

MODBUS: O QUE É, DIFERENÇAS ENTRE MODBUS RTU E TCP E SEGURANÇA INDUSTRIAL

Entenda o que é Modbus, diferenças entre RTU e TCP, coils, registers, function codes, endereçamento, gateways, polling, integração com SCADA e segurança.

SUMÁRIO

1. O QUE É MODBUS	4
2. ONDE O MODBUS É UTILIZADO	4
3. MODELO DE DADOS DO MODBUS	4
4. COILS E ENTRADAS DISCRETAS	5
5. INPUT REGISTERS E HOLDING REGISTERS	5
6. O PROBLEMA DO ENDEREÇAMENTO	5
7. PRINCIPAIS FUNCTION CODES	5
8. RESPOSTAS DE EXCEÇÃO	6
9. MODBUS RTU	6
10. TOPOLOGIA RS-485	6
11. MODBUS ASCII	6
12. MODBUS TCP	6
13. UNIT IDENTIFIER EM MODBUS TCP	7
14. MODBUS RTU VERSUS MODBUS TCP	7
15. GATEWAYS MODBUS	7
16. POLLING E DESEMPENHO	8
17. BANDA MORTA E ATUALIZAÇÃO	8
18. INTEGRAÇÃO COM SCADA	8
19. ENDIANNESS E ORDEM DE PALAVRAS	8
20. ESCRITA E COMANDOS	8
21. SEGURANÇA DO MODBUS	9
22. MODBUS SECURITY	9
23. SEGMENTAÇÃO E FIREWALL	9
24. MONITORAMENTO	9
25. PROJETO E DOCUMENTAÇÃO	9
26. TESTES E COMISSIONAMENTO	9
27. DIAGNÓSTICO DE FALHAS	10
27.1. SEM RESPOSTA	10
27.2. RESPOSTA COM VALORES INCORRETOS	10
27.3. COMUNICAÇÃO INTERMITENTE EM RS-485	10
27.4. GATEWAY RESPONDE, MAS DISPOSITIVO NÃO	10
27.5. LEITURA FUNCIONA E ESCRITA FALHA	10
28. ERROS COMUNS	10
28.1. CONFUNDIR 40001 COM OFFSET 40001	10

28.2. NÃO DOCUMENTAR ENDIANNESS	10
28.3. COLOCAR RS-485 EM ESTRELA	10
28.4. LIBERAR TCP 502 PARA TODA A REDE	11
28.5. POLLING EXCESSIVO	11
28.6. NÃO TESTAR COMANDOS	11
29. CONCLUSÃO	11

Modbus é um protocolo de comunicação industrial criado para permitir a troca de dados entre controladores, instrumentos, medidores, inversores, relés, gateways, sistemas supervisórios e outros dispositivos. Sua simplicidade contribuiu para uma ampla adoção em automação predial, industrial, elétrica e de utilidades.

O protocolo pode operar em redes seriais, principalmente como **Modbus RTU**, ou sobre Ethernet e TCP/IP, como **Modbus TCP**. Embora compartilhem o mesmo modelo básico de dados e funções, as duas variantes possuem diferenças de enquadramento, endereçamento, topologia, diagnóstico e desempenho.

Modbus foi desenvolvido em uma época na qual redes industriais eram isoladas e a cibersegurança não era um requisito central. Por isso, autenticação, criptografia e autorização não fazem parte do protocolo clássico. A proteção depende da arquitetura de rede, dos gateways, dos ativos, das regras de acesso e do monitoramento.

1. O QUE É MODBUS

Modbus é um protocolo de aplicação utilizado para ler e escrever dados em dispositivos industriais. A comunicação se baseia em solicitações e respostas.

Um cliente solicita uma operação, como leitura de registradores, e o servidor responde com os valores ou com um código de exceção.

Em terminologia histórica, também são utilizados os termos mestre e escravo. Documentações mais recentes preferem cliente e servidor.

2. ONDE O MODBUS É UTILIZADO

Aplicações comuns incluem:

O protocolo transporta dados. A semântica de cada registrador depende do mapa fornecido pelo fabricante.

3. MODELO DE DADOS DO MODBUS

O modelo clássico divide os dados em quatro áreas.

Área Tipo Acesso típico Coils bits leitura e escrita Discrete Inputs bits somente leitura Input Registers palavras de 16 bits somente leitura Holding Registers palavras de 16 bits leitura e escrita

Essa organização é lógica. O equipamento pode mapear internamente os dados de maneira diferente.

4. COILS E ENTRADAS DISCRETAS

Coils representam valores binários que podem ser lidos ou comandados, como ligar, desligar ou habilitar uma função.

Discrete Inputs representam estados binários de leitura, como contato aberto, fechado, alarme ativo ou condição de falha.

A nomenclatura não significa que todos os bits estão conectados diretamente a uma saída ou entrada física. O fabricante pode utilizar esses espaços para variáveis internas.

5. INPUT REGISTERS E HOLDING REGISTERS

Input Registers normalmente contêm medições e valores de leitura. Holding Registers podem armazenar ajustes, comandos e parâmetros.

Cada registrador possui 16 bits. Valores maiores podem ocupar dois ou mais registradores.

Podem ser representados:

A interpretação depende do mapa de registradores.

6. O PROBLEMA DO ENDEREÇAMENTO

Documentações podem apresentar endereços como 40001, 30001 ou simplesmente offset zero. Essa diferença gera erros frequentes.

O projeto deve distinguir:

Um registrador descrito como 40001 pode corresponder ao offset 0 dos Holding Registers. O comportamento precisa ser confirmado no manual do fabricante e em teste.

7. PRINCIPAIS FUNCTION CODES

Function codes indicam a operação solicitada.

Código Operação comum
01 ler coils
02 ler discrete inputs
03 ler holding registers
04 ler input registers
05 escrever uma coil
06 escrever um holding register
15 escrever múltiplas coils
16 escrever múltiplos registers

Outras funções existem, mas o suporte varia entre dispositivos.

8. RESPOSTAS DE EXCEÇÃO

Quando o servidor não consegue executar a solicitação, pode responder com código de exceção.

Exemplos:

Essas respostas devem ser registradas e tratadas pelo sistema supervisor.

9. MODBUS RTU

Modbus RTU é utilizado principalmente em comunicação serial, frequentemente sobre RS-485.

Características:

Os parâmetros incluem baud rate, bits de dados, paridade e bits de parada.

10. TOPOLOGIA RS-485

Uma rede RS-485 deve ser projetada como barramento, com derivações curtas e terminação adequada nas extremidades.

Aspectos importantes:

Topologias em estrela sem repetidores apropriados podem causar reflexões e comunicação intermitente.

11. MODBUS ASCII

Modbus ASCII utiliza caracteres ASCII e verificação LRC. Possui menor eficiência que RTU e é menos comum em projetos novos.

Pode existir em equipamentos legados. O levantamento deve confirmar a variante, porque Modbus ASCII e RTU não são intercambiáveis sem conversão.

12. MODBUS TCP

Modbus TCP transporta mensagens Modbus sobre TCP/IP. Utiliza normalmente a porta TCP 502.

A mensagem inclui um cabeçalho MBAP, que contém identificador de transação, protocolo, comprimento e Unit Identifier.

Vantagens:

O uso de TCP/IP não adiciona autenticação ou criptografia ao protocolo clássico.

13. UNIT IDENTIFIER EM MODBUS TCP

Em comunicação direta com um servidor Modbus TCP, o Unit Identifier pode ter uso limitado. Em gateways Modbus TCP para serial, ele pode identificar o dispositivo da rede RTU atrás do gateway.

A configuração deve ser documentada para evitar colisões e leituras do equipamento errado.

14. MODBUS RTU VERSUS MODBUS TCP

Aspecto	Modbus RTU	Modbus TCP	Meio comum
Identificação	endereço do dispositivo	endereço IP e Unit Identifier	serial RS-485 Ethernet e IP
Verificação	CRC	mecanismos de Ethernet/TCP, sem CRC	Modbus clássico
Concorrência	normalmente um mestre por barramento	vários clientes conforme capacidade do servidor	
Velocidade	limitada pela serial	maior capacidade de rede	
Topologia	barramento estrela, anel ou outra topologia	Ethernet	
Segurança	nativa	não no Modbus TCP clássico	
Diagnóstico	parâmetros físicos e seriais	rede, TCP, aplicação e servidor	

A escolha depende do equipamento, distância, ambiente, legado e requisitos de integração.

15. GATEWAYS MODBUS

Gateways conectam redes ou protocolos diferentes. Um gateway pode converter Modbus TCP para Modbus RTU, concentrar vários dispositivos ou publicar dados em MQTT e OPC UA.

O projeto precisa definir:

O gateway pode se tornar ponto único de falha e gargalo.

16. POLLING E DESEMPENHO

Sistemas supervisórios consultam dispositivos em ciclos. O tempo total depende de:

Ler registradores contíguos em blocos pode ser mais eficiente que realizar muitas solicitações individuais. Entretanto, o limite de cada dispositivo e a organização do mapa precisam ser respeitados.

17. BANDA MORTA E ATUALIZAÇÃO

Modbus normalmente responde quando consultado. A banda morta e a taxa de atualização são implementadas no SCADA, gateway ou aplicação.

O projeto deve definir:

18. INTEGRAÇÃO COM SCADA

A integração exige mais que cadastrar endereços.

Cada ponto deve possuir:

Uma lista de pontos incompleta gera valores invertidos, escalas erradas e comandos indevidos.

19. ENDIANNESS E ORDEM DE PALAVRAS

O protocolo define registradores de 16 bits, mas valores de 32 ou 64 bits podem ser organizados de diferentes formas.

Um fabricante pode utilizar:

A ordem deve ser confirmada por documentação e teste com valores conhecidos.

20. ESCRITA E COMANDOS

Funções de escrita podem alterar parâmetros ou comandar equipamentos. A aplicação precisa limitar quem pode utilizá-las.

Controles recomendados:

A segurança operacional não pode depender apenas do SCADA.

21. SEGURANÇA DO MODBUS

Modbus RTU e Modbus TCP clássicos não possuem autenticação, confidencialidade ou integridade criptográfica. Qualquer dispositivo com acesso ao caminho pode tentar ler ou escrever funções permitidas.

A proteção deve ser arquitetural:

22. MODBUS SECURITY

Existe uma especificação de Modbus Security que adiciona TLS e certificados ao transporte. O suporte depende dos dispositivos e aplicações.

Não se deve presumir que um equipamento identificado como Modbus TCP suporta Modbus Security. A interoperabilidade precisa ser verificada.

Em redes legadas, controles compensatórios continuam essenciais.

23. SEGMENTAÇÃO E FIREWALL

A porta TCP 502 não deve ser liberada entre redes inteiras sem necessidade. Regras devem limitar:

Dispositivos de campo não devem ser acessíveis diretamente pela internet ou pela rede corporativa.

24. MONITORAMENTO

Indicadores importantes:

O monitoramento passivo reduz risco de interferência em dispositivos sensíveis.

25. PROJETO E DOCUMENTAÇÃO

Um projeto Modbus pode produzir:

26. TESTES E COMISSIONAMENTO

Os testes devem verificar:

27. DIAGNÓSTICO DE FALHAS

27.1. SEM RESPOSTA

Verificar alimentação, meio físico, endereço, baud rate, paridade, porta TCP, rota, firewall e timeout.

27.2. RESPOSTA COM VALORES INCORRETOS

Verificar área, offset, base zero ou um, tipo de dado, escala e endianness.

27.3. COMUNICAÇÃO INTERMITENTE EM RS-485

Verificar terminação, topologia, blindagem, aterramento, derivações, interferência e colisões.

27.4. GATEWAY RESPONDE, MAS DISPOSITIVO NÃO

Verificar Unit Identifier, parâmetros seriais, fila, timeout e endereço do equipamento remoto.

27.5. LEITURA FUNCIONA E ESCRITA FALHA

Verificar função suportada, permissões, faixa de valor, modo local/remoto e intertravamentos.

28. ERROS COMUNS

28.1. CONFUNDIR 40001 COM OFFSET 40001

A referência do manual pode não ser o valor enviado na mensagem.

28.2. NÃO DOCUMENTAR ENDIANNESS

Valores de 32 bits podem aparecer invertidos ou incoerentes.

28.3. COLOCAR RS-485 EM ESTRELA

A topologia inadequada pode gerar reflexões e falhas intermitentes.

28.4. LIBERAR TCP 502 PARA TODA A REDE

A ausência de autenticação nativa amplia o risco de leitura e escrita indevidas.

28.5. POLLING EXCESSIVO

Consultas muito frequentes podem sobrecarregar dispositivos e gateways.

28.6. NÃO TESTAR COMANDOS

Escrita precisa ser validada com segurança e evidência.

29. CONCLUSÃO

Modbus permanece relevante por sua simplicidade e ampla disponibilidade em equipamentos industriais. Essa mesma simplicidade exige disciplina de engenharia para endereçamento, mapa de dados, polling, integração e segurança.

Projetos confiáveis documentam cada ponto, limitam funções de escrita, segmentam a rede, monitoram anomalias e testam a comunicação ponta a ponta. Assim, Modbus RTU e TCP podem ser integrados ao SCADA sem transformar o protocolo legado em um caminho não controlado para o processo.

[1] MODBUS ORGANIZATION. Modbus Application Protocol Specification V1.1b3.

[2] MODBUS ORGANIZATION. Modbus over Serial Line Specification and Implementation Guide V1.02.

[3] MODBUS ORGANIZATION. Modbus Messaging on TCP/IP Implementation Guide.

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

[5] ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. ABNT IEC/TS 62443-1-1:2023 — Segurança para sistemas de automação e controle industriais.

O que é Modbus? É um protocolo industrial de solicitação e resposta utilizado para ler e escrever dados em controladores, medidores, relés, inversores, gateways e outros dispositivos. **Qual a diferença entre Modbus RTU e Modbus TCP?** Modbus RTU opera principalmente em comunicação serial, como RS-485. Modbus TCP transporta as mensagens sobre Ethernet e TCP/IP. **O que são Holding Registers?** São registradores de 16 bits normalmente utilizados para valores que podem ser lidos e escritos, como

parâmetros e comandos. **Por que endereços como 40001 causam confusão?** Porque o manual pode usar um número de referência, enquanto a mensagem utiliza um offset iniciado em zero. A conversão depende do software e do fabricante. **Modbus possui segurança nativa?** O Modbus clássico não possui autenticação ou criptografia. A proteção depende de segmentação, firewall, controle de acesso, hardening e monitoramento. **Qual porta o Modbus TCP utiliza?** Normalmente TCP 502. A porta deve ser liberada somente entre clientes e servidores autorizados. **O que é Unit Identifier?** É um campo do Modbus TCP que pode ser utilizado por gateways para identificar dispositivos Modbus RTU atrás deles. **Como calcular o tempo de polling?** É necessário considerar quantidade de dispositivos, registradores, velocidade, timeout, tentativas e tempo de processamento. O valor deve ser validado em teste. **Como interpretar valores de 32 bits?** É preciso conhecer o tipo de dado e a ordem de bytes e palavras adotada pelo fabricante. **Como testar uma rede Modbus?** Devem ser verificados meio físico, parâmetros, endereços, funções, escala, endianness, timeout, exceções, escrita, gateways, firewall e integração com SCADA.

Soluções

Serviços de engenharia

Materiais técnicos complementares

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.