O Protocolo Modbus

Vitor Amadeu Souza
vitor@cerne-tec.com.br

Hoje irei abordar com o leitor um dos protocolos mais usados na área industrial, que é o protocolo Modbus.

1. Introdução

O protocolo MODBUS é uma estrutura de mensagem desenvolvida pela Modicon em 1979, usada para estabelecer comunicação entre os dispositivos mestre-escravo / cliente-servidor. Ele é de fato um padrão, muitos protocolos de rede industriais utilizam este protocolo em seu ambiente. O protocolo ModBUS disponibiliza uma padrão de indústria através do método MODBUS para trocar mensagens.

2. Comunicação entre os dispositivos MODBUS

Os dispositivos MODBUS comunicam utilizando a técnica mestre-escravo no qual permite que somente um dispositivo (o mestre) possa iniciar as transações (chamadas de queries). Os outros dispositivos (escravos) respondem de acordo com o pedido do mestre, ou de acordo com a tarefa em questão. Um dispositivo periférico escravo (válvula, drive de rede ou outro dispositivo de medição), que processa a informação e envia o dado para o mestre.

3. Mapa do registrador MODBUS

Os dispositivos MODBUS usalmente incluem um mapara de registro MODBUS. As funções do MODBUS funcionam sobre um registrador de mapa, configuração e controle de módulo I/O. Verifique a referência no mapa de registro do seu dispositivo para obter uma melhor compreensão da operação.

4. Modo de transmissão serial para a rede MODBUS

O modo de transmissão define o conteúdo de bit da mensagem a ser

transmitida na rede e como a informação da mensagem será empacotada na mensagem e descompactada.
O padrão MODBUS emprega os dois modos de transmissão:
ASCII Mode;
RTU Mode.
O modo de trasmissão é usualmente selecionado com outros parâmetros de porta de comunicação serial como baud rate, paridade e etc.

4.1 Modo de transmissão ASCII

No modo de tranmissão ASCII (American Standard Code for Information Interchange), cada byte de caracter em uma mensagem é enviado dois caracteres sem geração de erros.

4.2 RTU (Remote Terminal Unit)

No modo RTU (Remote Terminal Unit), cada mensagem de 8 bits contém dois caracteres hexadecimais de 4 bits.

5 Mensagem de Quadro MODBUS

Um quadro de mensagens é usado para marcar o início e o fim da mensagem permitindo que o dispositivo receptor determine qual dispositivo está sendo endereçado e saber quando a mensagem está completa.
Uma mensagem MODBUS é colocada no quadro e transmitida para o dispositivo. Cada palavra desta mensagem (incluindo o frame) está sendo colocada em um dado de quadro que adiciona um start-bit, stop bit e bit de paridade.
No modo ASCII, a palavra tem o tamanho de 7 bits enquanto no modo RTU a palavra é de 8 bits. Todavia, os 8 bits da mensagem RTU são na verdade 11 bits quando adicionado o bit de start, stop e paridade neste quadro.
Não confunda o quadro de mensagem com o quadro de dados de um único byte (Modo RTU) ou 7 bits de caracter (Modo ASCII). A estrutura do quadro de dados depende do modo de transmissão (ASCII ou RTU). Note que alguns tipos de redes, o protocolo de rede e o quadro de mensagens usam delimitadores de início e fim específicos para a rede.

5.1 Quadro de mensagens ASCII

Modo de mensagens ASCII inicia com um caracter “:” (ASCII 3Ah) e finaliza com um retorn de carro e avanço de linha (CR e LF, ASCII 0Dh e 0Ah). Somente são permitidos caracteres para todos os outros campos como os hexadecimais 0-9 & A-F. Lembre que somente 7 bits significantes são usados para representar a tabela ASCII. Além disso, o modo de dados MODBUS ASCII os caracteres são de somente 7 bits.
Para modo de transmissão ASCII, cada caractere precisa de 7 bits de

dados. Desta forma, cada caracter tem 10 bits quando adicionado o start bit, stop bit e o bit de paridade no quadro de dados.
Em modo ASCII, todas os dispositivos de rede continuam a monitorar a rede para o início de uma mensagem (caracter ":"). Quando ele é recebido, toda os dispositivos de rede decodificarm o próximo campo para determinar se o endereço corresponde com o seu.

5.2 Quadro de mensagens em modo RTU

O modo de mensagens RTU inicia com um intervalo de 3,5 caracter implementado como um caracter múltiplo do taxa de transmissão utilizada pela rede. O primeiro campo transmitido é o endereço do dispositivo. Os caracteres seguintes transmitem todos os campos hexadecimais de 0 a 9 e A a F.
Um dispositivo de rede monitora a rede, incluindo o intervalo de silêncio e quando o primeiro campo é recebido (o endereço) após o intervalo de silêncio de 3,5 caracter, o dispositivo decodifica e determina se este endereço é do dispositivo. Seguindo o último caracter transmitido, um intervalo de tempo similar dee 3,5 caracter finaliza o fim da mensagem e pode iniciar uma nova mensagem após o intervalo.
A mensagem inteira deve ser transmitida continuamente. Se o intervalo de silêncio demorar mais que 1,5 caracter ocorrer antes de completar o quadro, o dispositivo considera a mensagem incompleta e considera o próximo byte como o endereço da nova mensagem.
Em um caso similar, se a nova mensagem iniciar 3,5 caracter antes do início da nova mensagem, o dispositivo receptor assume que ele está continuando com a mensagem prévia. Isto irá gerar uma mensagem de erro, assim como o valor final do campo CRC não será válido para combinar a mensagem.

6. MODBUS Addresses

O endereço do dispositivo mestre específica o dispositivo escravo colocando 8 bits do endereço escravo no campo de endereço da mensagem (RTU mode). O endereço de campo da mensagem conterá dois caracteres (no modo ASCII), ou 8 bits (no modo RTU). Endereços válidos são de 1 até 247. Quando o escravo responde, ele coloca o seu próprio endereço no campo de resposta para deixar o mestre saber que o escravo respondeu.

7. Funções do MODBUS

A função do código de campo da mensagem é colocar dois caracteres (no modo ASCII), ou 8 bits (no modo RTU) que digam ao escravo que ação ele deve tomar. Funções válidas de código valem de 1 até 255, porém nem todos os códigosserão aplicados para o módulo e alguns códigos ficarão reservados para uso futuro.

8. Campo de dados do MODBUS

O campo de dados disponibiliza ao escravo alguma informação necessária pelo escravo para completar a ação específica pelo código da função. O dado é formado de bytes de caracteres múltiplos (um par de caracteres ASCII no modo ASCII), ou de dois dígitos hexadecimais no modo RTU, na faixa de 00h até FFh.

Os dados tipicamente incluem registradores de endereços, contadores de velores e escrita de dados.
Se nenhum erro é encontrado, o campo de dados da resposta do escravo retornará do pedido de dados. Se alguns erros ocorrem, o campo de dado retorna um código de exceção que a aplicação mestre pode usar para determinar a próxima ação a tomar.

9. Checagem de erro MODBUS

A rede MODBUS emprega dosi métodos de erro: checagem de paridade
1. Checagem de paridade do caracter do frame (par, impar, ou sem paridade);
2. Checagem de quadro na mensagem de quadro (CRC no modo RTU ou LRC no modo ASCII).

9.1 Checagem de paridade

Um dispositivo MODBUS pode ser configurado para paridades para ou impar, ou para nenhuma verificação de paridade. Isto determina como o bit de paridade do caracter do frame está configurado.
Se paridade par ou impar estão selecionados, o número de bits 1 do dado de cara caractere será contado. Cada caractere no modo RTU contem 8 bits. O bit de paridade será setado para 1 ou 0, o resultado destas paridades é de 1 bit.

9.2 Checagem de Quadro

LRC

No modo ASCII de transmissão., o caracter de quadro inclui o campo de LRC como o último campo precedente dos caracteres CR e LF. Este campo contém dois caracteres ASCII que representam o resultado do LRC para todos os campos exceto o início do caracter e fim com o par CR e LF.

CRC

O modo de mensagem RTU inclui um método de checagem de erro que é baseado no CRC. O campo de checagem de erro contem um valor de 16 bits (dois de 8 bits) que contem o resultado do calculo de CRC sobre o conteúdo da mensagem.