Capítulo V

Protocolos seriais para automação

Equipe de engenharia da Schweitzer Engineering Laboratories (SEL)

Na automação de subestações, as informações são adquiridas no processo elétrico por meio de Unidades Terminais Remotas (UTRs), Controladores Lógicos Programáveis (CLPs) ou relés de proteção; equipamentos que passaremos a chamar, de forma genérica, de *Inteligent Electronic Devices* (IEDs).

As informações adquiridas:

• Medidas digitais que traduzem as posições aberta ou fechada de disjuntores, seccionadoras e chaves em geral;

• Medidas analógicas, que informam principalmente as tensões (kV), correntes (A), potência ativa (MW), reativa (MVAr), frequência (Hz);

• Controle (telecomando) digital, para abrir e fechar remotamente um disjuntor ou seccionadora;

• Controle (telecomando) analógico, principalmente utilizado no Controle Automático de Geração (CAG).

Estas informações, processadas pelos IEDs, são transmitidas por meio de canais de comunicação, para outros equipamentos que delas necessitam. Para este transporte, são utilizados os protocolos de comunicação.

Neste capítulo, vamos abordar os protocolos que se utilizam de linhas de comunicações seriais, camadas físicas RS232 e RS485. No próximo capítulo, abordaremos o IEC 61850, que utiliza infraestrutura de rede TCP/IP e Ethernet.

A definição clássica de protocolos é:

• Regras que governam a comunicação entre dispositivos eletrônicos.

Protocolos de comunicação

Existem várias formas de classificar os protocolos. Vamos inicialmente verificar duas:

• Quantidade de dados transmitidos. Diferentes tipos de protocolos, cada tecnologia a seu tempo, com a sua função:

- IEDs que trocam alguns bits em milissegundos (válvulas on/off, chaves de nível, pressostatos, etc.): protocolos do tipo SensorBuses. Exemplo: Devicenet;
- IEDs que trocam informações de alguns bytes em dezenas de milissegundos (transmissores de pressão, vazão, temperatura, válvulas de controle, etc.): protocolos tipo FieldBuses. Exemplo: Profibus PA, Hart, Fieldbus Foundation H1;
- IEDs que trocam vários blocos de bytes em dezenas ou centenas de milissegundos (relés inteligentes, balanças, remote IO, etc.): protocolos tipo DeviceBuses. Exemplo: Profibus DP, ControlNet e DeviceNet, DNP3, MODBUS, IEC 60870-5-101;
- IEDs que trocam várias dezenas de blocos ou arquivos em segundos (UTRs, CLPs, SDCDs, etc.): Protocolos do tipo DataBuses. Exemplo: Ethernet TCP/IP, Profinet.

• Agilidade na comunicação ou throughput:

Definição: Tempo decorrido entre a detecção de um evento e a atuação de uma saída baseada em uma decisão lógica. O que determina o throughput:

- Taxa de transmissão

• 1,2 a 19,2 KBps – IEC60870 101, DNP3, MODBUS.

• 100 MBps – IEC 61850 – TCP/IP.

- Eficiência do Protocolo – Overhead ou Payload – Número total de bytes da mensagem em relação à mensagem útil – dados.
• IEC 60870 101, DNP3, Modbus – otimizados para mínimo overhead
• IEC 61850 TCP/IP – pouco otimizado em função das larguras de banda disponíveis atualmente
- Modelo da rede
• Origem/destino
• Produtor/consumidor (publisher/subscriber) (publicador/assinante) IEC 61850

Modelo OSI da ISO

ISO – *International Standard Organization.*
OSI – *Open Systems Interconnect.*

Na especificação de um protocolo, é procedimento usual adotar o modelo de dividir em camadas as várias tarefas necessárias para transmitir as informações do processo que queremos supervisionar e controlar. Cada camada do protocolo é encarregada de tarefas específicas.

O modelo OSI completo possui sete camadas (ver Figura 2), que prevê todas as tarefas de um protocolo completo. Mas, dependendo da complexidade (ou a falta de), o modelo pode ser simplificado com um número menor de camadas.

Vamos descrever os protocolos:

• MODBUS – Modelado com apenas duas camadas. Física e aplicação.
• IEC60870-101 – Modelado com três camadas. Física, enlace e aplicação.
• DNP3 – Modelado com quatro camadas. Física, enlace, transporte e aplicação. Já possui o conceito de rede, com endereços de origem, destino e mecanismo de fragmentação de mensagem.

O protocolo MODBUS, o mais antigo dos três, foi especificado na década de 1970, e podemos afirmar que é também o mais simples. Consiste em um protocolo ponto a ponto, mestre/escravo. A sua mensagem só carrega o endereço de destino, pois sempre haverá um IED que controla a comunicação, a quem todos os outros estão ligados, conhecido como mestre. Não existe nenhuma estrutura de formação dos "objetos de dados", ou seja, medições analógicas, digitais, pontos simples, duplos, etc. As informações são alocadas na memória do computador, sem nenhuma pré-formatação, sendo responsabilidade do configurador (um ser humano) alocá-los corretamente, para escrita e leitura.

Na sequência crescente de complexidade, temos o IEC 60870-101, especificado na década de 1980 e dominante

na Europa. Também tem a concepção mestre/escravo, mas os "objetos de dados" foram definidos atendendo às necessidades do setor elétrico. São as "ASDUs, *Aplication Services Data Units*" que carregam as formatações de medidas analógicas de 8, 16 ou 32 bits, pontos simples, pontos duplos, e "tipos", que definem se é uma leitura analógica, digital, um controle, etc.

Já na década de 1990 foi especificado o DNP3, que atendia a todos os requisitos do IEC 60870-101, já incorporava características de rede como conhecemos atualmente no TCP/IP e é dominante nos Estados Unidos.

Todos os protocolos têm em comum a primeira camada, chamada de camada física. Começaremos por ela.

Camada física

Camada física é onde são definidas as interfaces mecânicas (tipos de conectores, bitolas de cabos) e elétricas (níveis de tensão nos condutores, sinais elétricos nos pinos dos conectores, etc.).

As especificações mais comuns para os protocolos seriais que estamos abordando são EIA 232 e EIA 485. Existe a camada física Ethernet, que é abordada em capítulo específico. EIA 232 refere-se a "*Electronic Industries Association*", originário dos Estados Unidos. Também é utilizada a sigla RS, que significa "*Recomended Standard*".

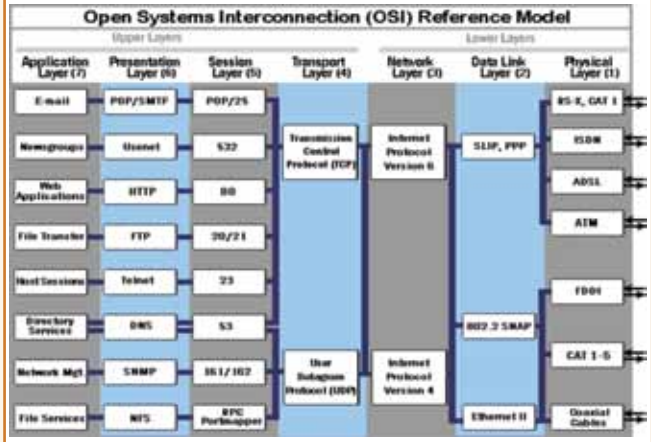

Figura 1 – Modelo OSI.

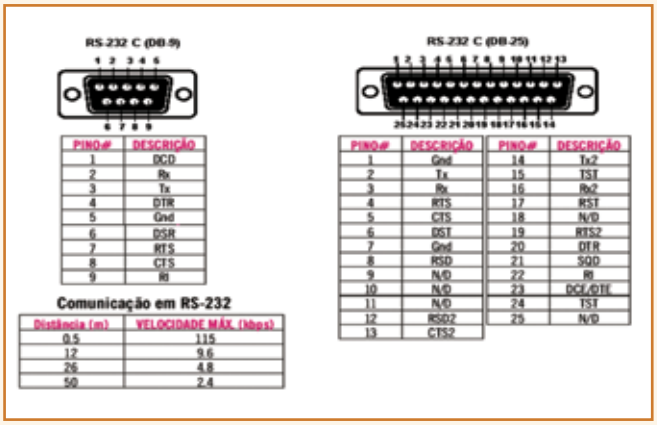

Figura 2 – Camada física EIA 232.

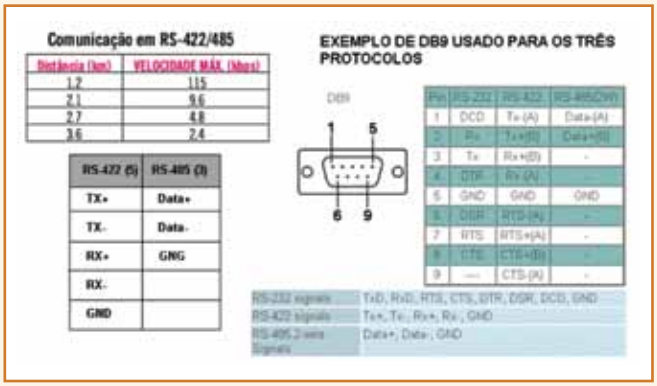

Figura 3 – Camada física EIA – 485.

Protocolo MODBUS

A estrutura da mensagem é sempre a mesma: endereço do escravo, função, quantidade de bytes, dados com 16 bits (bytes high e low) e CRC.

A função é que define o que realmente o protocolo irá fazer. As principais:

Número	Função
01	Read Coils
02	Read Discret Input
03	Read Holding Registers
04	Read Input Registers
05	Write Single Coil
06	Write Single Register

QUERY

Field Name	Example (Hex)	ASCII Characters	RTU 8–Bit Field
Header		: (colon)	None
Slave Address	06	0 6	0000 0110
Function	03	0 3	0000 0011
Starting Address Hi	00	0 0	0000 0000
Starting Address Lo	6B	6 B	0110 1011
No. of Registers Hi	00	0 0	0000 0000
No. of Registers Lo	03	0 3	0000 0011
Error Check		LRC (2 chars.)	CRC (16 bits)
Trailer		CR LF	None
	Total Bytes:	17	8

RESPONSE

Field Name	Example (Hex)	ASCII Characters	RTU 8–Bit Field
Header		: (colon)	None
Slave Address	06	0 6	0000 0110
Function	03	0 3	0000 0011
Byte Count	06	0 6	0000 0110
Data Hi	02	0 2	0000 0010
Data Lo	2B	2 B	0010 1011
Data Hi	00	0 0	0000 0000
Data Lo	00	0 0	0000 0000
Data Hi	00	0 0	0000 0000
Data Lo	63	6 3	0110 0011
Error Check		LRC (2 chars.)	CRC (16 bits)

Figura 4 – Mensagens MODBUS.

Uma das limitações do MODBUS é só possuir envio de informações por integridade, ou seja, uma vez interrogado pelo mestre, todas as informações do mapa de memória são enviados. Por este motivo é utilizado para quantidades pequenas de informações, da ordem de uma centena. Já os protocolos IEC61870-101 e DNP3

possuem características de envio espontâneo e por exceção, que lhes dá um poder muito maior que o MODBUS, como veremos nos itens que seguem.

Originalmente foram definidos mapas de memória para cada função:

• Função 0x04 (Read Input Register): 30001 em diante
(ex: 30015) Transmissão: 30015 –30001 = 14 = 0x0E

• Função 0x03 (Read Holding Register): 40001 em diante
(ex: 40002) Transmissão: 40002 –40001 = 01 = 0x01

Mais recentemente, cada fabricante define seu mapa e inclui no manual do equipamento.

Protocolo IEC60870-101

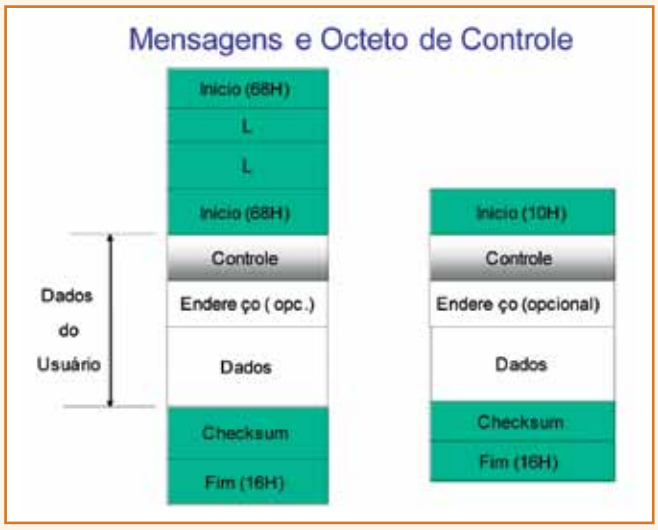

Figura 5 – Telegramas IEC 60870-10 fixo (byte de início = 10) e variável.

A estruturação de um telegrama IEC60870-101 é mais elaborada. Existem caracteres de início e fim de mensagem, comprimento e o octeto (byte) de controle. O processo de aquisição dos dados é feito por meio de varreduras efetuadas pelo mestre nos escravos, e estas ocorrem em períodos típicos de um segundo.

No início existe uma varredura de integridade e, posteriormente, só são enviadas as informações que mudaram (medição que excedeu a banda morta ou disjuntor/seccionadora que abriu/fechou).

Existe o octeto de controle, no qual estão as definições de mensagens que vão da estação primária (mestre), que farão as perguntas, para a estação secundária (escrava), que dará as respostas. Neste estão definidos os bits de controle de fluxo e demanda de acesso.

• Controle de fluxo DFC – Evita uma sobrecarga e perda de informações. Como um IED mestre pode controlar até centenas de IEDs escravos é possível, em situações de perturbações no sistema elétrico, que ocorra avalanches de informações.

• Demanda de acesso ACD – São definidas duas classes de informações para hierarquizá-las de acordo com a importância e frequência de ocorrência. Normalmente pertencem a classe 1 as informações digitais de disjuntores com religamento automático. Classe 2 são as medidas analógicas, que são enviadas quando excedida a banda morta.

Estes dados de controle estão localizados na camada de enlace.

Figura 6 – Octeto de controle.

As informações propriamente ditas, medições analógicas e digitais, são formatadas na camada de aplicação e estão contidas nas estruturas conhecidas como *Aplication Server Data Units* (ASDUs). A formatação destes dados segue as necessidades do processo elétrico. Uma das características fundamentais, a "estampa de tempo", para acompanhamento da "sequência de eventos", está definida nesta camada junto com outras informações do "objeto de dados". Temos o "tipo" da informação, ponto simples, duplo, medições, 8, 16, 32, etiquetas de tempo, etc.

É importante ressaltar que os detalhes da configuração do Protocolo estão em um documento conhecido como "interoperabilidade". Se dois IEDs que utilizam o mesmo Protocolo – mas possuem interoperabilidades diferentes – podem gerar muitos erros de comunicação ou até mesmo não completarem a conexão, isso causa muitos transtornos nos comissionamentos. Fique alerta.

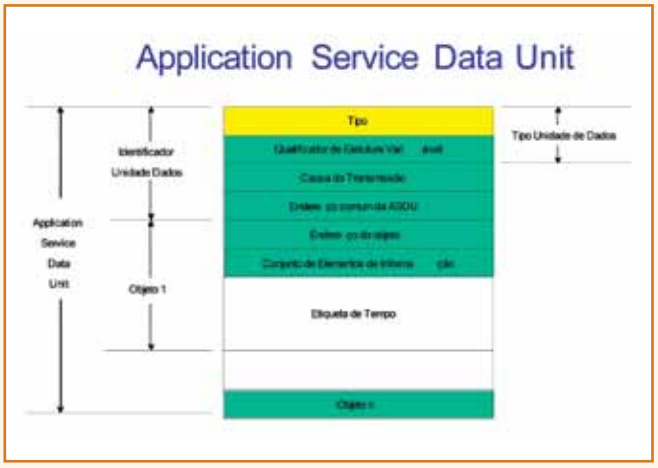

Figura 7 – ASDU – Application Service Data Unit.

As mensagens têm um tamanho típico de 250 bytes, deliberadamente pequena, por se tratar de uma aplicação de tempo real.

Protocolo Distributed Network Protocol (DNP3)

Foi desenvolvido pela GE Harris na década de 1990. Em 1996, a especificação foi liberada para uso público, se tornando um protocolo aberto. Como já indicado no nome – Protocolo de Rede Distribuída –, foi incluído nele o endereço de origem da mensagem (além do endereço de destino, que já estavam presentes no MODBUS e IEC60870-101), permitindo a primeira concepção de rede como conhecemos hoje, consagrada no TCP/IP.

Para o frame DNP3, ou seja, a estrutura da mensagem, foi utilizada a mesma especificação do IEC 60870-101, com octeto de controle, conforme já descrito. Estes recursos estão na camada de enlace. Também foi incluído o conceito de fragmentação de mensagens com o objetivo de permitir o transporte de grandes arquivos.

Apesar destas atualizações, rede e fragmentação, o DNP3 se consolidou no mesmo campo do IEC 61870-101, como Protocolo de Tempo Real, em linhas seriais, com mensagens curtas, de 250 bytes, mestre/escravo com varreduras a períodos típicos de um segundo, envio por exceção, etc.

O protocolo de rede que se tornou predominante foi o TCP/IP.

Na "camada de aplicação", estão definidos os "objetos de dados" que, no DNP3, incluem a variação.

- Objeto de dados. Exemplo: Medição analógica;
- Variação. Exemplo: 16 bits com tag de tempo.

Outra inovação incluída no DNP3 foi o "envio espontâneo de informação". Como analogia, foi dado ao escravo um primeiro item de liberdade.

O escravo pode formatar uma mensagem, sem antes perguntar para o mestre se pode. Com a evolução exponencial dos recursos de hardware, memória e velocidade de CPU, a possibilidade de congestionamento de dados diminuiu bastante. Obviamente, o sistema tem que ser bem projetado e especificado.

O documento que informa o "nível de implementação" do DNP3 é conhecido como perfil do protocolo (Profile), a exemplo da "interoperabilidade" no IEC60870-101. Dois equipamentos, ambos com DNP3, mas com perfis diferentes, podem não se comunicar.

* ***Equipe de engenharia da Schweitzer Engineering Laboratories (SEL)***

CONTINUA NA PRÓXIMA EDIÇÃO
Confira todos os artigos deste fascículo em www.osetoreletrico.com.br
Dúvidas, sugestões e comentários podem ser encaminhados para o e-mail redacao@atitudeeditorial.com.br