WHITEPAPER

IEC 60870-5-104: O QUE É, COMO FUNCIONA E SEGURANÇA NO TELECONTROLE DE SUBESTAÇÕES

Entenda a IEC 60870-5-104, APDU, ASDU, tipos de informação, causas de transmissão, eventos, comandos, TCP 2404 e segurança em subestações.

A3A® Engenharia de Sistemas

SUMÁRIO

IEC 60870-5-104, também chamada de IEC 104, é um protocolo de telecontrole utilizado para trocar estados, medições, eventos e comandos entre subestações, centros de operação, RTUs, gateways e sistemas SCADA por redes TCP/IP. Ele transporta as informações de aplicação da família IEC 60870-5-101 sobre uma camada de transporte baseada em TCP.

A IEC 104 foi concebida para supervisão e controle de sistemas elétricos distribuídos. O protocolo diferencia mensagens espontâneas, respostas a interrogação, comandos, sincronismo e outras causas de transmissão. Também utiliza números de sequência, confirmações e temporizadores para controlar o fluxo das mensagens.

Em subestações de distribuição, a IEC 104 costuma ser usada entre RTUs ou gateways e o centro de operação. Ela não substitui automaticamente a IEC 61850 dentro da subestação. É comum que IEDs comuniquem por IEC 61850 na rede local, enquanto uma RTU converte e concentra os dados para IEC 104 no enlace de telecontrole.

1. O QUE É IEC 60870-5-104

IEC 60870-5-104 é a especificação da família IEC 60870 que define o acesso à rede para a IEC 60870-5-101 utilizando perfis de transporte padronizados sobre TCP/IP.

A norma preserva o modelo de informações de telecontrole da IEC 101, incluindo tipos de ASDU, causas de transmissão, endereçamento e comandos. A principal diferença está no transporte: a IEC 101 foi concebida para enlaces seriais, enquanto a IEC 104 utiliza redes IP.

A migração para IP amplia flexibilidade e capacidade, mas também introduz roteamento, switches, firewalls, endereçamento, redundância e riscos de cibersegurança. Um projeto IEC 104 precisa tratar o protocolo e a infraestrutura como uma única cadeia operacional.

2. IEC 101 E IEC 104

IEC 101 utiliza enlace serial e mecanismos de camada de enlace definidos para telecontrole. IEC 104 utiliza TCP como transporte confiável e adiciona uma camada de controle de aplicação para sequência, confirmação e supervisão da conexão.

O modelo de dados e as ASDUs são amplamente relacionados, mas nem toda implementação IEC 101 pode ser convertida sem revisão. Endereços, tipos, causas, timestamps e comandos precisam ser mapeados.

Gateways IEC 101/104 podem preservar o conteúdo de aplicação, mas introduzem filas, buffers e comportamento de reconexão. O projeto deve definir como eventos são armazenados durante a perda de um dos lados.

3. ARQUITETURA CLIENTE-SERVIDOR

Na prática, a estação controladora inicia a conexão TCP com a estação controlada. A nomenclatura cliente-servidor descreve o estabelecimento da sessão, mas a troca de informações pode ocorrer em ambos os sentidos.

A estação controlada envia eventos espontâneos e respostas. A estação controladora envia interrogações, comandos e solicitações. A conexão precisa ser ativada para transferência de dados antes da troca normal de ASDUs.

Redundância pode envolver vários centros, vários canais ou múltiplas conexões. O comportamento de cada equipamento diante de conexões simultâneas precisa ser conhecido e ensaiado.

4. PORTA TCP 2404

A IEC 104 utiliza normalmente a porta TCP 2404. Essa convenção não justifica liberar a porta entre redes inteiras.

Firewalls devem restringir IP de origem, IP de destino, direção e caminhos redundantes. Quando possível, monitoramento deve identificar funções e padrões anormais dentro da sessão.

A porta não deve estar exposta à internet nem acessível diretamente pela rede corporativa. A DMZ entre TI e OT é utilizada para serviços intermediários, não para abrir acesso indiscriminado ao telecontrole.

5. APDU, APCI E ASDU

A unidade de dados da IEC 104 é a APDU. Ela combina o cabeçalho de controle, chamado APCI, com a ASDU quando a mensagem transporta informações de aplicação.

O APCI contém o byte de início, comprimento e campos de controle. A ASDU contém tipo, quantidade de objetos, causa de transmissão, endereço comum e objetos de informação.

Compreender essa estrutura é importante para diagnóstico. Uma conexão TCP pode estar estabelecida, mas a troca de ASDUs pode falhar por endereço, causa ou tipo incompatível.

6. FORMATOS I, S E U

Quadros do formato I transportam ASDUs e utilizam números de sequência de envio e recepção. Quadros S confirmam mensagens recebidas sem transportar uma ASDU. Quadros U executam funções de controle da conexão.

Entre as funções U estão STARTDT, STOPDT e TESTFR. STARTDT ativa a transferência de dados. STOPDT interrompe de forma controlada. TESTFR verifica a conexão durante períodos sem tráfego.

O analisador de protocolo deve diferenciar esses formatos. Repetições, sequências fora de ordem ou ausência de confirmação indicam falhas de sessão, temporização ou implementação.

7. NÚMEROS DE SEQUÊNCIA

Os números de sequência permitem controlar mensagens I enviadas e confirmadas. Cada lado mantém contadores de envio e recepção.

Quando existe divergência, a sessão pode ser encerrada ou reinicializada. Capturas de rede ajudam a identificar retransmissões, confirmações atrasadas e resets.

A sequência IEC 104 é adicional ao controle do TCP. Ela fornece supervisão no nível da aplicação e ajuda a garantir que ASDUs sejam processadas na ordem esperada.

8. PARÂMETROS K E W

O parâmetro k define a quantidade máxima de APDUs do formato I não confirmadas que podem estar em trânsito. O parâmetro w define após quantas mensagens recebidas uma confirmação deve ser enviada.

Valores muito altos aumentam dados pendentes diante de falha. Valores muito baixos podem reduzir desempenho em redes com latência.

Os parâmetros precisam ser compatíveis entre as implementações e validados no enlace real. Configurações copiadas de outro projeto podem não atender a largura de banda e latência disponíveis.

9. TEMPORIZADORES T0, T1, T2 E T3

A IEC 104 utiliza temporizadores para estabelecimento, confirmação e supervisão da conexão.

t0 limita o tempo de estabelecimento. t1 supervisiona o envio de APDUs e testes que exigem confirmação. t2 controla o tempo máximo antes de confirmar mensagens recebidas quando w ainda não foi atingido. t3 detecta períodos de inatividade e aciona teste de enlace.

Relações inadequadas entre temporizadores podem provocar desconexões ou atraso de confirmações. Os valores precisam considerar latência, perda, processamento e comportamento do firewall.

10. ESTRUTURA DA ASDU

A ASDU começa com o Type Identification, que define o tipo de informação. O Variable Structure Qualifier informa quantidade e organização dos objetos. A Cause of Transmission indica por que a mensagem foi enviada.

O endereço comum identifica a estação ou unidade lógica. Cada objeto possui Information Object Address, que identifica o ponto.

A parametrização precisa ser consistente entre RTU e SCADA. Um endereço pode existir em ambos os lados, mas ser interpretado com tipo ou causa incorretos.

A IEC 104 precisa ser parametrizada como sistema de telecontrole.

APDU, ASDU, Type ID, COT, IOA, qualidade, timestamps, k, w e temporizadores devem ser documentados antes da integração.

Conhecer a solução de Sistemas SCADA

11. TYPE IDENTIFICATION

O Type ID diferencia indicações simples, duplas, medições normalizadas, escaladas, em ponto flutuante, contadores, comandos e mensagens com timestamps.

A escolha precisa considerar precisão, faixa e necessidade de tempo. Uma medição em inteiro normalizado exige conversão; ponto flutuante pode simplificar integração, mas nem todos os equipamentos suportam os mesmos tipos.

Eventos binários podem utilizar CP24Time2a ou CP56Time2a, conforme tipo. O projeto deve definir resolução e fonte do tempo.

12. CAUSE OF TRANSMISSION

A Cause of Transmission, ou COT, informa se a mensagem é espontânea, resposta a interrogação, ativação, confirmação, término de ativação, solicitação ou outra condição.

O SCADA deve interpretar a causa. Um valor espontâneo representa mudança; um valor recebido em interrogação representa reconciliação do estado atual.

Comandos utilizam ativação, confirmação e término. Ignorar essas etapas pode fazer a interface considerar um comando concluído quando apenas foi aceito pela camada de aplicação.

13. ENDEREÇO COMUM E INFORMATION OBJECT ADDRESS

O endereço comum identifica a estação ou agrupamento lógico. O Information Object Address identifica cada ponto dentro desse contexto.

A lista de pontos deve registrar endereço comum, IOA, Type ID, COT esperada, escala, unidade, qualidade e permissão.

Endereços duplicados ou deslocados são causas comuns de integração incorreta. Testes devem comparar cada ponto com a origem física correspondente.

14. INTERROGAÇÃO GERAL E DE GRUPOS

A interrogação geral solicita o estado atual de um conjunto amplo de pontos. Interrogações de grupo permitem consultar subconjuntos.

A função é usada na inicialização, após reconexão e periodicamente para reconciliar o banco de dados.

Interrogações frequentes podem gerar tráfego elevado. A frequência deve considerar quantidade de pontos, eventos espontâneos e capacidade do enlace.

O SCADA precisa tratar início, respostas e término da interrogação. Uma resposta parcial não deve ser confundida com conclusão bem-sucedida.

15. TRANSMISSÃO ESPONTÂNEA

Eventos espontâneos são enviados pela estação controlada quando ocorre uma mudança relevante.

Essa função reduz latência e preserva sequência, principalmente quando combinada com timestamps na origem. A RTU precisa armazenar eventos durante interrupções.

Após reconexão, o comportamento deve ser definido. Algumas implementações recuperam eventos; outras dependem de interrogação e buffers proprietários. O requisito precisa ser ensaiado, não presumido.

16. QUALIDADE DO DADO

Qualificadores indicam condições como invalid, not topical, substituted, blocked e overflow.

O SCADA no setor elétrico deve apresentar essas condições. Um valor antigo ou substituído não pode aparecer como medição atual válida.

Gateways que convertem IEC 61850 ou Modbus para IEC 104 precisam mapear qualidade. Perder a qualidade durante conversão reduz a confiabilidade operacional.

17. TIMESTAMPS CP24TIME2A E CP56TIME2A

CP24Time2a representa tempo com minuto e milissegundos e depende de contexto de data. CP56Time2a inclui data e horário completos.

A escolha deve considerar interoperabilidade e necessidade de reconstrução de eventos. CP56Time2a é comum quando a data completa precisa acompanhar o objeto.

O relógio da RTU deve ser sincronizado. O servidor NTP em subestações pode atender muitos cenários; requisitos mais rigorosos podem exigir outras fontes.

O sistema precisa indicar quando o tempo é inválido ou não sincronizado.

18. MEDIÇÕES NORMALIZADAS, ESCALADAS E EM PONTO FLUTUANTE

Valores normalizados representam uma fração da faixa e exigem escala no sistema. Valores escalados utilizam inteiros. Ponto flutuante transmite diretamente a grandeza numérica.

O projeto deve documentar faixa, fator, unidade e limites. Escolher um tipo sem resolução suficiente pode perder precisão.

A comparação com instrumento ou valor de referência deve fazer parte do comissionamento.

19. COMANDOS SIMPLES, DUPLOS E SETPOINTS

A IEC 104 suporta comandos simples, duplos, ajustes e outras operações.

Comandos duplos podem representar aberto e fechado com estados intermediários ou inválidos. O mapeamento precisa refletir a lógica do equipamento.

Setpoints devem possuir faixa e unidade. O SCADA precisa impedir valores fora dos limites e registrar usuário, horário e resultado.

20. SELECT-BEFORE-OPERATE

Comandos podem utilizar seleção e execução. Na seleção, a estação controlada verifica disponibilidade. Na execução, realiza a operação dentro da janela prevista.

Esse mecanismo reduz risco de ponto errado, mas não substitui autorização, confirmação do operador e intertravamento local.

O timeout entre seleção e execução precisa ser compatível. Repetições automáticas devem ser controladas para evitar comando duplicado.

21. CONFIRMAÇÃO E TÉRMINO DE COMANDO

A confirmação de ativação indica aceitação ou rejeição. O término de ativação indica conclusão do processamento, quando aplicável.

Ainda assim, a confirmação física deve vir do estado de retorno do processo. Um disjuntor pode aceitar o comando e não mudar de posição.

O sistema deve distinguir comando enviado, aceito, concluído e confirmado pelo estado.

22. SINCRONISMO DE RELÓGIO

A IEC 104 possui mecanismos de sincronismo, mas o projeto pode utilizar NTP, PTP, IRIG-B ou arquitetura combinada.

A fonte deve ser definida e monitorada. Sincronizar pela mesma rede que está indisponível durante a contingência pode reduzir confiabilidade.

Logs, eventos e comandos precisam usar referência temporal consistente para auditoria.

23. REDUNDÂNCIA DE CANAIS E CENTROS

Subestações podem possuir dois enlaces, dois roteadores, dois servidores SCADA ou centros distintos.

A RTU precisa definir como trata múltiplas conexões. Eventos podem ser enviados a ambos, apenas ao ativo ou armazenados conforme política.

Failover deve evitar perda ou duplicidade. A arquitetura de telecomunicações operacionais precisa considerar roteamento, convergência e regras de firewall.

24. BUFFERS E RECUPERAÇÃO

Durante perda do canal, a RTU pode armazenar eventos. Capacidade, política de descarte e indicação de overflow devem ser conhecidas.

Após reconexão, o centro precisa recuperar os eventos na ordem correta. Se a implementação não oferece recuperação completa, a limitação deve constar nos critérios operacionais.

Testes de perda prolongada revelam o comportamento real.

25. INTEGRAÇÃO COM IEC 61850

Dentro da subestação, IEDs podem utilizar IEC 61850. A RTU ou gateway converte dados para IEC 104.

A subestação digital possui objetos, qualidade e eventos ricos. O mapeamento deve preservar essas informações.

GOOSE e Sampled Values não são transportados como equivalentes diretos pela IEC 104. O gateway publica estados e medições necessários ao telecontrole, não substitui as funções de tempo crítico locais.

26. RELAÇÃO COM DNP3

IEC 104 e DNP3 atendem telecontrole e possuem eventos, qualidade, timestamps e comandos.

DNP3 utiliza classes e grupos/variações. IEC 104 utiliza Type IDs, COT, endereço comum e IOA. A escolha depende de padrão da concessionária, legado e interoperabilidade.

Gateways entre os protocolos precisam mapear semântica, prioridade, qualidade e comandos. Conversão apenas de valores é insuficiente.

TCP 2404 deve permanecer restrito ao telecontrole autorizado.

Clientes, canais redundantes, firewall, certificados, jump server, logs e acesso remoto precisam ser tratados em conjunto na arquitetura OT.

Conhecer o serviço de Projeto de Telecomunicações

27. SEGURANÇA DA IEC 104

A IEC 104 clássica não fornece confidencialidade ou autenticação forte por padrão. TCP estabelece a sessão, mas não identifica de forma suficiente a entidade operacional.

A proteção depende de segmentação, firewall, listas de origem, hardening, controle de acesso remoto e monitoramento.

A porta 2404 deve ficar restrita. Conexões novas, comandos fora do padrão e mudanças de volume precisam gerar investigação.

28. IEC 62351 E PROTEÇÃO DO PROTOCOLO

A série IEC 62351 define mecanismos de segurança para comunicações de sistemas elétricos, incluindo proteção de perfis TCP/IP e mensagens de telecontrole.

A implementação pode envolver TLS, certificados, autenticação e gestão de chaves, conforme partes e perfis aplicáveis.

O artigo sobre IEC 62351 detalha esses mecanismos. Suporte precisa ser confirmado em RTU, SCADA e firmware.

29. FIREWALLS, DMZ E ACESSO REMOTO

A IEC 104 deve permanecer em zonas operacionais controladas. Usuários e fornecedores não precisam acessar diretamente a porta 2404.

Manutenção deve utilizar VPN, MFA, jump server e credenciais individuais. A sessão de administração deve ser separada do tráfego de telecontrole.

Firewalls precisam permitir canais principal e redundante, além de serviços auxiliares realmente necessários, como sincronismo e gerenciamento.

30. MONITORAMENTO E SIEM

Monitoramento passivo pode identificar STARTDT, sessões, comandos, COT, volume, reconexões e anomalias.

Firewalls, RTUs e SCADA devem enviar logs a uma plataforma central. Um SIEM em ambientes OT pode correlacionar novos clientes, falhas de autenticação, alterações e comandos.

O monitoramento não deve introduzir polling ativo que interfira em dispositivos sensíveis sem avaliação.

31. PROJETO E DOCUMENTAÇÃO

O projeto deve incluir arquitetura, endereçamento IP, endereço comum, IOAs, Type IDs, COT, escalas, unidades, qualidade, timestamps e permissões.

Também precisa registrar k, w, temporizadores, interrogações, espontâneos, buffers, redundância, firewall e segurança.

A lista de pontos é o contrato entre RTU e SCADA. Alterações precisam de versionamento e testes de regressão.

32. COMISSIONAMENTO E CRITÉRIOS DE ACEITE

O comissionamento deve testar sessão, sequência, dados, eventos, comandos e recuperação.

O roteiro mínimo inclui:

Os resultados devem ser registrados até a interface do operador. O Comissionamento e Aceite Técnico precisa comprovar desempenho e segurança.

O aceite precisa exercitar sessão, dados, eventos e comandos.

STARTDT, interrogações, espontâneos, qualidade, timestamps, buffers, temporizadores, failover e bloqueio de clientes indevidos devem ser comprovados.

Conhecer o serviço de Comissionamento e Aceite Técnico

33. DIAGNÓSTICO DE FALHAS

Conexão TCP sem transferência pode indicar ausência de STARTDT ou incompatibilidade. Desconexões periódicas podem estar ligadas a t1, t2, t3, firewall ou perda.

Pontos incorretos exigem verificar IOA, Type ID, escala e COT. Eventos ausentes podem decorrer de espontâneos desabilitados, buffer ou filtro.

Comandos rejeitados podem indicar seleção expirada, estado local, permissão, intertravamento ou COT negativa.

Captura de rede, logs da RTU e logs do SCADA devem ser analisados em conjunto.

34. ERROS COMUNS

Erros frequentes incluem liberar TCP 2404 amplamente, copiar temporizadores sem validação, ignorar qualidade e timestamp e tratar confirmação de comando como confirmação física.

Também é comum mapear IEC 61850 para IEC 104 sem preservar qualidade ou causa. A integração parece funcionar, mas perde contexto operacional.

Outro erro é testar apenas interrogação geral e não validar eventos espontâneos, buffers e failover.

35. CONCLUSÃO

IEC 60870-5-104 é uma base consolidada para telecontrole por redes IP. ASDUs, causas de transmissão, qualidade, timestamps, comandos e controle de sessão permitem integrar subestações e centros de operação.

A confiabilidade depende da combinação entre protocolo, rede e engenharia: endereçamento, temporizadores, redundância, segurança e testes de perda e recuperação. Quando esses elementos são documentados e comprovados, a IEC 104 oferece telecontrole previsível e rastreável.

[1] INTERNATIONAL ELECTROTECHNICAL COMMISSION. IEC 60870-5-104 — Telecontrol equipment and systems — Transmission protocols — Network access for IEC 60870-5-101 using standard transport profiles.

[2] INTERNATIONAL ELECTROTECHNICAL COMMISSION. IEC 60870-5-101 — Companion standard for basic telecontrol tasks.

[3] INTERNATIONAL ELECTROTECHNICAL COMMISSION. IEC 60870-5-5 — Basic application functions.

[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 IEC 60870-5-104? É um protocolo de telecontrole que transporta informações da IEC 101 sobre TCP/IP entre RTUs, subestações e centros de operação.**Qual porta a IEC 104 utiliza?** Normalmente TCP 2404, que deve ser restrita às estações controladoras e controladas autorizadas.**Qual é a diferença entre IEC 101 e IEC 104?** A IEC 101 foi concebida para enlaces seriais. A IEC 104 utiliza TCP/IP e mantém o modelo de informações de telecontrole.**O que são quadros I, S e U?** Quadros I transportam ASDUs, quadros S confirmam mensagens e quadros U controlam funções como STARTDT, STOPDT e TESTFR.**O que são k, w e temporizadores?** São parâmetros de janela, confirmação e supervisão da sessão IEC 104.**O que é Cause of Transmission?** É o campo que informa por que uma ASDU foi enviada, como espontânea, interrogação, ativação ou confirmação.**IEC 104 suporta eventos espontâneos?** Sim. A estação controlada pode enviar mudanças sem aguardar uma consulta.**IEC 104 possui segurança nativa?** A versão clássica possui limitações. A IEC 62351 define mecanismos adicionais, mas segmentação e controle de acesso continuam necessários.**IEC 104 substitui IEC 61850?** Não. IEC 61850 é comum dentro da subestação; IEC 104 é utilizada no telecontrole entre subestação e centro.**Como testar IEC 104?** Devem ser validados sessão, sequências, temporizadores, interrogações, espontâneos, qualidade, timestamps, comandos, buffers e failover.

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