CONTROLE PARA AUTOMAÇÃO 1º /2005
PROTOCOLO MODBUS

CONRAD ABREU DE A. FONSECA, 99/20650
GUSTAVO GUSMÃO DA HORA, 00/15865
NÉIO LÚCIO S. MOUTINHO, 99/20838

Resumo— Este documento tem como objetivo fazer uma breve descrição do protocolo MODBUS, criado com o intuito de fazer a comunicação entre os mais diversos tipos de aparelhos voltados para os variados tipos de automação, desde automação industrial a comercial.

Palavras-chave— MODBUS, protocolo, automação.

1. Introdução

O protocolo MODBUS foi criado em 1979 pela empresa Modicon. Trata-se de um protocolo para troca de mensagens na camada de aplicação do modelo OSI. Este protocolo visa permitir a comunicação entre diferentes aparelhos interligados em diferentes tipos de rede.

Figura 1: Camadas do modelo OSI.

Com a evolução dos protocolos de rede, o MODBUS também evoluiu permitindo sua integração com diversos tipos de rede existentes, tais como RS232, RS485 e TCP – permitindo a comunicação através de redes Ethernet ou até mesmo através da Internet.

O MODBUS foi criado baseado na arquitetura mestre/escravo, e oferece serviços de acordo com códigos de função. Os códigos de função são elementos de PDU's – *Protocol Data Unit* (Unidade de Dados do Protocolo).

2. Contexto

Em uma rede de automação, todo equipamento pode utilizar o protocolo MODBUS para acionar e/ou iniciar um processo ou uma operação remota. Para cada envio de solicitação de execução de uma ação, uma resposta é dada como retorno, informando o estado daquela solicitação.

Um fator de grande importância para o contínuo uso do MODBUS se encontra no fato dele estar implementado na camada de aplicação, o que torna possível sua integração nos mais variados ambientes de rede. Para que haja integração entre tais tipos de rede, são necessários conversores de protocolo, também chamados de *gateways*.

3. Definições

O protocolo MODBUS define uma simples unidade de dados, chamada de PDU. Este pacote é independente das camadas inferiores de comunicação e está inserido em um outro pacote de informações que varia de acordo com o ambiente. Este pacote mais amplo é chamado de ADU – *Application Data Unit* (Unidade de Dados da Aplicação). Um representação gráfica destes pacotes pode ser visualizada na figura 1.

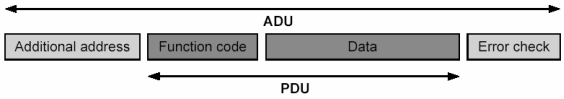

Figura 2: representação do ADU e do PDU.

O ADU é montado pelo aparelho que inicia a transação. O código da função define a ação executada e o pacote de dados integrante porta as informações necessárias para completar a ação. O intervalo de valores para o código da função varia de 1 a 255, sendo que valores acima de 127 são reservados para mensagens de resposta de erros. Para algumas ações, o campo de dados não é necessário, portanto, seu tamanho pode ser de 0 bytes.

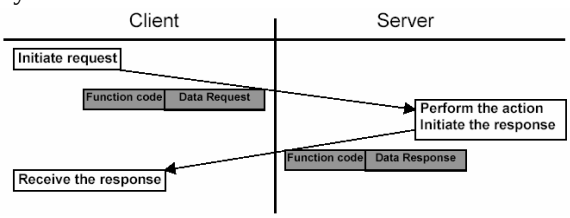

Figura 3: representação de uma transação ocorrida com sucesso.

Quando um erro ocorre no servidor, este retorna uma mensagem contendo um código de função referente ao erro (*function code*) e informações adicionais sobre este (no pacote de dados), como pode ser visto na figura 4.

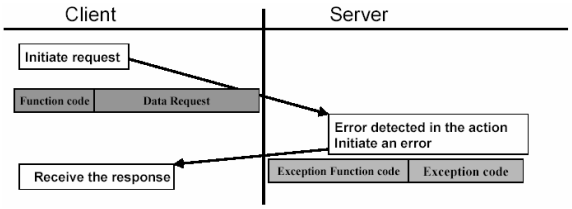

Figura 4: representação de uma transação ocorrida com erro.

O protocolo MODBUS define três PDU's. São eles:

- PDU de solicitação - mb_req_pdu
- PDU de resposta - mb_rsp_pdu
- PDU de resposta com erro - mb_execp_rsp_pdu

4. Modelo de dados

O modelo de dados do MODBUS é baseado em uma série de tabelas com características distintas. As quatro tabelas básicas são: *Discrete Inputs*, *Coils*, *Input Registers* e *Holding Registers*.

A primeira característica que distingue os tipos de dados é o tamanho destes. Os dois primeiros têm um *bit* de tamanho, enquanto os dois últimos têm 16 *bits* (*word*).

Os tipos *discrete inputs* e *Input Registers* são fornecidos por sistemas de *I/O* (entrada/saída), enquanto que os outros dois podem ser alterados pela aplicação.

Todos os dados utilizados em transações via MODBUS devem ser alocados fisicamente em memória, no entanto, a forma de organização desta ação se deve à arquitetura implementada pelo fabricante de cada aparelho.

Um exemplo de arquitetura utilizada para organização dos dados pode ser vista na figura 5. Neste exemplo, temos cada bloco separado fisicamente, uma vez que não há correlação entre eles e cada bloco é acessado por funções específicas.

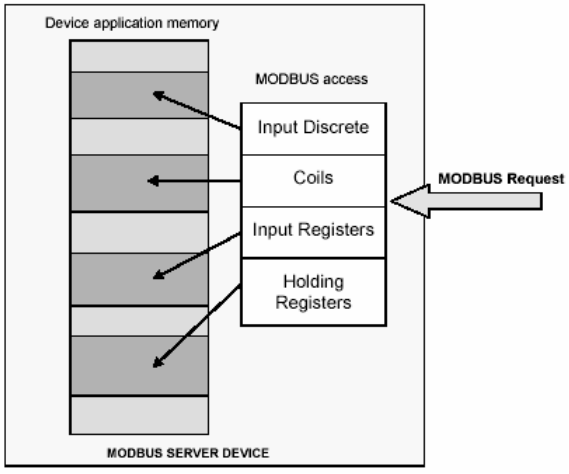

Figura 5: exemplo de organização física de dados.

5. Diagrama de estados

Uma transação via MODBUS tem início quando o cliente solicita ao servidor uma determinada ação, através do envio de um PDU de solicitação (mb_req_pdu). O servidor, ao receber esta PDU inicia uma série de verificações de erros. A cada verificação, caso seja encontrado um erro, o servidor retorna um PDU de resposta com erro, informando a natureza do erro encontrado. Caso não seja encontrado nenhum erro no PDU de solicitação, a ação é executada. Caso tenha sido completada com sucesso, o servidor retorna um PDU de resposta ao cliente. A representação gráfica deste processo, no formato de diagrama de estados, pode ser visualizada na figura 6.

6. Conversores de protocolo

Para que haja uma interconexão entre diferentes ambientes de redes, é necessária a conversão em nível da camada de enlace, alterando o ADU, de forma a adequá-lo ao ambiente de destino. Para executar tal tarefa, existem os chamados *gateways*. Estes aparelhos são a conexão entre as redes distintas e podem funcionar tanto como clientes ou como servidores.

Como já foi dito anteriormente, o PDU é independente do ambiente de rede em que transita, portanto o *gateway* não faz nenhuma alteração neste pacote.

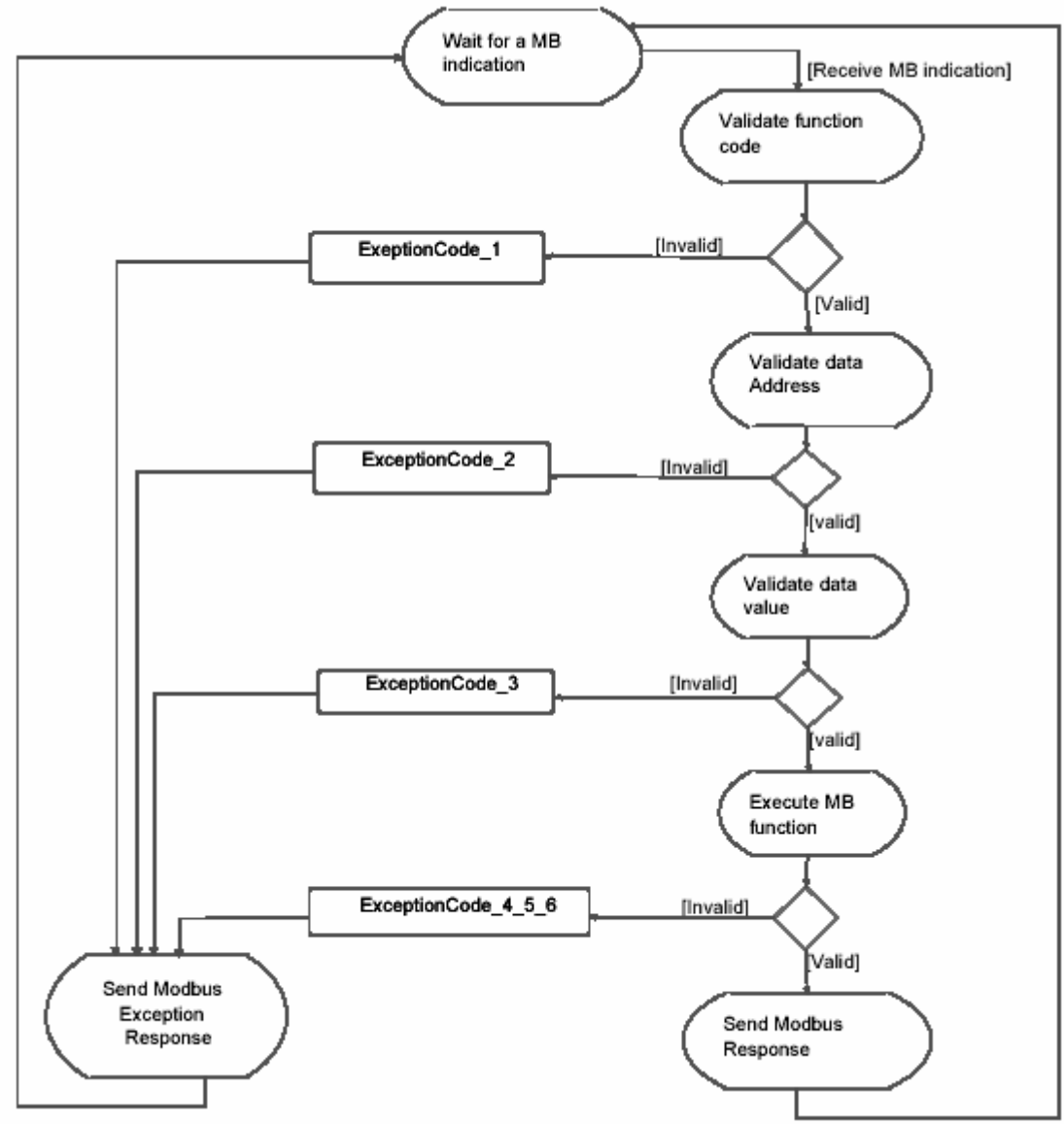

Figura 6: diagrama de estados de uma transação genérica via MODBUS.