

TELEMETRIA: O QUE É, COMO FUNCIONA E APLICAÇÕES EM SUBESTAÇÕES E SISTEMAS SCADA

Entenda o que é telemetria, aquisição de dados, RTUs, protocolos, redes, sincronismo, SCADA, segurança e aplicações em subestações.

SUMÁRIO

1. O QUE É TELEMETRIA	3
2. COMO FUNCIONA UM SISTEMA DE TELEMETRIA	3
3. COMPONENTES DA ARQUITETURA	4
4. TIPOS DE DADOS TELEMÉTRICOS	4
5. AQUISIÇÃO ANALÓGICA E DIGITAL	4
6. ESCALA, UNIDADE E PRECISÃO	5
7. QUALIDADE DO DADO	5
8. TIMESTAMP E SEQUÊNCIA DE EVENTOS	5
9. TELEMETRIA POR POLLING E POR EVENTO	6
10. TELEMETRIA E PROTOCOLOS INDUSTRIAIS	6
11. RTU, IED, CLP E GATEWAY	7
12. REDES E MEIOS DE COMUNICAÇÃO	7
13. ARQUITETURA EM SUBESTAÇÕES DE DISTRIBUIÇÃO	7
14. LISTA DE PONTOS E DICIONÁRIO DE DADOS	8
15. ALARMES E GESTÃO OPERACIONAL	8
16. SEGURANÇA DA TELEMETRIA	8
17. ARMAZENAMENTO, HISTORIADOR E RETENÇÃO	9
18. TELEMETRIA, IOT E NUVEM	9
19. PROJETO E DOCUMENTAÇÃO	9
20. COMISSIONAMENTO E CRITÉRIOS DE ACEITE	10
21. DIAGNÓSTICO DE FALHAS	10
22. ERROS COMUNS	10
23. CONCLUSÃO	11

Telemetria é o processo de medir variáveis em um local, transmitir essas informações por uma rede e disponibilizá-las para supervisão, registro, análise ou decisão remota. Em sistemas de energia, ela permite que o centro de operação conheça estados, medições, alarmes e condições de equipamentos instalados em subestações e outros pontos distribuídos.

Um sistema de telemetria é formado por sensores ou dispositivos de origem, unidades de aquisição, protocolos, rede de comunicação, servidores e aplicações consumidoras. A confiabilidade depende de toda essa cadeia. Um dado pode chegar ao SCADA e ainda estar incorreto por erro de escala, timestamp, qualidade ou mapeamento.

Telemetria não é sinônimo de SCADA, IoT ou telecomunicações. O SCADA utiliza telemetria para supervisionar e controlar processos; IoT é uma abordagem ampla de conexão de dispositivos e aplicações; telecomunicações fornece os meios para transportar as mensagens. O projeto precisa integrar essas camadas sem confundir suas responsabilidades.

1. O QUE É TELEMETRIA

Telemetria combina medição e transmissão a distância. O termo pode ser aplicado a energia, saneamento, indústria, agricultura, transporte, data centers e diversos outros setores.

Em uma subestação, a telemetria pode incluir posição de disjuntores, tensões, correntes, potência, energia, frequência, temperatura, alarmes de bateria, estado de carregadores, nível de combustível e disponibilidade de telecomunicações.

O valor operacional não está apenas na quantidade de pontos. Dados precisam possuir origem conhecida, unidade, escala, qualidade, timestamp e comportamento definido diante de falhas. Uma medição sem contexto pode gerar decisões incorretas.

2. COMO FUNCIONA UM SISTEMA DE TELEMETRIA

O processo começa na aquisição. Um sensor, medidor, relé, IED ou controlador produz um valor ou estado. Esse dado pode ser lido diretamente por uma RTU, por um CLP, por um gateway ou por uma aplicação local.

A unidade de aquisição converte, normaliza ou organiza a informação. Depois, um protocolo transporta o dado por rede serial, Ethernet, rádio, fibra, rede celular ou outro meio. No destino, o SCADA, historiador ou plataforma analítica interpreta e armazena a informação.

A cadeia pode possuir várias conversões. Um medidor pode disponibilizar Modbus RTU; um gateway converte para Modbus TCP ou OPC UA; o SCADA recebe a variável e a envia ao historiador. Cada etapa pode alterar timestamp, qualidade, escala ou nome.

Por isso, a [Integração de Sistemas](#) deve ser rastreável da origem à aplicação final.

3. COMPONENTES DA ARQUITETURA

Sensores e dispositivos de campo são responsáveis pela medição ou pelo estado. A unidade de aquisição concentra dados e executa lógica local. A rede transporta as mensagens. Servidores processam, armazenam e disponibilizam as informações.

Em instalações simples, um único equipamento pode acumular várias funções. Um medidor pode possuir sensor, processamento e comunicação. Em sistemas maiores, essas funções são distribuídas entre IEDs, RTUs, gateways, switches, roteadores, servidores SCADA e historiadores.

A arquitetura deve identificar limites de responsabilidade. Quando o valor está incorreto, a equipe precisa saber se a causa está no sensor, na aquisição, no protocolo, na conversão, no SCADA ou na visualização.

4. TIPOS DE DADOS TELEMÉTRICOS

Medições analógicas representam grandezas contínuas, como tensão, corrente, pressão e temperatura. Estados binários representam condições como aberto, fechado, ativo ou falha. Contadores acumulam pulsos, energia ou eventos.

Alarmes indicam condições que exigem atenção. Eventos registram mudanças com timestamp. Comandos seguem o caminho inverso e alteram o processo, mas fazem parte de telecontrole, não apenas de telemetria.

A distinção é importante. Uma aplicação destinada somente a monitoramento não deve receber permissões de comando. Separar fluxos de leitura e escrita reduz risco operacional.

5. AQUISIÇÃO ANALÓGICA E DIGITAL

Entradas analógicas podem receber sinais como 4–20 mA, 0–10 V, RTD ou protocolos digitais. A conversão precisa considerar faixa, resolução, isolamento, precisão e calibração.

Um sinal de 4–20 mA normalmente utiliza 4 mA como zero vivo. Valores abaixo ou acima da faixa podem indicar falha, mas o tratamento depende do instrumento e da aplicação. O SCADA deve distinguir medição válida, saturação e falha de sensor.

Entradas digitais exigem definição de polaridade, debounce e estado seguro. Um contato normalmente fechado pode representar normalidade quando energizado e falha quando abre. Sem documentação, a indicação pode ser invertida.

6. ESCALA, UNIDADE E PRECISÃO

Uma variável pode ser transmitida como inteiro e convertida por fator. Por exemplo, 1380 pode representar 138,0 kV. A lista de pontos precisa registrar fator, offset, unidade e faixa.

Precisão do sistema não é apenas precisão do sensor. Inclui conversores, transformadores, aquisição, arredondamento e comunicação. A resolução também precisa ser adequada ao uso.

Unidades devem ser padronizadas. Misturar °C e décimos de °C, kW e W ou valores percentuais e absolutos é uma causa frequente de erro.

7. QUALIDADE DO DADO

Qualidade informa se o valor é confiável. Um sistema pode indicar dado válido, inválido, substituído, forçado, fora de faixa ou sem comunicação.

Manter o último valor após perda de comunicação pode ser útil para visualização, mas ele não deve continuar marcado como atual. A aplicação precisa indicar idade e condição do dado.

Gateways e protocolos possuem mecanismos diferentes de qualidade. O mapeamento deve preservar a condição mais restritiva. Converter um dado inválido em valor válido porque a variável numérica ainda existe elimina uma informação operacional essencial.

8. TIMESTAMP E SEQUÊNCIA DE EVENTOS

O timestamp pode ser atribuído no dispositivo, na RTU, no gateway ou no servidor. Quanto mais próximo da origem, maior a capacidade de reconstruir a sequência real.

Em subestações, eventos rápidos exigem sincronismo consistente. O [servidor NTP em redes e subestações](#) atende muitos sistemas, enquanto aplicações de alta precisão podem exigir PTP, IRIG-B ou mecanismos específicos.

O projeto deve registrar origem do timestamp, resolução, precisão e comportamento quando o relógio perde sincronismo. Um evento com horário local incorreto pode parecer ter ocorrido antes de sua causa.

9. TELEMETRIA POR POLLING E POR EVENTO

Em polling, o sistema consulta periodicamente os dispositivos. A taxa de atualização depende da quantidade de pontos, velocidade, timeout e ciclo de varredura.

Em sistemas orientados a eventos, a unidade remota armazena mudanças e transmite notificações. Protocolos como DNP3 e IEC 104 possuem recursos para eventos e transmissão espontânea.

As duas abordagens podem coexistir. Polling reconcilia o estado atual; eventos preservam mudanças entre consultas. A escolha depende de criticidade, largura de banda e capacidade dos equipamentos.

Telemetria confiável depende do contrato de dados.

Origem, tipo, escala, unidade, qualidade, timestamp, frequência e comportamento diante de falhas precisam ser definidos antes da integração.

Conhecer a solução de Sistemas SCADA

10. TELEMETRIA E PROTOCOLOS INDUSTRIAIS

[Modbus](#) é comum em medidores, UPS, retificadores e controladores. Ele utiliza polling e depende de mapa de registradores.

DNP3 e IEC 60870-5-104 são utilizados em telecontrole e possuem eventos, qualidade e timestamps. IEC 61850 oferece modelos e serviços para automação de sistemas elétricos.

OPC UA pode consolidar e modelar dados para aplicações. [MQTT](#) favorece publicação para múltiplos consumidores. Nenhum protocolo deve ser escolhido apenas por moda; a decisão deve considerar função, interoperabilidade, segurança e ciclo de vida.

11. RTU, IED, CLP E GATEWAY

A RTU é tradicionalmente responsável pela aquisição e comunicação com o centro de operação. IEDs executam funções especializadas, como proteção, medição e controle. CLPs aplicam lógica e automação. Gateways convertem protocolos e agregam dados.

As fronteiras podem se sobrepor. Uma RTU moderna pode executar lógica e atuar como gateway; um IED pode comunicar diretamente com o SCADA. A arquitetura deve ser definida por funções, não apenas pelo nome do equipamento.

Redundância precisa considerar essas funções. Duplicar o servidor não resolve falha de uma RTU única que concentra todos os pontos.

12. REDES E MEIOS DE COMUNICAÇÃO

A telemetria pode utilizar fibra óptica, Ethernet, rádio, MPLS, redes celulares, enlaces IP ou combinações. O meio precisa atender disponibilidade, latência, capacidade, cobertura e segurança.

O artigo sobre [telecomunicações operacionais em subestações](#) detalha a integração entre voz, dados, teleproteção e redundância.

Enlaces de baixa capacidade exigem priorização. Eventos e comandos críticos não devem competir sem controle com transferências volumosas. QoS, filas e dimensionamento precisam refletir a função operacional.

A perda de enlace deve ser tratada. RTUs podem armazenar eventos; proxies podem reter dados; sistemas devem indicar indisponibilidade sem apagar o último histórico válido.

13. ARQUITETURA EM SUBESTAÇÕES DE DISTRIBUIÇÃO

Uma subestação pode ter aquisição local por IEDs e RTU, rede de estação, gateways, roteadores e canal até o centro de operação. Sistemas auxiliares podem utilizar protocolos diferentes da automação principal.

O [SCADA no setor elétrico](#) recebe pontos de várias instalações. Padronização de nomes, unidades, alarmes e qualidade permite operar sites distintos de forma consistente.

A arquitetura deve separar domínio de proteção, supervisão, manutenção e acesso corporativo. Uma plataforma analítica não precisa consultar diretamente cada IED. Servidores intermediários e uma [DMZ entre TI e OT](#) podem controlar a exposição.

14. LISTA DE PONTOS E DICIONÁRIO DE DADOS

A lista de pontos é o contrato entre campo e aplicação. Ela deve registrar identificação, descrição, origem, protocolo, endereço, tipo, escala, unidade, qualidade, timestamp, frequência e destino.

Pontos de comando precisam incluir permissões, intertravamentos, confirmação e estado de retorno. Alarmes precisam indicar severidade, condição, atraso, reconhecimento e retorno ao normal.

Nomes devem seguir padrão hierárquico. Incluir site, bay, equipamento e função facilita manutenção. Siglas sem dicionário tornam a base dependente de conhecimento informal.

Mudanças precisam de versionamento. Alterar endereço, escala ou significado sem atualizar consumidores pode produzir valores aparentemente válidos, porém incorretos.

15. ALARMES E GESTÃO OPERACIONAL

Nem toda medição fora do valor nominal deve gerar alarme. O projeto define limites, atrasos, histerese, severidade e condição operacional.

Alarmes repetitivos e sem ação clara causam fadiga. A análise deve considerar consequência e resposta esperada. Um alarme de temperatura pode exigir inspeção; uma indicação de comunicação perdida pode exigir verificar o enlace.

Dependências evitam cascatas. A perda do roteador não deve produzir centenas de alarmes independentes sem indicar a causa comum.

A conexão entre campo e centro de operação precisa ser segmentada.

Leitura, comando, acesso de fornecedores, gateways, DMZ, logs e sincronismo devem compor uma arquitetura de segurança OT, não controles isolados.

Conhecer o serviço de Projeto de Telecomunicações

16. SEGURANÇA DA TELEMETRIA

Telemetria conecta ativos de campo a sistemas centrais e pode ampliar a superfície de ataque. Protocolos legados não possuem autenticação ou criptografia suficientes.

A proteção envolve segmentação, firewalls, listas de origem, hardening, controle de acesso remoto, inventário e monitoramento. O [guia de hardening](#) complementa a proteção de RTUs, gateways e servidores.

Fluxos de leitura devem ser separados de comandos. Credenciais e certificados precisam de gestão. Acesso de fornecedores deve passar por jump server ou mecanismo controlado.

Logs devem registrar conexões, alterações, falhas e comandos. O horário precisa ser consistente para correlação.

17. ARMAZENAMENTO, HISTORIADOR E RETENÇÃO

O historiador armazena séries temporais e eventos. A política de retenção depende de uso operacional, análise, conformidade e capacidade.

Deadband e compressão reduzem volume, mas podem ocultar pequenas variações. Os parâmetros precisam considerar a dinâmica da grandeza e a finalidade analítica.

Durante perda de comunicação, a RTU ou gateway pode armazenar dados. O sistema deve prevenir duplicidade e preservar ordem quando o enlace retorna.

18. TELEMETRIA, IOT E NUVEM

Plataformas IoT e nuvem podem ampliar análise e manutenção preditiva, mas não devem receber acesso direto e irrestrito ao processo.

A publicação pode ocorrer por gateway ou broker em zona intermediária. Dados precisam ser classificados e minimizados. Informações destinadas a analytics normalmente não exigem capacidade de comando.

A arquitetura deve considerar dependência de internet, latência, custos, retenção, soberania e recuperação. Funções operacionais críticas precisam continuar disponíveis quando a nuvem está indisponível.

19. PROJETO E DOCUMENTAÇÃO

O projeto deve apresentar arquitetura, inventário, meios, protocolos, endereçamento, lista de pontos, matriz de fluxos, sincronismo, redundância e requisitos de segurança.

Também deve definir desempenho: taxa de atualização, latência, disponibilidade, capacidade de buffer e tempo de recuperação. Esses critérios precisam ser mensuráveis.

O [Projeto de Telecomunicações](#) integra rede, energia, infraestrutura e aplicações. Telemetria não deve ser especificada isoladamente do meio que a transporta.

20. COMISSIONAMENTO E CRITÉRIOS DE ACEITE

O comissionamento deve validar a cadeia ponta a ponta. Um valor precisa ser comparado com referência conhecida na origem e na tela final.

O roteiro mínimo inclui:

Critérios devem registrar tolerância, tempo de atualização e resultado esperado. O aceite precisa gerar evidências rastreáveis.

O aceite deve acompanhar o dado da origem à tela final.

Escala, qualidade, timestamp, armazenamento durante perda de enlace, redundância e recuperação precisam ser comprovados com critérios mensuráveis.

Conhecer o serviço de Comissionamento e Aceite Técnico

21. DIAGNÓSTICO DE FALHAS

Valor inexistente pode indicar sensor, alimentação, endereço, protocolo ou mapeamento. Valor fixo pode ser dado congelado ou leitura real. A qualidade e idade ajudam a diferenciar.

Escala incorreta produz valores sistematicamente deslocados. Timestamp incorreto aponta sincronismo ou atribuição em camada inadequada. Eventos fora de ordem podem decorrer de buffer, conversão ou relógios distintos.

Perda intermitente exige observar enlace, timeout, polling, congestionamento e qualidade do meio. Diagnóstico deve seguir da origem ao destino.

22. ERROS COMUNS

Erros recorrentes incluem cadastrar pontos sem qualidade, atribuir timestamp apenas no servidor, manter último valor como válido e misturar leitura e comando.

Também é comum escolher protocolo antes de definir requisitos. A tecnologia deve atender função, desempenho, segurança e interoperabilidade.

Outro problema é entregar a telemetria sem dicionário de dados, matriz de fluxo ou testes de falha. O sistema funciona enquanto a equipe original mantém conhecimento informal, mas se torna difícil de operar e ampliar.

23. CONCLUSÃO

Telemetria transforma medições de campo em informação disponível à distância. Em subestações, ela sustenta supervisão, alarmes, análise e tomada de decisão.

A confiabilidade depende da cadeia completa: sensor, aquisição, protocolo, rede, gateway, SCADA, historiador e operação. Projetos maduros preservam escala, qualidade, timestamp e rastreabilidade, segmentam acessos e testam perda e recuperação. Assim, a telemetria passa de simples coleta de pontos para uma função de engenharia operacional.

[1] INTERNATIONAL ELECTROTECHNICAL COMMISSION. IEC 60870-5 series — Telecontrol equipment and systems.

[2] IEEE. IEEE 1815 — Standard for Electric Power Systems Communications — Distributed Network Protocol.

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

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

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

O que é telemetria? Telemetria é a medição de variáveis em um local e a transmissão dessas informações para supervisão, registro ou análise remota. **Qual é a diferença entre telemetria e SCADA?** Telemetria realiza aquisição e transporte de dados. O SCADA utiliza esses dados para supervisão, alarmes, histórico e controle. **Quais dados são enviados por telemetria?** Medições analógicas, estados binários, contadores, eventos, alarmes, qualidade e timestamps. **O que é qualidade do dado?** É a indicação de validade e condição da informação, como válido, inválido, substituído, forçado ou sem comunicação. **Onde o timestamp deve ser gerado?** Preferencialmente próximo da origem quando a sequência de eventos é importante, com sincronismo adequado. **Qual protocolo usar para telemetria?** Depende da aplicação. Modbus, DNP3, IEC 104, IEC 61850, OPC UA e MQTT possuem funções e características diferentes. **Telemetria precisa de internet?** Não. Pode operar em redes privadas, rádio, fibra, MPLS, celular ou outros meios. **Telemetria é a mesma coisa que IoT?** Não. IoT é uma abordagem ampla. Telemetria é a função de medir e transmitir dados a distância. **Como garantir segurança?** Com segmentação, firewall, autenticação, hardening, controle de acesso remoto, logs e separação entre leitura e

comando. **Como testar telemetria?** É necessário validar valores, escala, qualidade, timestamp, perda de comunicação, recuperação, redundância e aplicação final.

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.