

RTU EM SUBESTAÇÕES: O QUE É, COMO FUNCIONA E INTEGRAÇÃO COM SCADA E IEDS

Entenda o que é RTU, entradas e saídas, protocolos, eventos, lógica, sincronismo, redundância, segurança e integração com SCADA e IEDs.

SUMÁRIO

1. O QUE É RTU	3
2. PRINCIPAIS FUNÇÕES DE UMA RTU	3
3. ARQUITETURA DE HARDWARE	4
4. CPU, MEMÓRIA E SISTEMA OPERACIONAL	4
5. ENTRADAS DIGITAIS	4
6. SAÍDAS DIGITAIS E COMANDOS	4
7. ENTRADAS E SAÍDAS ANALÓGICAS	5
8. CONTADORES E ACUMULADORES	5
9. AQUISIÇÃO POR PROTOCOLOS	5
10. BANCO DE DADOS DE PONTOS	5
11. EVENTOS E SEQUÊNCIA CRONOLÓGICA	6
12. SINCRONISMO DE TEMPO	6
13. LÓGICA LOCAL E AUTOMAÇÃO	6
14. MODO LOCAL E REMOTO	7
15. INTEGRAÇÃO COM IEDS	7
16. INTEGRAÇÃO COM SCADA	7
17. REDUNDÂNCIA DE CPU	7
18. REDUNDÂNCIA DE COMUNICAÇÃO	8
19. ALIMENTAÇÃO E SERVIÇOS AUXILIARES	8
20. AMBIENTE E COMPATIBILIDADE ELETROMAGNÉTICA	8
21. INTERFACES DE ENGENHARIA	8
22. CIBERSEGURANÇA DA RTU	9
23. GESTÃO DE FIRMWARE E CICLO DE VIDA	9
24. ARQUITETURA DE REDE E DMZ	9
25. MONITORAMENTO E DIAGNÓSTICO	10
26. PROJETO E DOCUMENTAÇÃO	10
27. FAT E TESTES DE FÁBRICA	10
28. SAT E COMISSIONAMENTO	10
29. DIAGNÓSTICO DE FALHAS	11
30. ERROS COMUNS	11
31. CONCLUSÃO	11

RTU é uma unidade terminal remota utilizada para adquirir sinais, executar funções locais, registrar eventos e trocar informações com sistemas SCADA ou centros de operação. Em subestações, ela pode concentrar dados de IEDs, medidores e sistemas auxiliares, além de receber comandos autorizados e encaminhá-los aos equipamentos de campo.

Uma RTU não é apenas um conversor de protocolos. Ela pode possuir entradas e saídas físicas, processamento, sincronismo, armazenamento de eventos, lógica, comunicação redundante, diagnóstico e mecanismos de segurança. O escopo varia conforme fabricante, arquitetura e geração do equipamento.

Em subestações digitais, algumas funções historicamente centralizadas na RTU podem ser distribuídas entre IEDs, gateways e controladores. Ainda assim, a RTU continua relevante como concentrador de telecontrole, fronteira com o centro de operação e elemento de integração entre redes locais e protocolos como DNP3 ou IEC 60870-5-104.

1. O QUE É RTU

RTU significa *Remote Terminal Unit*. A unidade é instalada próxima ao processo e mantém comunicação com uma estação central.

Sua função clássica é converter sinais físicos em pontos de telemetria e transformar comandos do centro em saídas controladas. Em arquiteturas modernas, a RTU também integra dispositivos digitais por Ethernet ou serial e publica um banco de dados consolidado.

O termo não define um conjunto único de recursos. Existem RTUs compactas, modulares, redundantes, distribuídas e incorporadas a gateways. A especificação deve descrever funções e desempenho, não apenas exigir “uma RTU”.

2. PRINCIPAIS FUNÇÕES DE UMA RTU

Uma RTU pode adquirir entradas digitais e analógicas, comandar saídas, contar pulsos, executar lógica, armazenar eventos, sincronizar tempo e comunicar com vários sistemas.

Ela pode atuar como mestre de dispositivos locais e como outstation ou servidor para o centro. Também pode converter IEC 61850, Modbus, DNP3, IEC 101, IEC 104 e protocolos proprietários.

Em projetos críticos, a RTU mantém operação local e buffers durante perda do canal remoto. O centro deve receber eventos acumulados após a recuperação.

3. ARQUITETURA DE HARDWARE

RTUs modulares normalmente possuem fonte, CPU, módulos de entrada e saída e interfaces de comunicação. Backplanes ou barramentos internos conectam os módulos.

A arquitetura precisa considerar falha de fonte, CPU, módulo e barramento. Uma fonte redundante não resolve falha de CPU única; CPUs redundantes não resolvem concentração em um único módulo de comunicação.

O projeto deve identificar componentes substituíveis em campo, tempo de reparo, estoque e compatibilidade entre versões.

4. CPU, MEMÓRIA E SISTEMA OPERACIONAL

A CPU executa aquisição, lógica, protocolos, eventos e diagnóstico. O dimensionamento considera quantidade de pontos, sessões, taxa de eventos, conversões e aplicação local.

Memória precisa armazenar firmware, configuração, logs e buffers. A capacidade de eventos durante perda de comunicação deve ser especificada em quantidade ou duração.

RTUs modernas podem utilizar sistemas operacionais embarcados. O fabricante deve informar ciclo de suporte, atualizações, hardening e mecanismos de recuperação.

5. ENTRADAS DIGITAIS

Entradas digitais recebem contatos de posição, alarmes e estados. A especificação deve definir tensão, isolamento, polaridade, debounce e detecção de transições.

Indicações simples representam dois estados. Indicações duplas utilizam dois contatos e podem representar posições intermediárias ou inválidas.

A RTU deve registrar mudança com timestamp adequado. Debounce excessivo pode atrasar eventos; debounce insuficiente pode gerar múltiplas transições.

6. SAÍDAS DIGITAIS E COMANDOS

Saídas digitais podem acionar relés intermediários ou circuitos de comando. O projeto deve definir pulso, duração, retenção, corrente, isolamento e estado seguro.

Comandos críticos precisam de permissões, seleção, execução e confirmação. Intertravamentos locais não devem depender apenas do SCADA.

A RTU precisa distinguir comando recebido, saída acionada e retorno físico. A confirmação real vem do processo.

7. ENTRADAS E SAÍDAS ANALÓGICAS

Entradas analógicas podem receber 4–20 mA, tensão, RTD ou outros sinais. A especificação inclui faixa, resolução, precisão, isolamento e diagnóstico.

Saídas analógicas são menos comuns em algumas subestações, mas podem existir em sistemas auxiliares. Limites e estado de falha precisam ser definidos.

Escala deve ser rastreável da entrada física ao valor apresentado no [SCADA](#).

8. CONTADORES E ACUMULADORES

Entradas de pulso podem representar energia, volume ou operações. A RTU precisa lidar com frequência máxima, rollover, retenção e sincronização.

Contadores devem sobreviver a reinicialização quando necessário. O comportamento após perda de alimentação precisa ser testado.

A aplicação central deve distinguir valor acumulado, incremento e qualidade.

9. AQUISIÇÃO POR PROTOCOLOS

Além de I/O físico, a RTU pode adquirir dados por [Modbus](#), IEC 61850, DNP3, IEC 101 e protocolos proprietários.

Cada driver possui limites de dispositivos, pontos, sessões e frequência. O dimensionamento deve considerar tempo de ciclo e comportamento diante de dispositivo lento.

A RTU deve marcar como inválidos os dados cuja origem perdeu comunicação, em vez de manter valores antigos como atuais.

10. BANCO DE DADOS DE PONTOS

O banco interno relaciona entradas físicas ou digitais a pontos de telecontrole. Cada ponto possui identificação, tipo, escala, qualidade, timestamp, classe e destino.

A lista de pontos precisa ser controlada por versão. Alterações de endereço ou tipo podem afetar SCADA e gateways.

Nomes internos devem seguir padrão. Identificadores genéricos tornam diagnóstico dependente do software de configuração.

A RTU deve ser especificada por funções e desempenho.

I/O, protocolos, buffers, lógica, sincronismo, redundância e capacidade de recuperação precisam ser definidos antes da escolha do equipamento.

Conhecer a solução de Sistemas Digitais de Supervisão e Controle

11. EVENTOS E SEQUÊNCIA CRONOLÓGICA

A RTU registra mudanças com timestamp e armazena eventos em buffer. A capacidade precisa atender o período de indisponibilidade esperado.

A sequência cronológica depende do sincronismo e da resolução. Eventos de IEDs devem preservar o horário da origem quando disponível.

Após reconexão, a RTU deve transmitir eventos na ordem correta e sinalizar overflow. O artigo sobre [Telemetria](#) aprofunda qualidade, timestamp e recuperação.

12. SINCRONISMO DE TEMPO

A RTU pode receber NTP, PTP, IRIG-B, GPS ou sincronismo por protocolo. A escolha depende da precisão e da arquitetura.

O [servidor NTP em redes e subestações](#) atende muitos sistemas de supervisão. Eventos de proteção podem exigir maior precisão.

A RTU deve monitorar estado da fonte e marcar tempo inválido quando perde sincronismo além do limite.

13. LÓGICA LOCAL E AUTOMAÇÃO

Algumas RTUs executam lógica IEC 61131-3 ou ambiente proprietário. Essa função pode implementar intertravamentos, sequências, cálculos e automação local.

A lógica precisa ser separada das funções de comunicação e documentada. Alterações devem passar por revisão, teste e versionamento.

Funções de proteção não devem ser transferidas para a RTU sem análise de desempenho, independência e requisitos normativos.

14. MODO LOCAL E REMOTO

O controle pode depender de seletores físicos, chaves locais ou estados lógicos. A RTU deve respeitar o modo local/remoto.

O SCADA precisa receber indicação clara. Um comando bloqueado por modo local deve retornar motivo, não apenas timeout.

A transição de modo deve ser registrada. Procedimentos operacionais definem quem pode alterar e em quais condições.

15. INTEGRAÇÃO COM IEDS

IEDs realizam proteção, medição, controle e monitoramento. A RTU pode coletar dados por IEC 61850, protocolos seriais ou contatos físicos.

A [subestação digital e IEC 61850](#) utiliza modelos, reports e eventos. A RTU deve preservar qualidade, timestamp e causa.

Duplicar o mesmo ponto por contato e protocolo pode ser útil para redundância, mas precisa de lógica de seleção e diagnóstico.

16. INTEGRAÇÃO COM SCADA

Para o centro, a RTU atua como outstation DNP3, estação controlada IEC 104 ou servidor de outro protocolo.

A lista de pontos deve mapear origem local para objeto remoto. Classes DNP3, Type IDs IEC 104, endereços e comandos precisam ser definidos.

O [DNP3](#) e a [IEC 104](#) possuem modelos distintos. A RTU deve manter configurações independentes e consistentes.

17. REDUNDÂNCIA DE CPU

Arquiteturas redundantes podem utilizar CPUs em hot standby. O objetivo é transferir processamento sem perder pontos, eventos ou sessões além do limite.

O projeto deve definir sincronização de banco de dados, lógica, buffers e estados de saída. Switchover não pode repetir comandos.

Testes devem incluir falha de CPU ativa, retorno, reintegração e divergência de versão.

18. REDUNDÂNCIA DE COMUNICAÇÃO

A RTU pode possuir interfaces e rotas redundantes. Protocolos podem operar com duas sessões ou apenas com caminho ativo.

A comutação depende da rede, roteadores e SCADA. O [PRP e HSR](#) atende redes locais específicas, enquanto enlaces WAN podem utilizar outras estratégias.

Regras de firewall devem contemplar todos os caminhos legítimos sem ampliar a superfície.

19. ALIMENTAÇÃO E SERVIÇOS AUXILIARES

RTUs em subestações são frequentemente alimentadas pelo sistema CC. A faixa de tensão, consumo, redundância e proteção precisam ser compatíveis.

O artigo sobre [serviços auxiliares](#) aborda baterias, retificadores e UPS.

A RTU deve sinalizar falha de fonte e manter configuração após interrupção. Reinicialização precisa ser controlada e registrada.

20. AMBIENTE E COMPATIBILIDADE ELETROMAGNÉTICA

Temperatura, umidade, vibração, interferência e surtos influenciam a seleção. Equipamentos instalados em painéis de subestação precisam atender requisitos ambientais.

Interfaces de campo devem possuir isolamento e proteção adequados. Aterramento e roteamento de cabos fazem parte do projeto.

Ventilação e dissipação devem ser verificadas no painel completo, não apenas pela especificação individual.

21. INTERFACES DE ENGENHARIA

Configuração pode ocorrer por software local, web, console ou rede. Interfaces não utilizadas devem ser desabilitadas.

Contas padrão precisam ser alteradas. Acesso de engenharia deve utilizar perfis individuais, logs e, quando remoto, jump server.

Backups devem incluir firmware, configuração, lógica e base de pontos. A restauração precisa ser testada em equipamento compatível.

A RTU concentra dados e comandos críticos.

Segmentação, contas, firmware, acesso de engenharia, backups, logs e protocolos legados devem ser tratados como requisitos de projeto, não como ajustes posteriores.

Conhecer o serviço de Projeto de Telecomunicações

22. CIBERSEGURANÇA DA RTU

RTUs são ativos críticos porque concentram dados e comandos. A proteção envolve segmentação, hardening, credenciais, firmware, logs e acesso remoto.

A [IEC 62443 em subestações](#) orienta zonas, conduítes e requisitos de segurança.

Serviços desnecessários devem ser removidos. Protocolos legados precisam de controles compensatórios. Alterações de configuração e login devem ser monitorados.

23. GESTÃO DE FIRMWARE E CICLO DE VIDA

Firmware corrige falhas e pode alterar comportamento. Atualizações devem ser avaliadas em laboratório, com backup e plano de retorno.

O fabricante precisa fornecer período de suporte, avisos de segurança e compatibilidade. Equipamentos sem suporte exigem plano de substituição ou controles adicionais.

Versões entre CPUs redundantes e módulos devem ser compatíveis. O inventário precisa registrar hardware, firmware e configuração.

24. ARQUITETURA DE REDE E DMZ

A RTU deve permanecer na zona operacional. Centros de operação conectam-se por canais definidos; usuários corporativos não acessam diretamente.

A [DMZ entre TI e OT](#) hospeda serviços intermediários. Acesso de manutenção passa por VPN, MFA e jump server.

A matriz de fluxo registra protocolos, portas, origem, destino e função. Regras genéricas devem ser evitadas.

25. MONITORAMENTO E DIAGNÓSTICO

A RTU deve fornecer estado de módulos, CPU, memória, fontes, interfaces, sincronismo, protocolos e buffers.

SNMP pode monitorar infraestrutura, enquanto logs e diagnósticos proprietários detalham a aplicação. O artigo sobre [SNMP](#) complementa essa camada.

Alarmes precisam chegar ao SCADA sem depender do mesmo componente que falhou quando possível.

26. PROJETO E DOCUMENTAÇÃO

O projeto deve incluir arquitetura, diagramas de I/O, lista de pontos, protocolos, endereços, lógica, sincronismo, redundância, alimentação e segurança.

Também deve apresentar matriz de comandos, modos local/remoto, buffers, critérios de desempenho e plano de testes.

A documentação as-built precisa refletir módulos, bornes, cabos, firmware e backups.

27. FAT E TESTES DE FÁBRICA

O FAT valida configuração antes da instalação. Simuladores podem reproduzir IEDs, SCADA e sinais físicos.

Devem ser testados pontos, lógica, protocolos, eventos, comandos, redundância e segurança. Pendências precisam ser registradas antes do envio.

O FAT não substitui o SAT, porque rede, cabos e equipamentos reais influenciam o resultado.

28. SAT E COMISSIONAMENTO

No campo, o SAT verifica a cadeia real. Cada ponto deve ser estimulado na origem e conferido no SCADA.

O roteiro mínimo inclui:

O [Comissionamento e Aceite Técnico](#) deve registrar evidências por ponto e cenário.

O aceite deve comprovar a cadeia física, lógica e remota.

Pontos, qualidade, eventos, comandos, failover, sincronismo, segurança e restauração precisam ser ensaiados da borneira até a tela do operador.

Conhecer o serviço de Comissionamento e Aceite Técnico

29. DIAGNÓSTICO DE FALHAS

Pontos físicos incorretos exigem verificar borne, tensão, polaridade, módulo e escala. Pontos digitais ausentes exigem analisar protocolo, endereço, qualidade e driver.

Eventos fora de ordem apontam sincronismo ou buffer. Comandos que não executam podem estar bloqueados por modo, intertravamento ou permissão.

Falhas após switchover indicam sincronização de CPU, sessão ou configuração. Logs devem ser analisados em conjunto com captura de rede e SCADA.

30. ERROS COMUNS

Especificar apenas quantidade de I/O sem desempenho, buffers e redundância produz uma RTU subdimensionada.

Outros erros incluem concentrar todos os protocolos em uma CPU única sem análise, manter contas padrão, não testar restauração e ignorar qualidade.

Também é comum aceitar a comunicação sem validar o ponto físico e a tela final. A conectividade não comprova integração funcional.

31. CONCLUSÃO

A RTU conecta o processo local ao centro de operação. Ela adquire sinais, integra IEDs, registra eventos, executa lógica e publica dados por protocolos de telecontrole.

Sua confiabilidade depende de hardware, banco de pontos, sincronismo, redundância, segurança e testes. Quando a RTU é projetada como componente crítico e não como simples gateway, ela preserva qualidade e controle mesmo diante de falhas de comunicação ou equipamentos.

[1] INTERNATIONAL ELECTROTECHNICAL COMMISSION. IEC 60870 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] INTERNATIONAL ELECTROTECHNICAL COMMISSION. IEC 62443 series — Security for industrial automation and control systems.

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

O que é uma RTU? RTU é uma unidade terminal remota que adquire sinais, registra eventos e comunica dados e comandos entre campo e centro de operação. **Qual é a diferença entre RTU e CLP?** As funções podem se sobrepor. RTUs são tradicionalmente voltadas a telecontrole distribuído, eventos e comunicação remota; CLPs focam automação e lógica de processo. **RTU e gateway são a mesma coisa?** Não necessariamente. Um gateway converte protocolos. Uma RTU pode também possuir I/O, lógica, eventos, comandos e redundância. **Quais protocolos uma RTU utiliza?** Pode utilizar DNP3, IEC 101, IEC 104, IEC 61850, Modbus e protocolos proprietários. **Como a RTU armazena eventos?** Ela utiliza buffers de eventos com timestamp e qualidade, transmitidos após recuperação do canal conforme capacidade. **RTU precisa de sincronismo?** Sim. O sincronismo é essencial para sequência de eventos e correlação com SCADA e IEDs. **RTU pode executar comandos?** Sim, por saídas físicas ou protocolos, respeitando permissões, modo local/remoto e intertravamentos. **Como proteger uma RTU?** Com segmentação, hardening, credenciais individuais, firmware suportado, logs, firewall e acesso remoto controlado. **O que testar no failover?** Devem ser verificados CPU, fonte, comunicação, sessões, buffers, comandos e recuperação sem duplicidade. **Como comissionar uma RTU?** Cada ponto deve ser testado da origem ao SCADA, incluindo qualidade, timestamp, comandos, redundância e segurança.

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.