

Capítulo

# 2

# Arquiteturas de sistemas de automação - Uma introdução

Autor: Prof. Constantino Seixas Filho  
Universidade Federal de Minas Gerais - Departamento de Engenharia Eletrônica

## Introdução

O Primeiro passo ao se conceber uma solução qualquer de automação é desenhar a arquitetura do sistema, organizado seus elementos vitais: remotas de aquisição de dados, PLCs, instrumentos, sistema de supervisão, etc. em torno de redes de comunicação de dados apropriadas. A escolha da arquitetura irá determinar o sucesso de um sistema em termos de alcançar os seus objetivos de desempenho, modularidade, expansibilidade etc.

As soluções irão depender das limitações de cada projeto em particular.

Existem vários pontos que o projetista deve verificar ao iniciar o projeto.

O melhor é estabelecer um *check list* de pontos importantes a serem verificados:

- Quantas são as áreas de processo ? Quais as distâncias entre as áreas ? Qual o *lay out* da instalação industrial ?
- Haverá uma sala de controle centralizada ou apenas púlpitos de comando locais ?
- Existe necessidade de um sistema de backup ? A que nível ?
- Quais são as condições ambientais ? Existe campo magnético intenso nas proximidades ? Existe interferência eletromagnética ?
- O cliente está familiarizado com novas tecnologia de redes de campo para instrumentação, sensores e acionamentos ?
- Existem sites fora da área industrial que devam ser conectados à planta ? Escritório central, centros de distribuição, unidades remotas como britagens móveis, instalações portuárias, etc. ?
- Quais as necessidades dos dispositivos em termos da velocidade de transmissão de dados ?
- Qual a capacidade de expansão dos módulos prevista para os próximos anos ?
- Existe preferência quanto ao atendimento aos padrões internacionais ou preferência por redes proprietárias ?

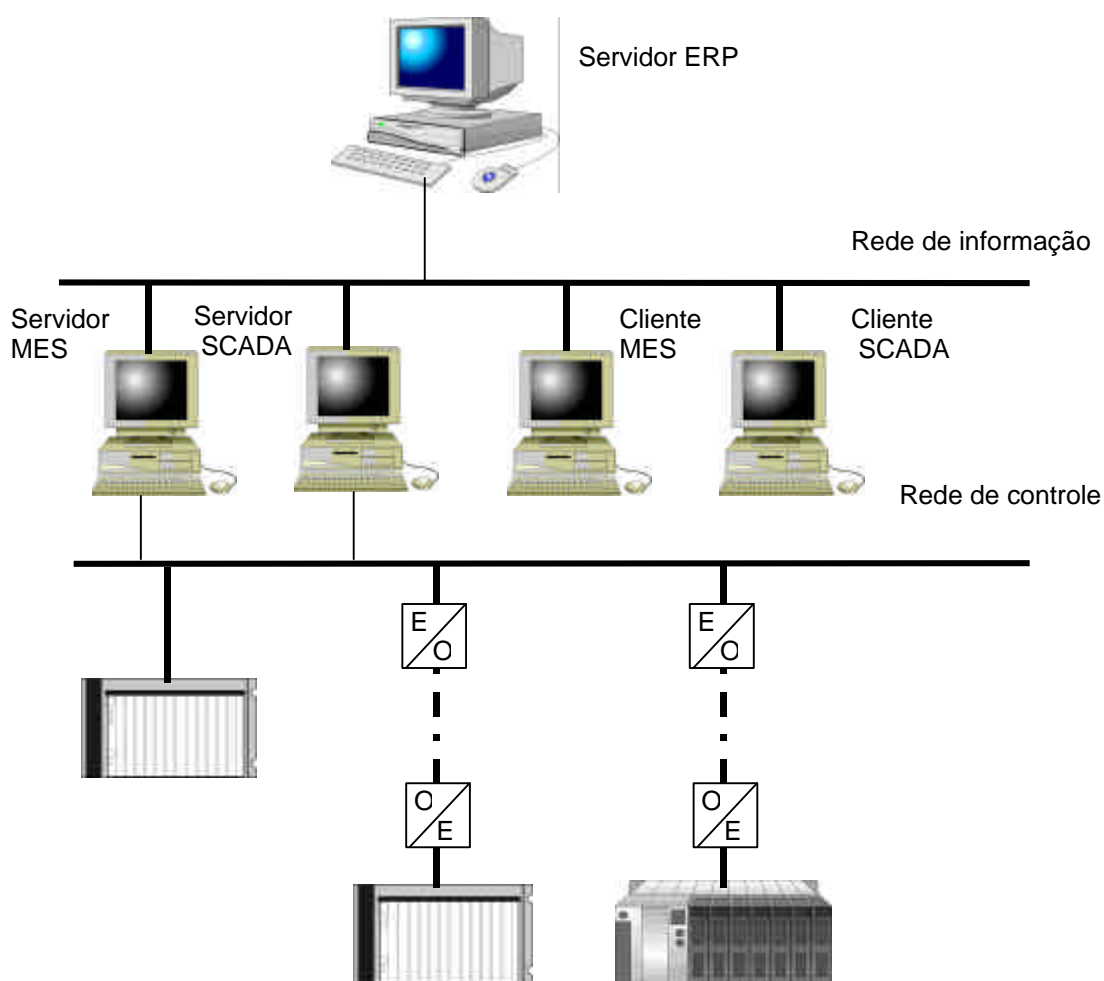
Uma das arquiteturas mais praticadas é a que define duas hierarquias de redes: uma rede de informação e uma rede de controle.

## Rede de informação

O nível mais alto dentro de uma arquitetura é representado pela rede de informação. Em grandes corporações é natural a escolha de um *backbone* de grande capacidade para interligação dos sistemas de ERP (*Enterprise Resource Planning*), *Supply Chain* (gerenciamento da cadeia de suprimentos), e EPS (*Enterprise Production Systems*). Este *backbone* pode ser representado pela rede ATM ou GigaEthernet ou mesmo por uma Ethernet 100-BaseT, utilizando como meio de transmissão cabo par trançado nível 5. Esta última rede vem assegurando uma conquista de espaço crescente no segmento industrial, devido à sua simplicidade e baixo custo.

## Rede de controle

Interliga os sistemas industriais de nível 2 ou sistemas SCADA aos sistemas de nível 1 representados por CLPs e remotas de aquisição de dados. Também alguns equipamentos de nível 3 como sistemas PIMS e MES podem estar ligados a este barramento. Até dois anos atrás o padrão mais utilizado era o Ethernet 10Base-T. Hoje o padrão mais recomendado é o Ethernet 100Base-T. Quase todos os grandes fabricantes de equipamentos de automação já possuem este padrão implementado.

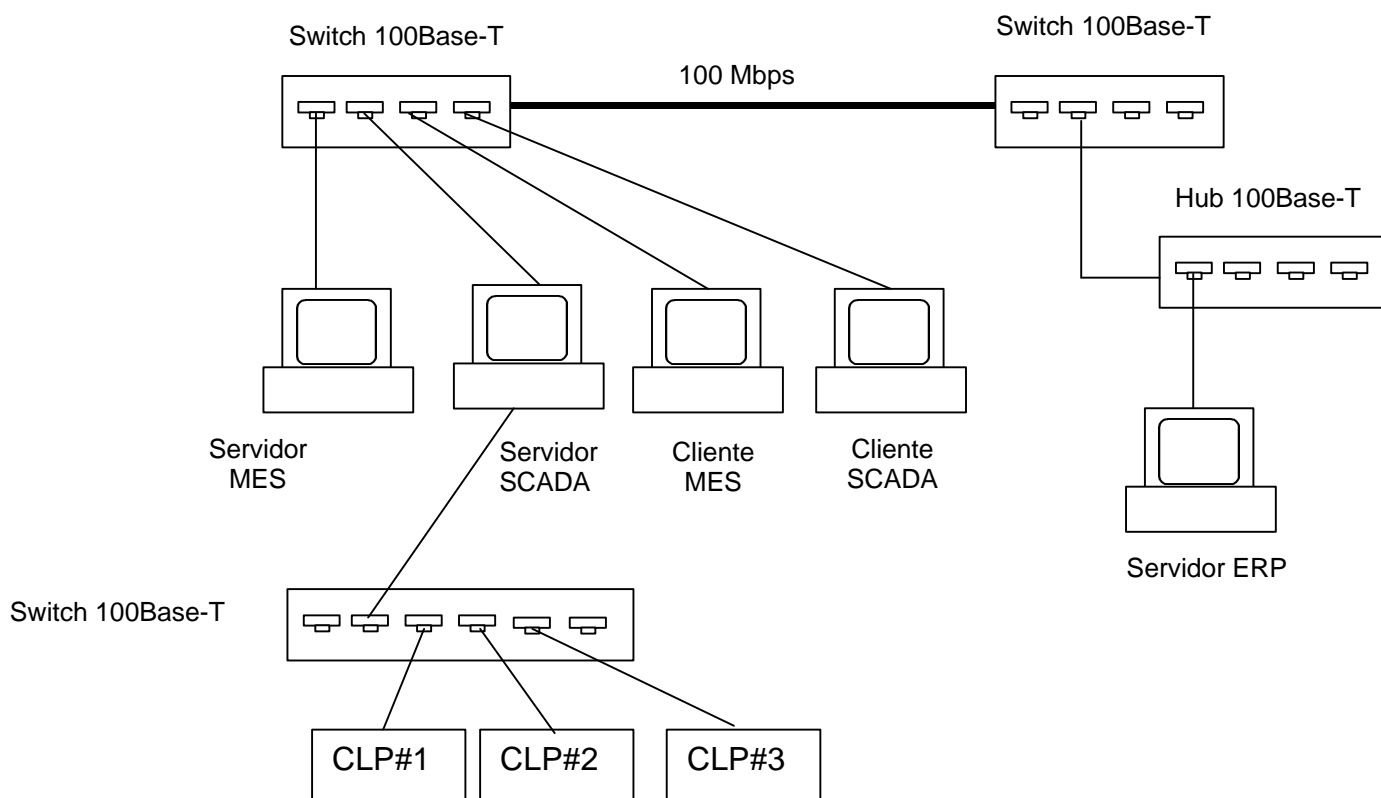


**Figura 1 - Arquitetura de uma rede de duas camadas - Unifilar**

As estações clientes se comunicam com seus servidores através da rede de informação. As estações Servidores se comunicam com os CLPs através da rede de controle.

Do ponto de vista de segurança, é interessante isolar o tráfego de controle do tráfego de informação através de equipamentos de rede. Hoje o equipamento mais utilizado para este fim é o switch Ethernet e o padrão mais utilizado é o 100Base-T. Além de evitar os problemas de divisão de banda, típico da arquitetura barramento, o switch segmenta a rede. O switch assegura a criação de uma rede

Ethernet livre de colisões. Esta nova concepção de rede é denominada de rede Ethernet Industrial

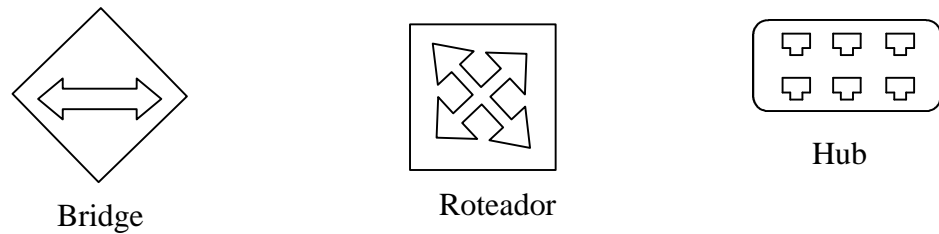


**Figura 2 - Arquitetura de uma rede de duas camadas (figura incluindo equipamentos de rede)**

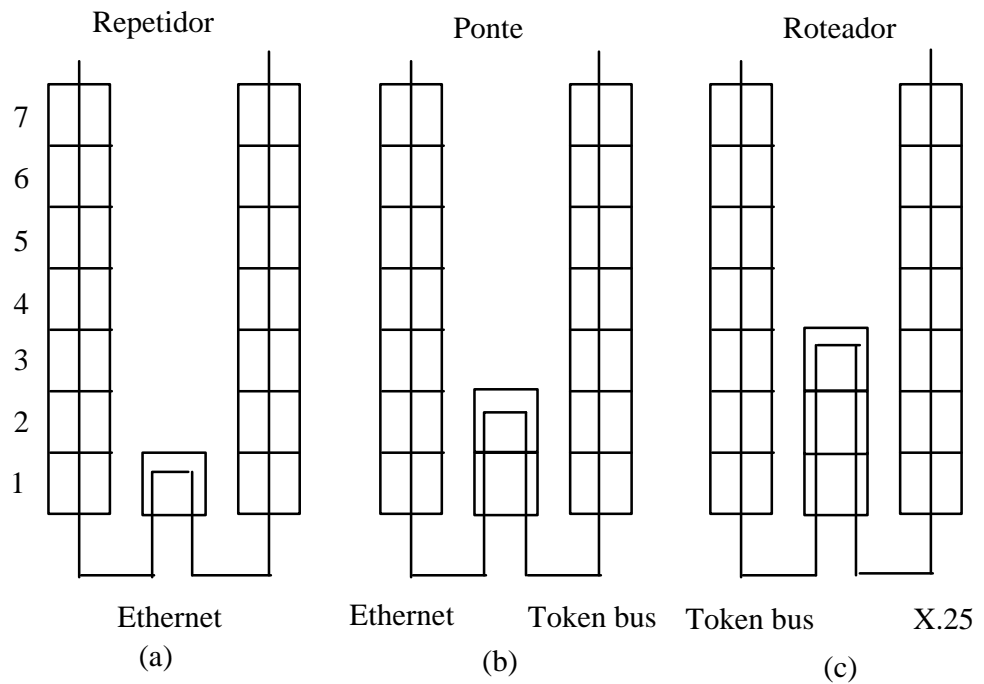
### **Equipamentos de integração de redes.**

- Repetidor (*Repeater*): Dispositivo não inteligente que simplesmente copia dados de uma rede para outra, fazendo que as duas redes se comportem logicamente como uma rede única. São usados para satisfazer restrições quanto ao comprimento do cabo, por exemplo.
- Distribuidores de conexão (*Hubs*): Servem para conectar os equipamentos que compõem uma LAN. Os equipamentos interligados a um hub pertencem a um mesmo segmento de rede, isto é os usuários do hub dividem a largura da banda. Se tivermos 10 usuários em um segmento de 100Mbps, cada usuário usufruirá em média de 10Mbps de banda de passagem. Cada hub possui de 4 a 24 portas 10Base-T com conectores RJ-45.
- Ponte (*Bridge*): Segmenta uma rede local em sub-redes com o objetivo de reduzir tráfego ou converter diferentes padrões de camadas de enlace (Ethernet para Token Ring por exemplo)
- Roteador (*Router*) Usado para interligar duas redes que possuem a mesma camada de transporte, mas camadas de rede diferentes. Os roteadores decidem sobre qual caminho o tráfego de informações (controle e dados) deve seguir.

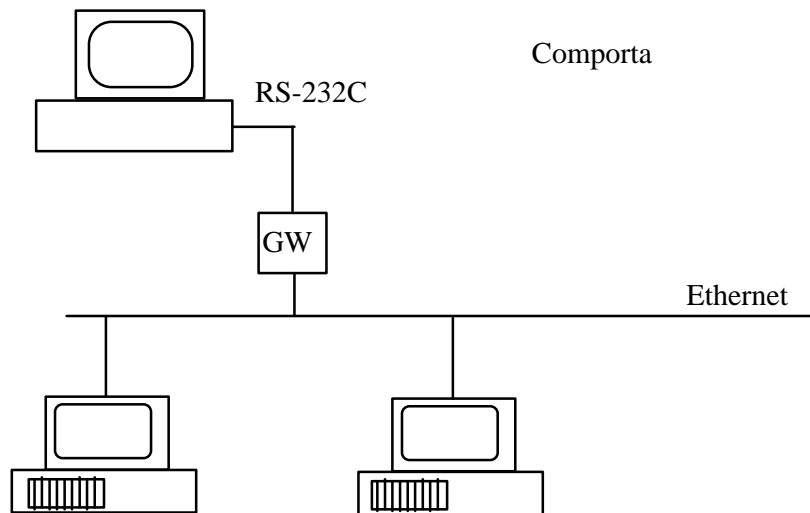
- Comporta (*Gateway*) Usado para dar acesso à rede a um dispositivo não OSI.
- *Switch*. São os dispositivos de mais amplo espectro de utilização, para segmentar a rede a baixo custo, sem necessidade de roteamento. Sua maior limitação está em não permitir *broadcasting* entre segmentos.



**Figura 3: Outras formas de representação dos equipamentos de rede**



**Figura 4: Conexão entre redes**

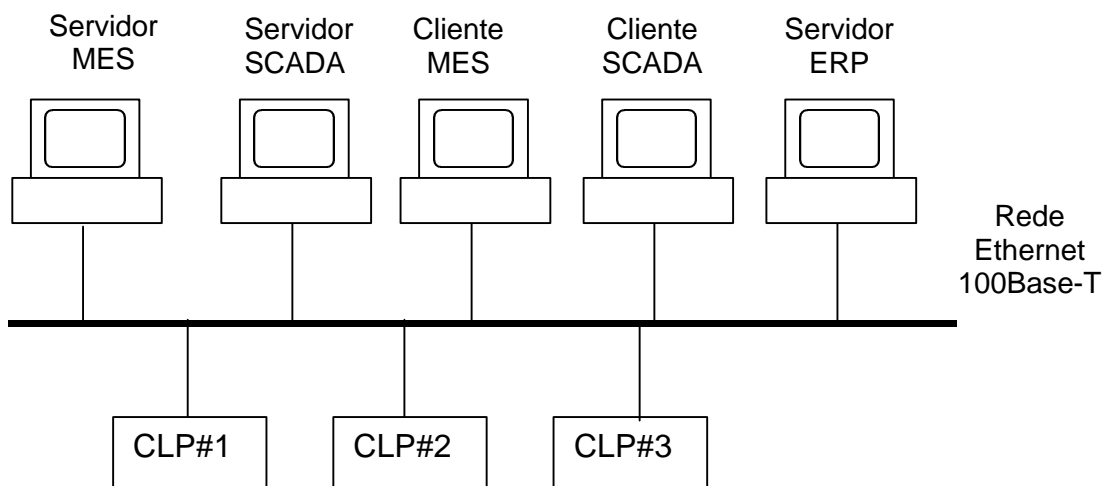


**Figura 5: Uso de gateway**

### Arquitetura de rede única.

As redes de controle e informação também podem estar fundidas em uma rede única. Esta topologia apresenta os seguintes inconvenientes:

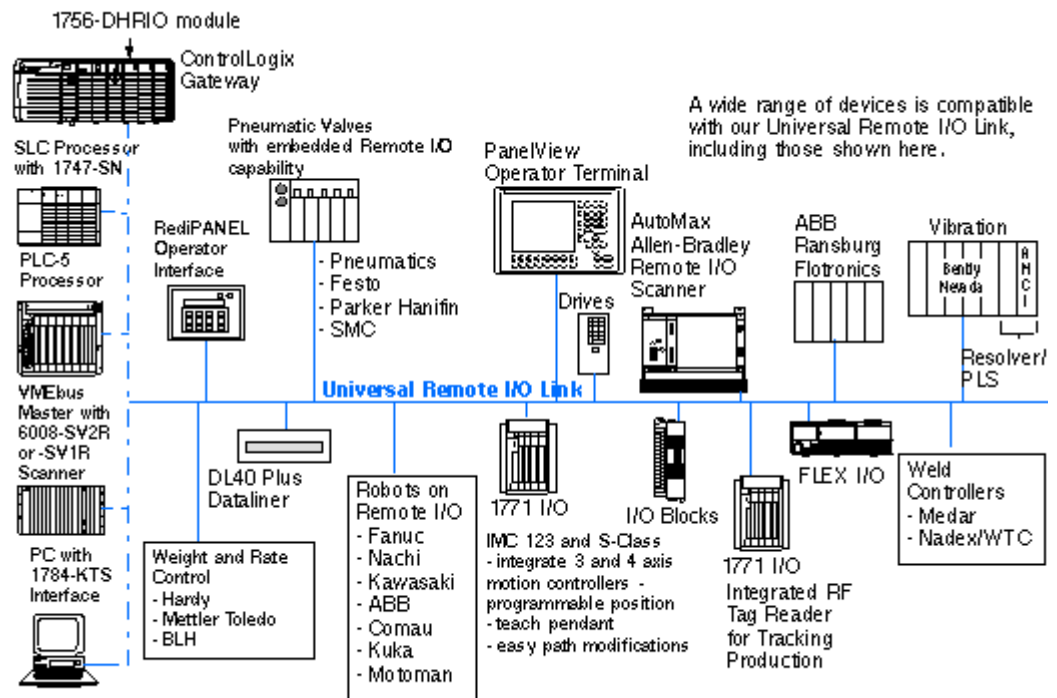
O tráfego na rede de controle é de natureza diversa do tráfego na rede de informação, caracterizando-se por mensagens curtas e muito frequentes. O tráfego da rede de informação é em geral representado por arquivos maiores transmitidos com baixa frequência. Os requisitos de performance e segurança das duas redes também são diferentes. Embora este tipo de topologia seja muito utilizado, a topologia anterior é mais recomendada por segmentar cada tipo de tráfego.



**Figura 6 - Barramento único**

## Redes proprietárias

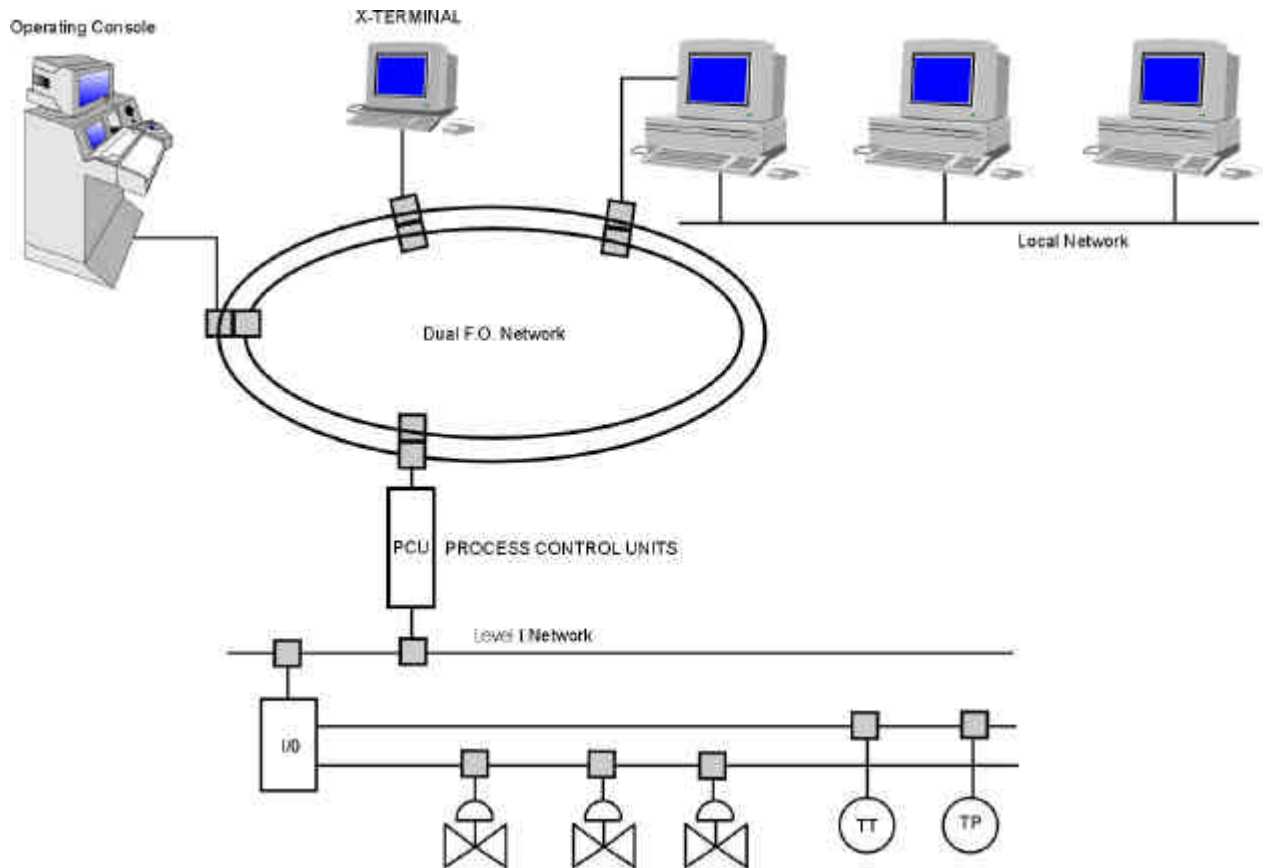
Apesar da rede Ethernet ser hoje a preferida da área industrial muitas redes proprietárias de concepção mais antigas são ainda muito usadas. Por exemplo a rede DH+ (*Data Highway plus*) da Rockwell.



**Figura 7: Exemplo de rede proprietária de nível 1: Remote IO da Rockwell**

## Arquitetura de um SDCD

Os SDCDs tradicionais se caracterizavam por um elevado nível de redundância: redundância de servidores, redundância de rede de comunicação de dados, de cartões de entrada e saída, etc. Além disso, possui sofisticados algoritmos de diagnóstico, que permitem localizar o cartão defeituoso a partir da console de operação. OS cartões de E/S com defeito podem ser trocados a quente.

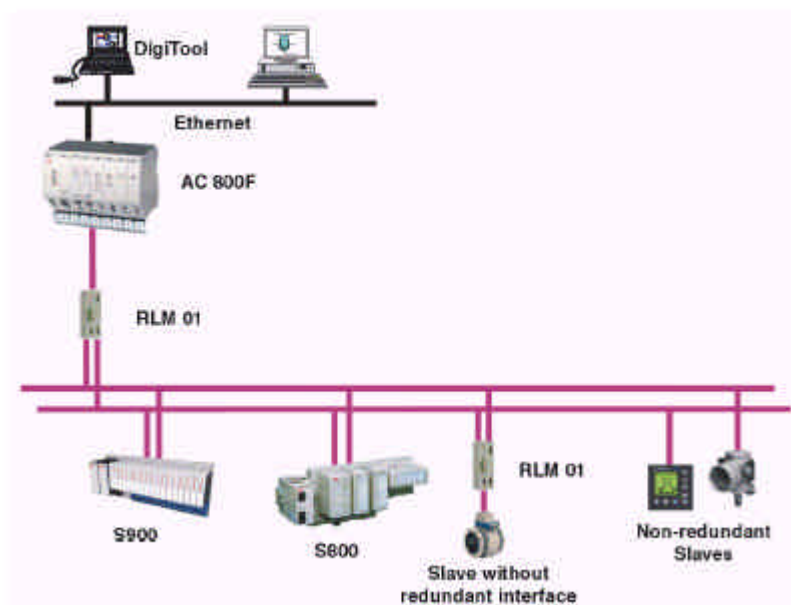


**Figura 8: Configuração de um SDCD**

## Sistemas híbridos

Atualmente os SDCDs têm um sucesso peso leve. Conhecido como sistema híbrido, este novo sistema alia a versatilidade e performance de um SDCD com o baixo custo de uma solução SCADA + CLP. São exemplos desta classe de sistema o INDUSTRIALIT (OPERATEIT/ CONTROLIT) da ABB, o Plant Web da Emerson e o PSC7 da Siemens.





**Figura 9: Sistema híbrido da ABB com rede Profibus redundante**

## Requisitos desejados para a arquitetura

Ao se fazer um projeto de automação, estamos interessados em requisitos de desempenho tais como:

### Redes de sensores e comandos:

1. Baixo tempo de varredura para leitura cíclica de todos os dispositivos em rede.
2. Determinismo no tempo.
3. Exigência para algumas aplicações de uma rede com topologia em anel com *self-healing* ou outro tipo de redundância, de tal forma que um cabo partido não interrompa todo o circuito.
4. Capacidade de comandar vários dispositivos sincronamente (*multicasting*, *broadcasting*).
5. Capacidade de expansão futura.
6. Obediência a padrões internacionais (padrão aberto).
7. Facilidade de aquisição de instrumentos de múltiplas fontes.
8. Possibilidade de utilização de meio óptico para uso externo, fora das salas elétricas.
9. Disponibilidade de sensores/atuadores do tipo desejado na aplicação dentro da tensão desejada (média tensão/ baixa tensão).

No caso de uma aplicação de CCM inteligente, o número máximo de nós suportados e o tempo máximo de resposta são quesitos de máxima importância.

### Redes de dados (informação e controle):

1. Padrão internacional e de fato (Ethernet 100Base-T é a melhor referência).
2. Alto desempenho medido pela velocidade de transmissão.
3. Capacidade de expansão futura

4. Possibilidade de uso de fibra ótica
5. Possibilidade de adição de redundância.

## O Protocolo OPC

Um dos grandes problemas de se interfacear equipamentos e sistemas no chão de fábrica reside em se compatibilizar os protocolos da camada de aplicação. O MMS - *Manufacturing Message Specification* foi uma tentativa de padronização que entretanto fracassou por falta de adeptos. O padrão OPC foi inicialmente liderado pela Microsoft e especificado pela *OPC Foundation*. Este protocolo é hoje o padrão de fato da indústria. Imagine como faríamos para interfacear um sistema SCADA com um CLP há 3 anos atrás. Imagine que este supervisor fosse o Factory Link da US Data e que o CLP fosse uma CPU da família 5 da Rockwell. O Factory Link era fornecido em várias versões, para diversos sistemas operacionais. O CLP 5 pode se comunicar com diversas redes diferentes, por exemplo com uma rede DH+. O PC pode utilizar cartões de comunicação Rockwell, Sutherland-Schultz ou outro. O número de combinações é muito grande. Na prática, nós teríamos que utilizar ou desenvolver um drive que atendesse perfeitamente à combinação: Sistema SCADA (existem dezenas) / sistema operacional (várias opções), cartão de comunicação PC/CLP (várias fontes e possibilidade de rede). Isto implicava na existência de centenas de drives de comunicação, que só atendiam a versões específicas da combinação de fatores apresentada acima. O protocolo OPC elimina esta situação. Um fabricante de CLP sempre fornecerá com o seu equipamento um servidor OPC. O fabricante de SCADA também fornecerá o cliente OPC. O mesmo acontece com um fornecedor de inversores, de relés inteligentes ou de qualquer outro dispositivo industrial inteligente. Um sistema SCADA também pode oferecer um servidor OPC para comunicação com outro sistema de aquisição de dados, por exemplo, um PIMS.

Como as aplicações precisam apenas saber como buscar dados de um servidor OPC, ignorando a implementação do dispositivo e o servidor precisa fornecer dados em um formato único: servidor OPC, a tarefa de escrever drives de comunicação fica muito facilitada.

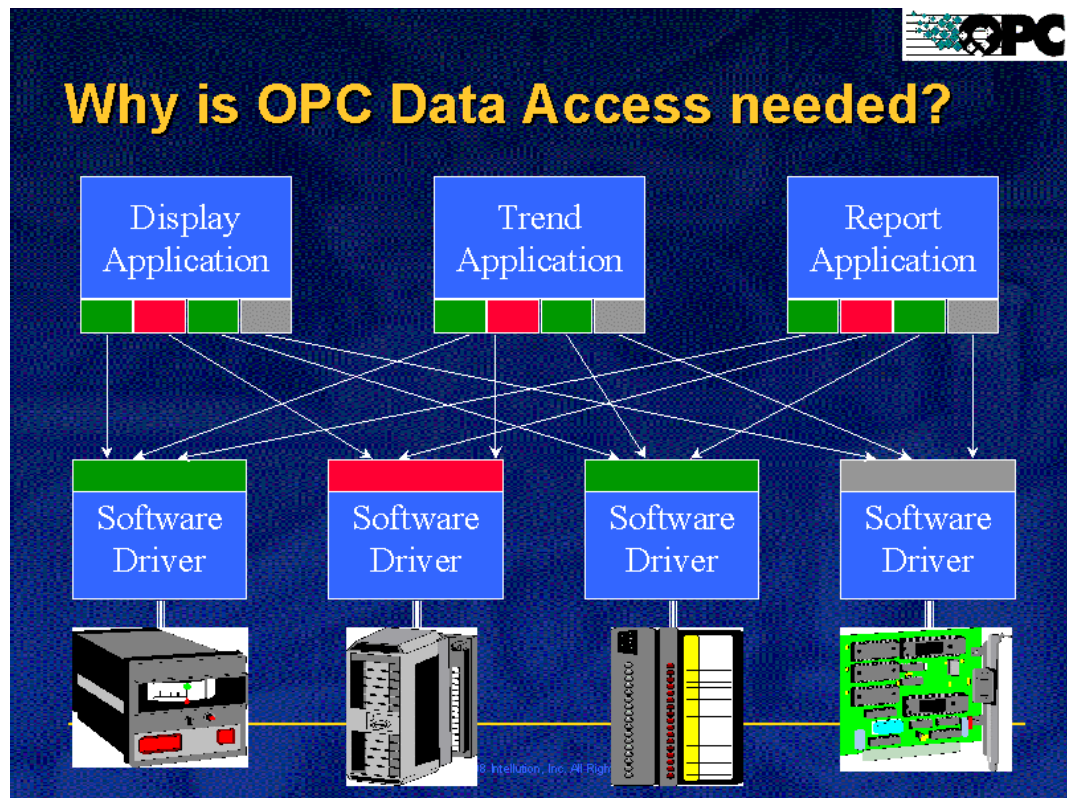


Figura 10: Acesso a dados de processo ponto a ponto antes do protocolo OPC

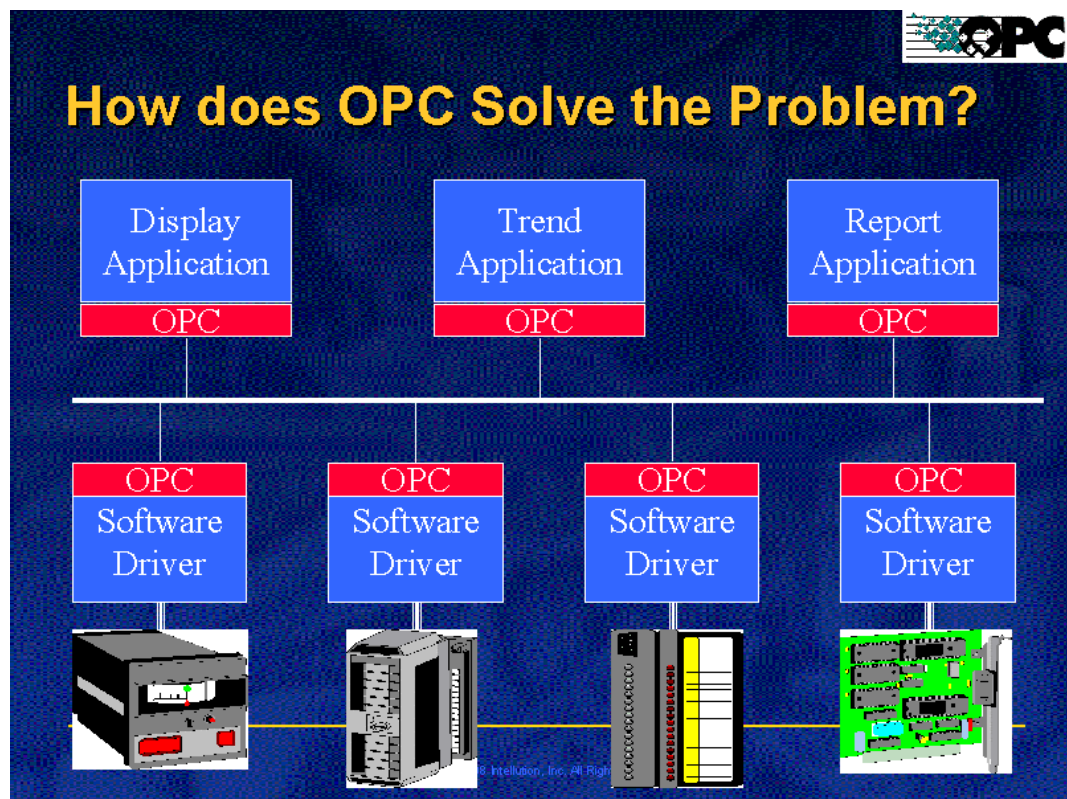


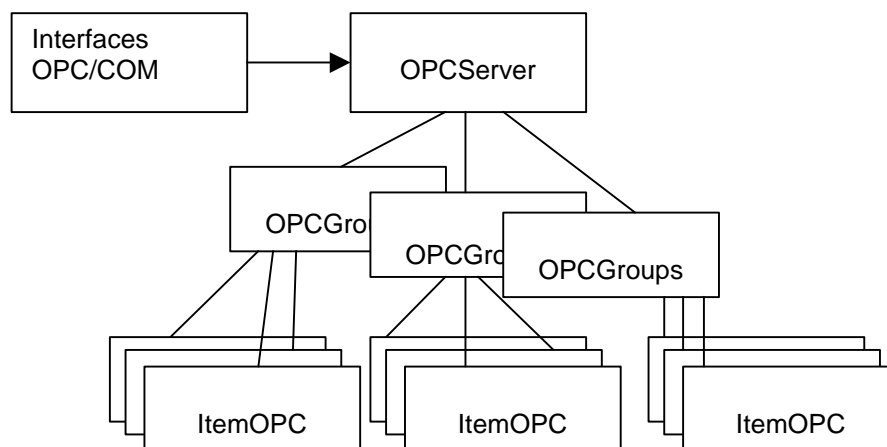
Figura 11: Acesso a dados de processo com protocolo OPC

Quais os tipos de dados providos pelo servidor OPC ? O servidor OPC fornece dados de tempo real proveniente de sensores (temperatura, pressão, etc.), comandos de controle (abrir, fechar, ligar, desligar, etc.), status de comunicação, dados de performance e estatística do sistema, etc. O protocolo OPC é baseado no modelo de componentização criado pela Microsoft e denominado COM (*Componet Object Model*), uma maneira eficiente de se estabelecer interfaces para aplicações que substitui as chamadas de procedimento e as DLL usadas inicialmente para encapsular uma aplicação. O nome OPC: OLE for Process Control foi cunhado na época em que o COM era um modelo embrionário de comunicação entre aplicativos como o nome de OLE (*Object Linking and Embedding*).

O padrão OPC é baseado em comunicações cíclicas ou por exceção. Cada transação pode ter de 1 a milhares de itens de dados, o que torna o protocolo muito eficiente, superando o MMS para aplicações práticas, segundo técnicos da divisão Powertrain da GM. O protocolo OPC não resolve o problema de nomes globais. Você deve saber exatamente em que servidor uma dada variável pode ser encontrada. As especificações do protocolo OPC estão disponíveis no sítio da OPC Foundation e incluem além da especificação básica para a construção de drives (*OPC Data Access Specification* - versão 2.05) outras especificações tais como padrão OPC para comunicação de alarmes e eventos (*OPC Alarms and Events Specification* - Versão 1.02), padrão OPC para dados históricos (*OPC Historical Data Access Specification* - Versão 1.01). padrão OPC para acesso de dados de processo em batelada (*OPC Batch Specification* - versão 2.00) e outros.

O servidor OPC é um objeto COM. Entre suas funções principais ele permite à aplicação cliente:

- Gerenciar grupos: Criar, clonar e deletar grupos de itens, renomear, ativar, desativar grupos.
- Incluir e remover itens em um grupo.
- Navegar pelas tags existentes (*browser interface*).
- Ver os atributos ou campos associado a cada tag.
- Definir a linguagem de comunicação (país) a ser usada.
- Associar mensagens significativas a códigos de erro
- Obter o status de funcionamento do servidor
- Ser avisada, caso o servidor saia do ar.



**Figura 12: Grupos e Itens OPC**

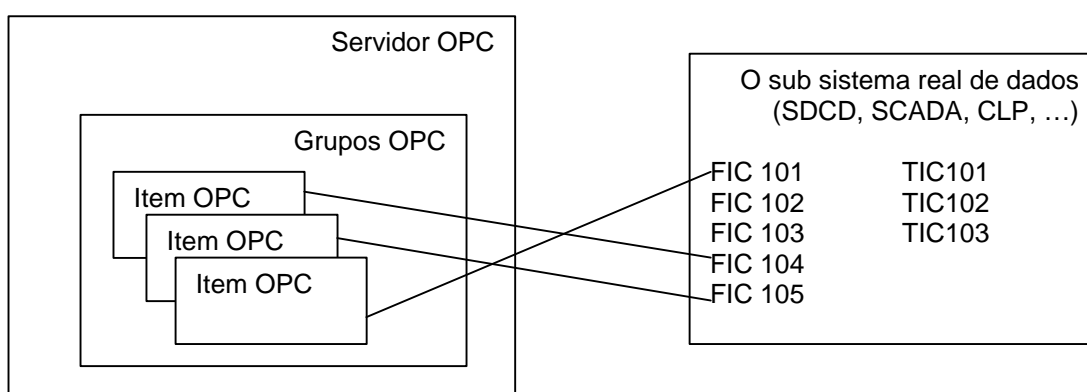
O grupo de dados constitui uma maneira conveniente da aplicação organizar os dados de que necessita. Cada grupo de dados pode ter uma taxa de leitura específica: pode ser lida periodicamente (*polling*), ou por exceção. O grupo pode ser ativado ou desativado como um todo. Cada tela sinóptica, receita, relatório, etc., pode usar um ou mais grupos.

A interface de grupo permite à aplicação cliente:

- Adicionar e remover itens dos grupos.
- Definir a taxa de leitura do dado no grupo.
- Ler e escrever valores para um ou mais itens do grupo.
- Assinar dados do grupo por exceção.

Cada item é um objeto OPC que proporciona uma conexão com uma entrada física de dados. Cada item fornece ao cliente informação de: valor, *time stamp*, qualidade do dado e tipo de dado. É possível definir um vetor de objetos como um único item. Isto otimiza a comunicação de dados já que apenas, um *time stamp* e uma palavra de qualidade de dados é utilizada para cada conjunto de dados.

As leituras de dados podem ser de três tipos: leitura cíclica (*polling*), leitura assíncrona (o cliente é avisado quando a leitura se completa) e por exceção (assinatura). As duas primeiras trabalham sobre listas (subconjuntos) de um grupo e o serviço de assinatura envia aos clientes qualquer item no grupo que mudar de valor.



**Figura 13: Mapeando itens OPC em variáveis de processo**

## Redes de campo

Os CLPs são usados para ler os sensores discretos ou digitais e os valores dos instrumentos analógicos.

Caso uma rede digital não seja usada, os sinais de campo serão conectados aos cartões de entrada e saída dos CLPs. Os sinais discretos são codificados na faixa de 0 a 24VCC ou 0-110VAC ou 0-220VAC. Já os sinais analógicos são geralmente codificados na faixa de 0 a 20 mA ou de 0-10V.

## Redes digitais:

Outra alternativa é o uso de uma rede digital de instrumentos e sensores. Este tipo de rede atende pelo nome genérico de *fieldbus* ou barramento de campo. Na verdade, devemos dividir estes tipos de rede em 3 tipos diferentes:

**Redes de sensores ou Sensorbus** - são redes apropriadas para interligar sensores e atuadores discretos tais como chaves limites (*limit switches*), contactores, desviadores, etc. São exemplos de rede Sensorbus: ASI da Siemens, Seriplex, CAN e LonWorks.

**Redes de Dispositivos ou Devicebus** - são redes capazes de interligar dispositivos mais genéricos como CLPs, outras remotas de aquisição de dados e controle, conversores AC/DC, relés de medição inteligentes, etc.

Exemplos:

Profibus-DP, DeviceNet, Interbus-S, SDS, LonWorks, CAN, ControlNet, ModbusPlus.

**Redes de instrumentação ou fieldbus** - São redes concebidas para integrar instrumentos analógicos no ambiente industrial, como transmissores de vazão, pressão, temperatura, etc, válvulas de controle, etc.

Exemplos:

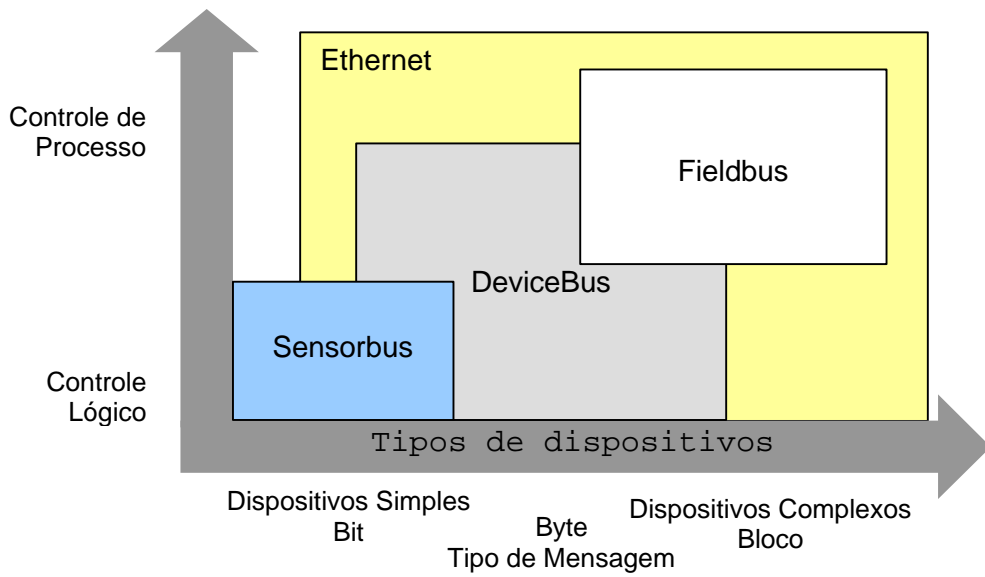
IECSP50-H1, HART, WorldFIP, Profibus-PA.

### Padronização internacional

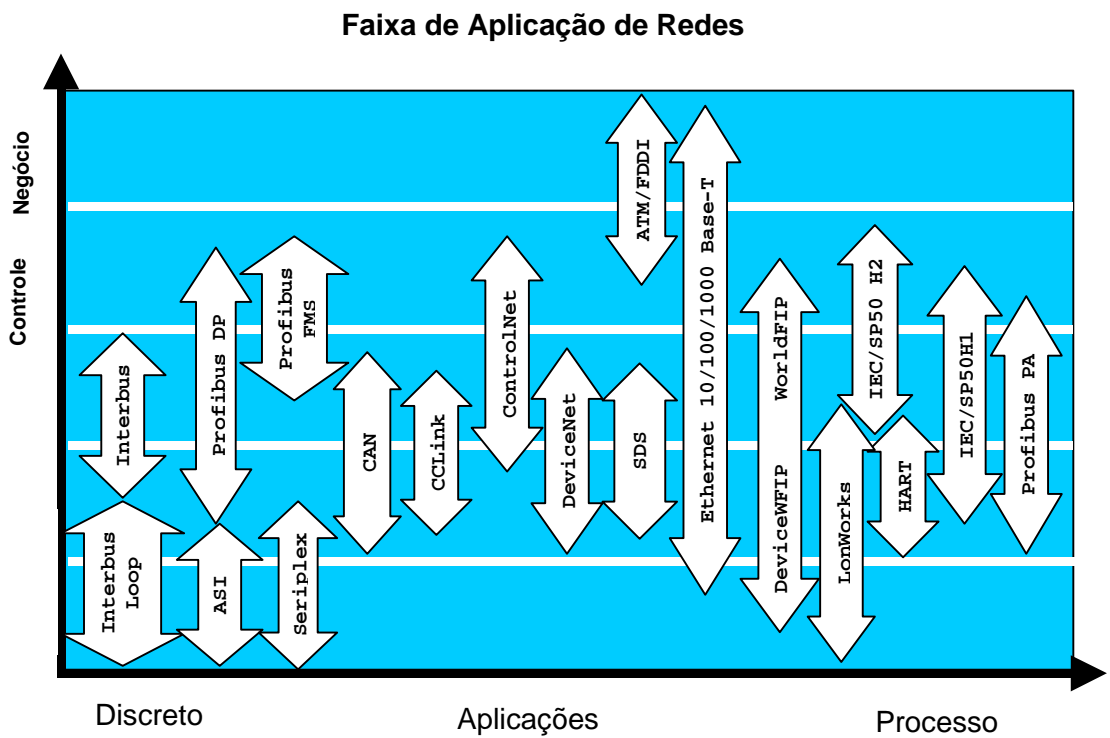
Hoje o standard Fieldbus está padronizando 8 famílias de redes:

<b>Tipo</b>	<b>Nome Comercial</b>
1	Fieldbus (mesmo que ANS/ISA S50.01)
2	ControlNet
3	Profibus
4	P-NET
5	Fieldbus Foundation HSE
6	SwiftNet
7	WorldFIP
8	Interbus

Existe forte tendência de todas estas redes venham a utilizar a Ethernet como plataforma básica num futuro próximo e que adotem forte orientação a objetos através de blocos de função padrões.

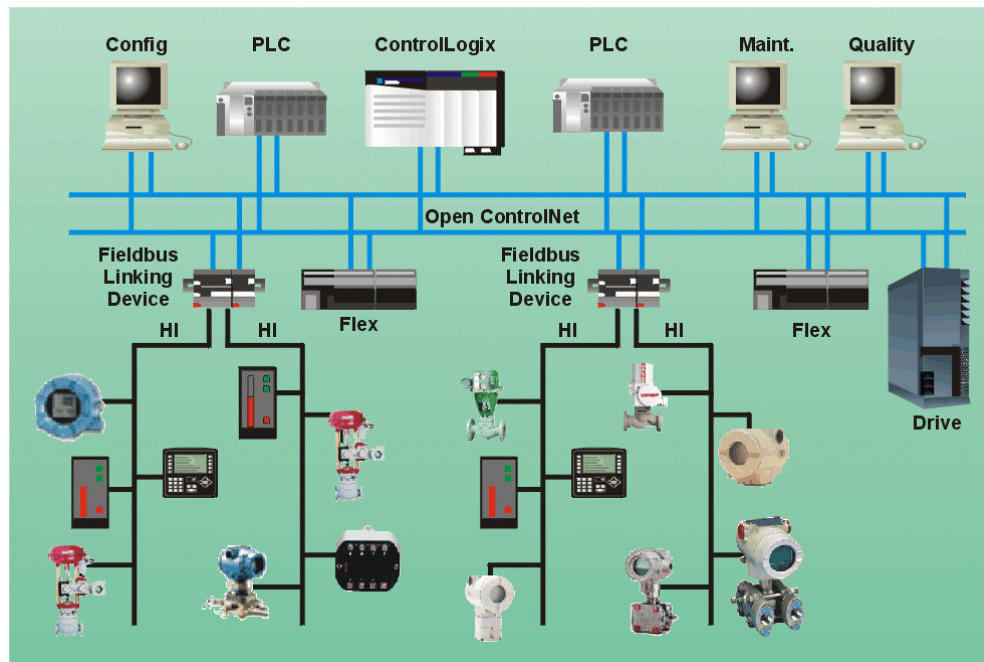


**Figura 14: Tipos de redes de campo segundo ARC**

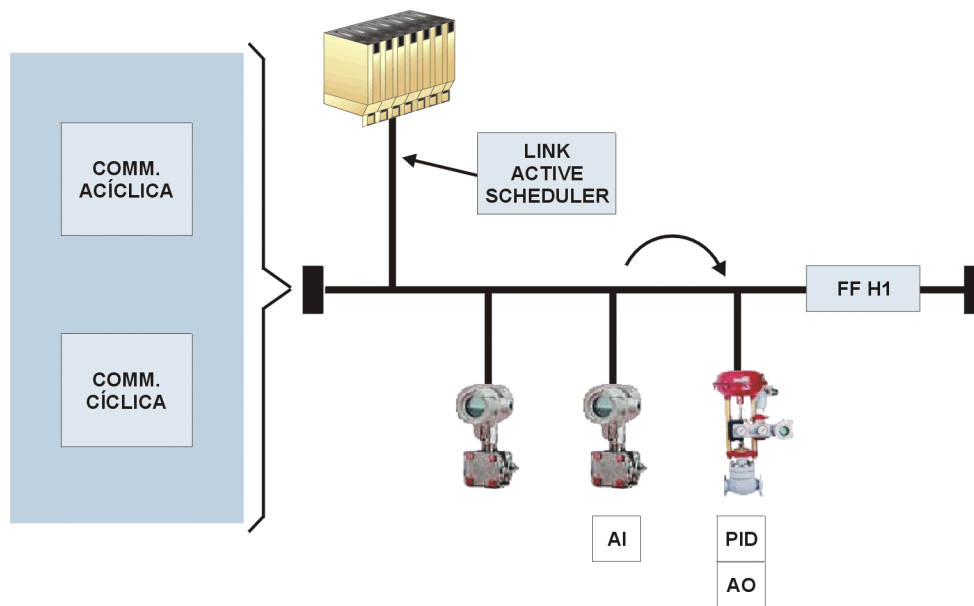


**Figura 15: Faixa de atuação das redes de campo segundo ARC**

O quadro a seguir compara as principais redes de campo quanto às suas características fundamentais.



**Figura 16:** Arquitetura de sistema de automação mostrando redes de instrumentos Fieldbus.



**Figura 17–** Uso de Redes de Instrumentos de Campo – Foundation Fieldbus

O tempo de resposta da rede depende de vários fatores, entre eles: a velocidade de transmissão dos dados, que pode ser função do comprimento da rede, do número de nodos instalados, do tamanho e natureza dos bloco de dados, etc. Os fabricantes oferecem gráficos e tabelas que nos permitem estudar o desempenho de uma rede para uma determinada aplicação.



Exemplo:

O gráfico abaixo mostra o desempenho de um anel ou segmento da rede Modbus Plus. Para se obter um tempo de resposta inferior a 200 ms, para transmissão de 400 registros por transação, o número máximo de dispositivos na rede deve ser 12. Qual o número máximo de dispositivos para a transmissão de 150 registros por transação, com o mesmo tempo de resposta?

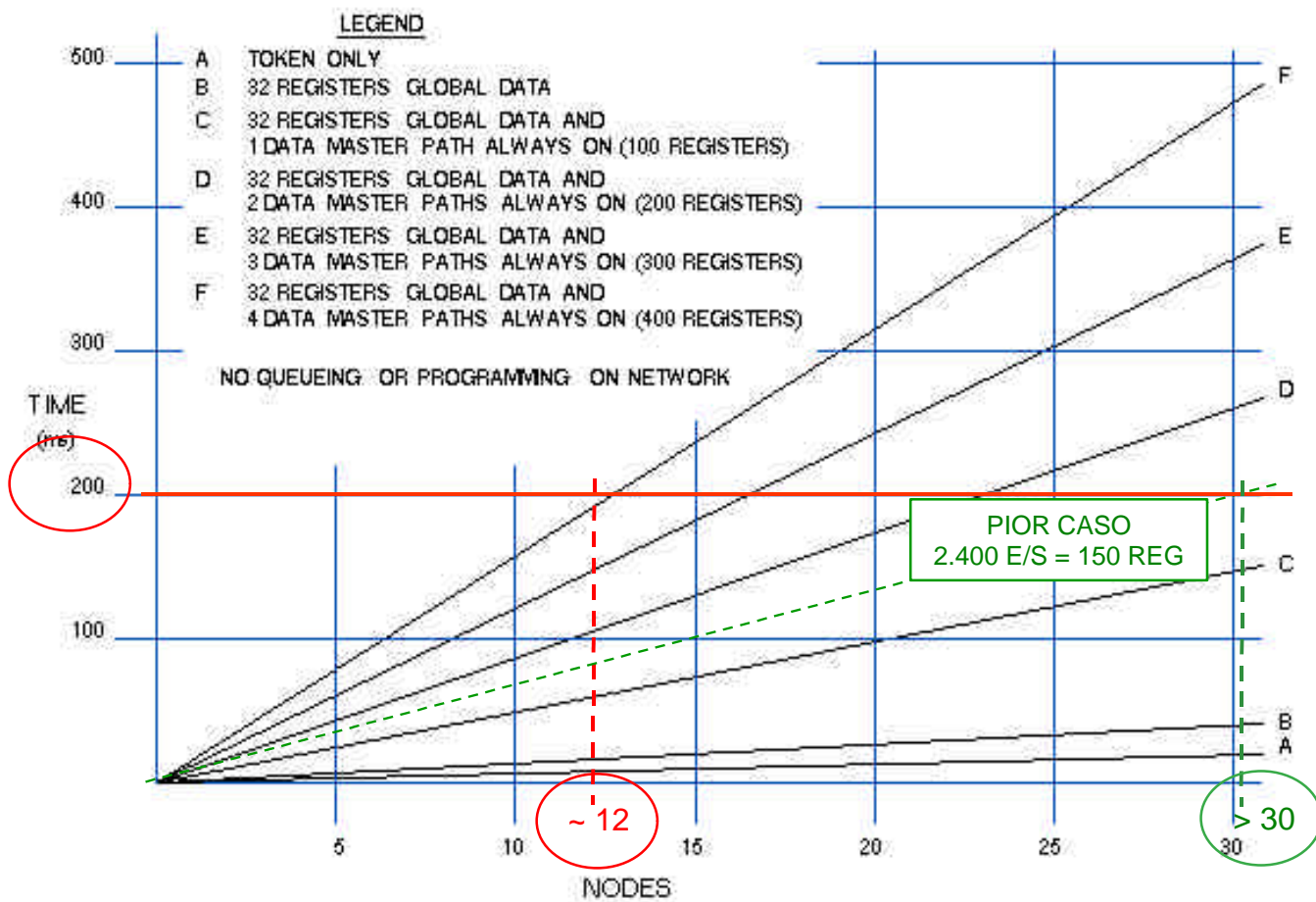
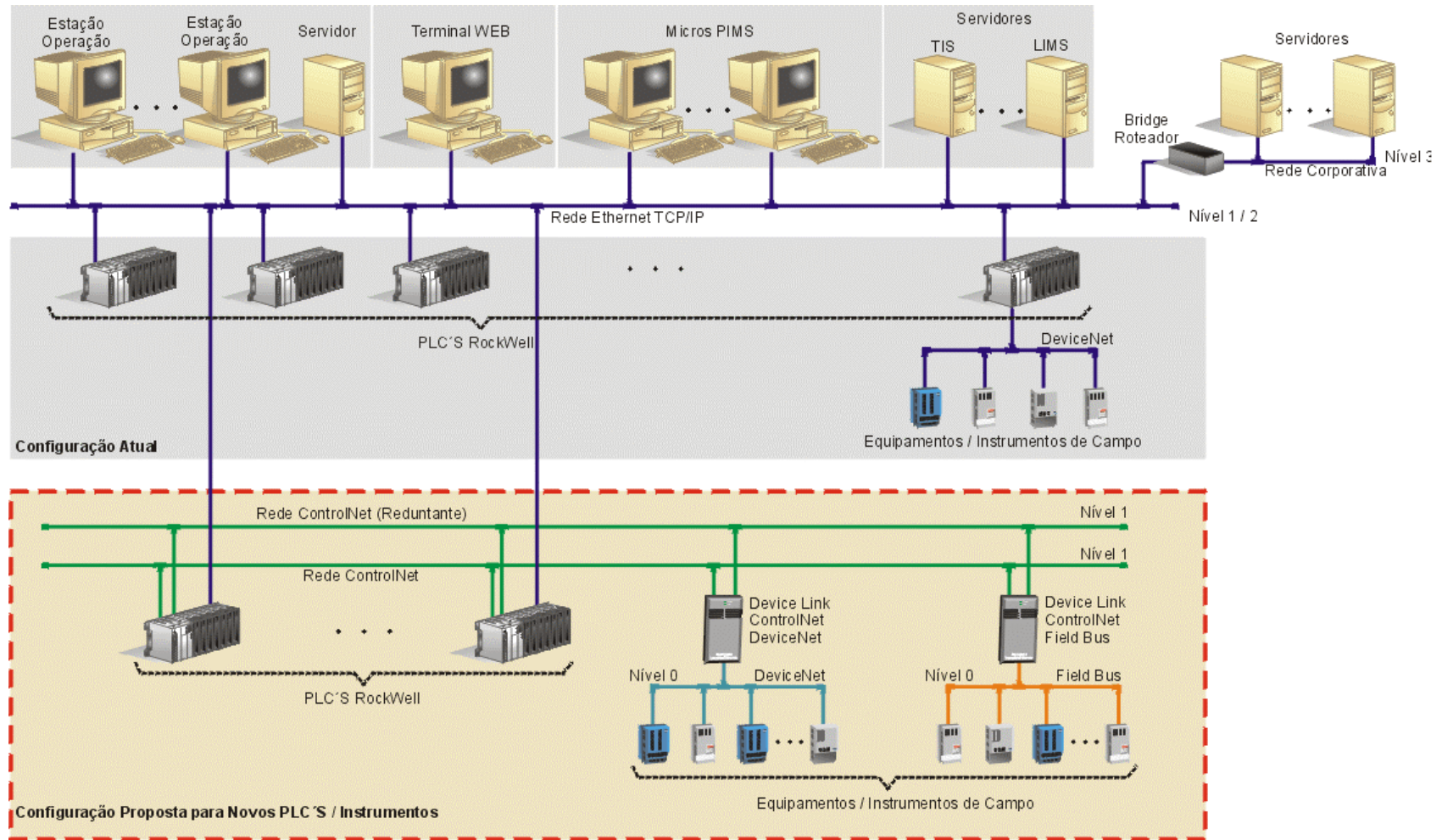


Figura 18 – Desempenho da rede Modbus Plus



**Figura 19: Arquitetura típica de uma rede de automação de múltiplas camadas**

## Comparação das redes de campo:

Características Físicas						Informação de background			
Rede	Topologia	Meio Físico	Número máximo de dispositivos	Distância Máxima	Velocidade da rede	Desenvolvedor da tecnologia	Ano de Introdução	Standard	Abertura
<b>DeviceNet</b>	Linha tronco / drop line com ramificações	Par trançado para sinal e potência	64 nodos	500m	500kbps, 250 kbps, 125 kbps	Allen-Bradley	1992	ISO 11898 & 11519	6 forn. chip 500+ produtos
<b>SDS</b>	Linha tronco/ drop line	Par trançado para sinal e potência	64 nodos 126 endereços	500m	1 Mbps, 500 kbps, 250 kbps, 125 kbps	Honeywell	1997	Especificação Honeywell submetida ao IEC, ISO11989	6 forn chip 200+ produtos
<b>Profibus</b>	Linha, estrela e anel	Par trançado ou fibra	127 nodos	24 Km (fibra)	DP até 12 Mbps PA 31.25 Kbps	PTO/Siemens	1995	DIN 19245 part 3/4	Produtos de >150 fornec.
<b>LonWorks</b>	Bus, anael, loop, estrela	Par trançado, fibra, linha de alimentação.	32000 nodos/domínio	2000m@ 78 kbps	1.25Mps full duplex	Echelon Corp.	1992-1996	ASHRAE do BACnet	Documentação do protocolo pública
<b>Asi</b>	Bus, anel, árvore de estrela	Cabo de dois fios	31 escravos	100 metros, 300 com repetidor	167 kbps	AS-I Consortium	1984	Submetido ao IEC	1 chip fornec. documentação pública
<b>CANopen</b>	Linha tronco/dropline	Par trançado para sinal e potência	64 nodos	500 metros	1Mbps, 500kbps, 250kbps, 125kbps	Philips/CiA	Março 1994	CIA	6 fornec. chips 100+ produtos
<b>ControlNet</b>	Linha tronco, estela, árvorePar trançado	Coax R6/U, fibra	99 nodos	5Km coax, 30Km + fibra	5Mbps	Allen-Bradley	Jan 1994	ControlNet International	Chips da AB, vários produtos
<b>FiledBus Foundation</b>	Multidrop com dispositivos alimentados pelo barramento	Par trançado	240/segmento, 65000 segmentos	1900m@31.25K 500m@2.5M	31.25 kbps 1Mbps .5 Mbps	Fielbus Foundation	DP - 1994 PA - 1995	ISA SP50/IEC TC65	Chip/Sw de vários fornec.
<b>IEC/ISA SP50 Fieldbus</b>	Estrela ou barramento	Par trançado, fibra e rádio	IS 3-7 não IS 128	1700m@31.25K 500M@5Mbps	31.25 kbps IS + 1, 2.6/5 Mbps	ISA&Fieldbus F.	March 1991	IEC 1158/ANSI 850	Vários fornec. chip
<b>InterBus</b>	Segmentada com drops em T	Par trançado, fibra e anel	256 nodos	400m/segmento 12.8Km total	500 kBits/s, full duplex	Phoenix Contact	Outono 1993	DIN 19258	Produtos de 400+ fornecedores

Mecanismos de Transporte						Performance		
Rede	Métodos de comunicação	Tamanho do pacote de dados	Método de arbitragem	Cheragem de Erro	Diagnósticos	Tempo de ciclo: 256 discretas 16 nodos com 16 I/Os	Tempo de ciclo: 128 Analógicas 16 nodos com 8 I/Os	Transferência de Bloco de 128 bytes 1 nodo
<b>DeviceNet</b>	Mestre/escravo, Multi mestre outros	8 byte mensagem variável	Carrier-Sonac Acesso Múltiplo	CRC	Monitoração do Barramento	3.5 ms polling Mestre-escravo	7.1 ms Mestre/Escravo polling	4.2 ms
<b>SDS</b>	Mestre/escravo peer to peer multi-cast multi-master	8 byte mensagem variável	Carrier-Sonac Acesso Múltiplo	CRC	Monitoração do Barramento Diagnóstico escravo	<1 ms, dirigido a eventos	<1 ms por evento	2 ms @ 1 Mbps
<b>Profibus</b>	Mestre/escravo peer to peer	244 bytes	Token passing	HD4 CRC	Diagnóstico da estação, módulos e cabais	Depende de configuração typ < 2ms	Dependente de configuração typ < 2ms	não disponível
<b>LonWorks</b>	Mestre/escravo peer to peer	228 bytes	CSMA	16bits CRC	Banco de dados de erros de CRC e dispositivos	20 ms	5ms @ 1 Mbps	5 ms @ 1 Mbps
<b>Asi</b>	Mestre/escravo com polling cíclico	31 escravos com 4 in e 4 out	Master/slave com polling cíclico	Código Manchester, Hamming-2, partly	Falha do escravo Falha do dispositivo	4.7 ms	impossível	impossível
<b>CANopen</b>	Mestre/Escravo	8 byte mensagem variável	Carrier-Sonac Acesso Múltiplo	CRC	Monitor de Barramento	-	-	-
<b>ControlNet</b>	Meste/escravo Multimestre Peer to peer	510 bytes	Time slice Multiple Access (CTDMA)	CCITT com polinômio de 16 bits	Falhas do dispositivo e escravos	2 ms	2 ms	2ms
<b>FiledBus Foundation</b>	Cliente/Servidor publisher/subscriber Event notification	16.6M objects/dispositivo	Escalonador determinístico centralizado, backup múltiplo	CRC 16 bits	Diagnóstico remotos, monitoração de rede	100ms @ 31.25k <1 ms @ 2.5 M	600ms @ 31.25 k < 8ms @ 2.5 M	36ms @ 31.25k < 8ms @ 2.5 M
<b>IEC/ISA SP50 Fieldbus</b>	Cliente/Servidor publisher/subscriber	674 bytes alta & 256 baixa prioridade	Escalonador, tokens ou master	CRC 16 bits	Gerenciamento da rede configurável	Dependente de configuração	Dependente de configuração	0.2 ms @ 5Mbps 1.0ms @ 1 Mbps
<b>InterBus</b>	Mestre/escravo com transferência total do quadro	512 bytes h.s. bloco ilimitado	Nenhum	CRC 16 bits	Erro de CRC localizado por segmento e quebra de cabo	1.8 ms	7.4 ms	140 ms

## Sistemas hot stand by

Num sistema *hot stand by* convencional, um computador reserva está energizado e pronto para atuar no caso de falha do computador primário. Quando este apresenta falha, um sistema de detecção de falhas irá comandar a comutação. Este sistema pode estar baseado num protocolo de comunicação entre os próprios micros ou em um software residente no CLP.

Nesta última situação, um computador deve escrever periodicamente que está vivo. O CLP lê esta palavra especial (palavra chave) e a apaga ciclicamente. Se o CLP, em uma de suas varreduras, detecta que o bit ou palavra chave não foi escrito, então sabe que o computador principal está em falha. O controle é então transferido ao micro reserva.

Como se aumenta a disponibilidade de um sistema computacional ? De duas formas aumentando-se o MTBF (*Mean Time Between Failures*) e o diminuindo-se o MTTR (*Mean Time To Repair*).

Ações para se obter um alto do MTBF (*Mean Time Between Failures*):

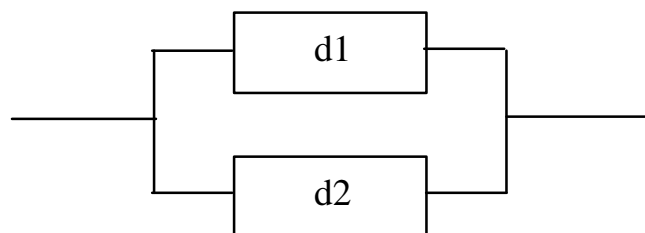
- Uso de um computador industrial
- Uso de *no break* com filtragem eletrônica da alimentação.
- Adição de redundância
- Uso de entrada e saídas isoladas galvanicamente.
- Uso de redes com fibra ótica.

Ações para se obter um baixo MTTR (*Mean Time To Repair*):

- Uso de um computador Modular.
- Ausência de *Motherboard* --> *Backplane* Passivo
- Cartões *All-in-One*
- Unidades de floppy e winchester *plug-in* de substituição independente.

Como a adição de redundância afeta a disponibilidade de um sistema computacional ?

$$\text{Disponibilidade} = \frac{MTBF}{MTBF + MTTR}$$



$$\text{Sistema redundante: } D = 1 - (1 - d1)(1 - d2)$$

## Glossário:

Definições (*Digital Equipment Corporation, depois Compaq depois HP*)

### Redundância

Elementos duplicatas ou extras que protegem um sistema ou parte dele de uma falha, ou que o habilita a manter o mesmo nível de performance em caso de uma falha.

### Failover

Processo de reconfiguração do sistema após uma falta ou devido a uma parada por manutenção preventiva. Pode ser manual ou automático.

### Falta

Evento que força o sistema a operar fora de suas especificações.

### *Fault tolerant system* (sistema tolerante a falhas)

Um sistema computacional que mantém a sua confiabilidade e disponibilidade apesar da existência de uma falha. O sistema tolera qualquer falha de componente de hardware individual e continua a servir a uma ou mais aplicações.

### Sistema dual

Sistema composto por dois computadores

### Hot standby ou Hot stand-by

Computador reserva (escravo) que já está em funcionamento e pronto para assumir o processamento da aplicação em caso de falha do processador primário (mestre).

## Revisão de conceitos básicos:

### Definições:

#### Sistemas distribuídos:

"Um sistema distribuído é um sistema de computação em que as funções computacionais são alocadas entre vários elementos físicos de computação. Estes podem estar geograficamente próximos ou separados uns dos outros" (Liebowitz & Carson, 1978)

#### Rede de Computadores:

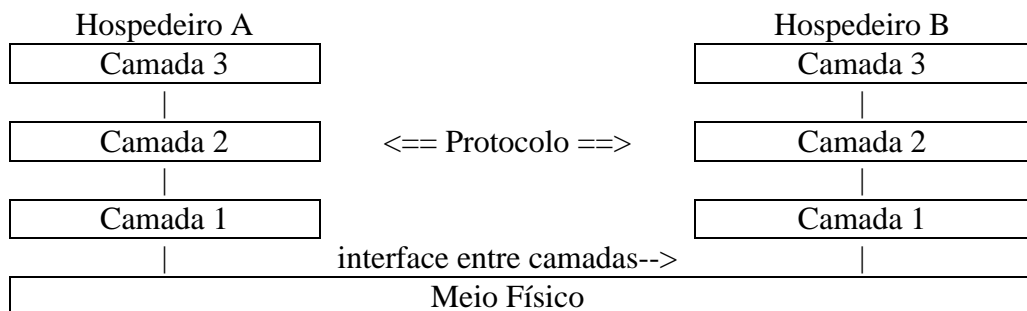
"Uma rede de computadores significa uma coleção de computadores autônomos e interconectados. Dois computadores são ditos interconectados, quando são capazes de trocar informação, o que pode ocorrer através de um meio físico de comunicação. Este é composto, por exemplo, de fios de cobre, microondas, fibras óticas ou satélites espaciais. O requisito de autonomia exclui sistemas nos quais existe um claro relacionamento do tipo Mestre-Escravo entre os computadores" (Tanenbaum, 1981)

### Modelamento em camadas

Nos sistemas modernos, todo o software de comunicação é estruturado em camadas, onde cada uma possui uma função e realiza certos serviços para as camadas superiores. Apesar do acréscimo em complexidade e do aumento do overhead em relação a comunicação de nível único, ganha-se em transparência, flexibilidade e facilidade de padronização.



**Figura 20: Sistema de camada única**



**Figura 21: Sistema multi camadas**

Os componentes ativos de cada camada se chamam ENTIDADES

Cada camada oferece SERVIÇOS às camadas superiores através de uma INTERFACE que define quais os serviços oferecidos e como os mesmos podem ser acessados.

Na conversação entre entidades de um mesmo nível existem regras e convenções que constituem o PROTOCOLO da camada.

Chamamos de ARQUITETURA do sistema de Inter conexão ao conjunto formado pelas camadas, protocolos e interfaces.

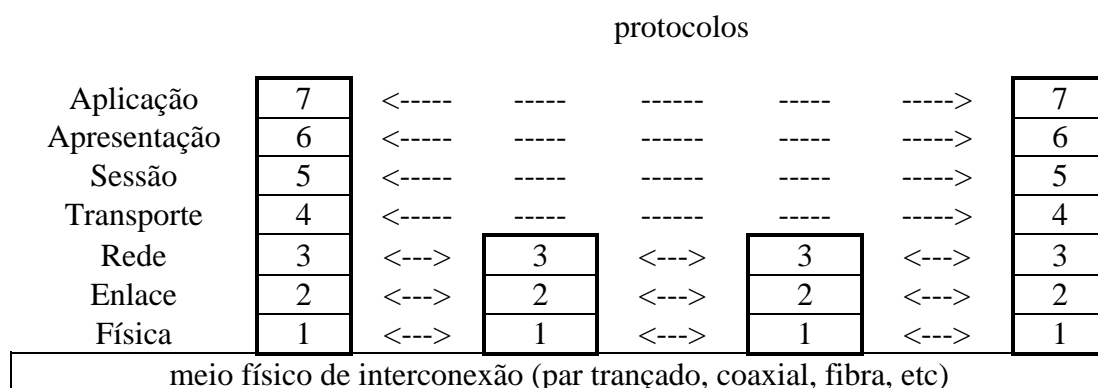
Cada camada deve executar uma série de FUNÇÕES para proporcionar o serviço desejado.

O modelo de referência OSI/ISO (1983)

(*Open Systems Interconnection / International Organization for Standardization*)

Seu principal objetivo era estabelecer um padrão que permitisse que equipamentos de fabricantes diferentes pudessem se comunicar.

Este modelo prevê 7 camadas:



**Figura 22 – Modelo OSI/ISO**

a) *Camada de Aplicação*

Proporciona serviços para os processos dos usuário finais. Entre os protocolos de aplicação mais importantes para a área de automação temos o FTAM e o MMS a serem discutidos a seguir.

b) *Camada de Apresentação*

Formata os dados de tal forma a compatibilizá-los com a camada de aplicação. São exemplos de funções implementadas por esta camada: conversão de códigos (ASCII para EBCDIC por exemplo), criptografia para segurança de dados, compressão de dados, etc. Um dos serviços fornecidos é o de terminal virtual que fornece um mapeamento dos recursos de um terminal real para outro virtual.

c) *Camada de Sessão*

Provê o gerenciamento de diálogos sincronizando conversações, quando um nodo fim mantém mais de uma conexão lógica com outro nodo fim. Foi padronizada pela norma ISO 8372. Um exemplo seria quando o estudante A estabelece uma conexão telefônica com o estudante B e várias pessoas em cada casa desejam participar da conversação através de extensões telefônicas.



Os estudantes desejam conferir seus trabalhos de casa, as mães querem trocar receitas e os pais falar de negócios. Cada conversação constitui uma sessão.

d) *Camada de Transporte*

É responsável pela transferência de dados livre de erros entre as entidades fim a fim. Entre as funções implementadas neste nível temos:

- a) Segmentação da mensagem em unidades menores, controle do seqüenciamento dos pacotes e reagrupamento das mensagens.
- b) Controle de fluxo de informação
- c) Detecção e correção de erros
- d) Multiplexação e Demultiplexação de conexões
- e) Mapeamento dos endereços de nível de transporte para o nível de rede

e) *Camada de Rede*

É responsável pelo roteamento e transferência dos dados aqui denominados de **pacotes** de um nodo da rede para outro via o sub sistema de transmissão.

As principais funções são:

- a) Controle de fluxo
- b) Seqüenciamento de pacotes
- c) Detecção e correção de erros de pacotes

O serviço típico oferecido é o de circuito virtual que corresponde a um canal de comunicação dedicado entre as duas estações comunicantes.

f) *Camada de Enlace*

Provê um canal de comunicação entre duas entidades comunicantes. Os dados são organizados em unidades denominadas **quadros**. Outra função importante desta camada é o controle de acesso ao meio de transmissão compartilhado.

g) *Camada Física*

Responsável pela transferência de bits pelo meio físico de transmissão. Se preocupa com as características mecânicas e elétricas da transmissão. Os meios físicos mais utilizados em automação industrial são o cabo coaxial, o par trançado, a fibra ótica e o espaço livre (radiodifusão).

## Protocolos da camada de aplicação usados em automação

### MMS - Manufacturing Message Specification (RS512->ISO 9506)

Foi definido durante o projeto do MAP (*Manufacturing Automation Protocol*) patrocinado pela GM. Enquanto o futuro do MAP é incerto, o protocolo MMS parece ter sucesso garantido. Pode rodar tanto sobre a pilha OSI/ISO como por exemplo sobre a pilha TCP/IP. Com este protocolo, qualquer programa rodando em um computador pode acessar dados em qualquer dispositivo orientado a manufatura conectado a rede. O MMS permite também que dois dispositivos de controle, como dois CLPs, comuniquem facilmente entre si via rede. O MMS é baseado no modelo cliente servidor. Este modelo assume que o servidor é o depósito de dados e que o cliente é um usuário ou fornecedor de dados. A aplicação servidora é baseada no conceito de Dispositivo de Manufatura Virtual (VMD). O VMD possui 6 objetos usados para facilitar o processo de transferência de informações. A especificação também define 84 serviços disponíveis para

manipular estes objetos. Estes serviços, agrupados em unidades funcionais são mostrados na tabela abaixo.

<i>Objeto</i>	<i>Descrição</i>
Domain	Grupo de utilidades VMD
Journal	Arquivo de transações
Operator Station	Console associada com um dispositivo real
Program Invocation	Inicialização de programa executável
Semaphore	flags para reportar uso de recursos
Variables	variáveis únicas, estruturas ou vetores

**Tabela 1: Objetos VMD**

<i>Unidade</i>	<i>Serviços</i>
Gerenciamento de Contexto	Initiate, Conclude, Abort, Cancel, Reject
Serviços Remotos	Read, Write, InformationReport, DefineNamedVariable, GetVariableAccessAttributes, DeleteVariableAccess, DefineScatteredAccess, GetScatteredAccessAttributes, DefineNamedVariableList, GetNamedVariableListDefinition, DeleteNamedVariableList, DefineNamedType, DeleteNamedType, GetNamedTypeDefinition
Diagnósticos	Status, UnsolicitedStatus, GetNameList, Identify, Rename
Comunicação com Operador	Input, Output
Serviços de carga de programa	InitiateDownloadSequence TransmitDownloadSequence TerminateDownloadSequence InitiateUploadSequence, TransmitUploadSequence, TerminateUploadSequence, RequestDomainDownload, RequestDomainUpload, DeleteDomain GetDomainAttribute, LoadDomainContent, StoreDomainContent
Coordenação	TakeControl, RelinquishControl, DefineSemaphore, DeleteSemaphore, ReportSemaphoreStatus, ReportSemaphorePoolStatus, ReportSemaphoreEntryStatus

Controle de dispositivos e Gerenciamento de tarefas	CreateProgramInvocation, DeleteProgramInvocation, Kill, Start, Stop, Resume, Reset, GetProgramInvocationAttributes
Serviços de arquivos	ObtainFile, FileOpen, FileRead, FileClose, FileRename, FileDelete, FileDirectory
Gerenciamento de eventos	DefineEventCondition, DeleteEventCondition, GetEventConditionAttributes, DefineEventAction, DeleteEventAction, GetEventActionAttributes, AlterEventConditionMonitoring, TriggerEvent, AlterEventEnrollments, GetEventEnrollments, EventNotification, AcknowledgeEventNotification, GetAlarmSummary, GetAlarmEnrollmentSummary, ReportEventConditionStatus, ReportEventActionStatus, ReportEventEnrollmentStatus,
Gerenciamento de jornal	ReadJournal, WriteJournal, InitializeJournal, ReportJournalStatus

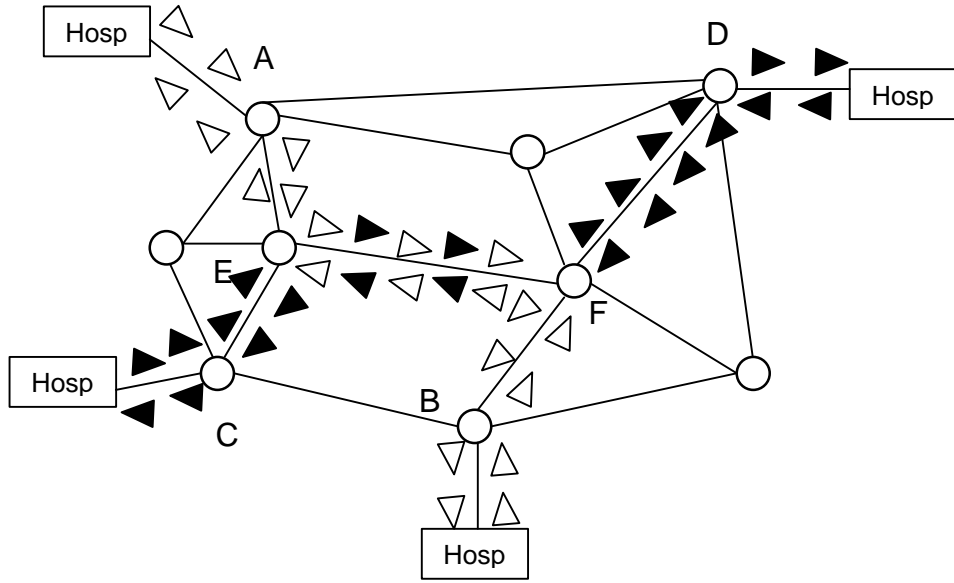
**Tabela 2: Serviços MMS**

## Controle de fluxo na rede

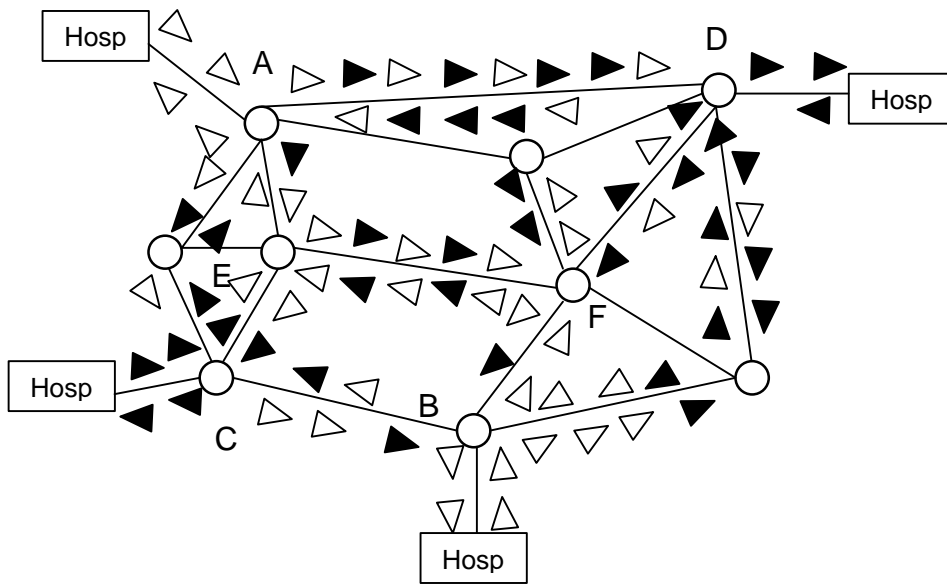
Os dois principais serviços são: datagrama e circuito virtual. No circuito virtual uma ligação física se estabelece entre as duas entidades comunicantes como numa ligação telefônica. O serviço de datagrama é menos confiável. Os pacotes constituintes da mensagem trafegam entre os diversos nodos da rede segundo rotas variadas até convergirem no nodo de destino.

Item	Circuito Virtual	Datagrama
Endereço do destinatário	Só é necessário ao estabelecer a conexão	Necessário em todos os pacotes
Tratamento de erros	Transparente para o hospedeiro (feito no subsistema de transmissão)	Feito explicitamente pelo hospedeiro
Controle de Fluxo	Fornecido pelo subsistema de transmissão	Não é fornecido pelo subsistema de transmissão
Sequenciamento de pacotes	Mensagens passadas para o hospedeiro na mesma ordem de envio	Mensagens passadas para o hospedeiro na ordem de recebimento

**Tabela 3: Modelos de controle de fluxo na em redes de computadores**



**Figura 23: Controle de fluxo através de Circuito virtual**

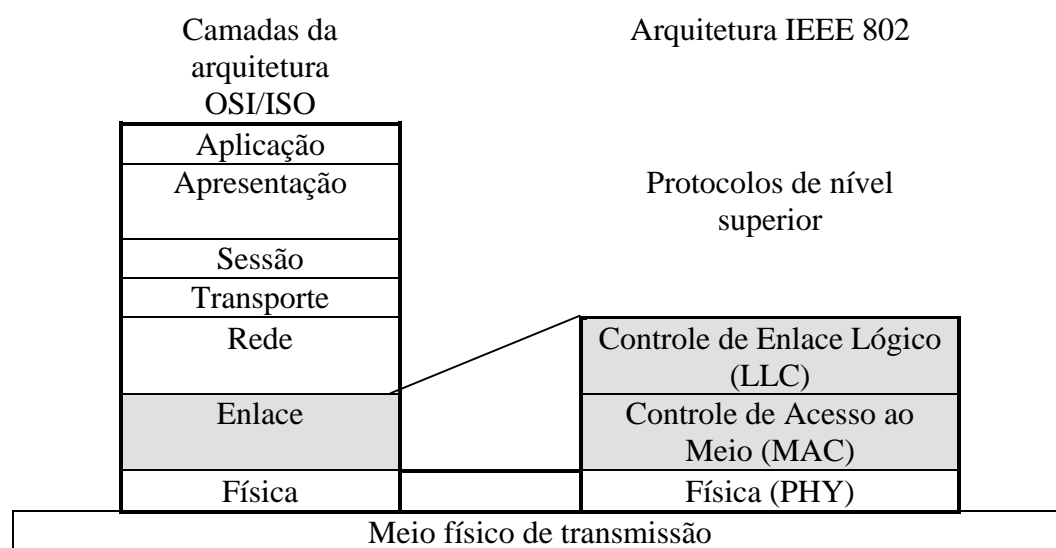


**Figura 24: Controle de fluxo através de Datagramas**

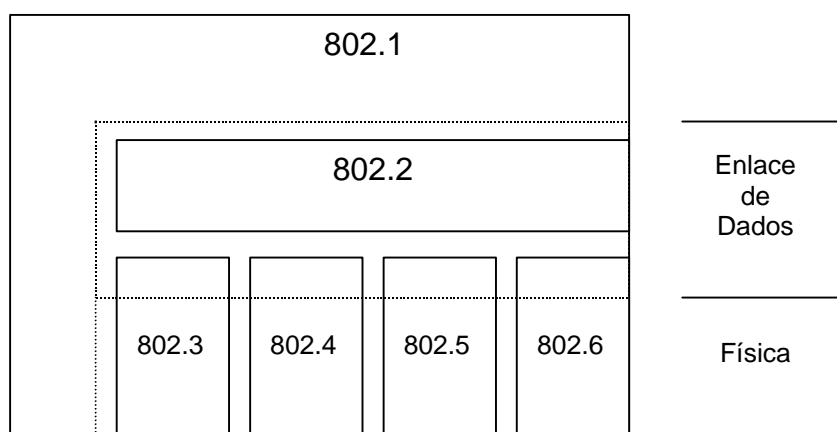
## O padrão IEEE 802

O IEEE através do projeto 802 estabeleceu uma arquitetura para redes locais nos moldes do padrão OSI-ISO. Aos dois níveis inferiores do padrão OSI-ISO correspondem três camadas:

Sub camada de Controle de Enlace Lógico	LLC
Sub camada de Controle de Acesso ao Meio	MAC
Camada Física	PHY



**Figura 25: Arquitetura IEEE 802 e modelo OSI/ISO**



**Figura 26: Padrões da Arquitetura IEEE 802**

Os principais padrões e processos de padronização em curso no IEEE são:

- IEEE 802 LMSC LAN MAN Standard Committee

- IEEE 802.1 HILI Higher Level Interface: descreve a relação entre os padrões IEEE 802 e OSI/ISO
- IEEE 802.2 LLC Logical Link Control (Protocolo de controle de Enlace lógico)
- IEEE 802.3 CSMA/ CD Carrier Sense Multiple Access with Collision Detection (Ethernet): barramento com controle de acesso CSMA-CD
- IEEE 802.4 TBUS Token Bus: barramento com controle por ficha (Token Bus)
- IEEE 802.5 TRING Token Ring: anel com controle por ficha (Token Ring)
- IEEE 802.6 DQDB Distributed Queue Dual Bus: método de controle de acesso a rede em área metropolitana
- IEEE 802.7 BBTAG Broadband Technical Advisory Group
- IEEE 802.8 FOTAG Fiber Optic Technical Advisory Group
- IEEE 802.9 ISLAN Integrated Services LAN
- IEEE 802.10 SILS Standard for Interoperable LAN Security
- IEEE 802.11 WLAN Wireless LANs
- IEEE 802.12 DPAP Demand Priority Access Protocol
- IEEE 802.14 CATV LANs in Cable Television Networks
- IEEE 802.15 WPAN Wireless Personal Area Networks (Bluetooth)
- IEEE 802.16 BWA Broadband Wireless Access
- IEEE 802.17 RPR Resilient Packet Ring

## Principais características dos protocolos de acesso ao meio:

### Token Bus

- Topologia: Barramento
- Determinístico no tempo: determinado pela ficha
- Mecanismo de funcionamento:
  - Passagem do bastão segundo anel lógico: cada estação recebe a ficha da antecessora e a passa a sua sucessora.
  - Cada estação deve conquistar a ficha, transmitir dados, e passar a ficha a seu sucessor no anel lógico.
  - Podem existir estações que não participam do anel. Estas podem receber dados e consultas (*poll*), mas não a ficha.
  - Necessidade de mecanismos extras:
    - Estabelecer anel lógico
    - Manter anel lógico
    - Reconfiguração dinâmica do anel

Exemplo: Saída do anel lógico

Mecanismo 1: (saída à francesa)

Estação desejando sair recebe ficha e a retém

O mecanismo de proteção da rede atua

Mecanismo 2:

Estação desejando sair aguarda a posse da ficha

Envia o endereço da sua sucessora à predecessora ("*Set Sucessor*")

Passa ficha para a sua sucessora

Muitas redes de automação utilizavam alguma forma de protocolo *token passing* modificado em relação ao padrão 802.4

A rede Arcnet seguia este padrão e foi muito usada nas décadas de 80 e 90.

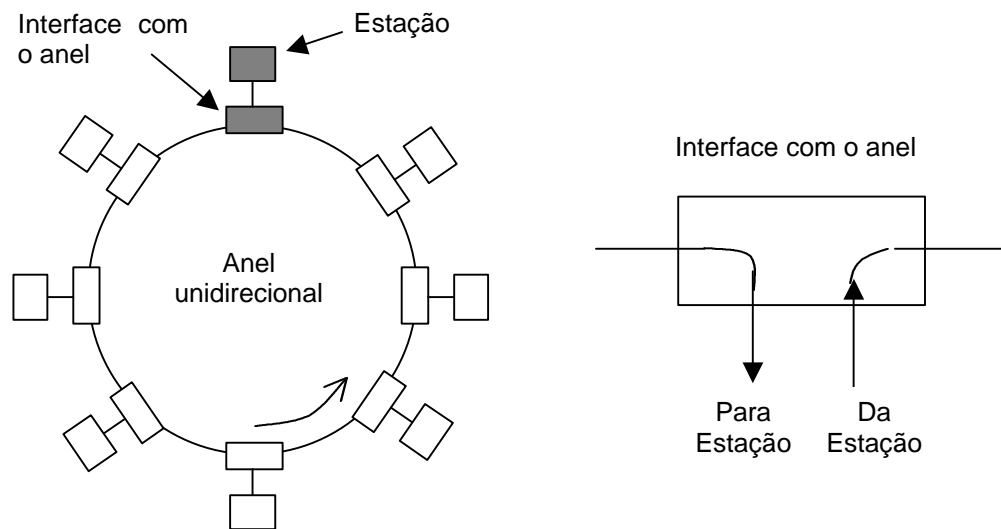
## Token-Ring

Lançada pela IBM em 1985

Mecanismo de envio de dados:

Cada nodo recebe dados do nodo anterior (NAUN= *nearest active upstream neighbor*) e o retransmite para o nodo posterior.

Se a mensagem não é para ele: retransmissão verbatim



**Figura 27: Esquema de transmissão de dados da rede Token Ring**

Token = mensagem de 24 bits

Mecanismo de passagem de token:

- A estação A deseja transmitir  
Após receber o token, e se sua prioridade for maior que a do token, ela transforma o token em um quadro:  
token + endereço de destino + seu próprio endereço + dado
- O quadro circula até a estação destino. A estação destino lê o dado, muda o bit de status para recebido e recoloca a mensagem no anel
- A mensagem volta ao emissor. Ele "limpa" o quadro e passa o token para a próxima estação.

O nível físico:

- Topologia: Anel ou estrela ?
  - Todos os cabos convergem para o MAU (*Medium Access Unit*)
  - Cada nodo se conecta via um cabo com dois pares: um para recepção e outro para transmissão.
  - O conector é hermafrodita.

Desvantagem:

- Gasta mais cabo

Vantagens:

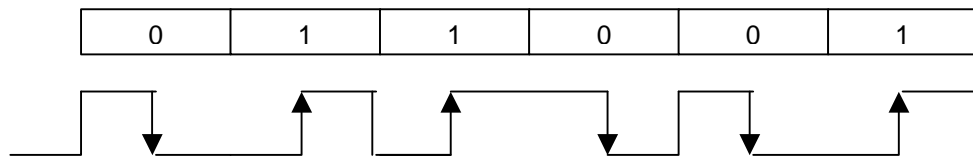


- Facilita adição e remoção de nodos
- Facilita "jumper" nodos defeituosos
- Cabo único

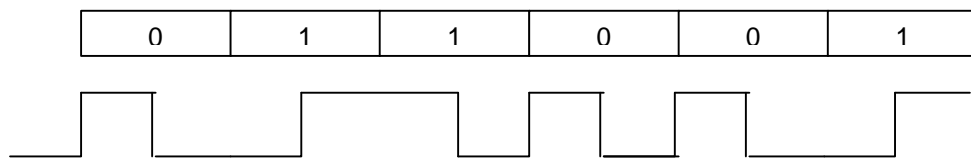
Limitações:

- Distância Estação - MAU: 300 metros (981')
- Velocidade: 16 Mbps

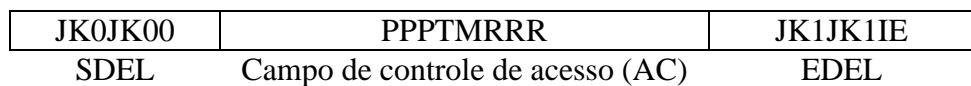
Codificação: Manchester diferencial  
 independe da polaridade  
 se tem transição no início é 0  
 se não tem é 1



**Figura 28: Codificação Manchester**



**Figura 29: Codificação Manchester Diferencial**



**Figura 30: Formato do token token ring**

- PPP      Prioridade. Indica a prioridade mínima da mensagem para usar o token
- T        Bit de token. Token e não quadro
- RR      Bits de reserva
- I        bit de quadro intermediário: o quadro é parte de uma seqüência
- E        Indicador de Erro Detectado (EDI)

SDEL	AC	FC	Dest Addr	Src Addr	Info	FCS	EDEL	FS
1	1	1	6	6	varia	4	1	1

**Figura 31: Formato de quadro token ring**

SDEL	Delimitador de início
AC	Campo de controle de acesso
FC	Campo de controle de quadro
Dest Addr	Endereço de destino
Src Addr	Endereço Fonte
Info	Dados
FCS	32 bits CRC de FC, Dest, Src e Info
EDEL	Delimitador de final
FS	Status do quadro

Endereçamento:

48 bits

É possível mandar mensagens:

- para 1 nodo
- para grupos de nodos
- para todos os nodos (*broadcast*)

Endereços funcionais:

Possibilitam mandar mensagens para um endereço de utilidade pública, sem conhecer endereço dos nodos: gerente de rede, monitor de erros, etc

Colocando a rede no ar:

O Monitor Ativo é eleito: "Beaconing" (beacon=farol)

Critério: Monitor = O nodo de maior endereço físico

Funções do Monitor ativo:

- Coloca anel em operação normal:
  - Limpa o anel
  - Cria o token
- Fornece sinal de clock para o anel: sincroniza demais estações
- Watchdog:
  - Mantém um token circulando
  - Regenera token e reinicializa o anel, se token for perdido em 10 ms.
  - Detecta token recirculando pela rede: quando um token ou quadro de mensagem passa, ele seta o monitor bit no campo de controle de acesso (AC). Se o quadro voltar ele será eliminado.
  - Assegura integridade dos demais nodos através de mensagem de *broadcast* periódica (AMP= Active Monitor Present). Se a mensagem falhar outro nodo assume o papel de monitor.

Mecanismo de prioridade:

8 níveis: 0-7

Token: carrega prioridade e aceita reservas: campo "Access control" (AC)

Se uma estação precisa enviar uma mensagem com urgência, ela seta os bits de reserva da mensagem que está passando com a sua prioridade (carona). A mensagem trafega na rede e volta ao emitente. O emitente examina o campo AC. Se houver pedido de transmissão com uma prioridade maior que a corrente, ele muda a prioridade do token para a prioridade máxima. O token circula pelas estações de baixa prioridade até a estação que ativou a reserva de alta prioridade. Quando a estação que promoveu a prioridade do token recebe o token de volta com a prioridade ainda alterada, restaura a prioridade anterior.

No mecanismo de reservas, promoções e restaurações são recursivas.

**Proteções:**

Monitor ativo:

Um token com prioridade circulando duas vezes = nodo com mal funcionamento.

Nodo que não passa no self test de transmissão se auto elimina da rede.

Cada nodo vistoria cada token ou mensagem que passa por ele e seta o bits de erro ("Error Detected Indicator", EDI) se detectar alguma anomalia. Cada nodo mantém um contador do número de vezes que ele seta o EDI. Este contador pode ser examinado pelo gerente da rede.

## CSMA-CD (Carrier Sense Multiple Access - Collision Detect)

São protocolos onde cada estação escuta o meio de transmissão para verificar se já existe uma portadora, sinal de que outra estação ocupa o meio, antes de transmitir. Os usuários não possuem nenhum tipo de sincronismo entre si. Este mecanismo teve como antecessor histórico o protocolo Aloha para transmissão via rádio.

A estação A deseja transmitir dados em um canal compartilhado

Aloha

```
Envia quadro
Se houve colisão
    então repita
        espera um tempo aleatório
        transmite quadro
    até sucesso
```

Algoritmo CSMA-CD persistente (ou 1 persistente):

```
A escuta o canal
Se canal ocupado
    então repita
        escuta canal
    até canal livre
transmite um quadro (com probabilidade 1)
Se ocorreu colisão
    então espera um tempo aleatório e tente de novo
```

Algoritmo não persistente:

```
A escuta o canal
Se canal ocupado
    então repita
        espera um tempo aleatório
        escuta canal
    até canal livre
transmite um quadro
Se ocorreu colisão
    então espera um tempo aleatório e tente de novo
```

Algoritmo p persistente:

```
A escuta o canal
Se canal ocupado
    então repita
        espera um tempo aleatório
        escuta canal
    até canal livre
```

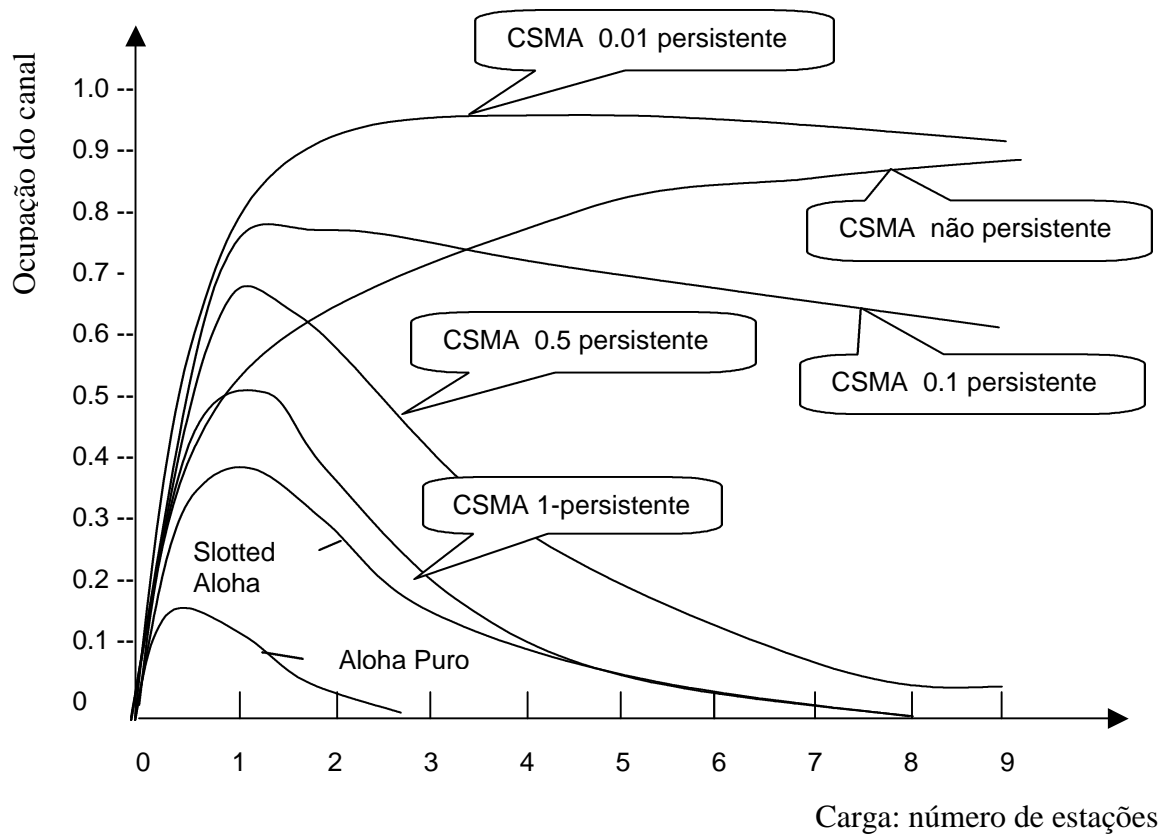
transmite um quadro com probabilidade  $p$  neste *slot* de tempo ou com probabilidade  $q=1-p$  no próximo *slot*.

Se ocorreu colisão

então espere um tempo aleatório e tente de novo

Os protocolos com detecção de colisão interrompem a transmissão do quadro no meio, assim que a colisão é detectada.

Uma grande limitação deste protocolo é a rápida degradação do seu desempenho quando submetido a altas cargas.



**Figura 32: Comparação do desempenho de protocolos segundo Tannenbaum**

## Exercícios:

- 1) Calcule a disponibilidade e o MTBF total de um sistema *hot-standby* com os seguintes componentes:

	MTBF (h)	MTTR (min)
Fonte de alimentação	150000	10
CPU	50000	10
Estabilizador	30000	180
Winchester	50000	30
Impressora	20000	120
Monitor	40000	120
Floppy	50000	30

- 2) Defina o valor verdade para as afirmações seguintes:

- Todo sistema redundante é tolerante a falhas.
- O algoritmo de exclusão mútua em ambiente distribuído estudado neste curso é tolerante a falhas.
- Existem processadores tolerantes a falhas que comparam o resultado das instruções de um programa uma a uma.
- Dois sensores exatamente da mesma marca, tipo e modelo, conectados a um processo, fornecerão sempre resultados idênticos.
- A partir da mesma Especificação Funcional, dois programadores podem produzir programas que apresentem resultados diferentes para os mesmos dados de entrada, mesmo utilizando os mesmos algoritmos.
- Em um sistema tolerante a falhas com quatro processadores, um dos processadores poderá influenciar de forma diferente os demais, de forma a dividir a sua opinião.
- No problema dos generais bizantinos, se tivermos 3 generais e um for traidor, não haverá solução para o problema da votação.
- Se tivermos 2 traidores precisaremos de no mínimo 7 generais para que o algoritmo funcione.

- 3) Compare as vantagens e desvantagens de duas filosofias de sistemas *hot-standby*:

- a) ambos os micros fazem acesso simultâneo e independente a rede de CLPs.
- b) Ambos os micros estão conectados à rede de CLPs, mas apenas um dos dois realiza acesso ativo a rede, comunicando o status das variáveis lidas ao outro via a rede de supervisão.

- 4) Comente como resolver as seguintes questões em um sistema *hot-standby*:

- a) Ambos os micros devem colher informações *on-line* da rede.
- b) Informações de configuração de um micro devem ser comunicadas ao segundo
- c) Partida a frio

d) Partida a quente após o micro ser consertado.

5) Como é detectada a falha do micro ativo em uma arquitetura *hot stand by* ?  
Apresente sugestões.

6) Comparação do *throughput* da rede QNX com diversas configurações de rede:

Rede	Cartão de Interface	Cartões	Taxa nominal	Throughput
Arcnet	Corman	1	2.5 Mbps	190 kbytes/s
Arcnet	Corman	2	2.5 Mbps	380 kbytes/s
Ethernet	16-bit ISA NE2000	1	10 Mbps	1015 kbytes/s
TCNS	16-bit ISA Thomas-Conrad	1	100 Mbps	1550 kbytes/s

Tente explicar o aparente paradoxo exibido nesta tabela.

7) O que diferencia a arquitetura de um sistema híbrido da arquitetura de um SDCD ?

8) Na arquitetura do desenho que se segue, comente como que o MES realizará a função de WIP (*Work in Progress*). Suponha que o esquema se refira a uma linha de bobinas de uma siderúrgica. As bobinas quando saem da produção são identificadas com RFIDS e devem ser trazidas para estoque através de pontes rolantes. Elas também são retiradas do estoque através de pontes e embarcadas em vagões ferroviários.

9) No protocolo OPC as características de leitura dos itens de um grupo podem ser definidas de uma única vez para todos os itens do grupo. Estas características são:

- Estado: ativo ou inativo
- Período de leitura
- Tipo de leitura: síncrona ou assíncrona
- Banda Morta, etc.

Mostre a utilidade deste conceito e discuta em que situações você utilizaria grupo de itens.

10) Analise o *data sheet* a seguir e responda as perguntas:

- a) Quais os tipos de dispositivos conectados nesta rede ?
- b) Como você classificaria esta rede: rede de sensores e atuadores (Sensorbus), redes de dispositivos (DeviceBus) ou rede de instrumentação (Fieldbus) ?
- c) Esta rede interliga dispositivos de que nível hierárquico ?
- d) Qual a maior distância atingida por esta rede ? Em que velocidade ?
- e) Qual a maior velocidade alcançada ? Qual o limite de distância nesta velocidade ?
- f) Atendo-se a definição de rede que você aprendeu neste curso você poderia classificar este modelo de interligação como rede ? Por que ?

- g) Durante um ciclo de *scan* quantos blocos de dados são transferidos ? Quantos pontos podem existir em cada bloco ?
- h) Para o controle de expedição em uma fábrica, que tipo de dispositivos você interligaria a esta rede ?
- i) Caso o cabo de rede estivesse passando próximo a uma máquina de solda, que tipo de cuidados você poderia tomar ?
- j) É possível enviar comandos diretamente de uma estação de supervisão ligada a um CLP através de uma rede DH+ para uma MMI ligada ao CLP via a RIO ?
- k) Que outro tipo de rede mais moderna é hoje utilizada em substituição à Remote IO ?
- l) Que tipo de módulo você utilizaria para colocar a aquisição de dados mais próxima do seu processo, evitando cabos longos até o I/O remoto ?
- m) Qual o protocolo de acesso ao meio ?
- n) Esta rede é determinística ?
- o) É possível realizar a leitura de dados por exceção (*unsolicited messages*) ?



# Universal Remote I/O Link



## Network Description

Our Universal Remote I/O Link connects our SLC and PLC processors to remote I/O chassis and a host of intelligent devices such as operator interfaces and ac and dc drives. I/O chassis and other devices can be mounted up to 10,000 feet from the PLC or SLC processor.

Our PLC and SLC processors access the Remote I/O Link through builtin scanners (as in our enhanced PLC5 processors) or through separate scanner modules (as with our SLC processors and the 1747SN scanner module). I/O products communicate with these scanners over the link through separate adapter modules (such as the 1771ASB adapter for the 1771 I/O chassis, 1747ASB adapter for the 1746 I/O chassis, and 1794-ASB adapter for FLEX I/O), or through builtin adapters (such as our 1791 I/O Blocks).

FLEX Integra I/O (1793 series) is a low-cost, small increment, modular I/O system for distributed applications that offers all the functions of larger I/O without the space requirements. It combines a terminal strip and I/O interface into one small module. FLEX Integra I/O is compatible with 1794 FLEX I/O communication adapters. FLEX Integra I/O requires only one 1794 FLEX I/O adapter for as many as eight I/O modules.

to our I/O, AB operator interfaces, ac and dc drive systems, intelligent sensing products, CNCs, devices are compatible with this link. Some products, such as [PanelView Operator Terminals](#), have "adapter" capability, while other products, such as our 1336 drives, require optional "adapter" modules on the link. Some products are installed in the 1771 I/O chassis and communicate over the backplane to a Remote I/O Adapter, which communicates to the programmable controller's scanner. In our 1784KTS communication interface card lets an ISA/EISA bus PC communicate directly with AB devices.

Other companies offer products such as robotic and welding controllers, scales, and wireless modems, that are compatible with the Universal Remote I/O Link as well. In total, there are approximately 100 devices available that can communicate on this link. By using these devices on the link, you speed communication and allow the devices to work together to help improve quality while lowering integration, maintenance, and training costs.

For distributed processing, you can put a PLC5 processor in "adapter mode" and install it in an I/O chassis where it can monitor its own resident I/O while communicating to a supervisory PLC5 processor over the Universal Remote I/O Link. You can also distribute SLC processors on the link where they can control I/O while communicating with a supervisory processor via a 1747 Direct Communication Module.

For highspeed processing applications, an [extendedlocal I/O link](#) is available, which provides a parallel I/O link (the practical equivalent of processorresidentchassis performance for I/O modules not placed in the processor's chassis). In addition, the AB [ControlNet network](#), which gives you deterministic, repeatable transfers of control data, is suitable for realtime, highthroughput applications.

The Network MediaChecker (1788-MCHKR) is a handheld diagnostic tool that analyzes Universal Remote I/O physical media.

## Features

- Uses transceivers communicating over a single channel

- Uses standard PVC twinaxial cable (cat. no. 1770CD) as the transmission medium
- Uses a daisychain connection with a maximum length of 3,048m (10,000 ft)
- Operates at the data rates listed in Specifications. A 1/2 watt terminating resistor is required at each end of the trunk line to eliminate reflections. Error checking is done using standard CRC16 checks.
- Is based on the master/slave model. The programmable controller's scanner is the master and the I/O chassis or adapter devices are slaves. The slave only responds when told to by the master.
- Provides transfer of a single unit (8, 16, or 32 bits) of I/O image data to/from each I/O module in each I/O chassis during each I/O scan. The size of the unit depends on the I/O addressing density selected at the I/O chassis. It can also provide block transfers of 64 words maximum to an individual I/O module (except when used with the 1747SN).
- Lets Remote I/O Scanners connect to a maximum of 32 I/O chassis or other adaptertype devices on a single link. Devices built to original Universal Remote I/O specifications are compatible with those built to the new specifications. However, if any of the devices on a link are built to the original specifications, the limit is 16 devices on a single link. In any case, for a specific scanner, the number of adaptertype devices is limited by the I/O rack addressing capability of the scanner. *For guidelines, see the PLC5 Design Manual, publication 17856.2.1*

## Specifications

Communication Rate	Distance meters (feet)	Termination Resistor
57.6k bit/s	3,048 (10,000)	150Ω ½ W or 82.5Ω ½ W
115.2k bit/s	1,524 (5,000)	150Ω ½ W or 82.5Ω ½ W
230.4k bit/s	762 (2,500)	82.5Ω ½ W

## Compatibility

The strength and versatility of the Universal Remote I/O link come from the breadth of products it supports.

In addition to 1771 I/O, the industry's largest I/O offering, a wide variety of devices can be connected to the Remote I/O Link, as listed below. NonAllenBradley devices are in italics.

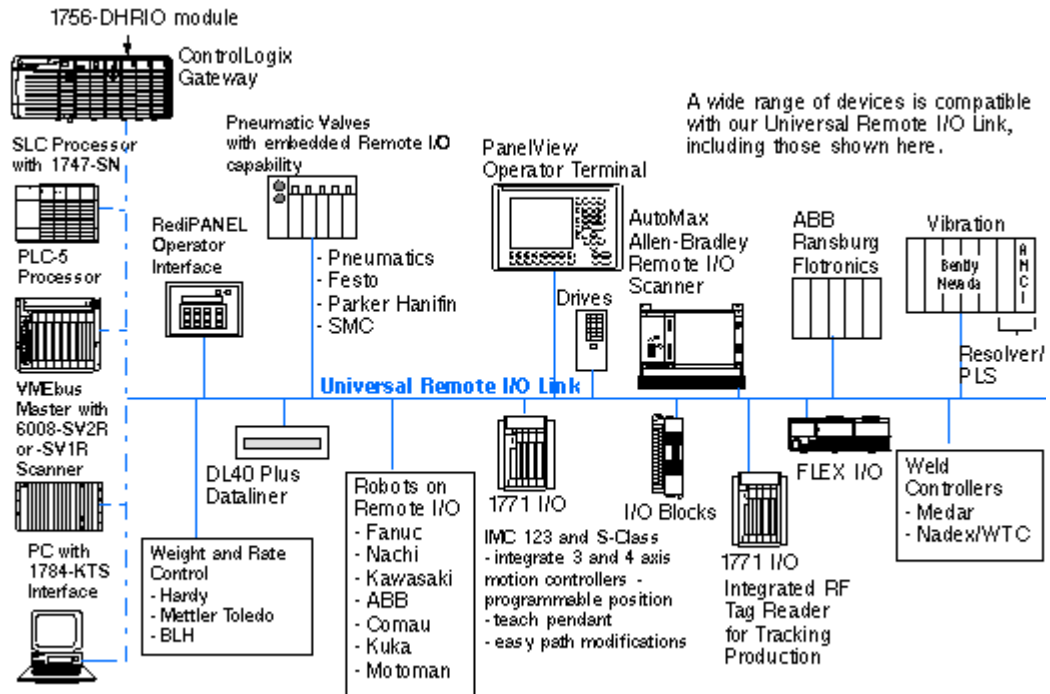
Scanners	Adapters	MMI	Input Devices	Output Devices
<ul style="list-style-type: none"> <li>• PLC-5/xx,</li> <li>• 1747-SN</li> <li>• VME Scanner</li> <li>• AutoMax® Allen-Bradley Remote I/O Scanner M/N 57C443</li> </ul>	<ul style="list-style-type: none"> <li>• 1771-ASB</li> <li>• 1747-ASB</li> <li>• 1791-Block</li> <li>• 1794-ASB</li> <li>• 1794-ASB2</li> <li>• 1747-DCM</li> </ul>	<ul style="list-style-type: none"> <li>• RediPANEL</li> <li>• PanelView</li> <li>• Dataliner</li> </ul>	<ul style="list-style-type: none"> <li>• <i>RF tag readers</i></li> <li>• <i>Weigh scales</i></li> <li>• <i>Vibration</i></li> </ul>	<ul style="list-style-type: none"> <li>• S Class, Creonics</li> <li>• 1336, 1395 Drives</li> <li>• 9/SERIES CNC</li> <li>• <i>Welders, Robots</i></li> <li>• <i>Pneumatic valve packs</i></li> <li>• <i>Voice Annunciators</i></li> </ul>

## Typical Applications

Typical applications range from simple I/O links with PLC processors and I/O, to links with a variety of other AB and thirdparty devices. When drives and other devices, including thirdparty devices are to be included in a programmable controller system, the Universal Remote I/O link provides the

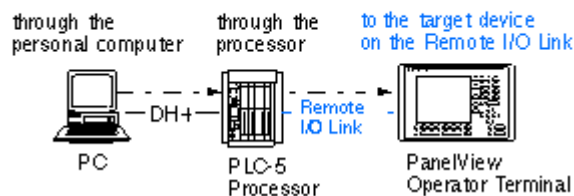
means to do that though remote I/O adapter modules and builtin remote I/O adapters.

Using the Universal Remote I/O Link instead of direct wiring a long distance to a local I/O chassis helps reduce installation, startup, and maintenance costs by placing the I/O chassis closer to the sensors and actuators. To install a Universal Remote I/O Link between buildings or in highnoise areas, such as next to arc welders, use AB fiberoptic repeaters 1771AF, -AF1).



Certain products, such as IMC™ controls, PanelView Operator Terminals, and Dataliner Displays, support "PassThru." This capability lets you configure devices remotely over the Data Highway Plus and Universal Remote I/O links. The example below shows a PanelView configuration file, originally generated using PanelBuilder software on a personal computer, being passed through to a PanelView Operator Terminal.

Certain products such as IMC, PanelView, and Dataliners, support "Pass-Thru," which lets you configure devices remotely.

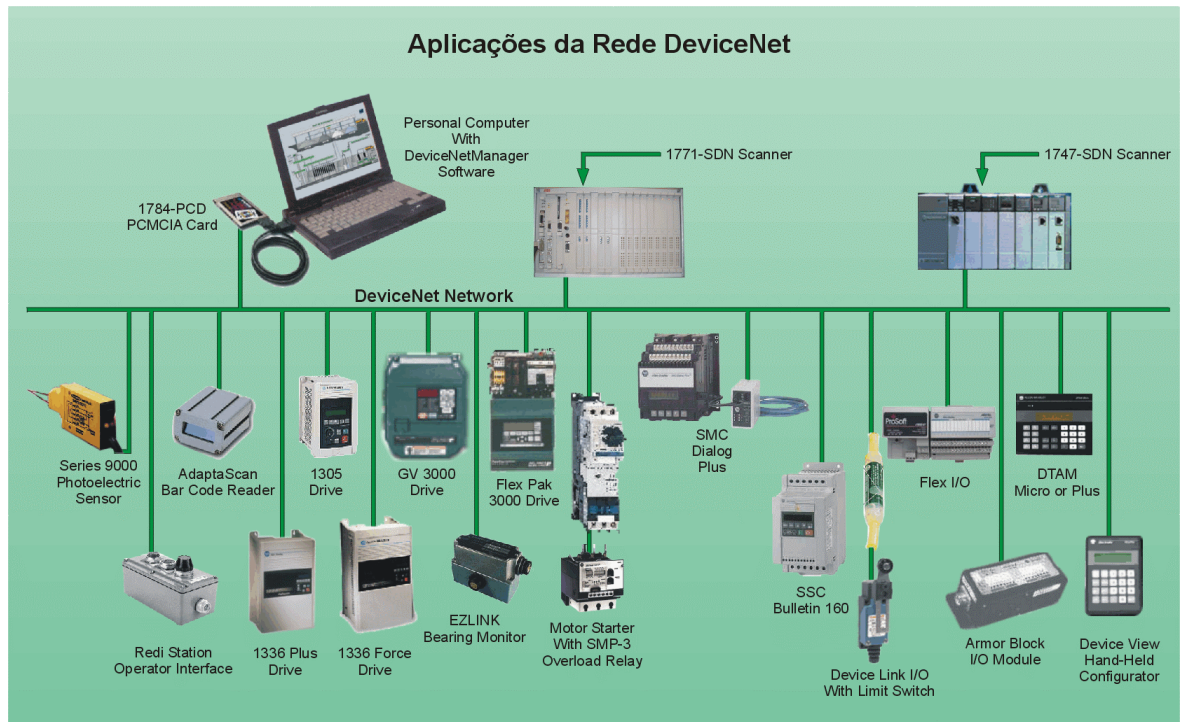


[Automation Systems Catalog](#), page last updated October 3, 2001.

11) Analise a topologia da arquitetura abaixo e responda:

- a) Quais os tipos de dispositivos conectados nesta rede ?
- b) Como você classificaria esta rede: rede de sensores e atuadores (*Sensorbus*), redes de dispositivos (*DeviceBus*) ou rede de instrumentação (*Fieldbus*) ?
- c) Este tipo de dispositivo está de acordo com o esperado pela classificação dada na apostila ?

- d) Que velocidades distâncias e velocidades de comunicação você esperaria desta rede ?
- e) Qual o protocolo de acesso ao meio ?
- f) Existe colisão nesta rede ?
- g) Esta rede é determinística ?
- h) Qual o número máximo de dispositivos suportados por esta rede ?



## Estudo Dirigido - FieldBus

A turma deve ser dividida em grupos de 2 alunos. Cada dupla irá pesquisar um padrão de rede de campo, utilizando o livro texto e a Internet, hoje a maior fonte de informações atualizadas sobre estes padrões (Devido a rápida evolução destas tecnologias, torna-se difícil para os autores de livros abordarem com maior profundidade este assunto)

Após escolhido o tema, responda ao questionário abaixo, tente formar uma opinião concreta sobre suas principais características e importância e prepare uma apresentação de cerca de 10 minutos para defender o padrão escolhido.

Redes		
1. ASI ( <i>Actuator Sensor Interface</i> )	2 .HART	3. SDS ( <i>Smart Distributed System</i> )
4. CAN ( <i>Controller Area Network</i> )	5 .Interbus-S	6. SERCOS
7. Device-net	8. Lon Works	9. Seriplex
10. Field Arcnet	11. P-net	12. SP 50 - Foundation Fieldbus
13. Genius Distributed I/O	14. Profibus DP	15. WorldFIP
16. Bacnet	17.ModbusPlus	18.SwiftNet

1. Nome do padrão:

2. Endereços Internet para informações:

<a href="http://www.">http://www.</a>
<a href="http://www.">http://www.</a>
<a href="http://www.">http://www.</a>
<a href="http://www.">http://www.</a>

3. Criador do padrão:

4. Data de criação:

5. Associação de usuários:

6. Principais expoentes a suportar o padrão:

7. Como você classificaria esta rede de campo ?

- Device Bus
- Fieldbus
- Sensorbus

8. Funções: Interligação de

9. Que PLCs suportam este padrão diretamente ?

10. Padrão físico da rede:

11. Existe *chipset* dedicado ?

12. Fornecedores:

13. Método de acesso ao meio (*token passing*, CSMA-CD, CSMA-CA, etc.)

14. Meios físicos suportados e velocidades de transmissão:

Meio físico	Velocidade (bps)	Distância máxima (m)	Tamanho máximo do pacote de dados (bytes)
◆ fibra-ótica			
◆ par trançado sem blindagem (UTP)			
◆ <i>power line</i> (sistema <i>carrier</i> )			
◆ cabo coaxial			
◆ par trançado blindado (STP)			
◆ infravermelho			
◆ rádio			
◆			

15. Suporta segurança intrínseca ?

16. Alimentação dos dispositivos pelo mesmo cabo de sinal ?

17. Estrutura da rede:

- OSI/ISO ?
- Quantas camadas ?

18. Serviços disponíveis:

19. Topologia da rede:

20. Número máximo de nodos:

21. Suporta conectividade (*repeaters, bridges, routers*) ?

22. *Lay-out* típico da rede:

23. Outras Informações que você julgar importantes:

- 
- 
- 
- 
- 
- 
-

## Bibliografia

- [TANENBAUM 89] Andrew Tanenbaum, Computer Networks, 2<sup>nd</sup> ed, Prentice Hall International Inc, 1989
- [COMER 91] Douglas E. Comer, Internetworking with TCP/IP, Vol I: Principles, Protocols, and Architecture, 2<sup>nd</sup> ed, Prentice-Hall International, 1991
- [Chisholm 98] Al Chisholm, OPC Data Access 2.0 Technical Overview - OLE for Process Control and Factory Automation - [www.Intellution.com](http://www.Intellution.com) - 10/98
- [Iwanitz 01] Frank Iwanitz, Jürgen Lange, OLE for Process Control Fundamentals, Implementation, and Application, Softing, 2001.

## Sites a visitar:

Industrial Ethernet Book	128.242.40.200/index.asp
OPC	www.opcfoundation.org <a href="http://www.matrikon.com">www.matrikon.com</a>
Profibus	www.profibus.com.br
ASi	www.as-interface.net
DeviceNet	www.odva.org
Remote IO	www.ab.com/catalogs/b113/comm/urio.html