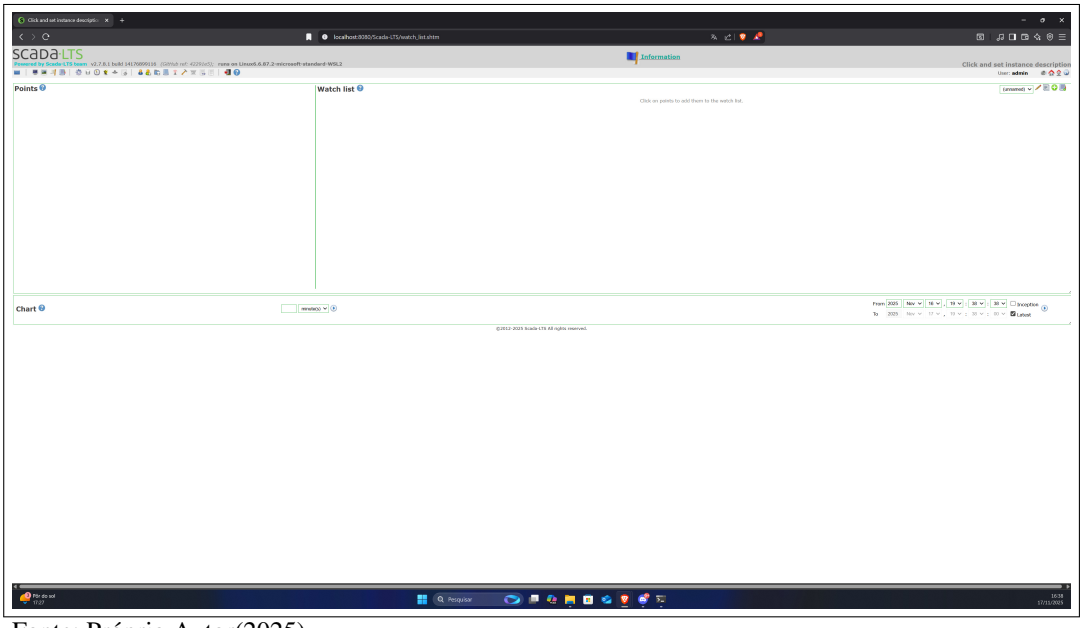
A porta 8080 refere-se à porta de comunicação configurada no contêiner Docker responsável pela execução da aplicação. O login padrão do sistema é realizado utilizando o usuário e a senha admin, o que possibilita o acesso à interface inicial do supervisório, conforme ilustrado na Figura 11 e na Figura 12.

Figura 11 – Tela de login do SCADA-LTS



Fonte: Próprio Autor(2025)

Figura 12 – Tela inicial



Fonte: Próprio Autor(2025)

3.2.2 IED de proteção utilizado (modelo e fabricante)

O modelo escolhido para o projeto foi o SEL - 751, fabricado pela Schweitzer Engineering Laboratories (SEL), é um relé de proteção microprocessado amplamente utilizado em sistemas de distribuição e em aplicações industriais. Ele foi projetado para oferecer proteção, controle, automação e monitoramento de alimentadores e equipamentos de média tensão, com alto desempenho e confiabilidade.

Segundo a SEL, ele oferece mitigação de arco elétrico, localização de faltas, detecção de faltas de alta impedância, detecção de condutores rompidos, análise de eventos e outras funcionalidades. Você pode integrar rapidamente o relé às comunicações em serial ou baseadas em Ethernet com as comunicações SEL, Modbus, DNP3, FTP, TCP/IP, Telnet, SNTP, IEC61850 Edition2, IEC60870-5-103, PRP, MIRRORED BITS, EVMSG, C37.118 (synchrophasors), and DeviceNet.

O relé SEL-751 é amplamente reconhecido por sua confiabilidade, robustez e facilidade de integração em sistemas de supervisão e controle. Sobre a fabricante segundo seu site, a SEL é especializada na criação de produtos e sistemas digitais que protegem, controlam e automatizam sistemas de potência em todo o mundo. Uma empresa 100% de propriedade dos colaboradores e com sede em Pullman, Washington, a SEL fabrica produtos nos Estados Unidos desde 1984 e atende clientes em todo o mundo.

O relé SEL-751 demostrado na Figura 13, foi selecionado para o projeto por atender plenamente aos requisitos de um relé principal na proteção da saída de alimentação da usina fotovoltaica. O equipamento oferece as funções essenciais para a proteção desse tipo de instalação, incluindo as proteções de sobrecorrente de fase (50/51) e de neutro (50N/51N), sequência negativa (46), sub e sobrefrequência (81U/81O), além da função de falha de disjuntor (50BF), entre outras funções. Tais características garantem a operação segura e confiável do sistema, atendendo às exigências técnicas e normativas aplicáveis.

Figura 13 – SEL-751

Fonte: SCHWEITZER ENGINEERING LABORATORIES (2025)

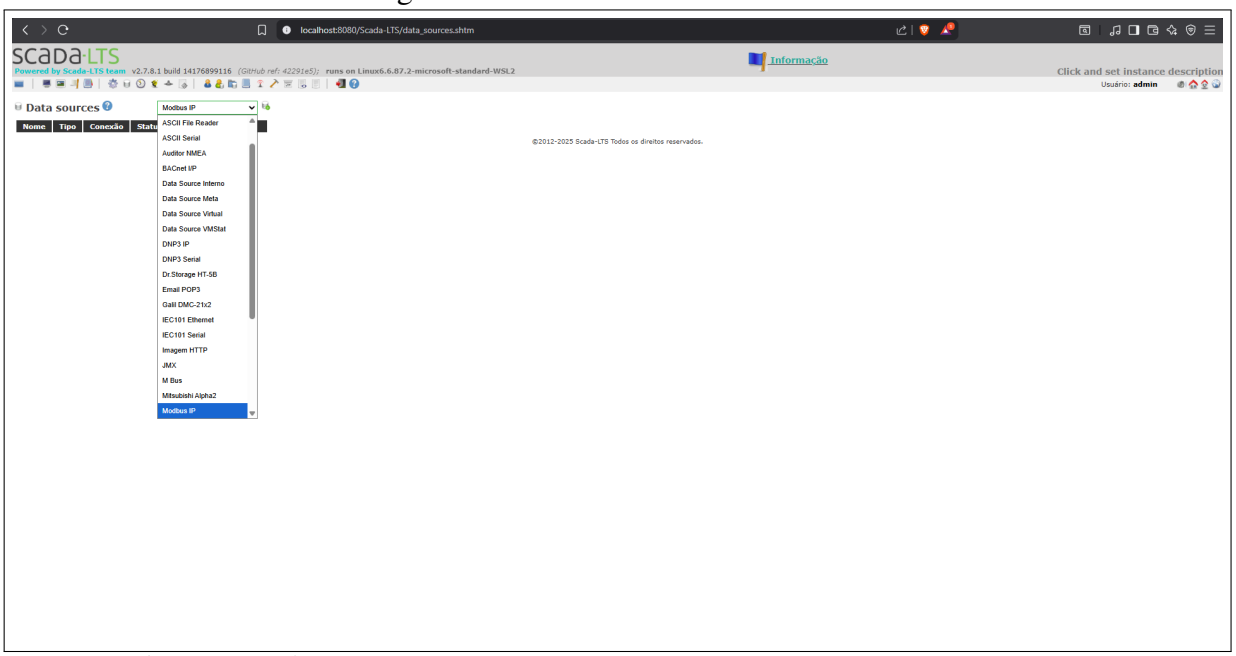
A escolha do relé utilizado neste estudo deveu-se, principalmente, à sua disponibilidade na bancada do laboratório do GREI (Grupo de Redes Elétricas Inteligentes), o que viabilizou a realização do trabalho experimental. Essa disponibilidade permitiu a execução de ensaios e testes em bancada, possibilitando a validação prática da arquitetura proposta e das estratégias de comunicação e supervisão adotadas.

3.3 Desenvolvimento do sistema

No sistema desenvolvido, a aquisição de informações operacionais ocorre a partir de uma fonte de dados (data source), nomenclatura empregada pelo SCADA-LTS para identificar os elementos responsáveis pela entrada de dados no supervisório. No contexto deste trabalho, a fonte de dados é o Relé IED, dispositivo encarregado de fornecer ao sistema supervisório as variáveis elétricas e os estados de proteção do sistema.

A configuração dessa comunicação é realizada na interface denominada *Data Sources*, na qual o usuário seleciona o protocolo adequado para o intercâmbio de dados com o relé IED, conforme ilustrado na Figura 14.

Figura 14 – Protocolos SCADA-LTS

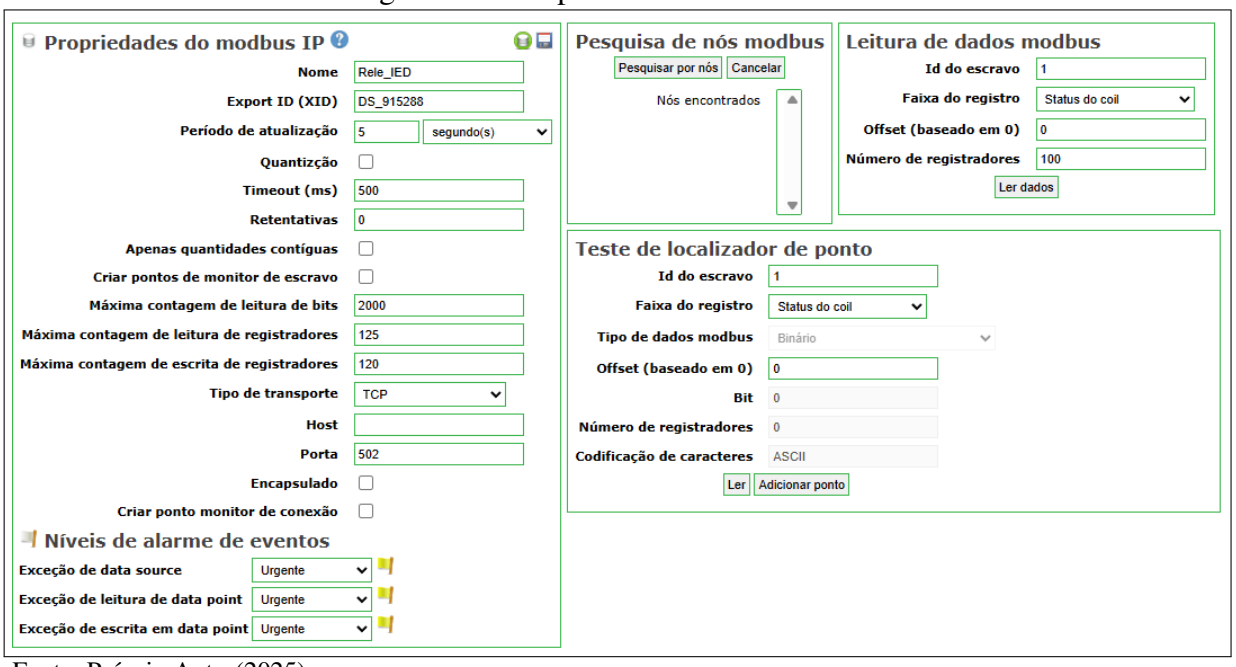


Fonte: Próprio Autor(2025)

Após a definição do protocolo de comunicação — neste caso, o Modbus IP — inicia-se a etapa de configuração das propriedades específicas do canal Modbus/TCP no SCADA-LTS. Nessa fase, são estabelecidos parâmetros fundamentais para o correto funcionamento da troca de dados entre o supervisório e o IED. Entre os ajustes necessários, destaca-se a atribuição de um nome ao *data source*, que permite sua identificação dentro do ambiente do SCADA, bem como a definição do período de atualização das leituras, responsável por determinar o intervalo em que o sistema requisitará novos dados ao dispositivo.

Essas opções influenciam diretamente a estabilidade e a forma de estabelecimento da conexão entre o SCADA e o IED. Por fim, é necessário especificar o endereço do Host (IP) e a porta de comunicação, que no caso do Modbus/TCP é tipicamente a porta 502. Esses parâmetros determinam o destino das requisições Modbus e garantem que o supervisório consiga estabelecer uma conexão confiável com o relé de proteção.

Figura 15 – Propriedades do modbus IP



Fonte: Próprio Autor(2025)

Por se tratar de uma aplicação voltada à proteção, adotou-se um período de atualização reduzido no supervisório, garantindo que o sistema seja capaz de detectar e acompanhar eventuais falhas em tempo hábil. Considerando que o relé utilizado não pertence à UFC, optou-se por omitir o endereço de rede (Host/IP) na Figura 15, preservando informações sensíveis do equipamento.

Após a criação da fonte de dados (data source), procedeu-se à configuração dos *data points*, que correspondem, em outros sistemas SCADA, ao conceito de tags. No SCADA LTS, cada *data point* é associado a um endereço definido na tabela de comunicação (Modbus Register Map) do relé, conforme especificado no respectivo manual. A partir desses endereços é possível mapear as variáveis disponibilizadas pelo equipamento, viabilizando a leitura de grandezas elétricas, a sinalização de falhas, o monitoramento de estados e a execução de comandos, entre outras funcionalidades relevantes para operação e proteção do sistema.

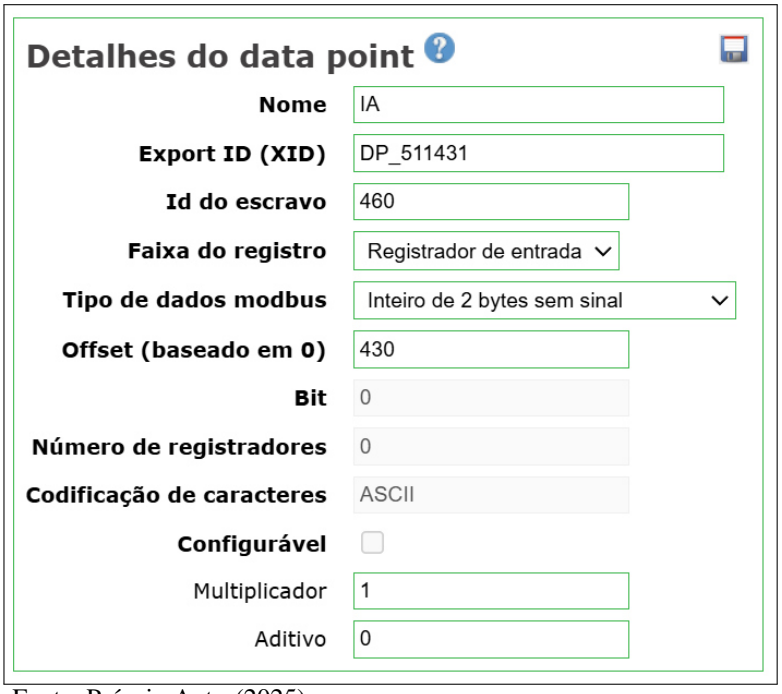
Para o desenvolvimento do projeto, foram selecionados diversos registradores Modbus para a criação dos *data points*. Conforme apresentado na Tabela 1, optou-se por incluir registradores associados às medições RMS disponibilizadas pelo relé, permitindo ao supervisório acompanhar, em tempo real, as grandezas elétricas fundamentais para a operação do sistema.

Além das variáveis de medição, foram incluídos também registradores referentes ao *trip status*, possibilitando identificar a causa da abertura do disjuntor durante eventos de proteção. Foram ainda configurados registradores destinados ao comando de *reset* de *trip* e ao acionamento

de *trip* remoto. Este último, por questões de segurança operacional, não está presente no mapa oficial do fabricante; entretanto, para fins de teste e validação do funcionamento do supervisório, foi utilizado um registrador do tipo *user*, configurado especificamente para simular o comando de *trip* durante os ensaios.

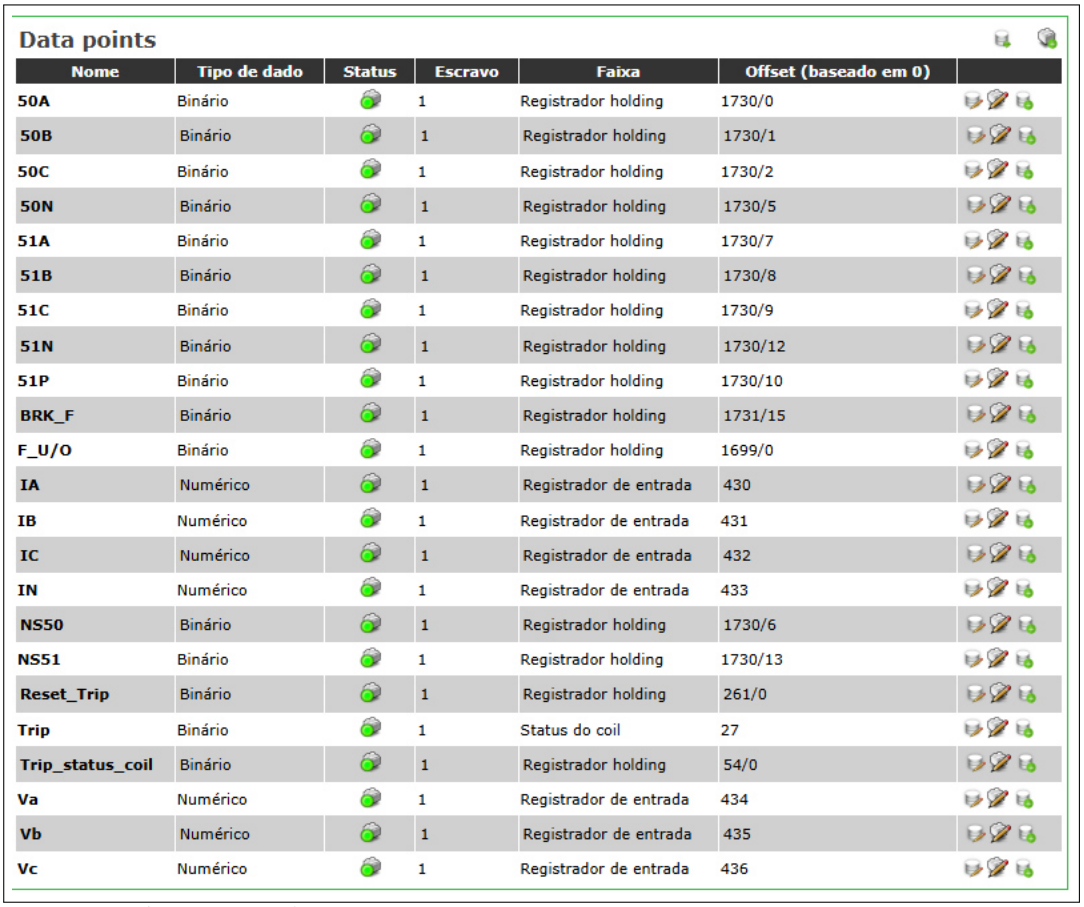
Conforme apresentado nas Figuras 16 e 17, é possível visualizar tanto os detalhes do processo de criação dos *data points* quanto o conjunto de pontos implementados no projeto. Destaca-se a necessidade de habilitar corretamente o *data source* e cada *data point* associado, pois somente após essa configuração o SCADA LTS é capaz de realizar a leitura, o monitoramento e o processamento das informações provenientes do IED.

Figura 16 – Data Point IA



Fonte: Próprio Autor(2025)

Figura 17 – Data Points



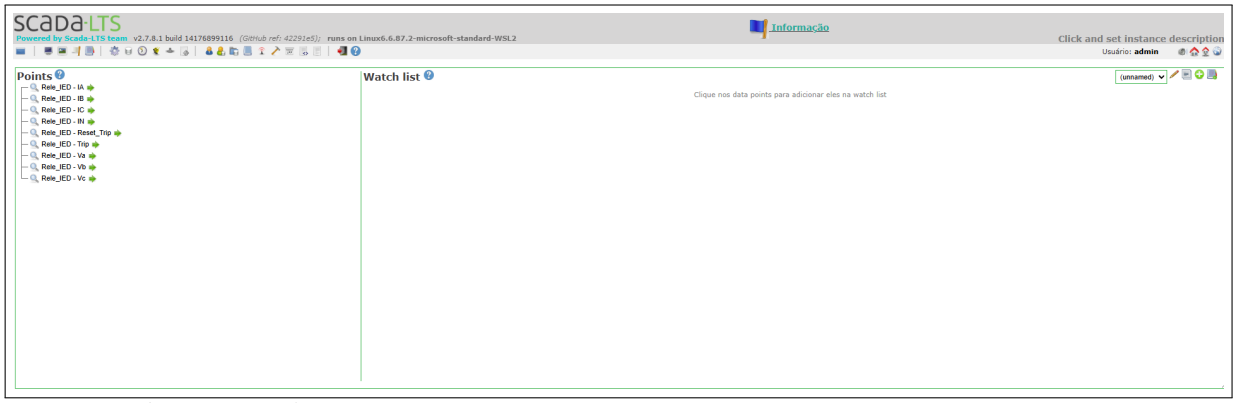
Data points

Nome	Tipo de dado	Status	Escravo	Faixa	Offset (baseado em 0)
50A	Binário		1	Registrador holding	1730/0
50B	Binário		1	Registrador holding	1730/1
50C	Binário		1	Registrador holding	1730/2
50N	Binário		1	Registrador holding	1730/5
51A	Binário		1	Registrador holding	1730/7
51B	Binário		1	Registrador holding	1730/8
51C	Binário		1	Registrador holding	1730/9
51N	Binário		1	Registrador holding	1730/12
51P	Binário		1	Registrador holding	1730/10
BRK_F	Binário		1	Registrador holding	1731/15
F_U/O	Binário		1	Registrador holding	1699/0
IA	Numérico		1	Registrador de entrada	430
IB	Numérico		1	Registrador de entrada	431
IC	Numérico		1	Registrador de entrada	432
IN	Numérico		1	Registrador de entrada	433
NS50	Binário		1	Registrador holding	1730/6
NS51	Binário		1	Registrador holding	1730/13
Reset_Trip	Binário		1	Registrador holding	261/0
Trip	Binário		1	Status do coil	27
Trip_status_coil	Binário		1	Registrador holding	54/0
Va	Numérico		1	Registrador de entrada	434
Vb	Numérico		1	Registrador de entrada	435
Vc	Numérico		1	Registrador de entrada	436

Fonte: Próprio Autor(2025)

Com os *data points* e o *data source* devidamente habilitados, estes passam a ser exibidos na *Watch List* do SCADA LTS, demostrada na Figura 18. Nessa interface, os valores recebidos podem ser acompanhados em tempo real, permitindo a verificação do funcionamento da comunicação, a análise das variáveis monitoradas e, quando aplicável, a configuração individual dos pontos para fins de ajuste ou depuração do sistema.

Figura 18 – Watch List



Fonte: Próprio Autor(2025)

Com os *data points* adicionados à *Watch List*, torna-se possível a criação de eventos associados às variações ou condições específicas observadas pelo SCADA. Além disso, esses pontos podem ser utilizados na geração de relatórios do sistema supervisório, permitindo documentar ocorrências, analisar o comportamento operacional do equipamento monitorado e apoiar processos de diagnóstico e tomada de decisão.

3.3.1 Configuração do IED e comunicação Modbus/TCP

O relé SEL-751 dispõe de suporte nativo à comunicação via protocolo TCP, permitindo sua integração a sistemas supervisórios por meio de redes Ethernet industriais. No presente projeto, a interligação entre o relé e o sistema SCADA foi realizada utilizando o switch gerenciável SEL-2730M, equipado com 24 portas, o qual opera como elemento central da rede local do laboratório. Esse arranjo garante a troca de dados de forma estruturada, segura e com baixa latência.

A Tabela 1 apresenta os registradores Modbus selecionados para a aquisição das grandezas elétricas monitoradas, bem como daqueles destinados à leitura do estado de *trip* e da identificação do tipo de atuação ocorrida. O endereço IP do SEL-751 foi configurado manualmente por meio da Interface Homem-Máquina (IHM) do próprio equipamento, assegurando sua correta integração à infraestrutura de comunicação da rede.

Tabela 1 – Principais registradores Modbus do SEL-751 utilizados no SCADA LTS

Nome	Função / descrição	Tipo	End. (dec)
IA RMS	Corrente de fase A	R	430
IB RMS	Corrente de fase B	R	431
IC RMS	Corrente de fase C	R	432
IN RMS	Corrente no neutro	R	433
VA RMS	Tensão de fase A	R	434
VB RMS	Tensão de fase B	R	435
VC RMS	Tensão de fase C	R	436
TRIP	Trip	R/W	27
RESET DATA	Comando de reset	R/W	261
TRIP STATUS LO	Trip status	R	1730
TRIP STATUS HI	Trip status	R	1731

Fonte: Elaborada pelo autor.

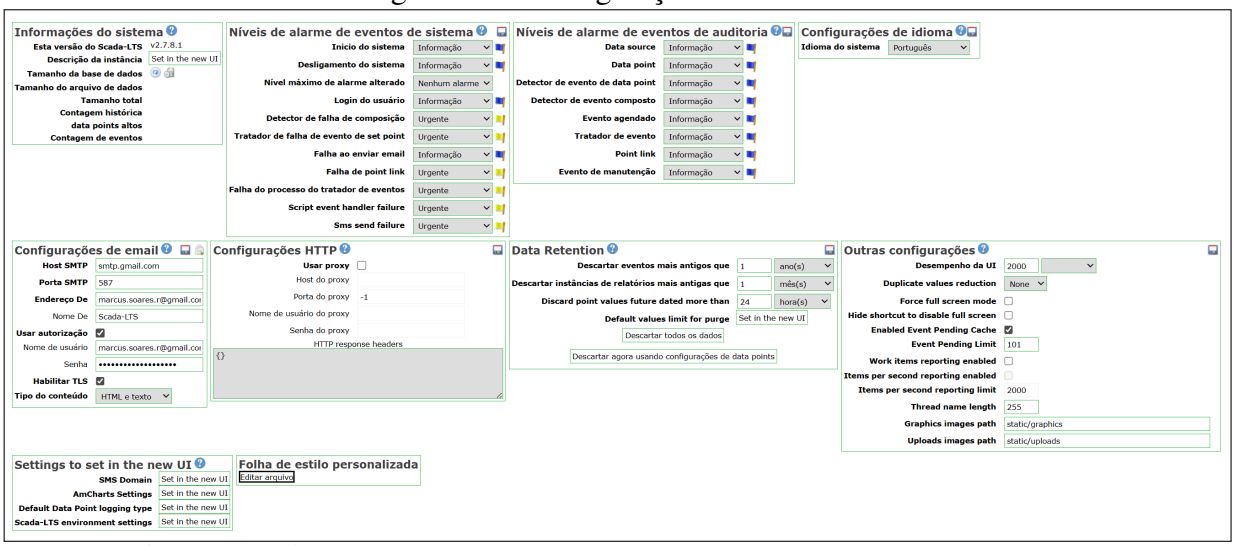
Conforme citado na seção anterior, foi configurado um registrador do tipo *user* para viabilizar a execução do comando de *trip* no escopo deste projeto. Tal abordagem tornou-se necessária porque o mapa de registradores do SEL-751 não disponibiliza um endereço específico para esse comando, em razão de critérios de segurança estabelecidos pelo fabricante. Dessa forma,

o registrador *user* permitiu a realização dos testes e o desenvolvimento da lógica supervisória, sem violar as restrições de segurança inerentes ao IED.

3.3.2 Configuração do SCADA LTS (telas, alarmes, relatórios)

O SCADA-LTS disponibiliza um conjunto abrangente de parâmetros para configuração do próprio sistema supervisório. No menu de Configurações do Sistema, é possível definir informações gerais, como a descrição da aplicação, os níveis de alarme, idioma da interface — incluindo a opção para o português —, configurações de envio de e-mails e demais ajustes específicos necessários ao funcionamento da plataforma. Essas configurações podem ser observadas na Figura 19.

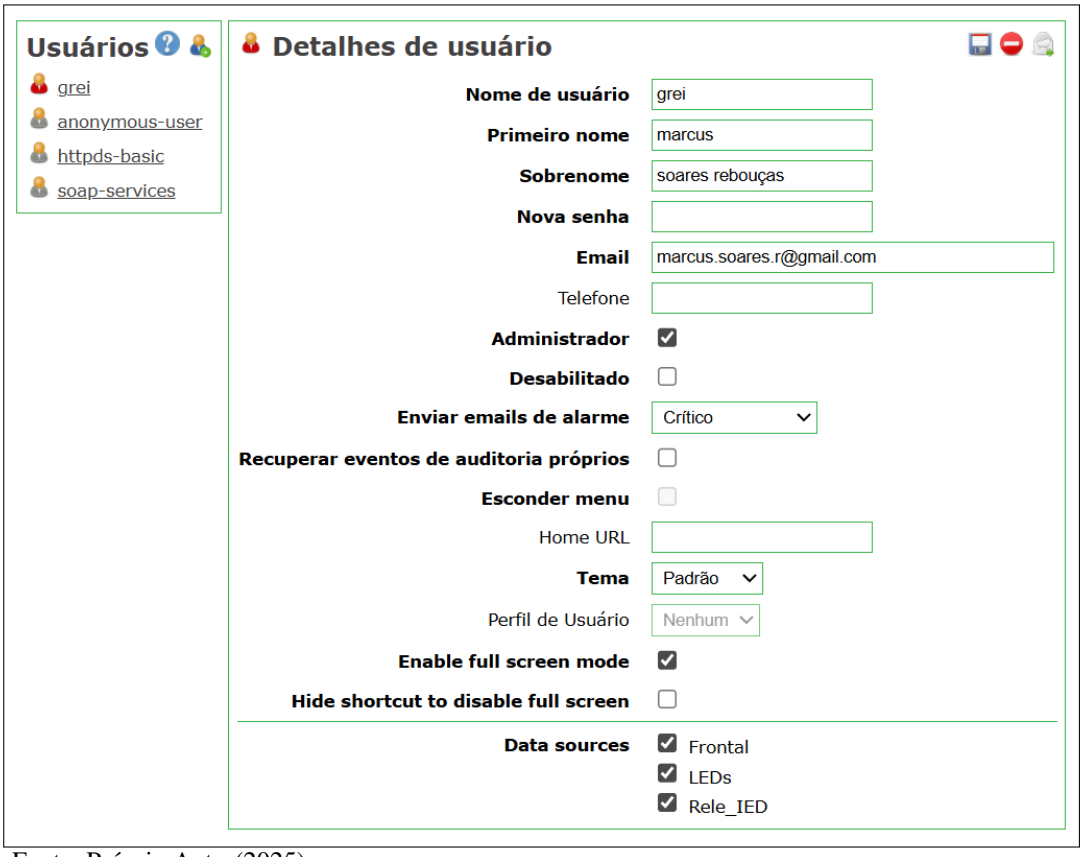
Figura 19 – Configurações do sistema



Fonte: Próprio Autor(2025)

Adicionalmente, o SCADA-LTS permite a gestão detalhada dos usuários que terão acesso ao sistema. Nessa seção é possível definir níveis de permissão, habilitar ou desabilitar privilégios, selecionar quais usuários devem receber notificações por e-mail e configurar preferências de interface. Na Figura 20 é apresentado essa interface de configuração.

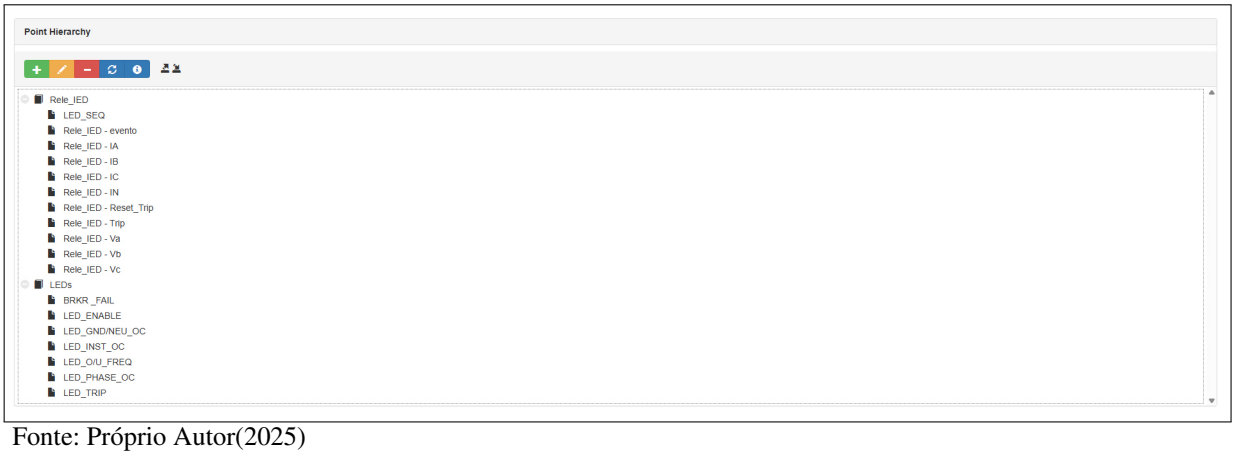
Figura 20 – Configurações do usuário



Fonte: Próprio Autor(2025)

Outro recurso relevante é a funcionalidade de Hierarquia, que possibilita organizar os *data points* em pastas e subpastas, facilitando a estruturação lógica do sistema supervisório. Essa organização é especialmente útil quando se trabalha com grande quantidade de variáveis, permitindo melhor categorização, navegação e, quando necessário, a criação de diferentes *watch lists* específicas para cada área de interesse. A Figura 21 ilustra essa estrutura.

Figura 21 – Hierarquia



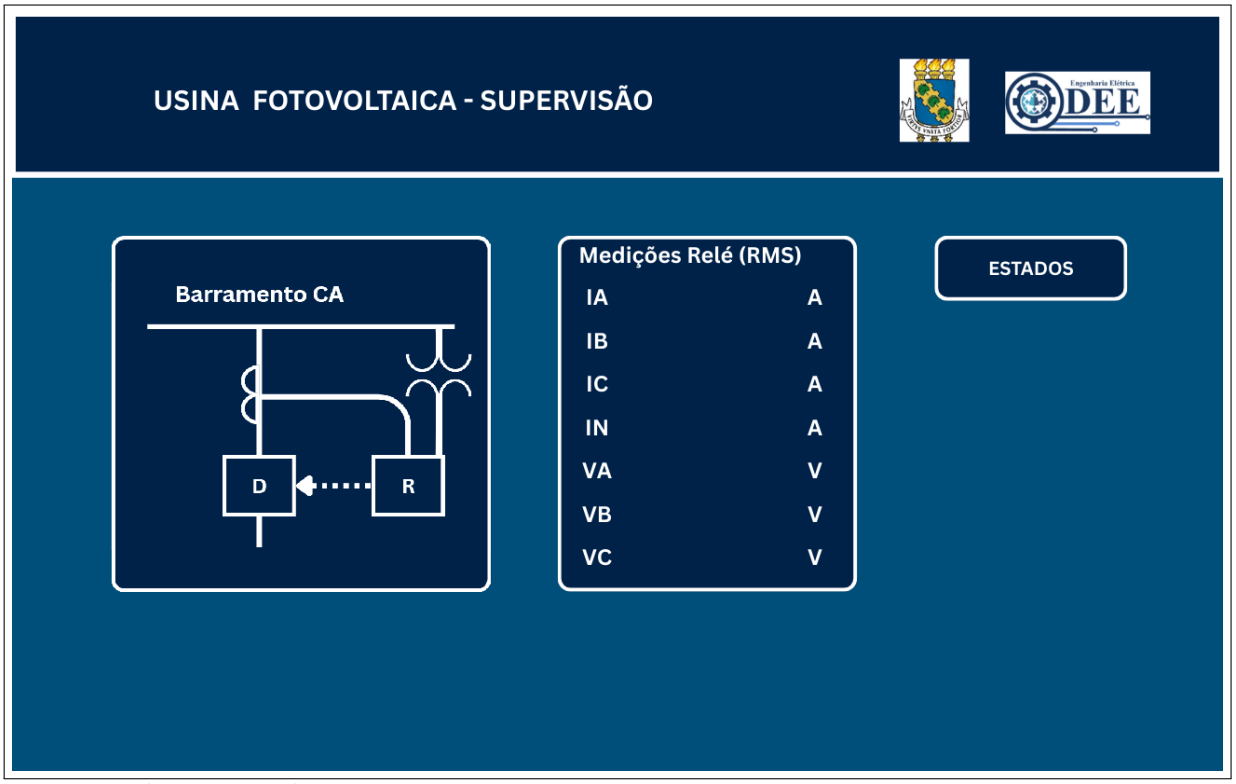
Fonte: Próprio Autor(2025)

3.3.3 Telas

A construção da interface supervisória do relé exige o acesso ao módulo de representação gráfica do SCADA-LTS, responsável pela criação dos elementos visuais de monitoramento. Inicialmente, seleciona-se o ícone destinado à elaboração de componentes gráficos. Em seguida, no ambiente de representação, utiliza-se a função “Nova Representação”, a partir da qual é gerada uma nova tela supervisória.

Após a criação do ambiente gráfico, procede-se à configuração do plano de fundo. Nessa etapa, define-se a imagem que servirá como base visual da interface. Nas Figuras 22 e 23 é visualizado as imagens utilizadas como fundo inicial, ambas previamente desenvolvidas no Canva e ajustadas para atender às demandas estéticas e funcionais do sistema.

Figura 22 – Fundo da tela de medições



Fonte: Próprio Autor(2025)

Figura 23 – Fundo da tela de estados

Fonte: Próprio Autor(2025)

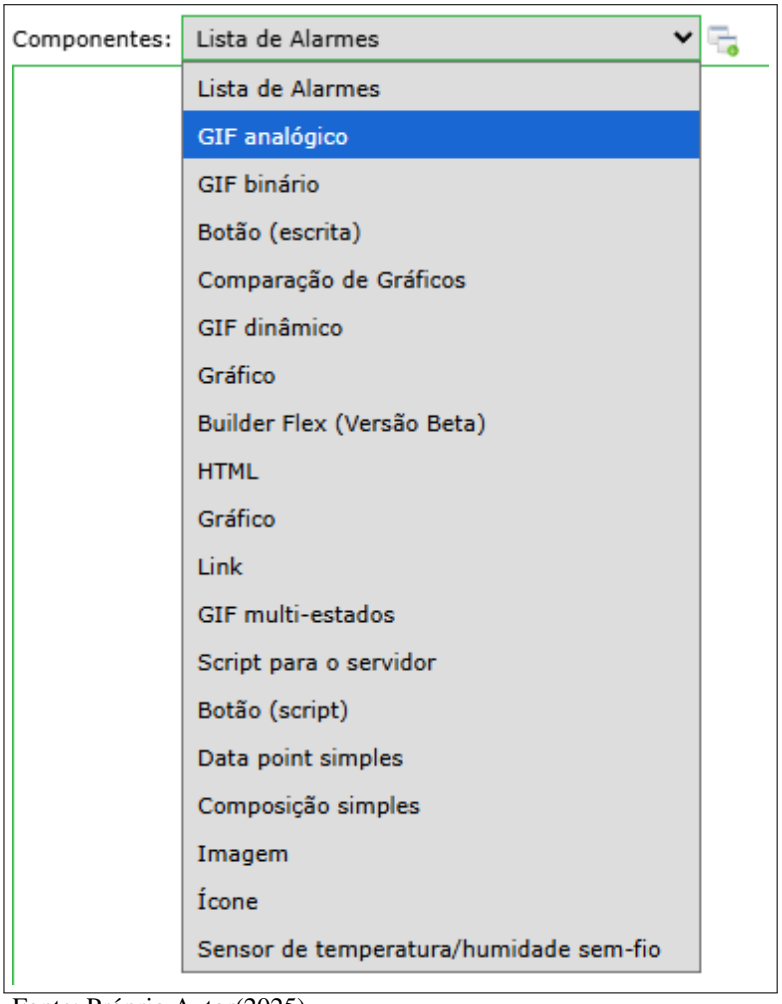
As propriedades gerais da representação podem ser observadas na Figura 24. Nessa janela, é possível selecionar a imagem de fundo e, posteriormente, inserir os componentes disponibilizados pelo SCADA-LTS. Esses componentes incluem botões de escrita associados a variáveis específicas, elementos animados (gifs) utilizados para representar estados do processo, indicadores de dados (data points) destinados à visualização de valores analógicos ou digitais, entre outros recursos necessários para a construção da interface interativa, os componentes são visto na Figura 25.

Durante o desenvolvimento, foram identificadas algumas limitações inerentes ao SCADA-LTS por se tratar de um software gratuito e de código aberto. Entre elas, destacam-se a impossibilidade de interação com variáveis posicionadas em camadas inferiores a outros elementos gráficos, bem como a limitação na personalização de formatos de certos componentes. Apesar dessas restrições, tais características são compreensíveis considerando que o SCADA-LTS se propõe a ser uma alternativa gratuita e acessível, diferentemente de soluções proprietárias mais completas, porém de alto custo.

Figura 24 – Propriedades da nova representação

Fonte: Próprio Autor(2025)

Figura 25 – Componentes



Fonte: Próprio Autor(2025)

Na primeira tela, denominada "Tela de Medições", mostrada na Figura 26, foram adicionados os componentes de *data points*, permitindo a visualização dos valores lidos pelo SCADA, provenientes do relé. Também foi inserida uma lista de alarmes, que exibe na tela os alarmes acionados. Os valores medidos incluem as correntes IA, IB, IC e IN, além das tensões Va, Vb e Vc.

Além disso, um link foi inserido para possibilitar a navegação para a tela seguinte, chamada "Tela de Estados". Este link foi estilizado com uma imagem de fundo, de forma a se assemelhar a um botão, proporcionando uma transição visualmente agradável entre as interfaces.

Figura 26 – Tela de medições

Fonte: Próprio Autor(2025)

Na segunda tela, denominada “Tela de Estados”, demostrada pela Figura 27 os indicadores visuais em forma de LEDs ou gifs binários foram configurados para refletir diretamente o estado dos bits dos *data points* correspondentes no relé SEL-751, oferecendo uma representação dinâmica e imediata dos eventos e condições do sistema de proteção. Esses indicadores correspondem a diversas funções de proteção e status do relé, tais como:

- **ENABLE**: Após ser energizado, o relé executa um autoteste interno e, se tudo estiver correto, o LED ENABLED acende;
- **TRIP**: Indica o acionamento de disparo (trip) pelo relé, ou seja, a atuação que resultará na

abertura do disjuntor;

- **INST OC**: Representa a função de sobrecorrente instantânea, atuando sem temporização e usada para detecção imediata de faltas de alta magnitude;
- **PHASE OC**: Indica a atuação da proteção de sobrecorrente temporizada de fase (*time-overcurrent*), responsável por detectar correntes anormais com curva de tempo inverso;
- **GND/NEU OC**: Indicam sobrecorrente residual/neutra, associada a faltas de terra ou desequilíbrios que envolvem o condutor neutro ou o sistema de aterramento;
- **NEG SEQ OC**: Sobrecorrente de sequência negativa, usada para detectar faltas desequilibradas, como curtos entre fases com assimetria ou faltas fase-terra desequilibradas;
- **O/U FREQ**: Refere-se à proteção de subfrequência/sobrefrequência (*under/over-frequency*), importante para garantir a estabilidade do sistema diante de variações críticas de frequência;
- **BRKR FAIL**: Sinaliza falha do disjuntor (*breaker failure*), indicando que o dispositivo não abriu ou não fechou dentro do tempo esperado após comando.

Esses alertas visuais refletem diretamente os elementos de proteção que o SEL-751 disponibiliza — sobrecorrentes fase, neutro/terra, sequência negativa, proteção de frequência, e falha de disjuntor, entre outras.

Adicionalmente, a "Tela de Estados" mantém um botão de escrita que permite ao supervisor acionar o *reset* do *trip* do relé via SCADA, restabelecendo condições operacionais após um disparo. A interface também oferece um link de retorno à tela anterior ("Tela de Medições"), preservando a consistência de navegação entre as telas.

O design visual da tela foi construído para imitar o painel real do relé SEL-751, de modo a fornecer familiaridade ao operador e facilitar o reconhecimento das funções e estados. Essa representação gráfica — com LEDs/gifs e layout similar ao hardware — otimiza o monitoramento e a supervisão remota do sistema, fornecendo um panorama claro da condição operacional e eventuais falhas sem a necessidade de acesso físico ao relé.

Figura 27 – Tela de estados

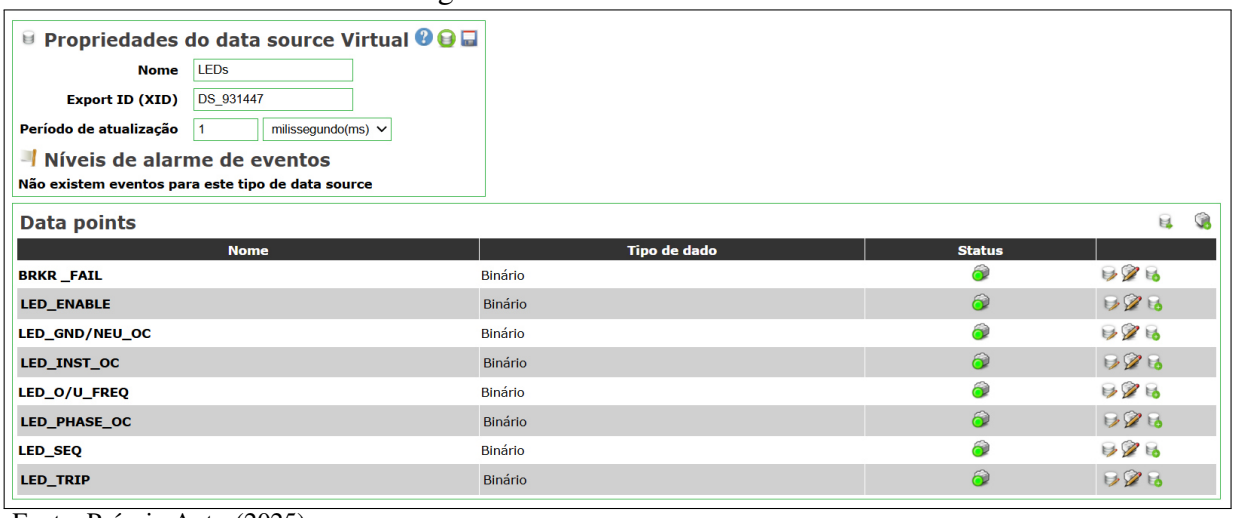
Fonte: Próprio Autor(2025)

Para a representação gráfica dos LEDs do relé, observou-se que o mapa de registradores do SEL-751 não disponibiliza registradores específicos para esses indicadores. Dessa forma, tornou-se necessária a criação de uma nova fonte de dados (data source) dedicada a essa funcionalidade.

Foi criado, portanto, o *data source* denominado LEDs, no qual foram definidos os respectivos *data points* responsáveis pelo acionamento dos LEDs associados a cada tipo de falha, bem como dos sinais de *enable* e *trip*, ilustrada pela Figura 28 e pela Tabela 2.

Adicionalmente, desenvolveu-se um script — apresentado em seção posterior — que implementa a lógica de correlação entre o registrador de evento *trip* e os LEDs correspondentes. Esse script garante que cada tipo de ocorrência registrada pelo relé acione corretamente o LED designado, assegurando coerência entre o estado operacional do equipamento e sua representação gráfica na interface SCADA.

Figura 28 – Data source LEDs



Fonte: Próprio Autor(2025)

Tabela 2 – Data points de LEDs configurados no SCADA LTS

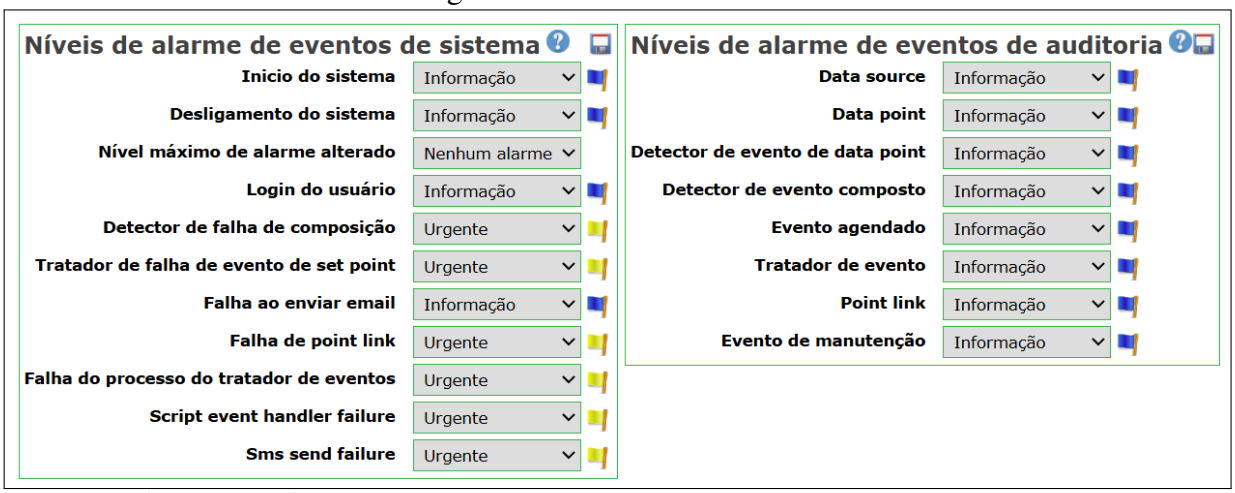
Nome	Função / descrição	Tipo	Origem
LED_ENABLE	Indicação de habilitação do relé / lógica ativa	Binário	Virtual
LED_TRIP	Indicação de atuação de *trip* do relé	Binário	Virtual
LED_INST_OC	Indicação de sobrecorrente instantânea (50)	Binário	Virtual
LED_PHASE_OC	Indicação de sobrecorrente temporizada (51)	Binário	Virtual
LED_GND/NEU_OC	Indicação de sobrecorrente de neutro (51N/50N)	Binário	Virtual
LED_SEQ	Indicação de sequência de fases ou distúrbio	Binário	Virtual
LED_O/U_FREQ	Indicação de sub ou sobretensão/sobrefrequência	Binário	Virtual
BRKR_FAIL	Indicação de falha no disjuntor	Binário	Virtual

Fonte: Elaborada pelo autor, 2025.

3.3.4 Alarmes

Os alarmes constituem uma funcionalidade essencial em sistemas supervisórios, pois possibilitam a identificação de situações anormais e condições operativas relevantes. Esses alarmes podem abranger diversos tipos de avisos, como falhas em *data points*, acessos de usuários, eventos de proteção e outros registros internos do sistema. No ícone de Configuração do Sistema, apresentado em seção anterior, é possível definir os níveis de severidade de cada alarme, atribuindo diferentes graus de urgência conforme a criticidade do evento. A Figura 29 ilustra essa interface de configuração.

Figura 29 – Níveis de alarme



Fonte: Próprio Autor(2025)

O SCADA-LTS também possibilita a associação de determinados *data points* a eventos específicos. Neste trabalho, foi desenvolvido um conjunto de eventos vinculados aos *data points* responsáveis por indicar a ocorrência de *trip* no relé. Para cada um desses *data points*, definiu-se um evento destinado ao tratamento de sua respectiva condição de acionamento. Foram selecionados três registradores que abrangem os eventos utilizados no projeto, conforme apresentado nas Tabelas 3 e 4.

Tabela 3 – Eventos trip associados ao registrador Modbus 1730 (TRIP STATUS LO) do relé SEL-751

Bit	Descrição do Evento
1	PHASE A1 50
2	PHASE B1 50
3	PHASE C1 50
5	NEUTRAL 50N1
5	GND/NEUT 50 Trip
6	NEG SEQ 50Q1
7	PHASE A 51
8	PHASE B 51
9	PHASE C 51
10	PHASE 51P1
12	NEUTRAL 51N1
13	NEG SEQ 51Q

Fonte: Elaborada pelo autor com base no manual do SEL-751, 2025.

Tabela 4 – Eventos trip associados ao registrador Modbus 1731 (TRIP STATUS HI) do relé SEL-751

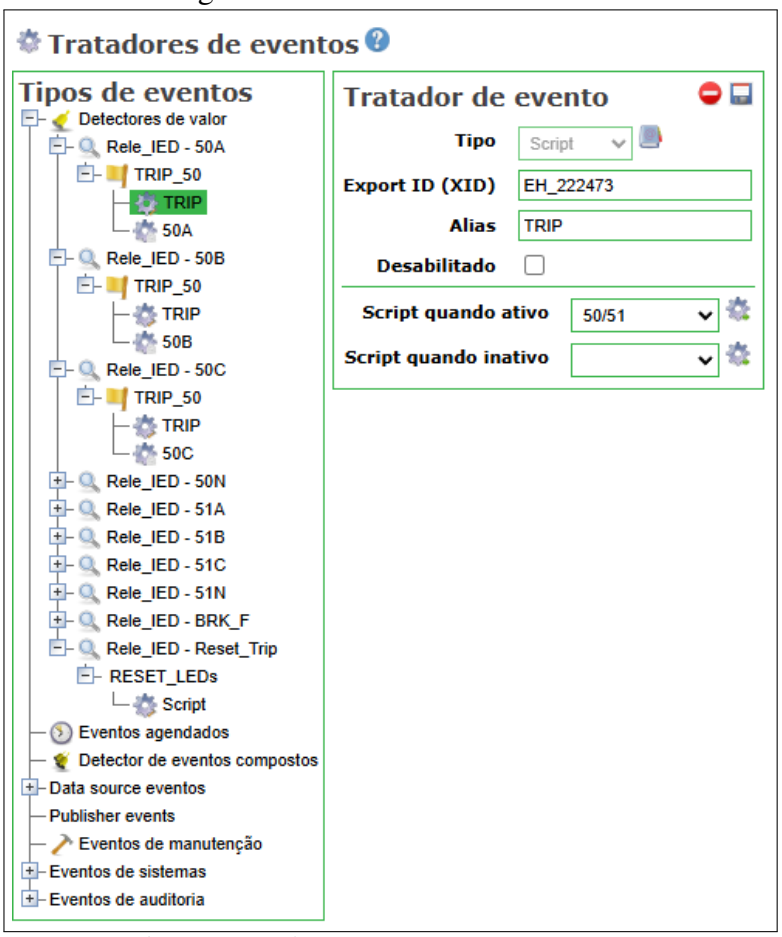
Bit	Descrição do Evento
15	BREAKER FAIL

Fonte: Elaborada pelo autor com base no manual do SEL-751, 2025.

O evento criado para cada *data point* foi configurado como do tipo “mudança de valor”, de modo que qualquer alteração nos *data points* indica a ocorrência de uma atuação do relé de proteção. Por se tratar de eventos associados a funções de proteção, o nível de alarme definido foi o nível crítico.

Após a criação do evento, o SCADA-LTS permite tratá-lo utilizando o menu Tratadores de Eventos, demostrado na Figura 30. Nessa interface, o usuário pode selecionar o evento desejado e definir ações automáticas, como envio de e-mails, alteração de *setpoints*, execução de comandos, acionamento de scripts ou envio de mensagens SMS.

Figura 30 – Tratadores de eventos



Fonte: Próprio Autor(2025)

No presente trabalho, foram configurados dois tratadores de eventos para cada tipo de trip:

- Um tratador de evento email destinado ao envio de notificações por e-mail ao usuário, assegurando a comunicação rápida em situações de ocorrência de eventos relevantes, no caso cada trip especifico manda um email com o nome do trip que ocorreu;

- Um tratador de evento do tipo *script*, utilizado para executar a lógica necessária à atualização da interface gráfica quando o evento é detectado.

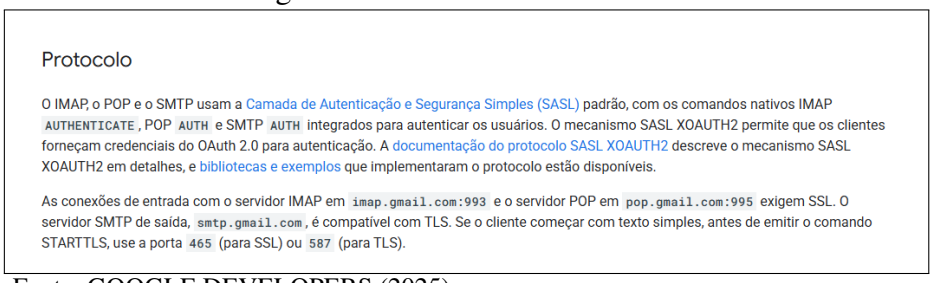
Além dos eventos baseados em *data points*, o SCADA-LTS também possibilita a criação de eventos programados, eventos compostos, eventos associados ao *data source*, eventos de sistema e eventos de auditoria, permitindo ampla flexibilidade na gestão das ocorrências dentro do supervisório.

3.3.5 Relatórios

O SCADA-LTS disponibiliza um mecanismo de envio automático de relatórios por e-mail, funcionalidade que pode ser empregada para manter operadores e responsáveis informados sobre o estado do sistema supervisório. A plataforma permite configurar diferentes critérios de disparo, como envio periódico por horário, acionamento a cada evento registrado ou emissão condicionada a alarmes específicos, oferecendo flexibilidade para adequar o fluxo de notificações às necessidades da operação. Além disso, o sistema possibilita a seleção do modelo de relatório, neste projeto, optou-se pela utilização do formato padrão disponibilizado pelo software.

Entretanto, observou-se certa complexidade durante a integração inicial com o serviço de e-mail utilizado (Gmail), uma vez que o procedimento de configuração não é totalmente intuitivo. Para estabelecer a comunicação, foi necessário identificar manualmente o servidor SMTP e a porta correspondente, sendo que a Figura 31 demostra o protocolo que auxiliou no correto preenchimento dos campos *host* e *port*. A principal dificuldade consistiu em determinar o método adequado para geração da credencial de acesso, visto que a documentação disponível nas configurações de e-mail do SCADA-LTS não esclarece esse procedimento de forma objetiva. Após investigação adicional, verificou-se que era indispensável criar uma “senha de aplicativo”, funcionalidade disponibilizada somente após a ativação da verificação em duas etapas na conta Google. Concluídas essas etapas, o sistema passou a enviar os relatórios de forma adequada, possibilitando a finalização da configuração de e-mail ilustrada na Figura 32.

Figura 31 – Host e Port do SMTP



Fonte: GOOGLE DEVELOPERS (2025)

Figura 32 – Propriedades relatorio

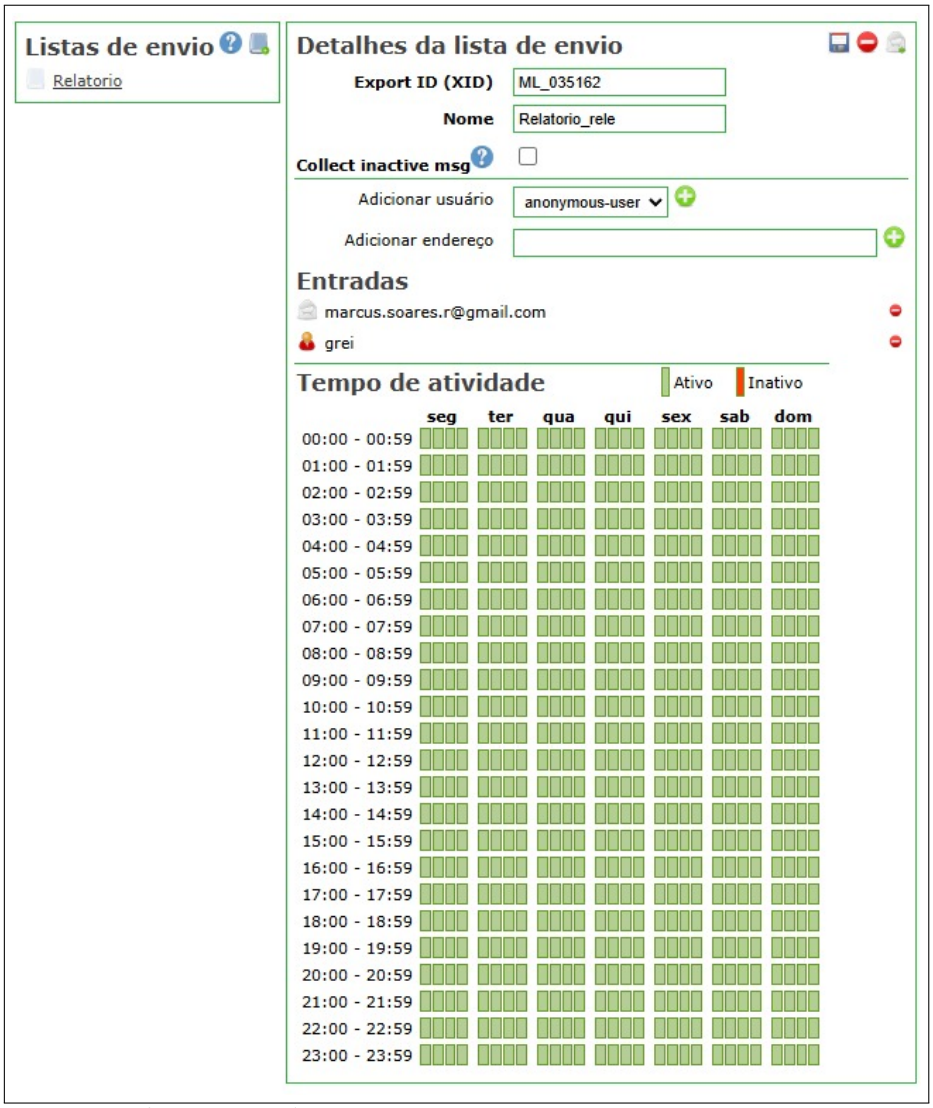
Fonte: Próprio Autor(2025)

Para este projeto, o SCADA-LTS foi configurado para enviar automaticamente um relatório sempre que ocorrer um evento de *trip* no relé, assegurando que o usuário seja imediatamente notificado sobre a atuação do equipamento. Essa funcionalidade contribui para o acompanhamento em tempo real do comportamento do sistema elétrico, favorecendo uma resposta rápida e informada diante de situações anormais.

Além disso, o SCADA-LTS disponibiliza um módulo específico para o gerenciamento das listas de envio, por meio do qual é possível configurar o envio periódico de relatórios. O operador pode selecionar os destinatários individualmente, utilizando usuários previamente cadastrados ou endereços de e-mail definidos manualmente. Também é possível estabelecer condições temporais para o envio, como restrições de horário ou períodos de indisponibilidade de determinados destinatários. Dessa forma, quando um usuário estiver marcado como inacessível em um intervalo específico, o sistema interrompe automaticamente o envio de relatórios para

aquele endereço, evitando falhas de comunicação ou notificações desnecessárias.

Figura 33 – Lista de envio



Fonte: Próprio Autor(2025)

3.3.6 Script

No menu de *Scripts*, o SCADA-LTS contempla a criação de rotinas em *JavaScript*, permitindo a seleção dos *data points* que serão manipulados e a atribuição de variáveis correspondentes a cada um deles. Essa funcionalidade possibilita o desenvolvimento de lógicas personalizadas, vinculadas diretamente à ocorrência de eventos específicos. Assim, sempre que determinado evento é acionado, o *script* associado é executado automaticamente.

No contexto deste trabalho, foram elaborados *scripts* distintos para cada função de proteção, de modo a viabilizar a correta identificação dos eventos e assegurar o funcionamento lógico da interface gráfica do sistema supervisório. No Código-fonte 1, apresenta-se o *script*

responsável pela implementação da lógica referente às funções 50/51. Nesse caso, quando os bits do registrador de *TRIP STATUS* são acionados, o *script* identifica qual condição de atuação ocorreu e aciona os LEDs correspondentes na interface gráfica, especificamente aqueles relacionados aos LEDs INST OC e *PHASE OC*.

Código-fonte 1 – Script em JavaScript para acionamento dos LEDs referentes as funções 50/51

```
var has50 = (p52.value == true || p53.value == true || p54.
   value == true);
var has51 = (p57.value == true || p58.value == true || p59.
   value == true || p36.value == true);

//Zera sempre os LEDs
DP.writeDataPoint('INST_L',  false);
DP.writeDataPoint('TEMP_L', false);
DP.writeDataPoint('TRIP_L',     false);


if (has50) {
    DP.writeDataPoint('INST_L', true);
    DP.writeDataPoint('TRIP_L', true);
} else if (has51) {
    DP.writeDataPoint('TEMP_L', true);
    DP.writeDataPoint('TRIP_L', true);
}
```

Fonte: Próprio Autor (2025).

3.3.7 Implementação do acesso remoto

O acesso remoto para os administradores, utilizado no trabalho será realizado por meio da integração entre os softwares Tailscale e RustDesk, que operam de forma complementar. O Tailscale atua como uma solução de VPN baseada no protocolo WireGuard, criando uma rede privada virtual criptografada na qual somente dispositivos autorizados podem ingressar. Dessa forma, os equipamentos passam a operar como se estivessem na mesma rede local (LAN),

cada um recebendo um endereço IP virtual seguro. Essa abordagem garante proteção adicional, uma vez que o acesso somente é possível após a autenticação e inclusão do dispositivo na rede privada.

Entretanto, o Tailscale não oferece funcionalidade de compartilhamento ou controle remoto de tela, sendo necessário um software adicional para essa finalidade. Para isso, adotou-se o RustDesk, uma ferramenta *open-source* que possibilita acesso remoto à área de trabalho utilizando conexões peer-to-peer (P2P) ou, quando necessário, servidores de retransmissão para descoberta e encaminhamento.

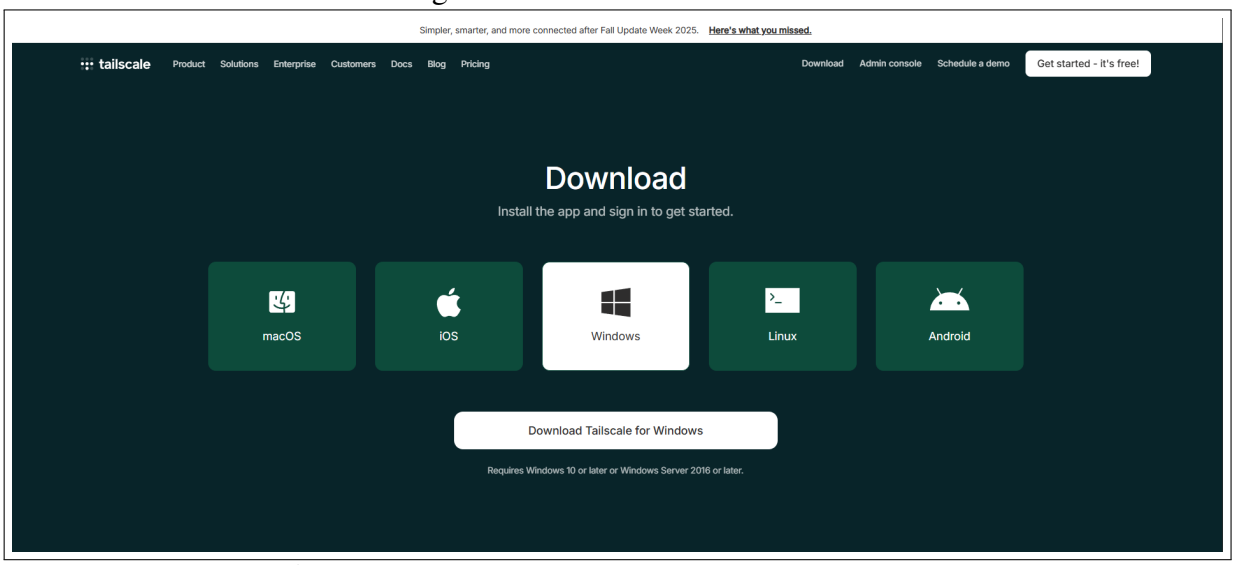
A utilização conjunta do Tailscale com o RustDesk proporciona diversas vantagens, como maior segurança, redução de latência, conexões mais estáveis e maior confiabilidade no acesso remoto.

A implementação do acesso remoto iniciou-se pela instalação dos softwares necessários nos dispositivos envolvidos no projeto, especificamente o computador pessoal utilizado para o desenvolvimento do sistema e o notebook do laboratório, por meio do qual é realizado o acesso ao relé de proteção.

O primeiro componente instalado foi o Tailscale. O download é realizado diretamente no site oficial da plataforma, onde o instalador correspondente ao sistema operacional do dispositivo é disponibilizado. Após o download, o processo de instalação é simples e não requer configurações avançadas, bastando aceitar os termos de licença. Em seguida, o usuário realiza a autenticação pelo navegador utilizando o e-mail escolhido, associando assim o dispositivo à sua rede Tailscale. A partir desse momento, o sistema atribui automaticamente um endereço IP virtual ao equipamento, permitindo o acesso remoto seguro enquanto ambos os dispositivos estiverem conectados à mesma Tailnet.

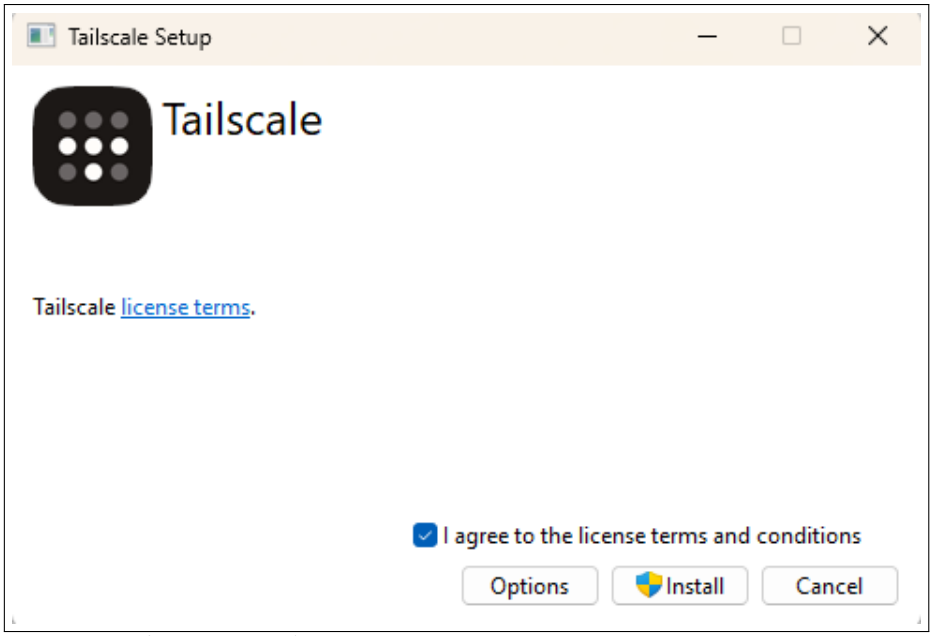
Esse procedimento assegura a criação de um túnel criptografado entre os dispositivos, possibilitando o acesso ao SCADA-LTS e ao relé por meio da rede privada virtual estabelecida. As Figuras 34, 35 e 36 ilustram as etapas de instalação, configuração e integração dos dispositivos à rede Tailscale. Nessas figuras, são apresentados, respectivamente, o site do Tailscale utilizado para o download do aplicativo, a janela do setup e a interface web da plataforma, na qual é possível visualizar e gerenciar os dispositivos integrantes da *tailnet*.

Figura 34 – Tailscale download



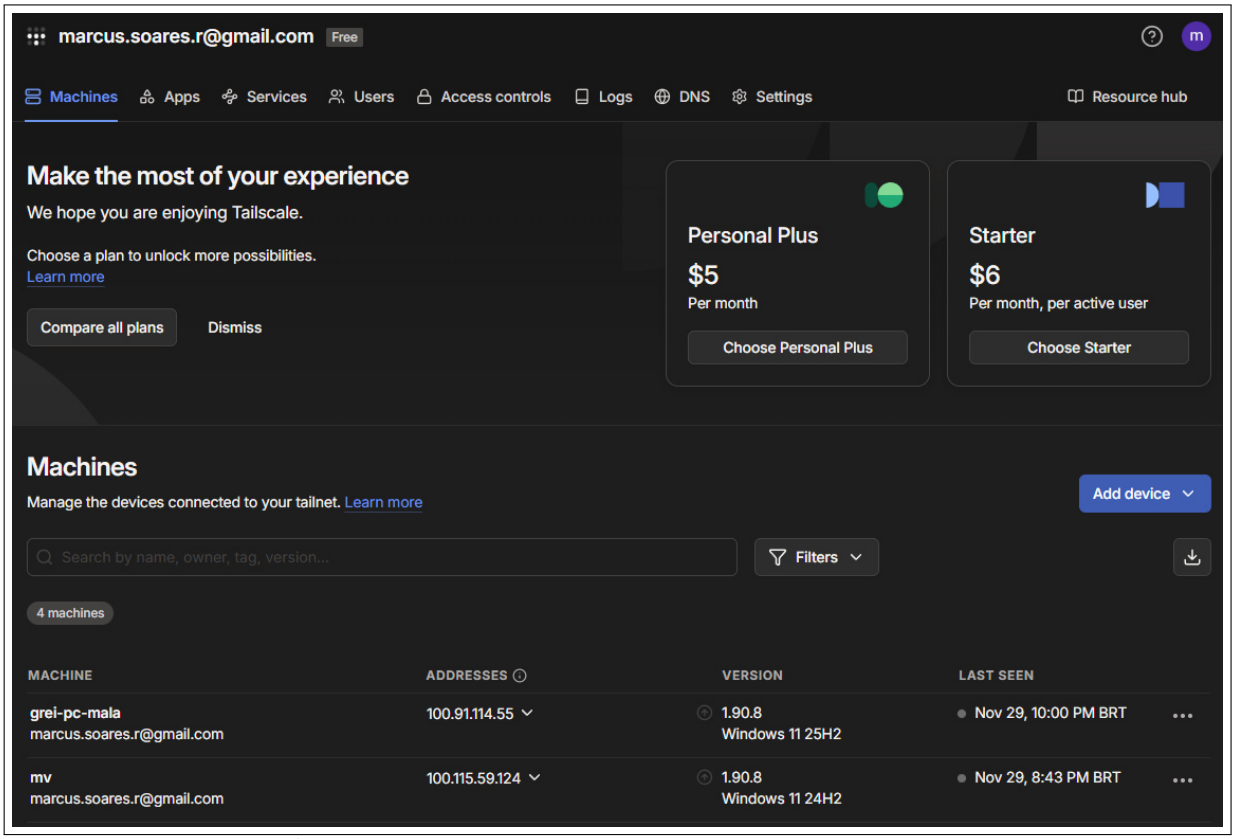
Fonte: TAILSCALE (2025)

Figura 35 – Tailscale setup



Fonte: Próprio Autor(2025)

Figura 36 – Tailscale dispositivos



Fonte: TAILSCALE (2025)

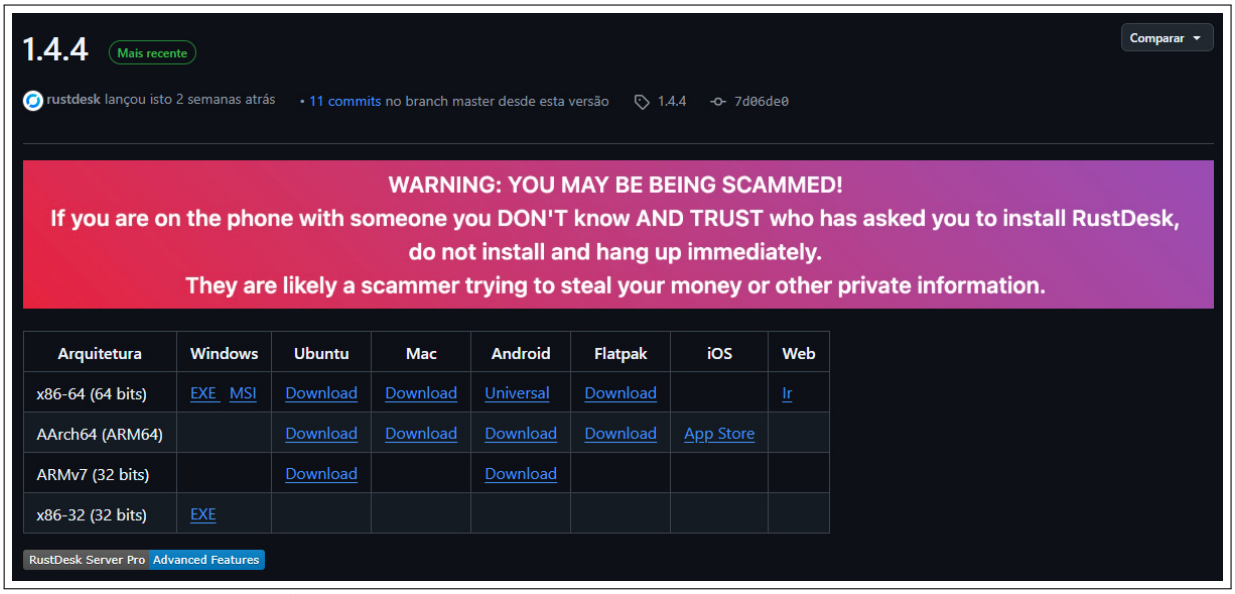
Após a instalação do Tailscale e a inclusão dos dispositivos na rede virtual, procedeu-se à implementação do RustDesk. Inicialmente, realizou-se o download do software por meio do repositório oficial no GitHub, selecionando-se a versão correspondente a cada sistema operacional utilizado. Concluída a instalação, tornou-se possível estabelecer a conexão remota entre os dispositivos para acesso à tela.

Entretanto, para que o RustDesk opere corretamente em conjunto com o Tailscale, é necessário ajustar algumas configurações de segurança do aplicativo. Primeiramente, deve-se desbloquear as opções avançadas de segurança do RustDesk. Em seguida, é preciso habilitar o acesso IP direto, permitindo que o software utilize os IPs virtuais atribuídos pelo Tailscale. Essa configuração garante que a transmissão de vídeo e controle remoto ocorra diretamente pela VPN, aumentando a segurança e a estabilidade da conexão.

Com essa configuração, o acesso remoto pode ser realizado a partir de qualquer local que disponha de conexão à internet, seja por meio de uma rede local, 5G ou qualquer outra forma de acesso. Assim, utilizando apenas esses dois softwares, ambos de fácil implementação e com elevados padrões de segurança, garante-se uma solução prática, eficiente e confiável para

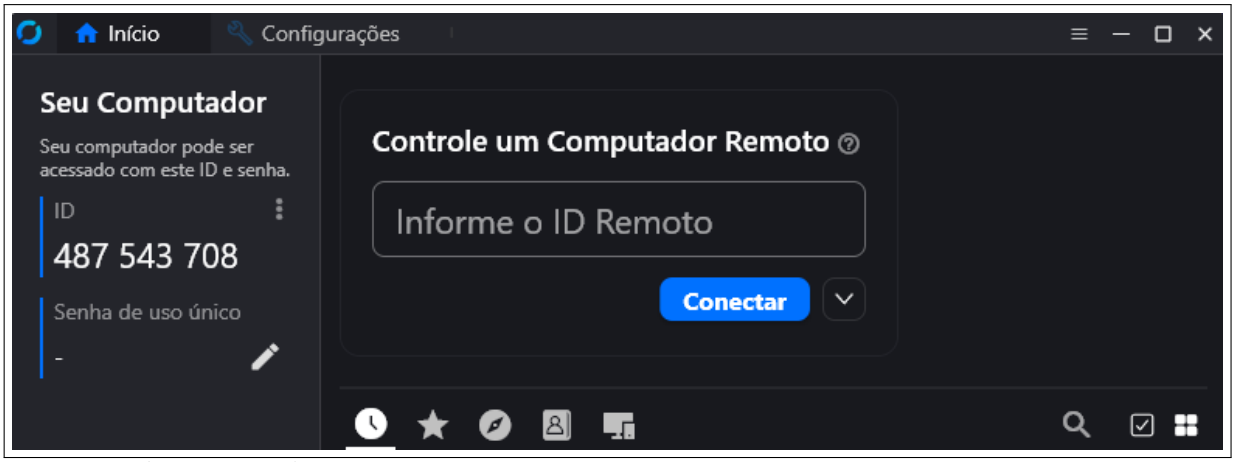
o acesso remoto aos dispositivos, as Figuras 37, 38 e 39 ilustram esse processo de instalação e configuração.

Figura 37 – RustDesk plataformas



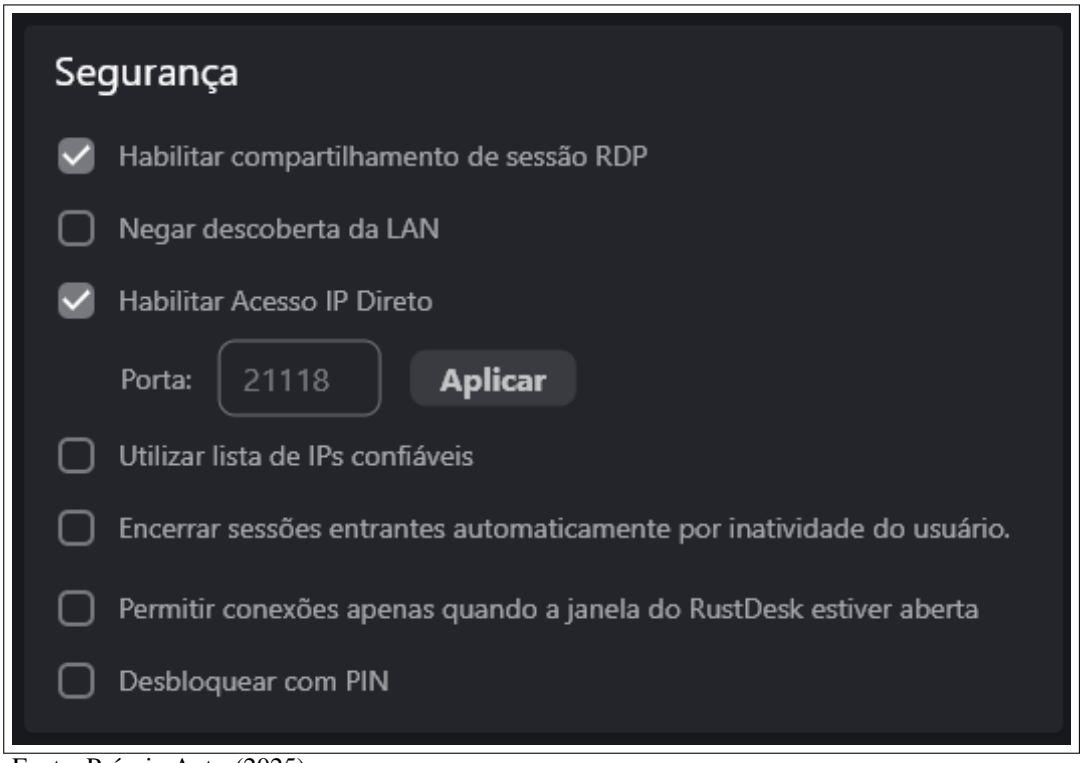
Fonte: RUSTDESK (2025)

Figura 38 – RustDesk acesso remoto



Fonte: Próprio Autor(2025)

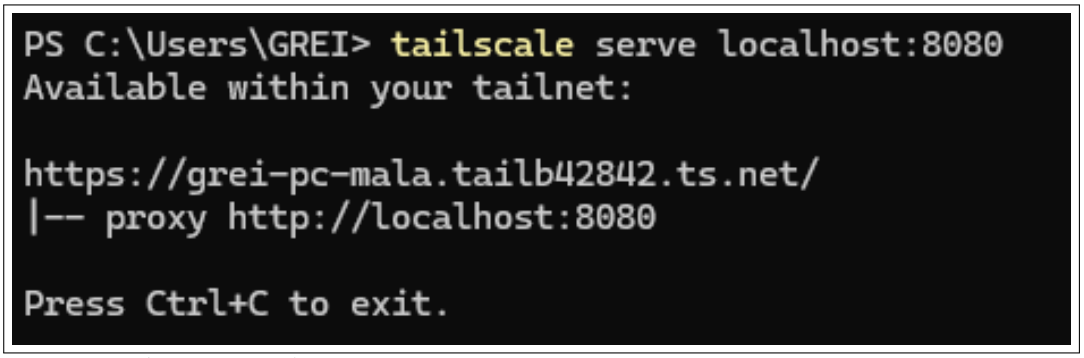
Figura 39 – Configurações de segurança



Fonte: Próprio Autor(2025)

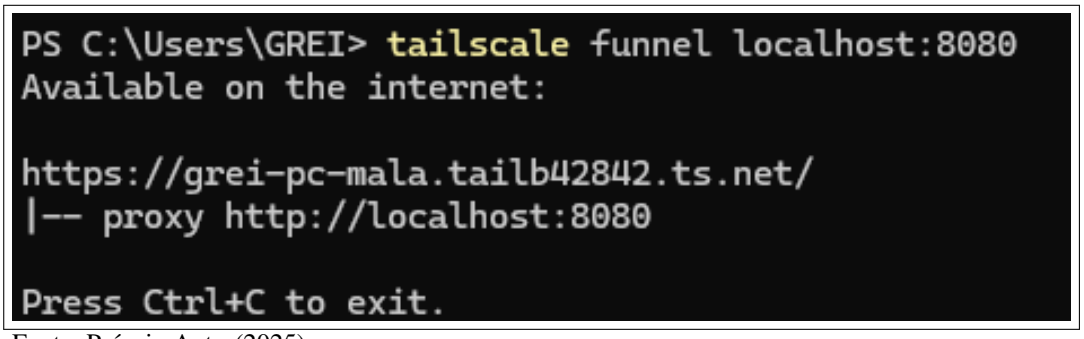
Para viabilizar o acesso dos operadores ao sistema em conformidade com o conceito de *zero trust*, utilizou-se uma funcionalidade da ferramenta Tailscale que permite a publicação controlada de serviços locais executados no próprio dispositivo. Por meio da execução do comando `tailscale serve localhost:8080` em um terminal do equipamento, configura-se um servidor local que disponibiliza um endereço de acesso restrito aos dispositivos previamente autenticados na *tailnet*. Caso seja necessária a disponibilização do acesso a dispositivos externos à *tailnet*, o comando pode ser substituído por `tailscale funnel localhost:8080`, possibilitando a exposição segura do serviço à internet pública, mantendo mecanismos de controle de autenticação. As Figuras 40 e 41 apresentam os comandos utilizados e os respectivos links gerados para acesso aos servidores.

Figura 40 – Comando para criação do servidor local



Fonte: Próprio Autor(2025)

Figura 41 – Comando para criação do servidor local para acesso externo a rede do tail



Fonte: Próprio Autor(2025)

Esse mecanismo possibilita que o operador acesse, por meio de um navegador web, o supervisório em execução na porta 8080, que, no contexto deste projeto, corresponde ao sistema supervisório SCADA-LTS. Após a criação do link, o acesso ao supervisório é realizado diretamente pelo navegador, sendo necessário acrescentar o sufixo /Scada-LTS ao final do endereço gerado, de modo a direcionar corretamente à interface do sistema supervisório.

3.4 Cenários de teste

Nessa seção, o sistema supervisório desenvolvido é submetido a diferentes cenários de teste, com o objetivo de avaliar seu desempenho e a correta interação com o relé de proteção. São analisadas três situações distintas: operação normal, simulações de falhas para verificação da atuação (trip) e testes de acesso remoto. Para a realização dessas simulações, utiliza-se uma mala de testes CE-6006, da Conprove, capaz de injetar valores controlados de tensão e corrente no relé, permitindo reproduzir condições reais de funcionamento e de anormalidade do sistema elétrico. Esse procedimento garante a validação prática das funcionalidades implementadas no

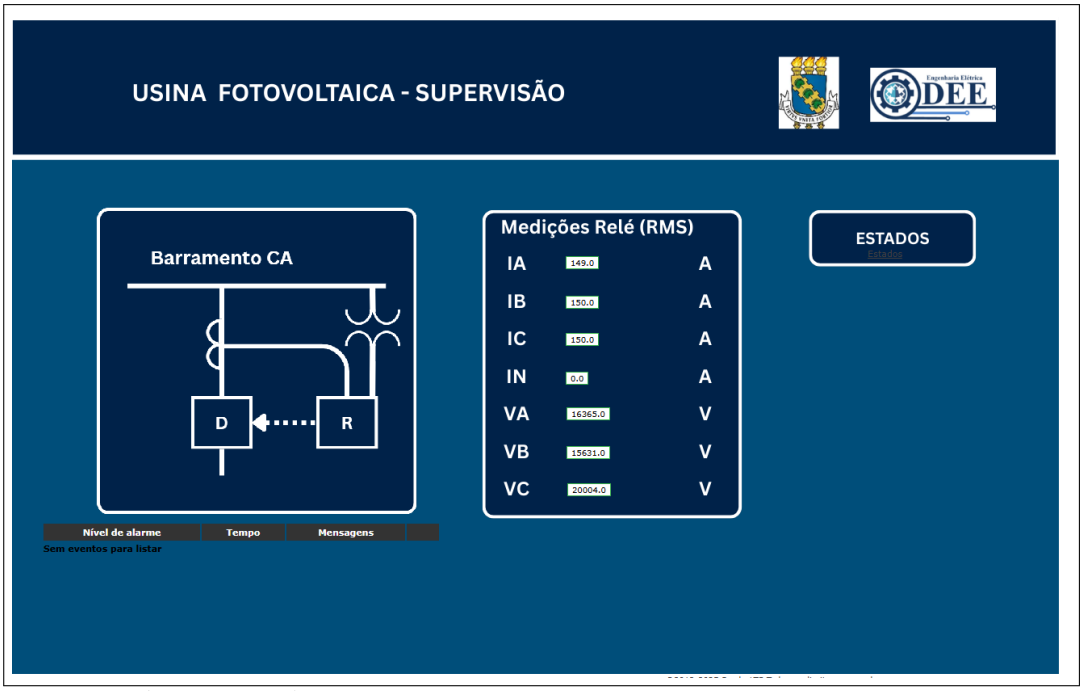
supervisório, bem como a confiabilidade da comunicação com o IED.

3.4.1 Simulação de operação normal

Nesta etapa do trabalho, o sistema supervisório foi configurado para adquirir e apresentar, em tempo real, os valores de medição fornecidos pelo relé, bem como seus respectivos estados operacionais. Assim, torna-se possível observar o comportamento da *watch list* do equipamento e analisar a resposta da interface gráfica durante a operação em condições normais do IED. A Figura 42 ilustra essa etapa, destacando a apresentação dos valores de medição na plataforma supervisória.

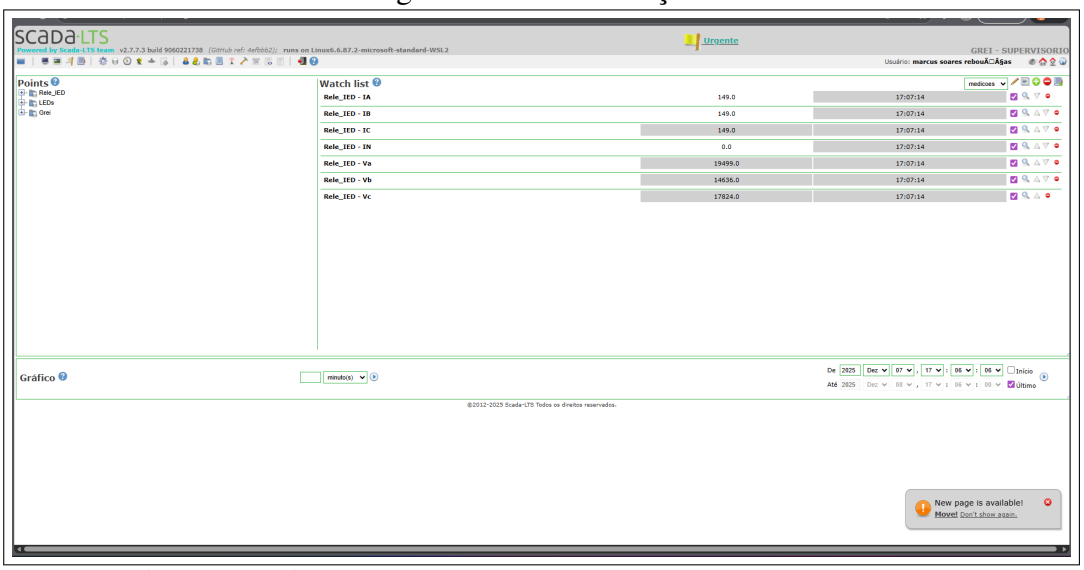
Mediante a injeção de valores no relé, verificou-se que o sistema supervisório interpretou e atualizou corretamente as medições recebidas, tanto na *watch list* quanto na interface gráfica. Esse resultado evidencia que, em condições normais de operação, o sistema é capaz de adquirir e apresentar de forma consistente e confiável os valores transmitidos pelo IED. Observa-se, ainda, nas Figuras 42 e 43, que os valores exibidos já correspondem ao resultado da aplicação da relação de transformação do TC configurada no relé, o que reforça a eficácia do processo de comunicação e interpretação dos dados.

Figura 42 – Operação normal supervisório



Fonte: Próprio Autor(2025)

Figura 43 – Tela medições



Fonte: Próprio Autor(2025)

Com isso, comprova-se que a comunicação entre o supervisório e o relé ocorre de maneira eficiente e responsiva, assegurando a correta obtenção dos valores disponibilizados pelo equipamento por meio do protocolo Modbus.

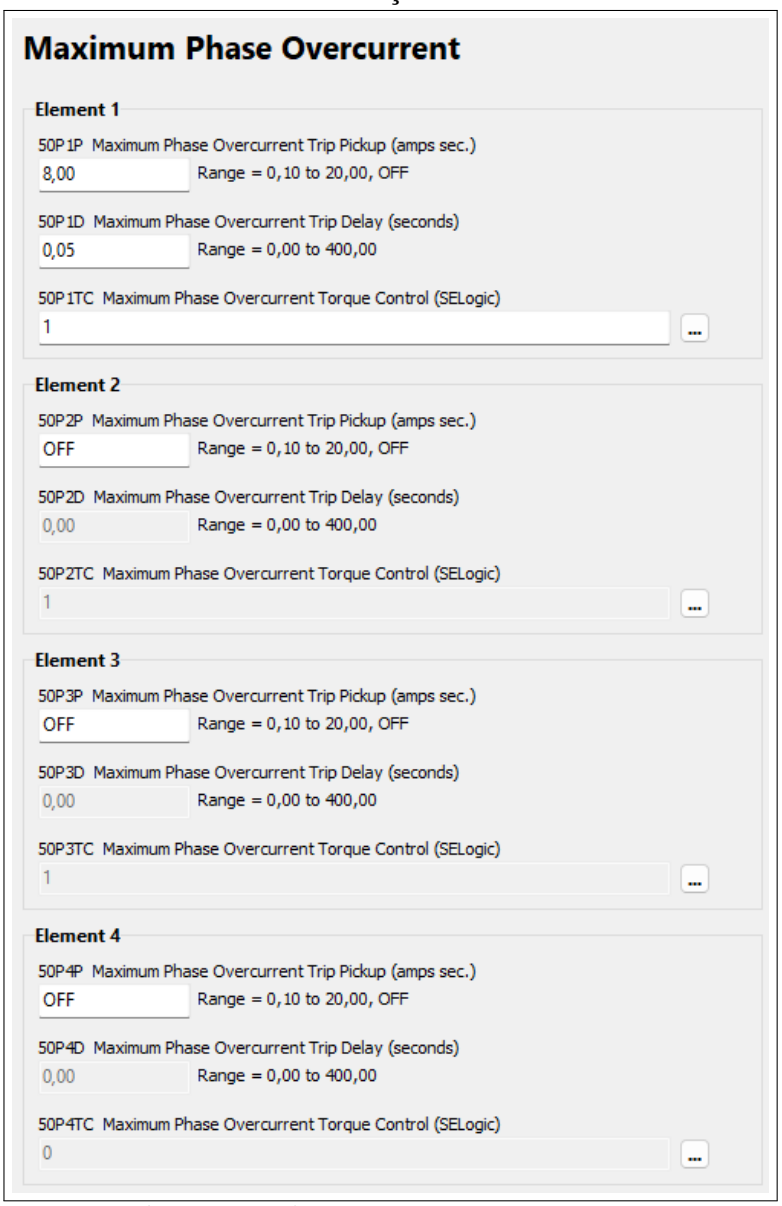
3.4.2 Simulação de falhas e atuação do IED

Nesta fase, considerada uma das mais críticas do projeto, o sistema supervisório é submetido a cenários simulados de falhas, de modo a provocar a atuação (trip) do relé de proteção. O objetivo principal é analisar a coerência entre o comportamento do IED e as rotinas implementadas no script e na interface gráfica, garantindo que ambos representem adequadamente o estado real do equipamento.

A simulação envolve a aplicação das funções 50/51 e 50/51N, que são algumas das funções mais importantes em qualquer relé de proteção. Para isso, serão injetados valores de corrente por meio da maleta de teste, utilizando o software, a fim de ativar as funções de proteção.

Antes de iniciar a injeção de valores por meio da maleta de testes, realizou-se a análise das configurações das funções de proteção no software acSELerator QuickSet, fornecido pela SEL. Essa etapa foi necessária para identificar os parâmetros de atuação e, consequentemente, definir os valores adequados a serem injetados para acionar a função desejada. Na Figura 44, são apresentados os parâmetros da proteção de sobrecorrente (função 50), configurada para atuar instantaneamente quando a corrente ultrapassa o valor de 8 A.

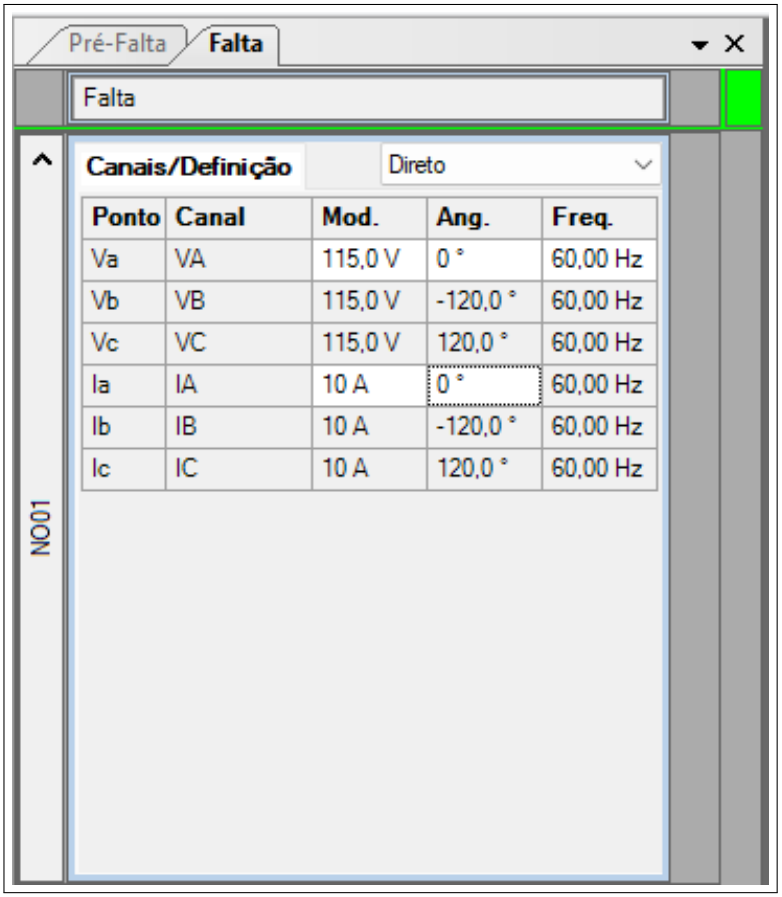
Figura 44 – Parâmetros no software acSELerator quickset da função 50



Fonte: Próprio Autor(2025)

Primeiramente, aplicaremos os valores no software, de forma a provocar a atuação da função 50. O objetivo é comparar a ativação dos LEDs na parte frontal do relé com os LEDs na interface gráfica de estados. Como ilustrado na Figura 45, os valores aplicados no software são mostrados abaixo.

Figura 45 – Valores injetados na maleta para ativação da função 50



Ponto	Canal	Mod.	Ang.	Freq.
Va	VA	115,0 V	0 °	60,00 Hz
Vb	VB	115,0 V	-120,0 °	60,00 Hz
Vc	VC	115,0 V	120,0 °	60,00 Hz
Ia	IA	10 A	0 °	60,00 Hz
Ib	IB	10 A	-120,0 °	60,00 Hz
Ic	IC	10 A	120,0 °	60,00 Hz

Fonte: Próprio Autor(2025)

Ao aplicar os valores, o relé atuará e o registrador do relé, vinculado ao trip específico, será configurado. Como apresentado anteriormente, isso resultará na geração de um evento, que fará com que o script seja executado. Em seguida, a parte gráfica do supervisório será espelhara o frontal do relé, refletindo o estado real através da ativação dos LEDs, como demonstrado nas Figuras 46 e 47.

Figura 46 – Relé após a atuação da função 50

Fonte: Próprio Autor(2025)

Figura 47 – Interface Gráfica após a atuação da função 50

Fonte: Próprio Autor(2025)

Para fins de ilustração, a Figura 48 apresenta a bancada utilizada na realização dos testes.

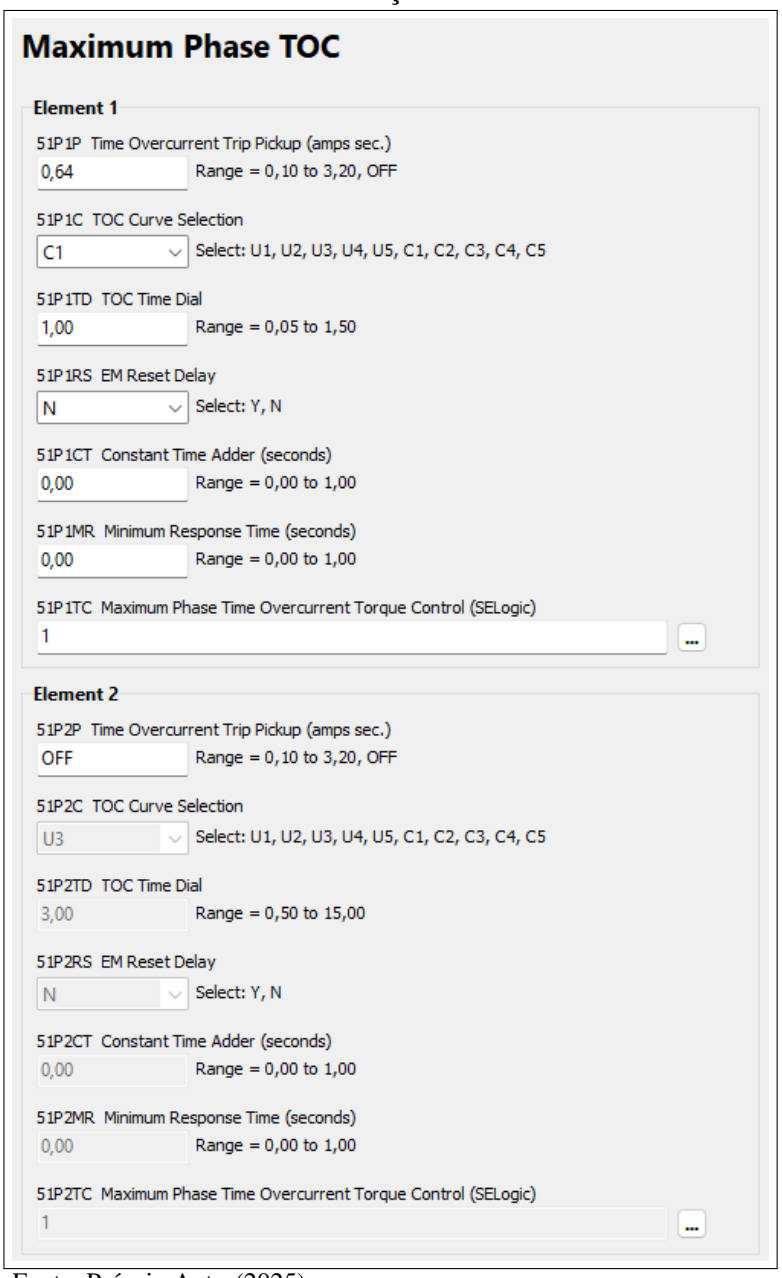
Figura 48 – Bancada de teste função 50

Fonte: Próprio Autor(2025)

Após esse procedimento, torna-se possível acionar o botão de *reset*, restaurando tanto o relé quanto a interface gráfica ao seu estado operacional normal. Essa interação é viabilizada pelo fato de o botão de *reset* estar vinculado ao registrador responsável pelo *reset* dos dados do *status* do relé, desempenhando funcionalidade equivalente ao botão físico localizado na parte frontal do equipamento.

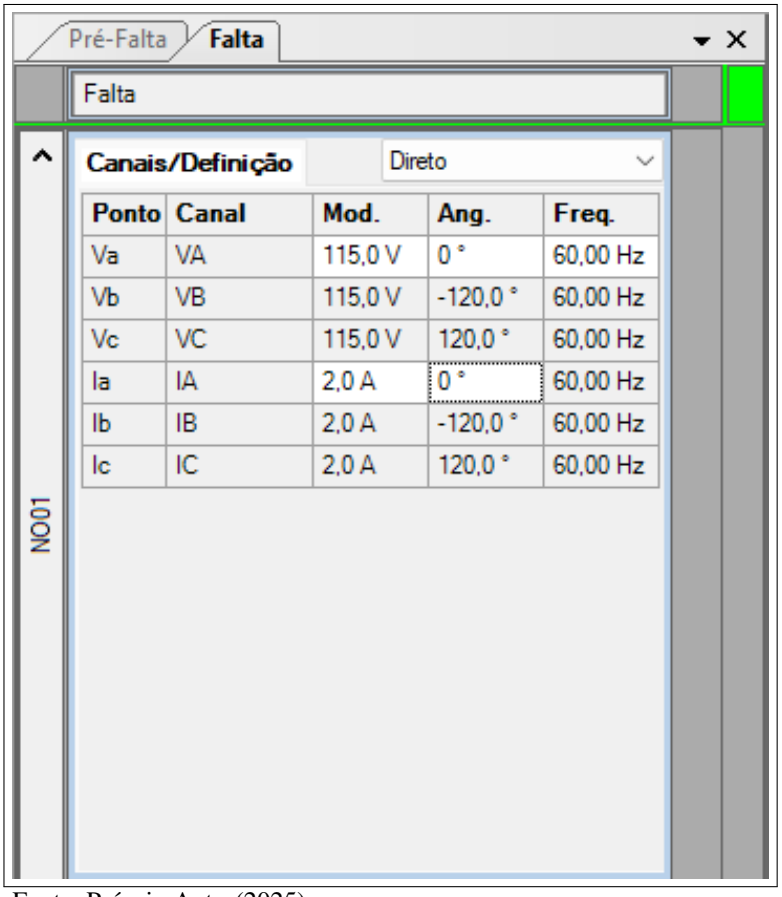
Em seguida, procede-se ao teste da função 51. Para essa etapa, são aplicados valores de corrente inferiores aos utilizados na função 50, porém ainda suficientes para provocar a atuação do elemento de sobrecorrente temporizada, adotando-se o mesmo procedimento empregado anteriormente. Contudo, como o script desenvolvido identifica especificamente qual função foi acionada e qual registrador de status foi alterado, o sistema aciona os LEDs correspondentes à proteção de sobrecorrente temporizada. As Figuras 49 e 50 apresentam, respectivamente, os parâmetros configurados para essa função e os valores injetados pela maleta de testes.

Figura 49 – Parâmetros no software acSELerator quickset da função 51



Fonte: Próprio Autor(2025)

Figura 50 – Valores injetados na maleta para ativação da função 51



Ponto	Canal	Mod.	Ang.	Freq.
Va	VA	115,0 V	0 °	60,00 Hz
Vb	VB	115,0 V	-120,0 °	60,00 Hz
Vc	VC	115,0 V	120,0 °	60,00 Hz
Ia	IA	2,0 A	0 °	60,00 Hz
Ib	IB	2,0 A	-120,0 °	60,00 Hz
Ic	IC	2,0 A	120,0 °	60,00 Hz

Fonte: Próprio Autor(2025)

Dessa forma, por meio das Figuras 51, 52 e 53, é possível observar a atuação dos LEDs correspondentes à função de sobrecorrente temporizada, bem como uma visão geral da bancada utilizada na execução do teste. Esses resultados demonstram, mais uma vez, que a interface gráfica apresenta um comportamento coerente com o painel frontal do relé, refletindo de forma fidedigna o estado físico do equipamento por meio de uma implementação simples, baseada nos registradores definidos no mapa disponibilizado pelo manual técnico.

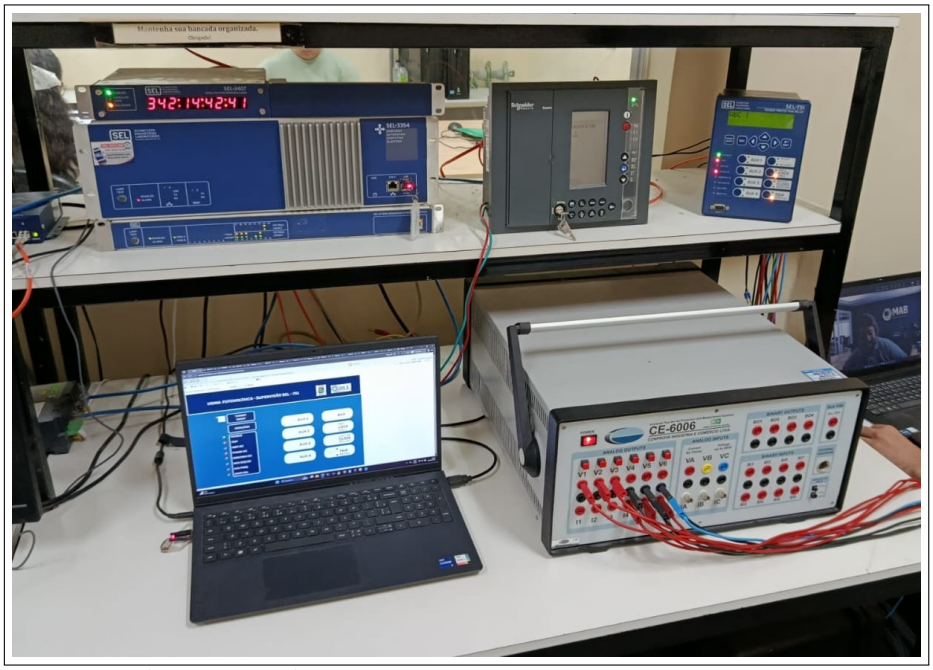
Figura 51 – Relé após a atuação da função 51

Fonte: Próprio Autor(2025)

Figura 52 – Interface Gráfica após a atuação da função 51

Fonte: Próprio Autor(2025)

Figura 53 – Bancada de teste função 51



Fonte: Próprio Autor(2025)

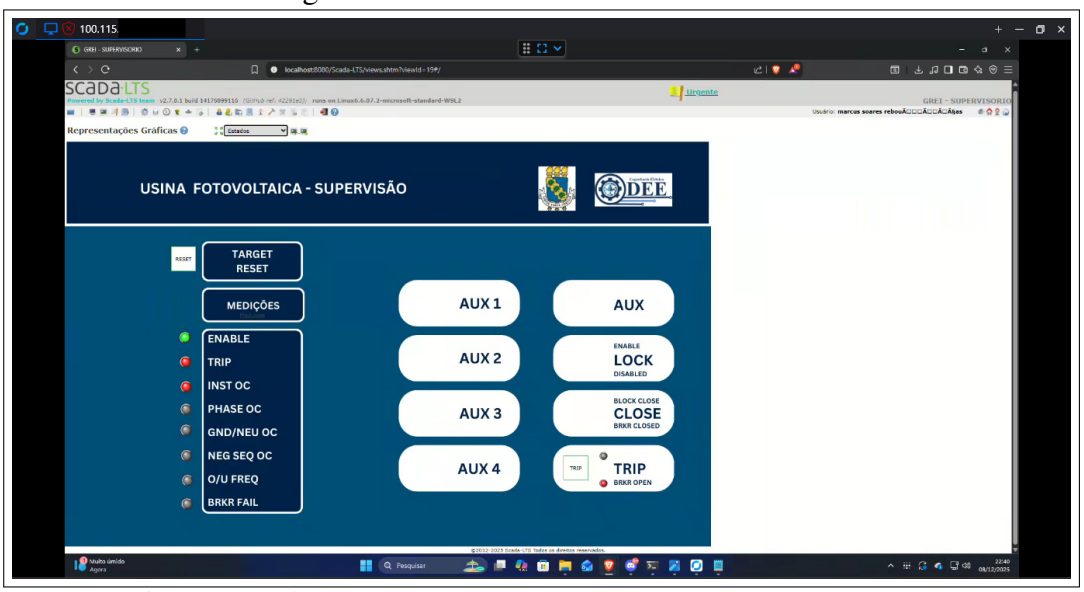
Com isso, demonstramos como o sistema supervisório funciona adequadamente ao refletir as falhas e as condições do relé na interface gráfica. A interação com o sistema é possível por meio do botão de reset, restabelecendo as condições operacionais após a atuação das funções de proteção.

3.4.3 Acesso remoto e supervisão

Por fim, foi avaliada a funcionalidade de acesso remoto ao sistema supervisório, com o objetivo de verificar sua capacidade de operar o relé à distância, incluindo o envio do comando de *reset* do estado de *trip*. Nessa etapa, analisou-se o comportamento da interface e a eficácia da supervisão remota na restauração e no monitoramento das condições operacionais do IED.

Os testes foram conduzidos por meio de um computador localizado fora da rede local do laboratório, conectado a uma rede móvel 5G. O acesso ao sistema supervisório, hospedado em um notebook integrado ao relé de proteção, foi realizado com êxito, possibilitando a visualização das medições, dos estados operacionais do equipamento e a interação remota com suas funções. O relé encontrava-se previamente em condição de *trip* e, por meio do acesso remoto, foi possível executar o comando de *reset*, comprovando a efetividade da intervenção operacional à distância. O primeiro ensaio corresponde à simulação do acesso do administrador via *RustDesk*, conforme ilustrado nas Figuras 54 e 55.

Figura 54 – Acesso remoto antes de reset



Fonte: Próprio Autor(2025)

Figura 55 – Acesso remoto supervisório em operação normal

Fonte: Próprio Autor(2025)

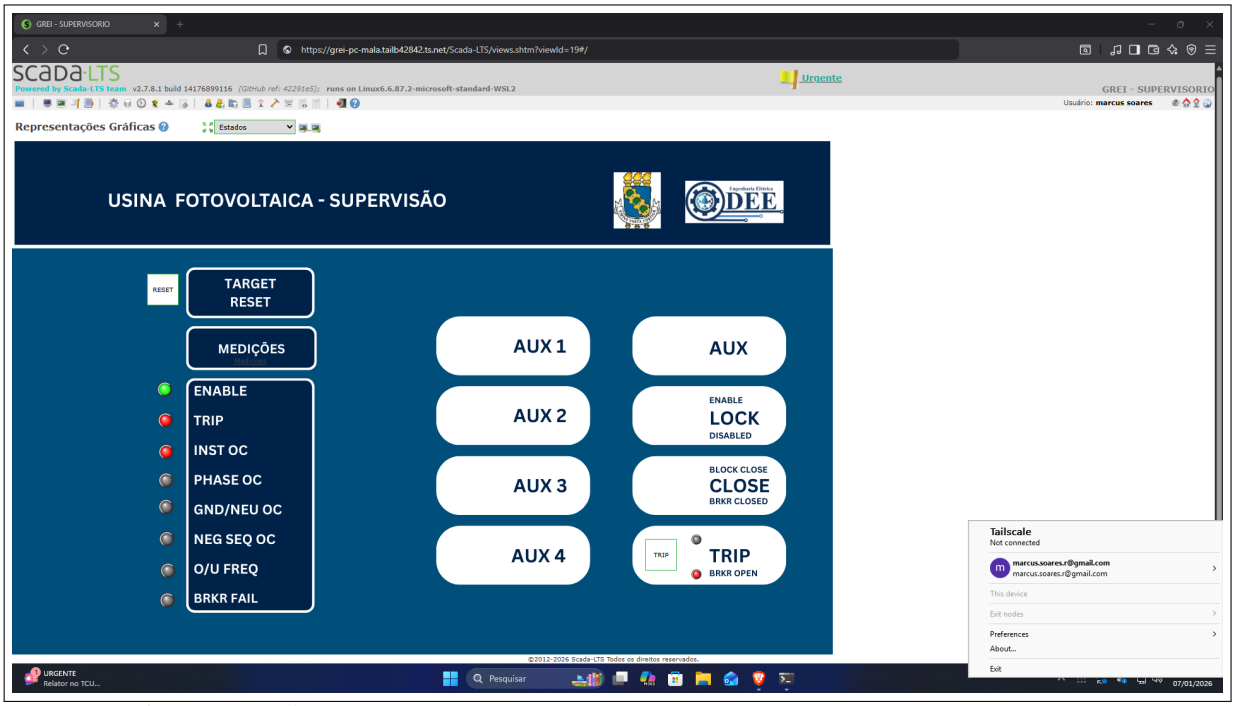
Além disso, o processo de acesso remoto ocorreu de maneira segura. Conforme discutido anteriormente, o RustDesk exige autenticação por senha para o controle do dispositivo, enquanto o Tailscale restringe o roteamento do endereço IP apenas a dispositivos previamente vinculados à conta e à rede privada configurada. Tais mecanismos reforçam a confiabilidade da solução implementada para supervisão remota.

Por fim, tem-se o acesso destinado ao operador. Para este ensaio, optou-se pela utilização do comando *funnel*, ainda que esta não seja a alternativa mais segura. Entretanto, trata-

se da opção que possibilita o acesso a partir de qualquer dispositivo conectado à Internet, o que a torna adequada para fins de validação experimental. Após a criação do servidor local por meio do comando tailscale funnel localhost:8080, o sistema pode ser acessado a partir de qualaquer dispositivo conectado à Internet, mesmo sem estar vinculado à *tailnet* do Tailscale, utilizando o endereço público gerado pela ferramenta. Nesse modo de acesso, o operador visualiza e interage exclusivamente com o sistema supervisório, não possuindo acesso direto ao equipamento onde o SCADA está em execução. Dessa forma, suas ações permanecem restritas às funcionalidades disponibilizadas pelo supervisório, assegurando maior controle e segurança operacional.

Para este teste, o relé foi mantido em condição de *trip*, de forma análoga ao ensaio anterior, sendo novamente executado o comando de *reset* por meio do acesso remoto. Nas Figuras 56 e 57 é possível observar a interface gráfica após o acesso remoto realizado via link disponibilizado, bem como a alteração visual resultante da execução do *reset*. Verifica-se que o endereço apresentado no navegador corresponde ao link gerado pelo comando ilustrado na Figura 41 e que, na parte inferior da tela, evidencia-se que o dispositivo não está conectado ao Tailscale. Dessa forma, demonstra-se que é possível disponibilizar acesso exclusivo ao sistema supervisório utilizando apenas o Tailscale, em conformidade com o conceito de *zero trust*, garantindo que o operador interaja exclusivamente com o SCADA e, consequentemente, aumentando significativamente o nível de segurança do sistema.

Figura 56 – Acesso remoto pelo link



Fonte: Próprio Autor(2025)

Figura 57 – Acesso remoto pelo link em operação normal

Fonte: Próprio Autor(2025)

4 RESULTADOS

4.1 Interface desenvolvida no SCADA LTS

A interface desenvolvida no SCADA demonstrou desempenho adequado durante a etapa de testes, cumprindo sua função de apresentar em tempo real os valores de medição e suas respectivas variações. O ambiente gráfico permitiu ao operador alternar entre as telas de supervisão e de informações do relé, proporcionando uma navegação intuitiva. Além disso, os botões implementados possibilitaram a interação direta com o sistema, permitindo, por exemplo, o envio de comandos de *Trip* e *Reset* ao IED.

Outro aspecto relevante foi a correta representação dos estados dos LEDs, os quais permitiram distinguir visualmente o tipo de atuação, replicando de forma fiel o painel do relé em tempo real. Esse resultado evidencia que a interface proposta não apenas cumpriu seu propósito funcional, como também contribuiu para maior clareza operacional e entendimento do comportamento dinâmico do sistema de proteção.

4.2 Comunicação e desempenho entre SCADA e IED

A comunicação entre o supervisório SCADA-LTS e o relé SEL-751 foi estabelecida com êxito. A partir das informações disponibilizadas no manual do equipamento e no mapa de registradores, tornou-se possível estruturar adequadamente a troca de dados, mediante a seleção precisa dos registradores necessários. Esse resultado foi favorecido tanto pela clareza e organização do mapa de registradores quanto pela facilidade de integração oferecida pelo SCADA-LTS.

Durante os testes, verificou-se uma resposta ágil do sistema supervisório, em conformidade com o tempo de atualização configurado no *data source*. Tal desempenho evidencia a eficiência do processo de comunicação, assegurando o sincronismo entre o SCADA e o IED nas funções de monitoramento e controle.

A análise das *watch lists* reforçou essa constatação, revelando a correta leitura e atualização das informações em tempo real, conforme previsto no manual do equipamento e transmitidas via protocolo Modbus. Dessa forma, confirmou-se a confiabilidade da comunicação adotada e sua aderência aos parâmetros especificados para operação.

4.3 Resultados dos testes de acesso remoto

O acesso remoto demonstrou-se plenamente funcional, possibilitando a interação com o relé mesmo a partir de redes externas ou de longas distâncias. Durante os testes realizados, verificou-se que essa comunicação ocorreu de forma estável, sem atrasos perceptíveis na execução dos comandos, assegurando a operabilidade do sistema em condições reais de uso. Tal funcionalidade representa uma vantagem significativa ao permitir que o operador, ao ser notificado de um evento de *Trip*, possa acessar o SCADA e realizar o comando de *Reset* de forma imediata, sem a necessidade de deslocamento físico até o local da instalação.

Constatou-se, nos ensaios executados, que a interação com o supervisório ocorreu de forma rápida e eficiente, permitindo identificar o tipo de *Trip* ocorrido, visualizar o estado da proteção e executar os comandos pertinentes. Dessa maneira, em cenários nos quais o operador encontra-se distante da subestação ou ponto de instalação do relé, o acesso remoto surge como solução adequada e eficaz para a restauração operacional do sistema, bastando que estejam devidamente configurados os recursos de acesso, como o Tailscale e o RustDesk, no computador responsável pela operação do supervisório.

4.4 Discussão dos resultados e comparação com soluções tradicionais

O sistema supervisório atendeu satisfatoriamente aos objetivos propostos, possibilitando a implementação das medições e dos estados operacionais do relé sem maiores dificuldades, resultando em desempenho adequado durante os testes realizados. Todo o desenvolvimento foi conduzido utilizando apenas ferramentas gratuitas, demonstrando que é viável implementar um sistema SCADA de baixo custo e de fácil integração, capaz de desempenhar funções presentes em soluções comerciais. Ainda que apresente algumas limitações, como a menor disponibilidade de recursos gráficos e a necessidade de conhecimentos básicos em *JavaScript* para a construção de lógicas específicas, o sistema mostrou-se funcional e eficiente para o propósito estabelecido.

Adicionalmente, o acesso remoto configurado por meio das plataformas Tailscale e RustDesk — ambas gratuitas — também apresentou simplicidade de implementação e não exigiu conhecimentos avançados em redes de comunicação. Esses recursos permitiram a configuração ágil e o uso efetivo do supervisório a distância, contribuindo para a flexibilidade e a aplicabilidade da solução proposta.

5 CONCLUSÕES

De forma geral, o objetivo deste trabalho — desenvolver um sistema supervisório específico para uma usina fotovoltaica utilizando soluções de baixo custo — foi plenamente alcançado. A implementação de um SCADA dedicado ao PCC demonstrou-se eficaz, cumprindo satisfatoriamente seu propósito durante os testes realizados, incluindo aqueles efetuados em bancada com o auxílio da maleta de testes. Além disso, a necessidade de acesso remoto foi suprida de maneira eficiente, permitindo que um usuário autorizado seja notificado sobre eventos operacionais e possa acessar o sistema de qualquer local com conectividade à rede, interagir com o relé e visualizar ocorrências por meio das informações disponibilizadas pelo próprio equipamento.

No decorrer da execução do projeto, alguns desafios foram identificados, especialmente no que se refere às limitações do SCADA-LTS. As restrições de recursos na interface gráfica demandam certo domínio de HTML para a construção das telas, situação semelhante ao desenvolvimento de scripts, que requer conhecimentos em JavaScript. Todavia, essas limitações são inerentes a ferramentas gratuitas e de código aberto, que naturalmente não dispõem do mesmo suporte e dos recursos visuais oferecidos por plataformas comerciais. Ainda assim, os resultados obtidos demonstram que o SCADA-LTS atende adequadamente às demandas de monitoramento e controle propostas neste trabalho.

Como perspectivas futuras, destaca-se a continuidade da integração com o relé SEL-751, uma vez que as funcionalidades exploradas nesta pesquisa representam apenas parte do potencial do equipamento. Ademais, sugere-se a avaliação de outros protocolos de comunicação e a implementação de novos relés de diferentes fabricantes, de modo a ampliar as possibilidades de interoperabilidade, robustez e escalabilidade do sistema supervisório desenvolvido.

REFERÊNCIAS

AGENCIA BRASIL. **A geração de energia solar superou a marca de 55 gigawatts (GW) de potência instalada operacional no Brasil**. 2025. Disponível em: <https://agenciabrasil.ebc.com.br/meio-ambiente/noticia/2025-03/com-22-da-matriz-eletrica-energia-solar-e-a-2-maior-fonte-do-pais>. Acesso em: 18 nov. 2025.

AGHENTA, L. O.; IQBAL, M. T. **Low-cost, open-source IoT-based SCADA system design using Thinger.IO and ESP32 Thing**. 2019.

AGÊNCIA NACIONAL DE ENERGIA ELÉTRICA. **Procedimentos de Distribuição de Energia Elétrica no Sistema Elétrico Nacional – PRODIST**: Módulo 5: Proteção e controle. 2023.

CALIXTO, C. M. C.; RAMOS, C. d. S.; SOUZA, G. G.; BRANDI, M. J. P.; FERREIRA, A. A. **Lei 14.300/22 e sua influência na implantação de painéis fotovoltaicos: um estudo de caso**. 2025. Autores vinculados ao Programa de Pós-Graduação em Ambiente Construído (PROAC), UFJF.

DOCKER. **Docker Desktop**. 2025. Disponível em: <https://www.docker.com/products/docker-desktop/>. Acesso em: 18 nov. 2025.

DOCKER. **Docker: Accelerate how you build, share, and run applications**. 2026. Acesso em: 26 jan. 2026. Disponível em: <https://www.docker.com/>.

EMPRESA DE PESQUISA ENERGETICA. **Geração Solar e Mudanças Climáticas**. 2025. Disponível em: <https://www.epe.gov.br/sites-pt/publicacoes-dados-abertos/publicacoes/PublicacoesArquivos/publicacao-852/topico-736/Gera%C3%A7%C3%A3o%20Solar%20e%20Mudan%C3%A7as%20Clim%C3%A1ticas.pdf#search=Gera%C3%A7%C3%A3o%20Solar%20e%20Mudan%C3%A7as%20Clim%C3%A1ticas>. Acesso em: 18 nov. 2025.

ENEL DISTRIBUICAO CEARA. **Especificação Técnica nº 0122**. Fortaleza: [s.n.], 2023.

ENEL DISTRIBUICAO CEARA. **Especificação Técnica nº 0005**. Fortaleza: [s.n.], 2024.

GOOGLE DEVELOPERS. **Protocolo SMTP do Gmail**. 2025. Disponível em: <https://developers.google.com/workspace/gmail/imap/imap-smtp?hl=pt-br>. Acesso em: 18 nov. 2025.

HEITOR THOMAZ. **Proteção Digital de Sistemas Elétricos de Potência: Modelagem de Relés no Simulink**. 2018.

IBERDROLA. **Sistema SCADA**. 2023. Disponível em: <https://www.iberdrola.com/quem-somos/nosso-modelo-inovacao/sistema-scada>. Acesso em: 26 jan. 2026.

INDÚSTRIA AUTOMÁTICA. **Evolução dos Relés de Proteção**. 2015. Disponível em: <https://industriaautomatica.wordpress.com/2015/09/24/evolucao-dos-reles-de-protecao/>. Acesso em: 26 jan. 2026.

KINDERMANN, G. **Proteção de Sistemas Elétricos de Potência**. Florianópolis: Editora da UFSC, 1999.

MAKERHERO. **O que é Modbus? Funcionamento do protocolo**. 2025. Disponível em: <https://www.makerhero.com/blog/o-que-e-modbus-funcionamento-protocolo/>. Acesso em: 18 nov. 2025.

MODBUS ORGANIZATION. **MODBUS Application Protocol Specification**. 2012. Disponível em: <https://www.modbus.org/file/secure/modbusprotocolspecification.pdf>. Acesso em: 16 dez. 2025.

PROMETHEUS GROUP. **What is a SCADA System?** 2026. Disponível em: <https://www.prometheusgroup.com/learning-center/what-is-scada-system/>. Acesso em: 26 jan. 2026.

RUSTDESK. **RustDesk: Acesso remoto seguro e gratuito**. 2025. Disponível em: <https://github.com/rustdesk/rustdesk/releases/tag/1.4.4>. Acesso em: 01 dez. 2025.

SCADA-LTS. **Scada-LTS**. 2025. Disponível em: <http://scada-lts.com/>. Acesso em: 26 jan. 2026.

SCADABR. **Cases**. 2017. Disponível em: <https://www.scadabr.com.br/index.php/cases-2/>. Acesso em: 26 jan. 2026.

SCHWEITZER ENGINEERING LABORATORIES. **SEL-751 Feeder Protection Relay Instruction Manual**. 2019.

SCHWEITZER ENGINEERING LABORATORIES. **Relé SEL-751: Proteção, controle e automação**. 2025. Disponível em: <https://selinc.com/pt/products/751/>. Acesso em: 18 nov. 2025.

TAILSCALE. **Tailscale: VPN sem complicação**. 2025. Disponível em: <https://tailscale.com/>. Acesso em: 25 nov. 2025.

THOMAS, M. S.; MCDONALD, J. D. **Power System SCADA and Smart Grids**. Boca Raton: CRC Press, 2015.

TOTVS. **O que é SCADA e qual a sua importância para a indústria**. 2023. Disponível em: <https://www.totvs.com/blog/gestao-industrial/scada/>. Acesso em: 26 jan. 2026.

APÊNDICE A – CÓDIGOS-FONTES UTILIZADOS PARA OS SCRIPTS DO SUPERVISÓRIO

Código-fonte 2 – Script em JavaScript para acionamento dos LEDs referentes as funcoes 50/51N

```
var has50 = (p52.value == true || p53.value == true || p54.
   value == true || p133.value == true);
var has51 = (p57.value == true || p58.value == true || p59.
   value == true || p36.value == true);

//Zera os LEDs
DP.writeDataPoint('INST_L',  false);
DP.writeDataPoint('TEMP_L', false);
DP.writeDataPoint('TRIP_L',     false);

//Se qualquer 50 atuar -> LED_INST_OC + TRIP
if (has50) {
    DP.writeDataPoint('INST_L', true);
    DP.writeDataPoint('TRIP_L', true);
}

//Se qualquer 51 atuar -> LED_PHASE_OC + TRIP
if (has51) {
    DP.writeDataPoint('TEMP_L', true);
    DP.writeDataPoint('TRIP_L', true);
}
```

Código-fonte 3 – Script em JavaScript para reset trip

```
var has50 = (p52.value == true || p53.value == true || p54.
   value == true || p133.value == true);
var has51 = (p57.value == true || p58.value == true || p59.
   value == true || p36.value == true);
```

```
3
4  //Zera os LEDs
5  DP.writeDataPoint('INST_L',  false);
6  DP.writeDataPoint('TEMP_L', false);
7  DP.writeDataPoint('TRIP_L',     false);
8
9  //Se qualquer 50 atuar -> LED_INST_OC + TRIP
10 if (has50) {
11     DP.writeDataPoint('INST_L', true);
12     DP.writeDataPoint('TRIP_L', true);
13 }
14
15 //Se qualquer 51 atuar -> LED_PHASE_OC + TRIP
16 if (has51) {
17     DP.writeDataPoint('TEMP_L', true);
18     DP.writeDataPoint('TRIP_L', true);
19 }
```

Código-fonte 4 – Script em JavaScript para acionamento dos LEDs referente a funcão 46

```
1  var has46 = (p56.value == true || p61.value == true);
2
3  //Zera os LEDs
4  DP.writeDataPoint('SEQ_L', false);
5  DP.writeDataPoint('TRIP_L', false);
6
7  var has46 = (p56.value == true || p61.value == true);
8
9  DP.writeDataPoint('SEQ_L', false);
10 DP.writeDataPoint('TRIP_L', false);
11
12 //Se qualquer 46 atuar -> LED_INST_OC + TRIP
```

```
13 if (has46) {
14     DP.writeDataPoint('SEQ_L', true);
15     DP.writeDataPoint('TRIP_L', true);
16 }
```

Código-fonte 5 – Script em JavaScript para acionamento dos LEDs referente a funcão 50BF

```
1  var has50BF = (p63.value == true);
2
3  //Zera sempre os LEDs
4
5  DP.writeDataPoint('BRK_F_L', false);
6  DP.writeDataPoint('TRIP_L', false);
7
8  //Se qualquer 50BF atuar -> LED_INST_OC + TRIP
9  if (has50BF) {
10     DP.writeDataPoint('BRK_F_L  ', true);
11     DP.writeDataPoint('TRIP_L', true);
12 }
```