

DNP3: O QUE É, COMO FUNCIONA, EVENTOS, CLASSES E SEGURANÇA EM SISTEMAS SCADA

Entenda o que é DNP3, controlling station, outstation, eventos, classes, integrity poll, objetos, tempo, comandos e segurança em SCADA.

SUMÁRIO

1. O QUE É DNP3	3
2. COMO FUNCIONA A COMUNICAÇÃO	3
3. ENDEREÇOS DNP3	4
4. DNP3 SERIAL E DNP3 SOBRE TCP/IP	4
5. DADOS ESTÁTICOS E EVENTOS	4
6. CLASSES 0, 1, 2 E 3	5
7. GRUPOS, VARIAÇÕES E TIPOS DE OBJETO	5
8. FLAGS E QUALIDADE	6
9. TIMESTAMPS E SINCRONISMO	6
10. INTEGRITY POLL E RECONCILIAÇÃO	6
11. SOLICITED E UNSOLICITED RESPONSES	7
12. DEADBAND E GERAÇÃO DE EVENTOS ANALÓGICOS	7
13. COMANDOS E SELECT-BEFORE-OPERATE	7
14. OPERATE, DIRECT OPERATE E CONFIRMAÇÃO	8
15. INDICADORES INTERNOS DA OUTSTATION	8
16. REDUNDÂNCIA DE MESTRES E SESSÕES	8
17. BUFFERS E PERDA DE COMUNICAÇÃO	9
18. DNP3 EM SUBESTAÇÕES	9
19. INTEGRAÇÃO COM RTU E SCADA	9
20. SEGURANÇA DO DNP3 CLÁSSICO	10
21. DNP3 SECURE AUTHENTICATION	10
22. RELAÇÃO COM IEC 62351	10
23. FIREWALL E MONITORAMENTO	10
24. PROJETO E DOCUMENTAÇÃO	11
25. COMISSIONAMENTO E CRITÉRIOS DE ACEITE	11
26. DIAGNÓSTICO DE FALHAS	11
27. ERROS COMUNS	12
28. CONCLUSÃO	12

DNP3 é um protocolo de telecontrole criado para transmitir estados, medições, contadores, eventos e comandos entre estações remotas e centros de operação. Ele é amplamente utilizado em sistemas elétricos, saneamento, óleo e gás e outras infraestruturas distribuídas nas quais a comunicação pode apresentar baixa largura de banda, latência elevada ou interrupções temporárias.

Seu diferencial não está apenas em consultar o estado atual dos pontos. DNP3 permite armazenar eventos na estação remota, classificá-los por prioridade, associar qualidade e timestamp e transmiti-los depois que o canal é restabelecido. Isso ajuda o centro de operação a reconstruir o que ocorreu durante uma indisponibilidade.

Em subestações de distribuição, o protocolo pode interligar RTUs, gateways, IEDs e sistemas SCADA. Ele pode operar em enlaces seriais ou sobre TCP/IP. A utilização segura exige segmentação, controle de comandos, autenticação quando suportada, sincronismo, registro de eventos e testes de perda e recuperação.

1. O QUE É DNP3

DNP3 significa *Distributed Network Protocol version 3*. O protocolo foi desenvolvido para aplicações de supervisão e controle distribuído. Sua padronização atual está associada à IEEE 1815.

A arquitetura tradicional utiliza uma estação controladora, frequentemente chamada de *controlling station* ou mestre, e uma ou mais estações remotas, chamadas de *outstations*. A estação controladora solicita dados, envia comandos e gerencia sessões. A outstation responde com valores estáticos, eventos e diagnósticos.

As denominações mestre e escravo ainda aparecem em documentações antigas. Os termos estação controladora e outstation descrevem melhor as funções sem depender dessa terminologia histórica.

2. COMO FUNCIONA A COMUNICAÇÃO

DNP3 organiza a comunicação em camadas. A camada de enlace identifica origens e destinos e fornece verificação do quadro. A função de transporte fragmenta mensagens de aplicação maiores. A camada de aplicação define funções, objetos, confirmações e sequência.

Em uma solicitação típica, o SCADA pede classes ou objetos específicos. A outstation responde com dados, eventos pendentes e indicadores internos. Quando existem respostas não solicitadas, a outstation também pode iniciar a transmissão de eventos.

O protocolo possui números de sequência e confirmações para determinadas mensagens. Esses mecanismos ajudam a detectar duplicidade e perda no nível da aplicação, mas não substituem autenticação ou criptografia.

3. ENDEREÇOS DNP3

Cada dispositivo possui endereço de enlace. O endereço identifica a estação controladora e a outstation dentro da arquitetura DNP3. Ele não deve ser confundido com endereço IP, porta TCP ou índice de ponto.

Em redes IP, um equipamento pode ser identificado simultaneamente por IP, porta e endereço DNP3. Gateways podem concentrar várias outstations atrás do mesmo caminho de rede.

O projeto precisa documentar todos esses níveis. Endereços duplicados ou mapeamentos inconsistentes podem fazer o sistema consultar o equipamento errado ou rejeitar mensagens válidas.

4. DNP3 SERIAL E DNP3 SOBRE TCP/IP

DNP3 pode operar em enlaces seriais, rádio ou outros meios compatíveis com o enquadramento de enlace. Em redes IP, o protocolo é normalmente transportado sobre TCP, utilizando a porta 20000 por convenção.

TCP oferece entrega ordenada e controle de congestionamento, mas não acrescenta autenticação ao DNP3 clássico. Liberar TCP 20000 entre redes inteiras cria exposição desnecessária.

A migração de serial para IP não elimina os conceitos de classes, eventos, objetos e confirmações. Apenas muda o transporte. Parâmetros e comportamento precisam ser testados novamente porque latência, sessões simultâneas e reconexão podem mudar.

5. DADOS ESTÁTICOS E EVENTOS

Dados estáticos representam o valor ou estado atual. Eventos representam mudanças ocorridas desde a última coleta ou confirmação.

Se um disjuntor abre e fecha durante uma interrupção do canal, a leitura estática posterior mostra apenas o estado final. Os eventos preservados pela outstation podem registrar as duas transições, com timestamps e qualidade.

A capacidade depende do buffer do equipamento. Quando o buffer enche, eventos antigos podem ser descartados. O projeto deve estimar a quantidade de eventos durante o maior período de perda esperado e definir alarmes de overflow.

6. CLASSES 0, 1, 2 E 3

Classe 0 corresponde à leitura de dados estáticos. Classes 1, 2 e 3 agrupam eventos. A associação entre prioridade operacional e número da classe é definida pelo projeto.

Uma prática frequente é utilizar Classe 1 para eventos críticos, Classe 2 para eventos operacionais e Classe 3 para dados de menor prioridade. Entretanto, essa convenção precisa ser documentada; o protocolo não atribui automaticamente significado operacional.

Colocar todos os pontos na mesma classe reduz a capacidade de priorização. Durante uma contingência, eventos menos importantes podem competir com alarmes e mudanças críticas.

A varredura de Classe 0 continua necessária para reconciliar o banco de dados. Ela confirma o estado atual e pode detectar discrepâncias após perda de eventos.

7. GRUPOS, VARIAÇÕES E TIPOS DE OBJETO

DNP3 utiliza grupos e variações para representar entradas binárias, saídas, contadores, valores analógicos, tempo, comandos e outros objetos.

A variação define detalhes como tamanho do valor, presença de flags e inclusão de timestamp. Um valor analógico pode ser representado como inteiro de 16 ou 32 bits, ponto flutuante ou outra forma suportada.

Mestre e outstation precisam utilizar variações compatíveis. O projeto deve registrar a variação de cada grupo, principalmente quando diferentes fabricantes escolhem padrões distintos.

A conversão para o SCADA deve preservar tipo, sinal, escala, unidade e qualidade. Um valor recebido corretamente pode ser apresentado incorretamente se a aplicação interpretar outra variação.

8. FLAGS E QUALIDADE

Os objetos podem incluir flags que indicam online, restart, communication lost, remote forced, local forced, over-range e outras condições.

O SCADA não deve exibir apenas o valor numérico. Um ponto marcado como communication lost ou forced precisa ser diferenciado visualmente e nos históricos.

A qualidade deve ser propagada por gateways. Quando DNP3 é convertido para [OPC UA](#), o gateway precisa mapear flags para códigos de qualidade equivalentes.

9. TIMESTAMPS E SINCRONISMO

Eventos podem incluir timestamps gerados na outstation. Isso permite ordenar mudanças ocorridas durante perda do canal.

A precisão depende do relógio local e do método de sincronismo. O [servidor NTP em redes e subestações](#) atende muitas aplicações, mas sistemas com requisitos mais rigorosos podem utilizar outras fontes.

O projeto precisa definir origem do horário, fuso, resolução e comportamento após perda de sincronismo. Um timestamp presente, porém incorreto, pode produzir uma sequência enganosa.

10. INTEGRITY POLL E RECONCILIAÇÃO

O *integrity poll* solicita uma visão abrangente dos dados estáticos e, conforme a configuração, eventos pendentes. Ele é utilizado na inicialização, após reconexão ou periodicamente para reconciliar o banco de dados.

Executá-lo com frequência excessiva pode gerar grande volume e competir com eventos. Executá-lo raramente aumenta o tempo durante o qual discrepâncias permanecem ocultas.

A frequência deve considerar quantidade de pontos, capacidade do enlace, criticidade e comportamento das outstations.

11. SOLICITED E UNSOLICITED RESPONSES

Respostas solicitadas são enviadas após requisição da estação controladora. Respostas não solicitadas, chamadas de *unsolicited responses*, permitem que a outstation envie eventos sem aguardar a próxima consulta.

Unsolicited reduz latência de alarmes, mas exige configuração coordenada. O mestre deve habilitar e confirmar as mensagens. Firewalls e NAT precisam permitir o fluxo da sessão existente.

O uso não elimina polling. Consultas periódicas continuam necessárias para disponibilidade, reconciliação e recuperação de eventos.

Durante comissionamento, é preciso verificar inicialização, habilitação, confirmação, repetição e comportamento após reconexão.

DNP3 precisa ser projetado para eventos, não apenas para polling.

Classes, variações, qualidade, timestamps, deadbands e buffers definem se o centro de operação conseguirá reconstruir o que ocorreu durante uma falha de comunicação.

Conhecer a solução de Sistemas SCADA

12. DEADBAND E GERAÇÃO DE EVENTOS ANALÓGICOS

Medições analógicas não devem gerar evento para qualquer pequena variação. Deadband define o quanto o valor precisa mudar para produzir novo evento.

Deadband muito pequena aumenta tráfego e ocupa buffers. Deadband muito grande oculta mudanças relevantes. O valor deve considerar resolução do sensor, ruído e necessidade operacional.

Deadbands podem ser configuradas na outstation ou em outra camada. A lista de pontos deve registrar onde são aplicadas e quem possui autoridade para alterar.

13. COMANDOS E SELECT-BEFORE-OPERATE

DNP3 suporta comandos diretos e *select-before-operate* (SBO). No SBO, o mestre seleciona o ponto e, dentro de uma janela, envia a operação correspondente.

Esse processo ajuda a reduzir comandos dirigidos ao ponto errado, mas não substitui autenticação, autorização, confirmação do operador e intertravamentos locais.

A aceitação da mensagem também não comprova a mudança física. O sistema precisa acompanhar o estado de retorno do equipamento.

Pontos de comando devem ser separados de leitura na matriz de permissões. Acesso de manutenção ou analytics não deve possuir escrita sem necessidade.

14. OPERATE, DIRECT OPERATE E CONFIRMAÇÃO

Direct operate envia a operação diretamente. *Direct operate no acknowledgment* reduz confirmação e deve ser utilizado apenas quando requisitos e riscos justificarem.

O projeto deve definir qual mecanismo é permitido por tipo de comando. Operações críticas podem exigir SBO, dupla confirmação na interface e registro de usuário.

Repetição automática de comandos após timeout é perigosa. A estação controladora precisa distinguir ausência de resposta de ausência de execução.

15. INDICADORES INTERNOS DA OUTSTATION

DNP3 possui *Internal Indications* (IIN) que informam condições como reinicialização, necessidade de sincronismo, overflow de classe, função não suportada e configuração corrompida.

Essas indicações precisam ser monitoradas e apresentadas. Ignorar IIN pode ocultar perda de eventos ou necessidade de intervenção.

Após restart, o mestre deve executar a sequência prevista: sincronizar horário quando necessário, realizar integrity poll e reconciliar dados.

16. REDUNDÂNCIA DE MESTRES E SESSÕES

Sistemas SCADA podem possuir servidores redundantes. A outstation pode suportar uma ou várias sessões simultâneas, dependendo da implementação.

Dois mestres ativos podem duplicar consultas, confirmar eventos de forma inesperada ou disputar comandos. O comportamento precisa ser conhecido e testado.

A arquitetura deve definir mestre ativo, standby, endereços, takeover e tratamento de eventos durante failover. Regras de firewall precisam incluir os caminhos redundantes.

17. BUFFERS E PERDA DE COMUNICAÇÃO

A outstation armazena eventos enquanto o canal está indisponível. O dimensionamento deve considerar taxa normal, contingências e tempo máximo de restauração.

Overflow precisa gerar indicação. Quando eventos são perdidos, o operador deve saber que a sequência ficou incompleta.

Após retorno, o sistema precisa recuperar eventos sem duplicar alarmes ou reordenar timestamps. Testes de perda prolongada são essenciais.

18. DNP3 EM SUBESTAÇÕES

Em subestações, DNP3 pode transmitir posição de disjuntores, alarmes, medições, contadores e comandos entre a RTU e o centro de operação.

IEDs locais podem utilizar IEC 61850, enquanto a RTU converte dados para DNP3. A [subestação digital](#) possui modelos ricos; o gateway deve preservar qualidade, timestamp e causa na conversão.

A arquitetura não deve expor diretamente todos os IEDs ao centro apenas por conveniência. RTUs e gateways controlam concentração, diagnóstico e segurança.

19. INTEGRAÇÃO COM RTU E SCADA

A RTU mapeia entradas, saídas e dados de IEDs para objetos DNP3. A lista de pontos deve registrar índice, grupo, variação, classe, deadband, qualidade, timestamp e permissão.

No [SCADA do setor elétrico](#), cada ponto precisa possuir descrição, unidade, severidade e comportamento durante perda de comunicação.

Conversões devem ser rastreáveis. Um evento de IEC 61850 convertido para DNP3 não deve perder o horário original ou a indicação de qualidade.

Telecontrole não deve depender apenas da confiança na rede.

TCP 20000, mestres autorizados, comandos, acesso remoto, autenticação segura e logs precisam compor uma arquitetura de telecomunicações e cibersegurança OT.

Conhecer o serviço de Projeto de Telecomunicações

20. SEGURANÇA DO DNP3 CLÁSSICO

DNP3 clássico foi criado para redes controladas e não possui confidencialidade ou autenticação forte em todas as mensagens.

A proteção depende de segmentação, listas de origem, firewalls, hardening, monitoramento e controle de acesso remoto. TCP 20000 deve ser permitido apenas entre mestres e outstations autorizados.

A [DMZ entre TI e OT](#) deve intermediar acessos corporativos. Ativos de telecontrole não devem ser acessíveis diretamente por usuários ou serviços genéricos.

21. DNP3 SECURE AUTHENTICATION

Secure Authentication adiciona mecanismos para autenticar operações críticas e reduzir comandos forjados. O suporte depende de versão, firmware, mestre e outstation.

A implantação exige gestão de chaves, usuários, algoritmos, atualização e recuperação. Equipamentos que anunciam DNP3 podem não implementar o perfil necessário.

A autenticação deve ser testada com mensagens válidas, inválidas, repetidas e fora de sequência. Também é necessário verificar logs e alarmes.

Secure Authentication não fornece confidencialidade completa do tráfego. Outros controles de rede continuam necessários.

22. RELAÇÃO COM IEC 62351

A série IEC 62351 trata segurança de comunicações de sistemas elétricos, incluindo mecanismos aplicáveis a protocolos de telecontrole.

O artigo sobre [IEC 62351](#) aprofunda autenticação, certificados, gestão de chaves e monitoramento.

O projeto deve distinguir os mecanismos implementados pelo equipamento de referências normativas genéricas. Conformidade precisa ser demonstrada por funcionalidades e testes.

23. FIREWALL E MONITORAMENTO

Regras devem limitar IP, porta, direção e, quando a tecnologia permitir, funções DNP3. Servidores redundantes e canais de contingência precisam estar incluídos.

Monitoramento passivo pode identificar novos mestres, varreduras, função de escrita, volume anormal e mudanças de padrão.

Logs do SCADA, firewall, RTU e sistema de acesso remoto devem compartilhar horário consistente. Um [SIEM em ambientes OT](#) pode correlacionar eventos de segurança e operação.

24. PROJETO E DOCUMENTAÇÃO

O projeto deve produzir arquitetura, endereçamento, matriz de fluxos, lista de pontos, grupos, variações, classes, deadbands, buffers, polling, unsolicited, comandos e requisitos de segurança.

Também precisa registrar comportamento de redundância, sincronismo, perda de canal, overflow e recuperação.

A documentação deve indicar responsáveis por alterações. Mudar classe ou deadband pode afetar tráfego, alarmes e capacidade de buffer.

25. COMISSIONAMENTO E CRITÉRIOS DE ACEITE

Os testes devem validar leitura estática, eventos, classes, qualidade, timestamps, comandos e segurança.

O roteiro mínimo inclui:

Os resultados precisam ser comparados com a lista de pontos e registrados como evidência. O [Comissionamento e Aceite Técnico](#) deve validar a cadeia até a tela do operador.

O aceite precisa testar perda, retenção e recuperação.

Eventos, buffers, unsolicited responses, IIN, comandos, failover e sincronismo devem ser comprovados ponta a ponta com evidências.

Conhecer o serviço de Comissionamento e Aceite Técnico

26. DIAGNÓSTICO DE FALHAS

Sem resposta, verifique rota, TCP 20000, endereço DNP3, sessão, timeout e estado da outstation. Respostas parciais podem indicar variação não suportada ou solicitação excessiva.

Eventos ausentes exigem analisar classes, buffers, confirmações, deadbands e filtros. Timestamps incorretos apontam sincronismo ou conversão.

Comandos rejeitados podem decorrer de SBO expirado, modo local, intertravamento, autenticação ou permissão.

27. ERROS COMUNS

Tratar DNP3 como polling simples elimina eventos, classes e qualidade. Configurar todos os eventos na mesma classe reduz priorização.

Outros erros incluem buffers pequenos, timestamps gerados apenas no SCADA, TCP 20000 amplamente liberado e comandos sem rastreabilidade.

Também é inadequado presumir interoperabilidade completa porque dois equipamentos suportam DNP3. Grupos, variações, secure authentication e sessões redundantes precisam ser confirmados.

28. CONCLUSÃO

DNP3 foi concebido para telecontrole em redes distribuídas e imperfeitas. Eventos, classes, qualidade, timestamps e buffers preservam contexto durante interrupções.

Em subestações, a confiabilidade depende do projeto completo: lista de pontos, priorização, sincronismo, segurança, comandos, redundância e ensaios de perda e recuperação. Quando esses elementos são comprovados ponta a ponta, o protocolo oferece uma base sólida entre campo e centro de operação.

[1] IEEE. IEEE 1815 – Standard for Electric Power Systems Communications – Distributed Network Protocol.

[2] DNP USERS GROUP. DNP3 Technical Overview and Application Notes. Disponível em: <https://www.dnp.org/>. Acesso em: 13 jul. 2026.

[3] IEEE. IEEE 1815.1 – Exchanging Information between Networks Implementing IEC 61850 and IEEE Std 1815.

[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 DNP3? DNP3 é um protocolo de telecontrole usado para transmitir medições, estados, eventos e comandos entre estações remotas e centros de operação. **O que são Classes 0, 1, 2 e 3?** Classe 0 representa dados estáticos. Classes 1, 2 e 3 agrupam eventos conforme a prioridade definida pelo projeto. **Qual porta o DNP3 utiliza?** DNP3 sobre TCP utiliza normalmente a porta 20000, que deve ser restrita aos mestres e outstations autorizados. **O que é integrity poll?** É uma consulta ampla usada para reconciliar dados estáticos e eventos, especialmente após inicialização ou reconexão. **O que é unsolicited response?** É uma resposta iniciada pela outstation para enviar eventos sem aguardar nova consulta do mestre. **O que é select-before-operate?** É um comando em duas etapas no qual o mestre seleciona o ponto e depois envia a operação dentro de uma janela. **DNP3 preserva eventos durante perda de comunicação?** A outstation pode armazenar eventos em buffers e transmiti-los após a recuperação, conforme capacidade e configuração. **DNP3 possui segurança?** O protocolo clássico possui limitações. Secure Authentication adiciona autenticação para operações críticas, mas controles de rede continuam necessários. **Como integrar DNP3 e IEC 61850?** RTUs ou gateways convertem modelos e eventos, preservando qualidade, timestamps e significado dos pontos. **Como testar DNP3?** Devem ser testados classes, eventos, buffers, timestamps, unsolicited, comandos, redundância, segurança e perda e recuperação do canal.

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.