WHITEPAPER

TELEPROTEÇÃO EM SUBESTAÇÕES E LINHAS DE TRANSMISSÃO: ESQUEMAS, CANAIS E COMISSIONAMENTO

Entenda como funciona a teleproteção em subestações e linhas de transmissão: POTT, PUTT, transferência de disparo, canais, redundância, latência e testes ponta a ponta.

A3A® Engenharia de Sistemas

SUMÁRIO

A **teleproteção** integra sistemas de proteção elétrica e telecomunicações para permitir que informações críticas sejam trocadas entre terminais de linhas, subestações e equipamentos de proteção. Seu objetivo não é transportar dados de forma genérica, mas sustentar funções que precisam atuar com segurança, seletividade e desempenho temporal compatível com a filosofia de proteção adotada.

Em uma linha de transmissão ou em uma interligação entre subestações, a proteção local nem sempre dispõe de todas as informações necessárias para eliminar uma falta com rapidez e seletividade. O canal de teleproteção permite transmitir permissivos, bloqueios, comandos de disparo, estados ou grandezas entre os terminais. Por isso, o desempenho do conjunto depende tanto dos relés e lógicas de proteção quanto da arquitetura de comunicação.

Essa interface exige coordenação entre engenharia de proteção, telecomunicações, automação, serviços auxiliares, operação e manutenção. Um canal com alta disponibilidade aparente pode ser inadequado se introduzir assimetria, variação de atraso, perda de integridade ou falhas de modo comum entre os sistemas principal e alternado.

1. O QUE É TELEPROTEÇÃO

Teleproteção é a aplicação de meios de telecomunicações para suportar funções de proteção de sistemas elétricos. A comunicação pode transportar comandos binários, sinais permissivos, bloqueios ou dados necessários a funções diferenciais e esquemas baseados em informações provenientes dos dois terminais.

Ela se diferencia de SCADA e supervisão porque atua em uma camada diretamente associada à eliminação de faltas. Dados de supervisão podem admitir segundos de atualização em determinadas aplicações; já uma função de proteção pode depender de tempos de transferência muito menores e de comportamento previsível durante condições anormais.

Também não deve ser confundida com teleassistência. A teleassistência apoia operação remota, diagnóstico, visualização e resposta a eventos. A teleproteção, por sua vez, participa da lógica de proteção e pode resultar diretamente em disparos, permissões ou bloqueios.

2. POR QUE A PROTEÇÃO DE LINHA DEPENDE DE TELECOMUNICAÇÕES

Proteções de linha precisam distinguir faltas internas, faltas externas, condições de carga, oscilações de potência e situações de fraca alimentação. Em muitos esquemas, a informação disponível em apenas um terminal não é suficiente para garantir simultaneamente velocidade e seletividade em toda a extensão protegida.

A comunicação entre terminais permite que uma proteção confirme a direção da falta, receba um permissivo, compare grandezas ou envie uma ordem direta de abertura. O canal torna-se parte funcional da proteção, ainda que esteja fisicamente implementado em equipamentos de telecomunicações.

Isso significa que a indisponibilidade do canal, a inversão de sinais, o atraso excessivo ou uma falha comum podem alterar o comportamento do sistema de proteção. Por esse motivo, projeto, testes e manutenção precisam tratar relés, interfaces, equipamentos de teleproteção, rede, fibras, sincronismo e alimentação como um conjunto.

3. PROTEÇÃO PRINCIPAL E PROTEÇÃO ALTERNADA

Em instalações de alta criticidade, os sistemas principal e alternado são concebidos para reduzir a probabilidade de falha simultânea. A independência não se limita ao uso de dois relés: deve ser analisada em hardware, software, circuitos de corrente contínua, interfaces, equipamentos de telecomunicações, rotas, fibras, fontes de sincronismo e caminhos lógicos.

Duas portas de um mesmo equipamento não representam necessariamente dois sistemas independentes. Da mesma forma, duas VLANs no mesmo switch, duas fibras no mesmo cabo ou dois canais que atravessam o mesmo enlace podem continuar sujeitos ao mesmo modo de falha.

O projeto deve identificar os pontos únicos de falha e estabelecer onde a duplicação precisa ser física, lógica, energética ou funcional. Essa análise deve incluir gabinetes, fontes, distribuidores ópticos, switches, multiplexadores, roteadores, enlaces WAN, interfaces com os relés e supervisão.

4. PRINCIPAIS ESQUEMAS DE TELEPROTEÇÃO

A escolha do esquema depende da filosofia de proteção, da configuração da linha, dos relés, dos requisitos do agente e do desempenho disponível no canal. Os nomes e detalhes podem variar entre fabricantes e documentos técnicos, mas os princípios gerais permanecem.

4.1. ESQUEMAS PERMISSIVOS

Nos esquemas permissivos, um terminal transmite uma autorização para que o terminal remoto efetue o disparo quando sua própria função local também reconhece a condição prevista. A mensagem remota não atua isoladamente; ela complementa uma decisão local.

Esse princípio reduz o risco de uma atuação indevida causada apenas por um comando recebido, mas exige coordenação das zonas, direcionalidade, temporizações e lógicas especiais para condições como terminal fraco.

4.2. POTT

O **Permissive Overreach Transfer Trip** utiliza, de forma simplificada, elementos de sobrealcance nos terminais para transmissão e recepção do permissivo. Quando cada terminal identifica a falta na direção da linha e recebe a autorização remota, o esquema permite atuação rápida.

Como os elementos de sobrealcance podem enxergar além da linha protegida, a segurança depende da lógica direcional, do canal e do tratamento de condições especiais. Podem ser necessários recursos como transient blocking, echo e weak infeed, conforme a aplicação.

4.3. PUTT

O **Permissive Underreach Transfer Trip** utiliza um elemento de subalcance para iniciar o envio do permissivo. O terminal remoto combina a mensagem recebida com sua própria detecção direcional ou de sobrealcance.

A lógica pode oferecer boa segurança porque o envio parte de uma zona que não ultrapassa o terminal remoto. Entretanto, a cobertura instantânea e o comportamento para faltas próximas às extremidades precisam ser analisados dentro da filosofia completa.

4.4. ESQUEMAS DE BLOQUEIO

Em esquemas de bloqueio, a lógica local pode estar preparada para atuar rapidamente, mas o terminal remoto transmite um sinal quando identifica uma condição que deve impedir o disparo. O tempo de transmissão e a confiabilidade do sinal de bloqueio são críticos, porque a ausência indevida da mensagem pode permitir atuação incorreta.

4.5. TRANSFERÊNCIA DIRETA DE DISPARO

Na transferência direta de disparo, também chamada em determinados contextos de TDD ou DTT, a mensagem recebida pode comandar a abertura remota de forma direta ou com verificações específicas. É utilizada quando uma atuação local precisa provocar a abertura no outro terminal, inclusive em situações nas quais a proteção remota não detectaria a condição por suas próprias grandezas.

Por possuir impacto direto sobre o disjuntor remoto, esse tipo de comando exige alta segurança contra sinais espúrios, validação das interfaces, supervisão, redundância adequada e testes completos.

5. ECHO, WEAK INFEED E TRANSIENT BLOCKING

O **echo** permite que um terminal devolva o permissivo recebido quando determinadas condições são atendidas. O recurso pode ser necessário quando um terminal não possui contribuição suficiente para sensibilizar normalmente seus elementos de proteção.

A lógica de **weak infeed** trata justamente condições de fraca alimentação, nas quais a corrente local pode ser insuficiente para uma detecção convencional, apesar de existir uma falta interna. Sua aplicação precisa considerar tensão, estado dos disjuntores, lógica permissiva e segurança operacional.

O **transient blocking** evita atuações indevidas durante transitórios associados à eliminação sequencial de faltas, especialmente em circuitos paralelos. Não é um recurso genérico a ser habilitado sem estudo; deve ser configurado de acordo com a filosofia, os relés e os cenários analisados.

6. PROTEÇÃO DIFERENCIAL DE LINHA E COMUNICAÇÃO

A proteção diferencial de linha compara grandezas dos terminais para determinar se a corrente diferencial é compatível com uma falta interna. Diferentemente dos esquemas que transmitem comandos binários, a função 87L pode depender da troca contínua de dados entre relés.

Nesse caso, atraso, assimetria, perda de quadros, interrupções e sincronização podem afetar a disponibilidade ou o desempenho da função. O canal precisa ser compatível com o protocolo do fabricante e com os requisitos de tempo, integridade e simetria definidos para a aplicação.

A existência de uma função diferencial não elimina automaticamente a necessidade de outras funções de proteção. A filosofia pode combinar 87L, distância, sobrecorrente direcional, transferência de disparo e esquemas de retaguarda.

7. REQUISITOS DOS CANAIS DE TELEPROTEÇÃO

O canal deve ser especificado a partir da função que transportará. Não basta registrar que haverá “fibra óptica” ou “rede Ethernet”. O projeto precisa definir o tipo de informação, a quantidade de comandos, a largura de banda, o tempo máximo de transferência, a simetria, a variação do atraso, a taxa de erro, a supervisão e a resposta durante falhas.

RequisitoQuestão de engenhariaTempo de transferênciaQuanto tempo a mensagem pode levar entre os pontos de interface?SimetriaOs dois sentidos apresentam comportamento equivalente?Variação de atrasoO canal permanece previsível durante mudanças de rota ou carga?IntegridadeComo erros, duplicações, perdas e mensagens inválidas são detectados?DisponibilidadeQual indisponibilidade é admissível para a função protegida?IndependênciaPrincipal e alternada compartilham algum ponto de falha?SupervisãoFalhas e degradações são sinalizadas local e remotamente?ManutençãoÉ possível testar o enlace sem provocar comandos reais?CibersegurançaComo acessos, configurações e mensagens são protegidos?

Para instalações enquadradas no Submódulo 2.11 dos Procedimentos de Rede, o documento estabelece requisitos específicos para canais, independência, redes locais e externas, monitoramento e desempenho. Em redes de distribuição ou instalações fora desse escopo, os critérios devem ser definidos pelos padrões do agente, requisitos do empreendimento e estudos de engenharia aplicáveis.

8. CANAIS FÍSICOS DEDICADOS E CANAIS LÓGICOS

Um canal físico dedicado utiliza recursos de comunicação reservados para a função, reduzindo a dependência de tráfego compartilhado. A implementação pode empregar fibras, equipamentos de teleproteção, multiplexação ou interfaces específicas.

Um canal lógico pode compartilhar a infraestrutura de transporte com outras aplicações, desde que receba recursos compatíveis com a criticidade: banda reservada, qualidade de serviço, caminhos independentes, supervisão e comportamento determinístico suficiente para a função.

A palavra “dedicado” precisa ser tecnicamente definida. Um circuito lógico pode possuir identificação exclusiva, mas atravessar os mesmos equipamentos, fontes e fibras de outro circuito. Nessa situação, a separação administrativa não representa independência física.

9. FIBRA ÓPTICA, OPGW, OPLAT E REDES DIGITAIS

A fibra óptica é amplamente utilizada devido à imunidade eletromagnética, capacidade, alcance e possibilidade de construção de rotas redundantes. Pode estar instalada em OPGW, ADSS, cabos dielétricos subterrâneos ou enlaces internos da subestação.

O OPGW e o ADSS são meios de infraestrutura óptica; não constituem o sistema de proteção ou o SAS por si próprios. Eles oferecem fibras que podem ser alocadas a teleproteção, automação, voz, dados, vídeo e outros serviços, conforme projeto.

O OPLAT utiliza a própria linha de transmissão como meio para sinais de comunicação. Ainda pode existir em instalações legadas ou aplicações específicas, mas sua modernização exige análise de acoplamento, disponibilidade, interfaces, desempenho e estratégia de migração.

Redes SDH, MPLS-TP, Ethernet industrial e outras tecnologias podem transportar canais de proteção quando configuradas e validadas para os requisitos da função. A escolha não deve ser baseada apenas na capacidade nominal da rede, mas no comportamento ponta a ponta, na independência das rotas e na operação durante contingências.

10. LATÊNCIA, ASSIMETRIA E VARIAÇÃO DO TEMPO DE PROPAGAÇÃO

Latência é o tempo gasto para transportar a informação entre os pontos considerados. Para teleproteção, é necessário definir claramente onde a medição começa e termina: contato do relé, interface binária, porta do equipamento, pacote na rede ou atuação final.

A assimetria ocorre quando os dois sentidos apresentam atrasos diferentes. Isso pode ser relevante para funções diferenciais, medição de tempo e diagnóstico. A variação do atraso, frequentemente chamada de jitter em redes de pacotes, também precisa ser controlada quando interfere na previsibilidade da aplicação.

O tempo medido deve incluir os componentes reais do caminho: conversões de interface, equipamentos de teleproteção, multiplexadores, switches, roteadores, enlaces e processamento. Medir apenas um segmento pode ocultar a parcela dominante do atraso.

No contexto específico das redes locais de proteção abrangidas pelo Submódulo 2.11, há referência a requisitos temporais para mensagens de disparo e a limiares de monitoramento de latência. Esses valores não devem ser generalizados para toda aplicação sem verificar a função, a norma de implementação e o escopo regulatório aplicável.

11. REDUNDÂNCIA E FALHAS DE MODO COMUM

Redundância significa que a perda de um elemento não elimina a função prevista. Independência significa que os sistemas redundantes não dependem do mesmo recurso cuja falha poderia derrubá-los simultaneamente.

Devem ser analisados, entre outros:

A independência deve ser demonstrada em diagramas e matrizes, não apenas declarada na especificação. O projeto precisa indicar os pontos em que os caminhos se aproximam, cruzam ou compartilham infraestrutura.

12. SINCRONISMO DE TEMPO

Algumas funções de proteção, registros e medições dependem de referência temporal. GNSS, relógios locais, PTP, IRIG-B e outros mecanismos podem participar da arquitetura, conforme os equipamentos e requisitos.

O sincronismo precisa ser tratado como serviço crítico: fonte principal, fonte alternativa, distribuição, holdover, supervisão, alarmes e comportamento durante perda do sinal externo. Principal e alternada não devem compartilhar inadvertidamente um único ponto de falha quando a independência temporal for necessária.

Além da proteção, o tempo comum permite correlacionar eventos de relés, equipamentos de telecomunicação, registradores, SCADA e sistemas de monitoramento. Essa correlação é essencial em análise de ocorrências e aceitação de testes ponta a ponta.

13. MONITORAMENTO DAS REDES UTILIZADAS PARA PROTEÇÃO

A supervisão deve detectar não apenas a perda total do canal, mas também anomalias que degradam sua confiabilidade. Conforme a arquitetura, podem ser monitorados integridade das mensagens, ausência de tráfego previsto, perda de sincronismo, mensagens não esperadas, intervalos anormais e latência.

O monitoramento não deve interferir no desempenho da proteção nem depender exclusivamente do mesmo equipamento que está sendo supervisionado. Registros precisam possuir tempo coerente com os dispositivos da rede para permitir análise conjunta.

Alarmes devem ser classificados e encaminhados aos responsáveis. Um canal em condição degradada pode continuar transportando dados, mas já não atender ao nível de confiança necessário para a proteção.

14. CIBERSEGURANÇA EM REDES DE TELEPROTEÇÃO

A criticidade operacional não elimina a necessidade de cibersegurança. Redes locais e externas precisam de mecanismos compatíveis com o risco, sem introduzir atrasos ou dependências que prejudiquem as funções de proteção.

O projeto deve considerar segmentação, controle de acesso administrativo, autenticação, gestão de credenciais, registro de mudanças, atualização de firmware, acesso remoto de fornecedores, proteção das estações de engenharia e controle dos arquivos de configuração.

Não se deve aplicar controles de TI de forma automática. Firewalls, inspeções, criptografia e autenticação precisam ser avaliados quanto à compatibilidade, latência, disponibilidade e comportamento em falha. A engenharia deve definir onde cada controle será implementado e quais caminhos permanecerão permitidos.

15. PROJETO E DOCUMENTAÇÃO DE TELEPROTEÇÃO

Um projeto de teleproteção precisa estabelecer a fronteira de responsabilidade entre proteção e telecomunicações. A matriz de interfaces deve indicar quais sinais são originados pelos relés, como são entregues ao sistema de comunicação, como são transportados e como chegam ao terminal remoto.

Entre os entregáveis podem estar:

O escopo pode abranger projeto básico, projeto executivo, apoio à aquisição, análise de propostas, fiscalização, integração, comissionamento ou Owner's Engineering.

16. MODERNIZAÇÃO DE SISTEMAS EXISTENTES

Sistemas legados podem combinar OPLAT, canais analógicos, multiplexadores SDH, interfaces binárias, fibras antigas e relés de diferentes gerações. A modernização não deve começar pela substituição isolada de um equipamento.

O levantamento precisa identificar cada sinal, interface, canal, rota, alimentação, alarme, ajuste e dependência operacional. Também deve registrar o que ocorrerá durante a transição: operação paralela, janelas de indisponibilidade, bloqueios, retorno à condição anterior e coordenação entre os dois terminais.

Migrações para fibra ou redes de pacotes exigem testes de desempenho e validação da independência. Um canal novo pode apresentar maior capacidade, mas criar uma falha comum se principal e alternado forem consolidados na mesma plataforma sem as separações necessárias.

17. FAT, SAT E TESTES PONTA A PONTA

O **FAT** verifica equipamentos, lógicas, interfaces e configurações antes do envio a campo. Pode incluir simulação de entradas e saídas, transmissão e recepção de sinais, alarmes, supervisão, troca de canais, falhas de alimentação e integração entre relés e equipamentos de telecomunicações.

O **SAT** verifica o sistema instalado, incluindo cabos, fibras, rotas, alimentação, interfaces reais e comunicação entre os terminais. O teste ponta a ponta avalia a cadeia completa e precisa coordenar equipes nos dois lados.

Um roteiro consistente deve verificar:

1. identificação de equipamentos, firmware e configuração; 2. correspondência entre matriz de sinais e fiação; 3. transmissão e recepção de cada comando; 4. polaridade e lógica das interfaces; 5. tempos ponta a ponta; 6. canal principal e canal alternado; 7. perda, retorno e comutação dos canais; 8. falhas de alimentação e alarmes; 9. bloqueio das saídas durante testes; 10. comportamento de echo, weak infeed e demais lógicas aplicáveis; 11. registros de eventos e sincronismo; 12. recuperação após reinicialização; 13. comunicação com sistemas de supervisão; 14. documentação dos resultados e pendências.

18. CRITÉRIOS DE ACEITE

O aceite deve ser definido antes dos testes. Cada requisito precisa estar associado a método, condição inicial, resultado esperado, tolerância e evidência.

Não é suficiente registrar que o canal “funcionou”. É necessário demonstrar que os sinais corretos foram transmitidos, que os tempos atendem à aplicação, que principal e alternado são independentes, que falhas foram detectadas e que a manutenção pode ser executada sem risco de disparo indevido.

As evidências podem incluir relatórios dos relés, registros dos equipamentos de telecomunicações, capturas, oscilografias, listas de eventos, medições de tempo, diagramas marcados, fotografias, backups de configuração e atas de teste.

19. ERROS COMUNS EM PROJETOS DE TELEPROTEÇÃO

19.1. TRATAR TELEPROTEÇÃO COMO TRÁFEGO COMUM DE DADOS

A capacidade de banda não comprova desempenho temporal, integridade, independência ou comportamento durante contingências.

19.2. DECLARAR REDUNDÂNCIA SEM ANALISAR A ROTA COMPLETA

Dois canais podem convergir no mesmo cabo, equipamento, fonte, sala ou enlace contratado.

19.3. PROJETAR PROTEÇÃO E TELECOMUNICAÇÕES SEPARADAMENTE

A ausência de uma matriz de interfaces favorece divergências de sinais, contatos, lógicas, tempos e responsabilidades.

19.4. MEDIR SOMENTE O ATRASO DA REDE

O tempo relevante pode incluir interfaces, conversores, relés e processamento, não apenas switches e enlaces.

19.5. NÃO TESTAR CONDIÇÕES DE FALHA

O sistema precisa ser verificado durante perda de canal, comutação, ausência de sincronismo, falha de fonte e retorno à operação.

19.6. MODERNIZAR SEM MAPEAR O LEGADO

A substituição de multiplexadores ou relés pode interromper sinais compartilhados, alarmes e dependências que não aparecem nos diagramas disponíveis.

19.7. GENERALIZAR REQUISITOS DO ONS

Os Procedimentos de Rede possuem escopos definidos. Para instalações de distribuição ou outros ativos, devem ser considerados os padrões do agente e requisitos contratuais aplicáveis.

20. COMO CONTRATAR PROJETO, INTEGRAÇÃO E COMISSIONAMENTO

A contratação deve informar terminais envolvidos, filosofia de proteção, equipamentos existentes, meios disponíveis, requisitos do agente, condições de operação e fronteiras entre fornecedores.

Um escopo tecnicamente completo pode incluir levantamento, diagnóstico, projeto, especificação, análise de propostas, apoio à aquisição, coordenação com fabricantes, supervisão de montagem, FAT, SAT, testes ponta a ponta, documentação final e suporte à entrada em operação.

Em contratos com múltiplos fornecedores, a atuação de Owner's Engineering ajuda a controlar interfaces, documentos, pendências, responsabilidades e critérios de aceite. O objetivo é evitar que cada parte demonstre apenas seu equipamento, sem comprovar o desempenho do sistema integrado.

21. CONCLUSÃO

A teleproteção é uma disciplina de interface. O relé, o canal, o meio óptico, a rede, a alimentação, o sincronismo e a lógica precisam responder como um único sistema durante faltas, contingências, manutenção e modernização.

Projetos consistentes partem da função de proteção, transformam seus requisitos em critérios de telecomunicações e encerram o ciclo com testes ponta a ponta e evidências de aceite. Essa abordagem reduz falhas de integração e cria uma base técnica para operação, manutenção e futuras ampliações.

[1] OPERADOR NACIONAL DO SISTEMA ELÉTRICO. Procedimentos de Rede — Submódulo 2.11: Requisitos mínimos para os sistemas de proteção, de registro de perturbações e de teleproteção. Revisão 2024.05.

[2] OPERADOR NACIONAL DO SISTEMA ELÉTRICO. Procedimentos de Rede — Submódulo 2.15: Requisitos mínimos para telecomunicações.

[3] OPERADOR NACIONAL DO SISTEMA ELÉTRICO. Procedimentos de Rede — Submódulo 2.12: Requisitos mínimos de supervisão e controle para a operação.

[4] ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. ABNT NBR IEC 61850-10: Redes e sistemas de comunicação para automação de sistemas de potência — Parte 10: Ensaios de conformidade. Rio de Janeiro, 2018.

O que é teleproteção? É o uso de telecomunicações para suportar funções de proteção elétrica entre terminais, permitindo transmitir permissivos, bloqueios, comandos de disparo ou dados necessários à atuação coordenada dos relés.**Qual é a diferença entre teleproteção e SCADA?** SCADA está associado à supervisão, aquisição de dados e comandos operacionais. A teleproteção participa diretamente das funções de proteção e, por isso, exige desempenho temporal, segurança e independência compatíveis com a eliminação de faltas.**Teleproteção pode utilizar uma rede compartilhada?** Pode ser implementada por canais lógicos em infraestrutura compartilhada quando a arquitetura garante os recursos exigidos pela aplicação, como banda, qualidade de serviço, tempo de transferência, supervisão e independência. A adequação precisa ser comprovada no projeto e nos testes.**Duas VLANs representam dois canais independentes?** Não necessariamente. Se atravessarem os mesmos equipamentos, fibras, fontes ou rotas, continuam sujeitas a falhas de modo comum. A independência deve ser analisada em toda a cadeia física, lógica e energética.**O que é um teste ponta a ponta de teleproteção?** É o ensaio coordenado entre os terminais que verifica a cadeia completa: relés, interfaces, equipamentos de telecomunicações, canais, lógicas, tempos, alarmes e registros.**Qual é a diferença entre POTT e PUTT?** No POTT, o permissivo é normalmente iniciado por elementos de sobrealcance; no PUTT, por elementos de subalcance. A implementação completa depende da filosofia, dos relés e das lógicas adotadas.**Teleproteção por fibra óptica dispensa redundância?** Não. A fibra reduz interferências e oferece bom desempenho, mas ainda podem existir falhas comuns em cabos, rotas, distribuidores, equipamentos, fontes e plataformas de transporte.**Os requisitos do ONS valem para qualquer subestação?** Não. Cada Submódulo possui escopo próprio. Para instalações fora desse enquadramento, devem ser considerados os padrões do agente, requisitos contratuais, normas aplicáveis e estudos de engenharia.**O que deve constar em um projeto de teleproteção?** Entre os principais entregáveis estão filosofia funcional, matrizes de sinais e canais, diagramas, rotas, interfaces, requisitos de desempenho, alimentação, supervisão, planos de FAT e SAT, testes ponta a ponta e documentação como construída.**A mesma empresa pode desenvolver projeto e comissionamento?** Sim, desde

que o escopo, as responsabilidades e os critérios de independência e aceite sejam claramente definidos. Também é possível contratar Owner’s Engineering para fiscalizar fabricantes, integradores e testes.

Sobre a A3A Engenharia de Sistemas

Com 30 anos de história, a A3A Engenharia de Sistemas se consolidou como referência em serviços de Engenharia, oferecendo soluções integradas de Telecomunicações, Segurança Eletrônica, Segurança Digital e Instalações Elétricas.

A empresa atua em todas as etapas do ciclo de Engenharia, desde a elaboração de projetos e consultoria técnica até a implantação, manutenção e retrofit de sistemas, sempre em conformidade com as normas técnicas e melhores práticas do setor.

A3A® Engenharia de Sistemas