



Universidade Federal
de São João del-Rei

Universidade Federal de São João del-Rei

Campus Alto Paraopeba

MODBUS

Aluno (s): Breno Augusto Miranda Valente

Isabelle Mayumi Koga

Pedro Morais Campos Pinto

Rodrigo Ferreira Souza

Wallyson Wesley Lima e Silva

Relatório apresentado a disciplina de Redes Industriais,
ministrada pelo professor Rone Ilídio da Silva, ao
curso de Engenharia Mecatrônica.

Ouro Branco, MG

Novembro de 2018

Automação Industrial

Atualmente, entende-se por automação industrial qualquer sistema, apoiado em equipamentos eletrônicos, que substitua o trabalho humano em favor da segurança, da qualidade, da eficiência produtiva ou da redução de custos.

A automação industrial pode ser entendida como uma tecnologia integradora de três áreas: a eletrônica responsável pelo hardware, a mecânica na forma de dispositivos mecânicos (sensores e atuadores) e a informática responsável pelo software, o qual irá controlar todo o sistema. Pode ser dividida em níveis de abstração, conforme ilustra a figura abaixo.

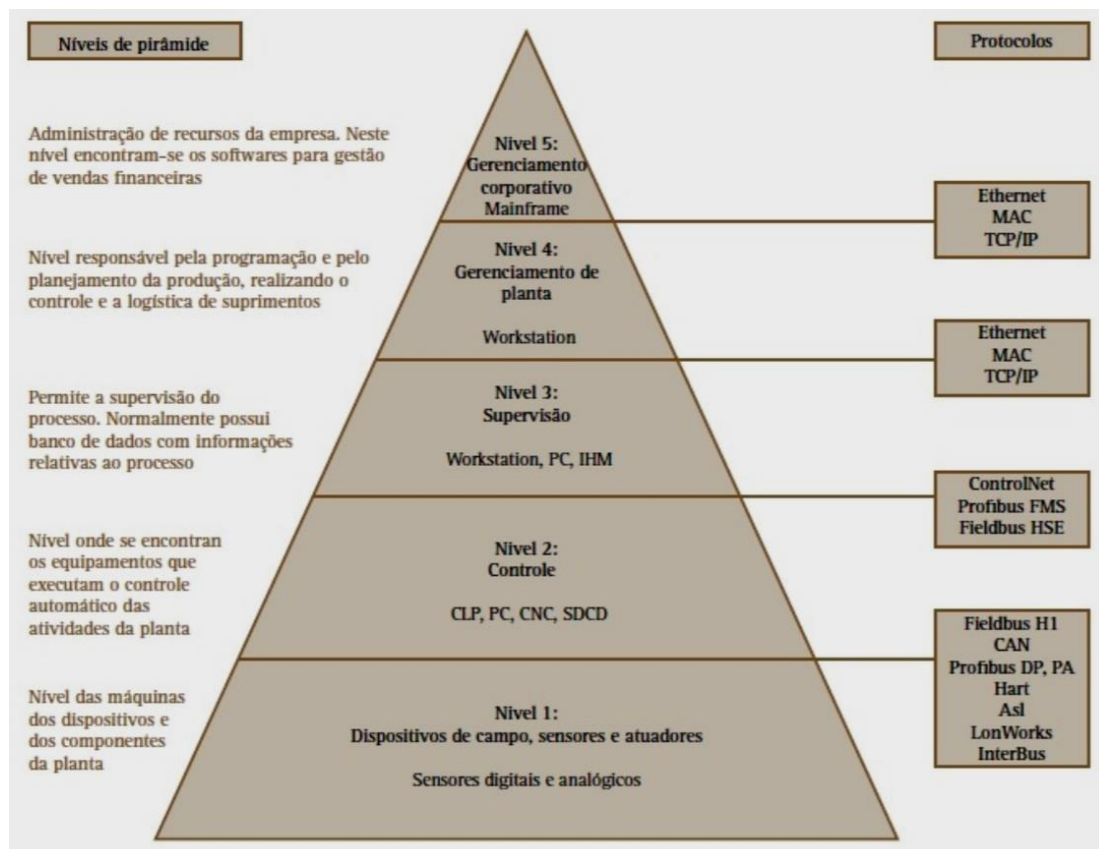


Figura 1 - Níveis de abstração da automação industrial

Nível 1 – Aquisição de Dados e Controle Manual: O primeiro nível é majoritariamente composto por dispositivos de campo. Atuadores, sensores, transmissores e outros dispositivos presentes na planta compõem este nível.

Nível 2 – Controle Individual: O segundo nível compreende equipamentos que realizam o controle automatizado das atividades da planta. Aqui se encontram CLP's (Controlador Lógico Programável), SDCD's (Sistema Digital de Controle Distribuído).

Nível 3 – Controle de Célula, Supervisão e Otimização do Processo: O terceiro nível destina-se a supervisão dos processos executados por uma determinada célula de trabalho em uma planta. Na maioria dos casos, também obtém suporte de um banco de dados com todas as informações relativas ao processo.

Nível 4 – Gerenciamento da Planta: O quarto nível é responsável pela parte de programação e também do planejamento da produção. Auxilia tanto no controle de processos industriais quanto também na logística de suprimentos.

Nível 5 – Planejamento Estratégico e Gerenciamento Corporativo: O quinto e último nível da pirâmide da automação industrial se encarrega da administração dos recursos da empresa. Neste nível encontram-se softwares para gestão de venda, gestão financeira e BI (Business Intelligence) para ajudar na tomada de decisões que afetam a empresa como um todo.

Redes Industriais

As redes industriais surgiram com a necessidade de se realizar a comunicação entre dispositivos de campo e controladores lógicos programáveis (CLP), permitindo-se, portanto, a aquisição de informações sobre estes dispositivos e reduzindo-se a utilização de cabos de comunicação para cada instrumento. Desta maneira, com uma rede industrial, é possível que apenas um cabo trafegue informações entre uma grande quantidade de instrumentos, sendo essa quantidade definida de acordo com o protocolo utilizado.

Além de realizar entre dispositivos de campo e controladores lógicos programáveis, as redes industriais também permitem a comunicação com sistemas supervisórios e sistemas de gerenciamento de produção.

Percebe-se a clara divisão entre os níveis da pirâmide da automação: nível de campo, onde se encontram dispositivos como sensores e atuadores; nível de controle, onde se encontra o PLC com sua respectiva rede de controle; nível de supervisão, onde os equipamentos estão conectados na rede de supervisão e nível de gerenciamento da planta.

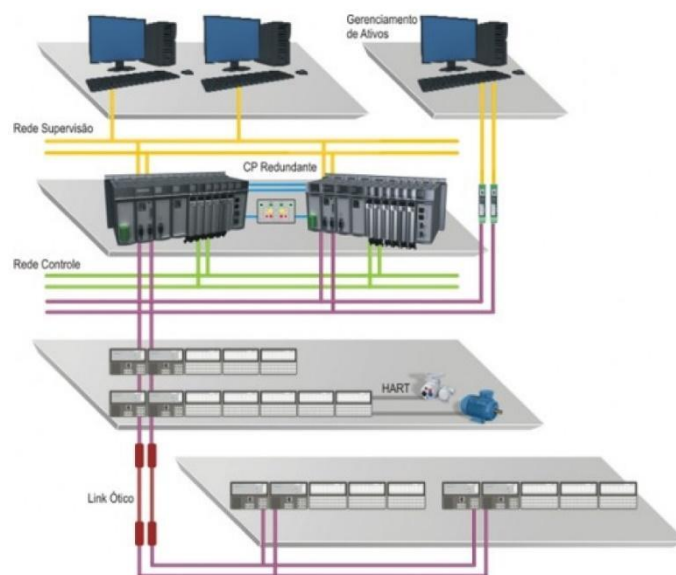


Figura 2- Arquitetura típica de um sistema automatizado

O conceito de redes de comunicação consiste em 2 ou mais equipamentos conectados entre si para que possam compartilhar informações. Os tipos de dados compartilhados dependem da aplicação e dos equipamentos utilizados. Em uma rede de comunicação industrial a comunicação acontece normalmente da seguinte maneira:

- Tipicamente um dispositivo A realiza algum questionamento ou comando para um dispositivo B;
- O dispositivo B processa a informação e retorna uma resposta indicando sucesso ou não da solicitação;
- Caso o dispositivo B não responda, o dispositivo A finaliza a comunicação após certo período de tempo, conhecido como timeout.

A estrutura de uma rede em que existe um tráfego de informações e a maneira como os dispositivos estão interligados é definida como topologia. As topologias utilizadas em redes industriais são:

- **Topologia Barramento**

Possui a organização mais simples de uma rede, todos os dispositivos estão ligados a uma mesma linha de transmissão através de cabo. Apesar de os dados não passarem por dentro de cada um dos nós, apenas um dispositivo pode enviar os dados no barramento num dado momento.

Neste tipo de topologia a comunicação é feita por broadcast, isto é, os dados são enviados para o barramento e todos os dispositivos veem esses dados, no entanto, eles só serão recebidos pelo destinatário.

Quando um dispositivo estiver a transmitir um sinal, toda a rede fica ocupada e se outro computador tentar enviar outro dado ao mesmo tempo, ocorre uma colisão e é preciso reiniciar a transmissão.

Esta topologia tem a vantagem da facilidade de instalação. Por outro lado, é extremamente vulnerável, já que se o cabo principal falhar, toda a estrutura colapsa.

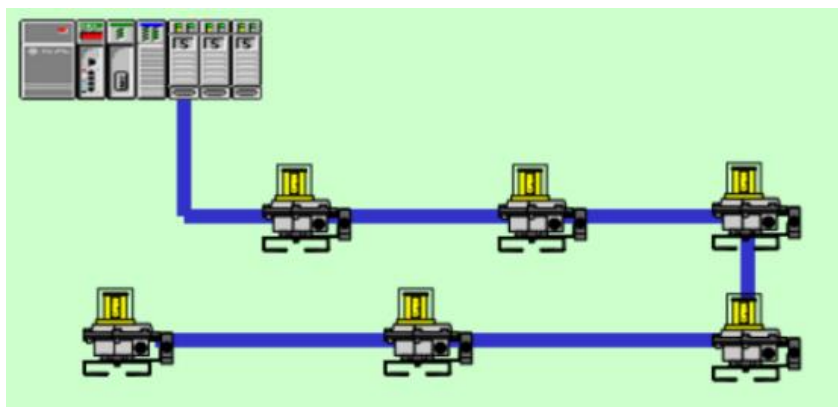


Figura 3 - Topologia Linha ou Barramento

- **Topologia Anel**

Na topologia em anel os dispositivos são conectados através de um circuito fechado, em série. Os dados são transmitidos unidirecionalmente, sendo enviada por um dispositivo, que passa por outros dispositivos, através das retransmissões, até ser processada pelo dispositivo de destino. Ocorre um atraso em cada dispositivo devido ao processamento dos dados.

Esse tipo de topologia possui a desvantagem de que caso ocorra uma falha em um dispositivo todo o restante da rede será afetado.

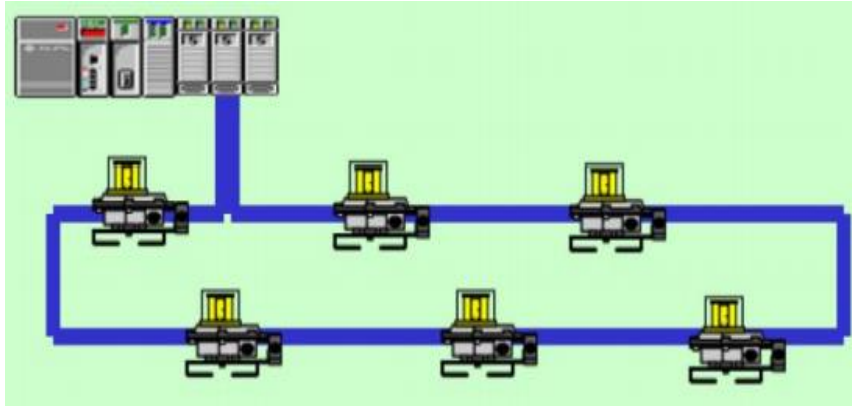


Figura 4 - Topologia Anel

- **Topologia Estrela**

A topologia em estrela é caracterizada por um dispositivo central que "gerencia" o fluxo de dados da rede, estando diretamente conectado (ponto-a-ponto) a cada dispositivo. O dispositivo central encarrega-se de encaminhar o sinal especificamente para as estações solicitadas, economizando tempo.

Caso ocorra falha de um dispositivo o restante da rede não será afeta, mas se o dispositivo central falhar toda a rede será afetada. Por esse motivo, são utilizados dispositivo em duplicidade, redundância, para garantir confiabilidade para o sistema.

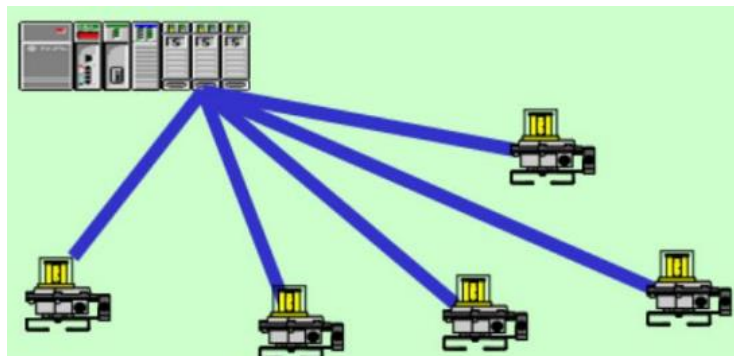


Figura 5 - Topologia Estrela

- **Topologia Árvore**

Existe apenas um caminho para se chegar a um nó, sendo assim não existem problemas de distribuição (roteamento), porém se qualquer conexão for quebrada, interrompe-se a comunicação porque não há rotas alternativas.

Um exemplo de redes em estruturas em árvore acontece frequentemente em sistemas de fabricação onde diferentes processos de diferentes níveis devem alimentar

de informações um computador de nível hierárquico superior para fins de gerenciamento, controle e planejamento.

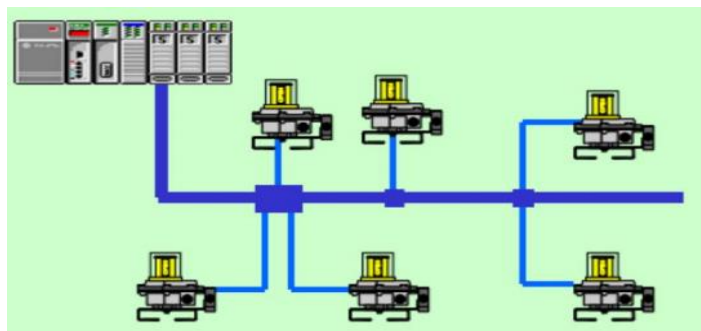


Figura 6 - Topologia Árvore

Redes Modbus

Modbus foi desenvolvida pela Modicon (que se tornou Schneider Electric) em 1979 e posteriormente se transformou em um protocolo aberto. É um protocolo de requisição-resposta, e por ser totalmente aberta é utilizada em qualquer equipamento industrial ou aplicações que não estão no ambiente industrial que necessitam realizar uma comunicação de leitura e escrita. Utiliza o RS-232, RS-485 ou Ethernet como meio físico.

O padrão RS-232 ou EIA-232, é utilizado em comunicações do tipo ponto a ponto, admitindo-se, portanto, apenas dois dispositivos na rede, no caso do Modbus representa um mestre e um escravo. Esse padrão possui uma taxa de comunicação de aproximadamente 115Kbps, podendo haver em alguns casos taxas maiores, a distância máxima entre dispositivos da rede é de aproximadamente 30m.

O padrão RS-485 ou EIA-485 possui uma taxa de comunicação de 50Mbps, e uma distância máxima da rede em torno de 1200m e número máximo de 32 dispositivos por barramento. É importante lembrar que a velocidade de comunicação da rede está associada ao seu comprimento, portanto, quanto maior o comprimento da rede, menor a velocidade de comunicação.

O padrão Ethernet no protocolo Modbus, pode chegar a uma taxa de comunicação de 100Mbps ou até 10Gbps e sua distância pode variar de 100m até aproximadamente 200m dependendo do tipo de cabo e das condições de instalações. Em alguns casos é possível a utilização de cabos de fibra ótica e utilização wireless, permitindo alcançar distâncias maiores e melhores taxas de comunicação.

Funcionamento

Esse protocolo utiliza um relacionamento mestre-escravo. Em um relacionamento assim, a comunicação sempre ocorre em pares (um dispositivo inicia a requisição e então aguarda por uma resposta). O dispositivo que iniciador é chamado de mestre, e tipicamente é uma IHM (Interface homem-máquina) ou um sistema SCADA (Supervisory Control and Data Acquisition) e o escravo é um sensor, CLP (Controlador lógico programável) ou CPA (Controlador programável para automação), ou seja, o processo consiste em uma estação mestre que envia mensagens solicitando dos escravos que enviem os dados lidos pela instrumentação ou a estação mestre envia sinais a serem escritos nas saídas para o controle dos atuadores.

A figura 1 abaixo, demonstra um exemplo de rede Modbus.

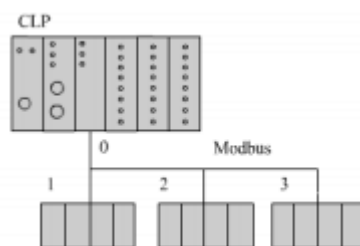


Figura 7 - Exemplo de Rede Modbus. ^[4]

De acordo com a figura 7, observa-se que essa rede Modbus é constituída de um mestre no caso um CLP, e 3 escravos que podem ser atuadores, sensores entre outros. Em cada ciclo de comunicação, o CLP lê e escreve valores em cada um dos escravos. É importante salientar que como o sistema de controle de acesso é do tipo master-escravo, os módulos escravos só iniciam a comunicação para responder as solicitações do mestre.

As interações mestre-escravo podem ser realizadas de duas maneiras. A primeira é denominada Unicast e é composta por duas mensagens: Uma mensagem do mestre realizando um pedido a um escravo de forma individual e uma mensagem do escravo retornando a mensagem ao mestre. É importante ressaltar que cada escravo deve possuir um único endereço, conhecido como SlaveID. Já a segunda maneira é denominada Broadcast, o mestre pode enviar um pedido a todos os escravos e nenhuma resposta é devolvida para transmitir os pedidos enviados pelo mestre e ao contrário do Unicast, o escravo não envia uma resposta ao mestre. Os pedidos enviados pelo mestre são,

necessariamente, a escrita de comandos. No Broadcast todos os dispositivos devem permitir a transmissão para a função de escrita, e o endereço 0 é reservado para identificar a troca de transmissão.

Os dados são enviados em bits, onde cada bit é enviado como uma tensão, sendo a tensão positiva equivalente ao bit 0, e a tensão negativa equivalente ao bit 1, como demonstrado na figura 6 abaixo.

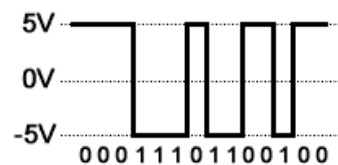


Figura 8 - Envio de dados. ^[5]

Os dados são armazenados no escravo em quatro tabelas diferente, onde duas tabelas armazenam valores discretos como on/off das bobinas e as outras duas tabelas armazenam valores numérico que seriam os registros. Ou seja, duas tabelas do tipo apenas leitura e duas tabelas do tipo leitura-escrita.

Números Bobinas/Registros	Endereço do Dado	Tipo	Nome da Tabela
1-9999	0000 to 270E	Read-Write	Saídas Discretas (Bobinas)
10001-19999	0000 to 270E	Read-Only	Entradas Discretas (Contatos)
30001-39999	0000 to 270E	Read-Only	Registros de Entradas Analógicas
40001-49999	0000 to 270E	Read-Write	Registros de Saídas Analógicas

Figura 9 - Armazenamento de dados no Modbus. ^[5]

De acordo com a figura 9, observa-se que cada tabela pode possuir até 9999 valores, cada bobina ou contato atribui 1 bit um endereço entre 0000 e 270E, e que cada registro é uma palavra (word) de 16 bits e, portanto, pode ter endereço de dados entre 0000 e 270E.

A aquisição e reposta utilizado no protocolo Modbus é realizada da seguinte forma:

- Mensagem de consulta: O mestre envia uma mensagem ao escravo informando qual tabela deve ser acessada para que a ação desejada seja realizada. Os bytes de dados possuem informações para o escravo e posteriormente o campo de verificação é utilizado afim de que o escravo valide seus dados recebidos.
- Mensagem de reposta: O código da função é repetido de volta ao mestre. Os bytes de dados possuem os dados coletados pelo escravo ou o seu estado. Caso ocorra um erro, o código de função é modificado afim de indicar que a reposta é uma resposta de erro, assim, os bytes de dados possuirão um código que descreverá o erro. A verificação de erro permite ao mestre validar os dados recebidos.

Variações do Modbus

- **Modbus RTU** - O Modbus RTU é o protocolo que utiliza para a transmissão e decodificação para o formato binário. Esse protocolo apresenta a maior densidade de caracteres porque não apresenta bits de paridade (servem para identificação de erros) e outras informações juntas com cada caractere.

O formato dos pacotes que são transmitidos pode ser visto na figura 10 abaixo:

Address	Function	Data	CRC Check
8 bits	8 bits	N x 8 bits	16 bits

Figura 10 - Formato ModbusRTU

Os dados podem ter um tamanho de 0 a 252 bits. Para a verificação de erro é utilizado um método chamado de CRC que é baseado no resto da divisão polinomial dos bits de dados e essa divisão é novamente realizada pelo receptor da mensagem e deve bater com os bits do CRC Check, caso contrário é considerado que a mensagem foi corrompida.

- **Modbus ASCII** - Contrário ao RTU que utiliza formato binário o ASCII utiliza os caracteres da tabela ASCII. Cada palavra desse formato é composto de 10 bits que 1 bit é para dar o start, 7 bits que identifica os caracteres, 1 bit de paridade (caso exista) e dependendo se houver o bit de paridade podem existir 1 ou 2 bits de stop. O formato da mensagem pode ser visto na figura 11 abaixo:

Start	Address	Function	Data	LRC Check	End
1 char	2 chars	2 chars	n chars	2 chars	2 chars CRLF

Figura 11 - Formato Modbus ASCII

- **Modbus TCP** - O protocolo Modbus TCP utiliza um sistema que encapsula as informações que seriam enviadas em frames TCP, assim pode utilizar o cabo Ethernet e o protocolo CSMA-CD para controlar como as informações serão transmitidas. O formato dessa mensagem possui um cabeçalho específico que é chamado de MBAP (Modbus Application Protocol).

MBAP	Function code	Data
------	---------------	------

Figura 12 - Formato Modbus TCP

- **Modbus Plus** - O Modbus Plus é um protocolo de rede peer-to-peer de alta velocidade baseado em comunicação de passagem de token. Os nós do Modbus Plus acessam a rede após o recebimento de um quadro de token. Após isso, ele pode iniciar transações com outros dispositivos na rede. Além disso, essa versão possui vários recursos adicionais de roteamento, diagnóstico, endereçamento e consistência de dados.

No lado negativo, o Modbus Plus ainda é mantido sob domínio da Schneider Electric e só pode ser implantado sob licença deste fabricante.

Referências

- [1] Comparativo entre Redes de Automação Industrial e suas Características
- [2] <https://www.embarcados.com.br/protocolo-modbus/>
- [3] <http://www.ni.com/white-paper/52134/pt/>
- [4] [http://www.politecnica.pucrs.br/professores/tergolina/Redes_e_Protocolos_Industriais/APRESENTACAO - Aula_09_Modbus.pdf](http://www.politecnica.pucrs.br/professores/tergolina/Redes_e_Protocolos_Industriais/APRESENTACAO_-_Aula_09_Modbus.pdf)
- [5] <https://www.citisystems.com.br/modbus/>

