WHITEPAPER

IED EM SUBESTAÇÕES: O QUE É, FUNÇÕES, COMUNICAÇÃO E INTEGRAÇÃO COM IEC 61850

Entenda o que é IED, funções de proteção, medição e controle, logical nodes, SCL, GOOSE, Sampled Values, segurança e testes em subestações.

A3A® Engenharia de Sistemas

SUMÁRIO

IED é um dispositivo eletrônico inteligente utilizado em sistemas elétricos para executar funções de proteção, controle, medição, supervisão, registro e comunicação. Em subestações, relés de proteção, controladores de bay, medidores e unidades de aquisição podem ser classificados como IEDs quando possuem processamento, configuração e interfaces digitais.

Um IED recebe grandezas e estados do processo, aplica algoritmos e lógica e produz saídas, eventos, registros e mensagens. Dependendo da função, ele pode comandar disjuntores, detectar faltas, registrar oscilografias, publicar GOOSE, disponibilizar dados por MMS ou comunicar com uma RTU e o SCADA.

A presença de Ethernet ou IEC 61850 não define sozinha um IED adequado. O projeto precisa considerar funções, desempenho, entradas e saídas, sincronismo, segurança, arquivos de engenharia, interoperabilidade, testes e ciclo de vida.

1. O QUE É UM IED

IED significa *Intelligent Electronic Device*. O termo descreve dispositivos com microprocessador e capacidade de executar funções especializadas no sistema elétrico.

Relés numéricos substituíram vários dispositivos eletromecânicos e eletrônicos separados. Um único equipamento pode reunir proteção, medição, lógica, oscilografia, supervisão de circuito e comunicação.

A concentração oferece recursos, mas aumenta a importância da configuração. Uma alteração de firmware, lógica ou matriz de sinais pode afetar várias funções simultaneamente.

2. TIPOS DE IED EM SUBESTAÇÕES

Relés de proteção detectam condições anormais e comandam a abertura de disjuntores. Controladores de bay executam intertravamento, supervisão e controle. Medidores registram grandezas e energia.

Unidades de aquisição, merging units, registradores de perturbação e controladores de serviços auxiliares também podem ser IEDs.

O projeto deve classificar cada equipamento por função primária e secundária. Chamar todos de IED não elimina a necessidade de requisitos específicos.

3. FUNÇÕES DE PROTEÇÃO

IEDs de proteção implementam funções identificadas por números ANSI, como sobrecorrente, distância, diferencial, subtensão, sobretensão e frequência.

Os ajustes dependem de estudos de proteção e coordenação. O artigo não substitui esses estudos. A configuração deve ser produzida e revisada por profissionais responsáveis pela proteção do sistema.

A atuação precisa ser independente de sistemas supervisórios. O SCADA monitora e permite operações autorizadas, mas a proteção deve funcionar mesmo sem comunicação externa.

4. FUNÇÕES DE CONTROLE

IEDs podem comandar disjuntores, seccionadoras e outros equipamentos. A lógica verifica permissivos, bloqueios e intertravamentos.

O controle pode ocorrer localmente, por estação de operação, RTU ou SCADA. Modos local/remoto e autoridade de comando precisam ser claros.

O retorno físico do equipamento confirma a operação. O aceite da mensagem ou acionamento de uma saída não demonstra que o dispositivo primário mudou de estado.

5. MEDIÇÃO E SUPERVISÃO

IEDs medem corrente, tensão, potência, frequência, fator de potência e outras grandezas. A precisão deve ser compatível com proteção, supervisão ou faturamento.

Também monitoram circuitos de trip, bobinas, fontes, entradas, temperatura e estado interno. Alarmes de autodiagnóstico precisam chegar ao operador.

Qualidade e validade devem acompanhar as medições quando publicadas por protocolos digitais.

6. ENTRADAS E SAÍDAS

Entradas digitais recebem posição, alarmes e contatos. Saídas digitais comandam relés e circuitos. Entradas analógicas recebem sinais de TCs, TPs, sensores ou transdutores.

A especificação deve definir quantidade, isolamento, tensão, corrente e tempo de atuação. Módulos adicionais podem aumentar capacidade, mas também complexidade e pontos de

falha.

A matriz de I/O precisa mapear borne, função interna, lógica e destino de comunicação.

7. LÓGICA PROGRAMÁVEL

IEDs modernos permitem lógica configurável. Ela pode implementar intertravamentos, bloqueios, transferência, supervisão e automação de bay.

A lógica precisa ser documentada em diagramas ou descrição funcional. Blocos genéricos sem comentários tornam revisão e manutenção difíceis.

Mudanças devem passar por controle de versão, simulação e testes. A proteção e a segurança operacional não podem depender de lógica não rastreável.

8. GRUPOS DE AJUSTES

Muitos relés permitem vários grupos de ajustes para diferentes condições operacionais.

A troca pode ocorrer localmente, por entrada, lógica ou comando. O sistema deve indicar qual grupo está ativo e registrar mudanças.

Comandos remotos para alteração de grupo exigem controle de acesso e validação. Um grupo incorreto pode alterar sensibilidade e coordenação.

9. REGISTROS DE EVENTOS

O IED registra mudanças de estado, atuações, comandos, alarmes e alterações de configuração. Esses registros apoiam análise de ocorrências.

Timestamps precisam ser sincronizados. A resolução deve atender a sequência esperada. O servidor NTP em redes e subestações atende muitas funções, mas proteção pode exigir PTP ou IRIG-B.

Os registros devem ser preservados após perda de alimentação conforme requisitos e exportados em formato utilizável.

10. OSCILOGRAFIA E COMTRADE

Relés podem registrar formas de onda e grandezas durante faltas ou gatilhos. Arquivos COMTRADE facilitam análise em ferramentas independentes.

O projeto deve definir taxa de amostragem, duração pré e pós-falta, canais e gatilhos. Memória insuficiente pode sobrescrever registros antes da coleta.

Horário e configuração associados ao registro precisam ser preservados. Uma oscilografia sem ajustes e eventos relacionados perde contexto.

11. AUTODIAGNÓSTICO

IEDs monitoram memória, CPU, fontes, entradas, comunicação e circuitos internos. Falhas devem acionar contato de watchdog e alarme digital.

O contato físico pode oferecer uma indicação independente da rede. A arquitetura deve decidir como ele chega à RTU ou SCADA.

Autodiagnóstico não substitui monitoramento externo. Um equipamento travado pode deixar de publicar seu próprio alarme.

12. COMUNICAÇÃO SERIAL E ETHERNET

IEDs legados podem utilizar Modbus, DNP3, IEC 101 ou protocolos proprietários por RS-485 ou fibra.

Equipamentos modernos usam Ethernet e IEC 61850, DNP3 TCP, IEC 104, SNMP ou interfaces de engenharia.

Cada interface aumenta a superfície e precisa de função definida. Protocolos e portas não utilizados devem ser desabilitados.

O IED precisa ser especificado pela função completa.

Proteção, controle, medição, I/O, registros, comunicação, sincronismo, lógica e arquivos de engenharia devem compor um único requisito verificável.

Conhecer a solução de Sistemas Digitais de Supervisão e Controle

13. IEC 61850 E MODELOS DE DADOS

A IEC 61850 define modelos orientados a objetos para automação de sistemas elétricos. Funções são representadas por Logical Nodes, Data Objects e atributos.

Um IED pode expor nós de proteção, medição, controle e supervisão. A estrutura facilita interoperabilidade quando os modelos são aplicados corretamente.

O artigo sobre subestação digital e IEC 61850 aprofunda Station Bus, Process Bus, GOOSE e Sampled Values.

14. LOGICAL NODES

Logical Nodes agrupam dados e serviços de uma função. Exemplos incluem proteção, disjuntor, medição e controle.

O nome de instância identifica cada aplicação dentro do IED. Prefixos e sufixos devem seguir convenção de projeto.

Modelagem inconsistente dificulta engenharia e integração. A SCD deve refletir a função real, não apenas os defaults do fabricante.

15. MMS E RELATÓRIOS

MMS é utilizado para comunicação cliente-servidor na IEC 61850. Sistemas supervisórios navegam no modelo, leem dados e recebem reports.

Report Control Blocks definem conjuntos de dados, gatilhos, buffers e integridade. Configuração inadequada pode gerar perda ou excesso de mensagens.

Buffered Reports armazenam eventos durante interrupções até o limite. Unbuffered Reports não preservam da mesma forma. O comportamento precisa ser ensaiado.

16. GOOSE

GOOSE distribui eventos rápidos em camada 2, frequentemente para intertravamentos, bloqueios e sinais entre IEDs.

A mensagem é retransmitida com intervalos variáveis para aumentar confiabilidade. Recebedores monitoram estado, sequência e tempo permitido.

VLAN, prioridade, multicast e arquitetura de rede precisam ser definidos. O PRP e HSR pode fornecer redundância sem tempo de recuperação em aplicações compatíveis.

A lógica associada ao GOOSE deve prever perda, qualidade e estado inicial. Testes precisam verificar publicação, assinatura, latência e falha de caminho.

17. SAMPLED VALUES

Sampled Values transportam amostras de corrente e tensão por Ethernet, normalmente entre merging units e funções de proteção ou medição.

A aplicação exige sincronismo, capacidade e desempenho de rede rigorosos. Não deve ser tratada como tráfego Ethernet comum.

Switches, VLANs, prioridade, PTP, redundância e monitoramento fazem parte do sistema de proteção.

18. ARQUIVOS SCL

A IEC 61850 utiliza arquivos SCL para descrever capacidades, configuração e sistema.

ICD descreve capacidades do IED. CID representa configuração carregada no equipamento. SCD representa a configuração integrada da subestação. SSD descreve a especificação do sistema, conforme processo adotado.

Os arquivos precisam de governança. Versões divergentes entre ferramenta, IED e SCD geram problemas difíceis de identificar.

19. ICD, IID, CID E SCD

O fluxo de engenharia deve definir quem fornece e aprova cada arquivo. Dados de fabricante entram na ferramenta de sistema; conexões e datasets são configurados; arquivos finais são gerados para os IEDs.

Alterar diretamente o IED sem atualizar a SCD quebra a fonte de verdade. A próxima engenharia pode sobrescrever a mudança ou perder rastreabilidade.

Backups precisam incluir arquivos e versões das ferramentas.

20. DATASETS E CONTROL BLOCKS

DataSets agrupam dados utilizados por reports, GOOSE ou Sampled Values. Control Blocks definem comportamento de publicação ou relatório.

Itens desnecessários aumentam tráfego. Itens ausentes impedem supervisão. O projeto deve mapear cada sinal à função consumidora.

Alterações em DataSets e control blocks exigem teste de todos os subscribers e clientes afetados.

21. SINCRONISMO PTP, NTP E IRIG-B

NTP pode atender logs e supervisão. PTP é utilizado quando a aplicação exige maior precisão. IRIG-B continua presente em muitas subestações.

A fonte e a hierarquia precisam ser definidas. IEDs devem indicar estado de sincronismo e qualidade do tempo.

A perda da fonte deve gerar alarme e comportamento conhecido. Proteções dependentes de amostras sincronizadas precisam considerar holdover e falha.

22. INTEGRAÇÃO COM RTU

A RTU em subestações pode adquirir reports IEC 61850, ler protocolos legados ou receber contatos.

O mapeamento deve preservar qualidade e timestamp. Duplicar o mesmo sinal por duas rotas exige critério de seleção.

A RTU pode converter para DNP3 ou IEC 104. A conversão precisa documentar origem, objeto e classe ou Type ID.

23. INTEGRAÇÃO COM SCADA

O SCADA pode acessar IEDs diretamente ou por gateway/RTU. A escolha depende de arquitetura, segurança, escala e responsabilidade.

Acesso direto simplifica alguns fluxos, mas aumenta número de conexões e exposição. Concentração facilita controle e padronização, mas cria dependência do gateway.

O projeto deve evitar que aplicações corporativas conectem diretamente aos IEDs.

24. REDUNDÂNCIA DE REDE

IEDs podem possuir duas portas para RSTP, PRP, HSR ou arquiteturas proprietárias.

Duas portas não significam redundância sem perda. O protocolo e a topologia determinam o tempo de recuperação.

Os modos devem ser compatíveis com switches e SCD. Ensaios precisam interromper cada caminho.

25. REDUNDÂNCIA FUNCIONAL

Proteções críticas podem utilizar sistemas principal e alternado independentes. A independência deve considerar IED, alimentação, TCs/TPs, bobinas, comunicação e cabos.

Compartilhar componentes pode criar falha comum. A arquitetura precisa identificar dependências.

Mensagens entre sistemas redundantes devem ser justificadas para não reduzir independência.

26. ALIMENTAÇÃO E AMBIENTE

IEDs são alimentados pelo sistema CC e precisam atender faixa, consumo, imunidade e interrupções.

Temperatura, umidade, vibração, surtos e compatibilidade eletromagnética devem ser compatíveis com o painel e a subestação.

Aterramento, blindagem e separação de cabos influenciam entradas e comunicação.

Configuração e segurança precisam permanecer rastreáveis.

Contas, firmware, certificados, arquivos SCL, serviços, acesso de engenharia e backups devem ser controlados ao longo de todo o ciclo de vida.

Conhecer o serviço de Projeto de Telecomunicações

27. CIBERSEGURANÇA DO IED

IEDs possuem contas, serviços, firmware, portas e interfaces de engenharia. O hardening em ambientes OT deve ser adaptado às limitações embarcadas.

Contas padrão precisam ser alteradas. Serviços não usados devem ser desabilitados. Acesso remoto deve passar por jump server e MFA.

A IEC 62351 define mecanismos de segurança para comunicações de sistemas elétricos. O suporte real depende de firmware e interoperabilidade.

28. CONTROLE DE ACESSO E PERFIS

Usuários de operação, proteção, manutenção e auditoria precisam de permissões distintas.

Alterações de ajustes e lógica devem exigir credenciais individuais e gerar logs. Contas compartilhadas reduzem rastreabilidade.

Senhas e certificados precisam de ciclo de vida. Procedimentos de emergência devem existir sem manter acesso permanente excessivo.

29. FIRMWARE E VULNERABILIDADES

O inventário deve registrar versão de firmware, hardware e bibliotecas. Avisos do fabricante precisam ser avaliados.

Atualizações não devem ser aplicadas diretamente em produção sem análise e teste. Mudanças podem afetar proteção, comunicação e arquivos SCL.

Equipamentos sem suporte exigem plano de substituição, segmentação e monitoramento adicionais.

30. BACKUPS E RECUPERAÇÃO

Backup deve incluir ajustes, lógica, CID, certificados, usuários e registros necessários.

A restauração precisa ser testada em equipamento de reposição ou ambiente controlado. Arquivos proprietários dependem de versão compatível da ferramenta.

O procedimento deve incluir verificação após troca: calibração, entradas, saídas, comunicação e proteção.

31. PROJETO E DOCUMENTAÇÃO

O projeto deve incluir diagramas funcionais, lista de I/O, funções ANSI, ajustes aprovados, lógica, matriz de sinais, SCL, rede, sincronismo e segurança.

Também precisa registrar datasets, reports, GOOSE, Sampled Values, VLANs e subscribers.

Documentação as-built deve corresponder ao IED carregado. Diferenças precisam ser resolvidas antes do aceite.

32. FAT

O FAT valida configuração, lógica e comunicação antes da instalação.

Devem ser testadas funções, entradas, saídas, reports, GOOSE, registros, sincronismo e interfaces. Simuladores podem representar equipamentos e rede.

Resultados precisam ser rastreáveis a requisitos e ajustes. Pendências devem ser classificadas antes do envio.

33. SAT E COMISSIONAMENTO

O SAT verifica o IED conectado ao processo real. Testes devem respeitar procedimentos de segurança e planejamento da instalação.

O roteiro mínimo inclui:

O Comissionamento e Aceite Técnico deve produzir evidências sem substituir responsabilidades específicas dos ensaios de proteção.

O aceite deve comprovar função, comunicação e recuperação.

I/O, lógica, ajustes, reports, GOOSE, registros, sincronismo, redundância, usuários e backup precisam ser verificados com evidências.

Conhecer o serviço de Comissionamento e Aceite Técnico

34. DIAGNÓSTICO DE FALHAS

Ausência de comunicação pode envolver rede, VLAN, certificado, arquivo CID, dataset ou control block. Valores incorretos podem resultar de escala, modelo ou mapeamento.

GOOSE não recebido exige verificar APPID, VLAN, MAC multicast, dataset, estado e supervisão. Reports ausentes podem estar desabilitados ou com buffer cheio.

Atuação inesperada exige análise de ajustes, lógica, entradas e registros. Oscilografia e eventos devem ser correlacionados com o sistema.

35. ERROS COMUNS

Tratar o IED como caixa fechada reduz rastreabilidade. Outro erro é alterar configuração diretamente sem atualizar SCD e documentação.

Também são comuns serviços desnecessários habilitados, contas compartilhadas, backup não testado e redundância presumida apenas por existir duas portas.

Por fim, testar apenas comunicação não comprova função. Proteção, controle, registros, segurança e recuperação precisam de critérios próprios.

36. CONCLUSÃO

IEDs concentram funções essenciais de proteção, controle, medição e comunicação. Em subestações digitais, eles participam de modelos IEC 61850, reports, GOOSE e Sampled Values.

A confiabilidade depende de engenharia integrada: funções, ajustes, lógica, rede, tempo, segurança, arquivos SCL e ensaios. Quando configuração e documentação permanecem sincronizadas, o IED pode ser operado e mantido ao longo de todo o ciclo de vida.

[1] INTERNATIONAL ELECTROTECHNICAL COMMISSION. IEC 61850 series — Communication networks and systems for power utility automation.

[2] INTERNATIONAL ELECTROTECHNICAL COMMISSION. IEC 60255 series — Measuring relays and protection equipment.

[3] IEEE. IEEE C37.111 — Common Format for Transient Data Exchange (COMTRADE) for Power Systems.

[4] INTERNATIONAL ELECTROTECHNICAL COMMISSION. IEC 62351 series — Power systems management and associated information exchange — Data and communications security.

[5] NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. NIST SP 800-82 Rev. 3 — Guide to Operational Technology Security. Gaithersburg, 2023.

O que é um IED? É um dispositivo eletrônico inteligente que executa funções de proteção, controle, medição, registro e comunicação em sistemas elétricos.**Todo relé digital é um IED?** Relés numéricos com processamento, configuração e comunicação são normalmente classificados como IEDs.**O que são Logical Nodes?** São blocos do modelo IEC 61850 que representam funções de proteção, controle, medição e supervisão.**O que é GOOSE?** É um serviço IEC 61850 de mensagens rápidas em camada 2 utilizado para eventos e sinais entre IEDs.**O que são Sampled Values?** São mensagens que transportam amostras digitalizadas de corrente e tensão, geralmente entre merging units e IEDs.**Qual é a diferença entre ICD, CID e SCD?** ICD descreve capacidades do IED, CID representa sua configuração e SCD integra a configuração da subestação.**Como o IED se integra à RTU?**

Por IEC 61850, DNP3, Modbus, protocolos seriais ou contatos, preservando qualidade e timestamp.**IED precisa de sincronismo?** Sim. Eventos, registros e algumas funções de processo exigem referência temporal consistente.**Como proteger um IED?** Com contas individuais, hardening, firmware suportado, segmentação, acesso remoto controlado e logs.**O que testar no comissionamento?** Funções, ajustes, I/O, lógica, registros, comunicação, sincronismo, redundância, segurança e integração.

Soluções relacionadas

Serviços relacionados

Artigos e materiais técnicos relacionados

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