

**LIGA DE ENSINO DO RIO GRANDE DO NORTE
FACULDADE NATALENSE PARA O DESENVOLVIMENTO DO RN
ESPECIALIZAÇÃO EM REDES DE COMPUTADORES**

GLAUCUS BRELAZ

**INTRODUÇÃO A
REDES INDUSTRIAIS
PARA PROFISSIONAIS DE TI**

**NATAL/RN
2010**

GLAUCUS BRELAZ

INTRODUÇÃO A
REDES INDUSTRIAIS
PARA PROFISSIONAIS DE TI

Monografia apresentada ao curso de Especialização em Redes de Computadores da Faculdade Natalense para o Desenvolvimento do Rio Grande do Norte como requisito parcial para a obtenção do título de Especialista em Redes de Computadores.

Orientador:
Prof. Dr. Antonio Luiz P. S. Campos

NATAL/RN
2010

GLAUCUS BRELAZ

INTRODUÇÃO A
REDES INDUSTRIAIS
PARA PROFISSIONAIS DE TI

Monografia apresentada ao curso de Especialização em Redes de Computadores da Faculdade Natalense para o Desenvolvimento do Rio Grande do Norte como requisito parcial para a obtenção do título de Especialista em Redes de Computadores.

Orientador:
Prof. Dr. Antonio Luiz P. S. Campos

COMISSÃO EXAMINADORA

Prof. Msc. Aluísio Ferreira Rocha Neto
FARN - Faculdade Natalense para o Desenvolvimento do RN

Prof. Dr. Antonio Luiz Pereira de Siqueira Campos
FARN - Faculdade Natalense para o Desenvolvimento do RN

NATAL, 24 de setembro de 2010

RESUMO

Este trabalho apresenta uma abordagem introdutória às Redes Industriais, dirigida a profissionais de Tecnologia da Informação (TI), com o objetivo de apresentar uma visão geral sobre as tecnologias de comunicação relacionadas aos sistemas de automação e controle encontrados na Indústria, Domótica, em Segurança Eletrônica e em Geração e Conservação de Energia entre outras aplicações. Considerando que essas tecnologias, por estarem intimamente relacionadas aos sistemas de controle, são da competência de engenheiros de automação, o trabalho inicia com um breve histórico da evolução da automação, oportunidade em que são introduzidos alguns conceitos, terminologias e equipamentos empregados nestes sistemas. Uma visão geral da hierarquia de redes em instalações industrial é apresentada, conceituando os barramentos de instrumentação e de campo. Seguem-se as descrições de alguns padrões de comunicações de chão de fábrica, tentando-se manter uma ordem de cronológica e de complexidade, desde simples padrões até os protocolos mais complexos. Ao final são apresentadas as redes que representam a tendência dos processos de automação trazendo os conceitos de sensores inteligentes, *smart objects* e *IP Enabled Smart Objects*.

Palavras-chave: Redes Industriais. Automação Industrial. Sensores. Atuadores. Barramentos de Campo. Controladores Lógicos Programáveis. Sensores Inteligentes.

ABSTRACT

This paper presents an introductory approach to Industrial Networks, addressing Information Technology (IT) Professionals, with the aim of presenting an overview of the communication technologies related to automation and control systems found in industry, Home Automation, Electronic Security and Energy Generation and Conservation among other applications. Keeping in mind that these technologies, being closest to control systems, are under automation engineer's domain, this paper begins with a brief history of automation, opportunity where some concepts, terminology and equipment used in these systems are introduced. An overview of the networks hierarchy in industrial installations is presented, conceptualizing instrumentation and fieldbuses. Following are descriptions of some factory floor communication standards, trying to keep chronological and complexity sequence, ranging from simple standards, to more complex protocols. At the end of this paper, the networks that represent the trend of automation processes are presented, together with the concepts of smart sensors, smart objects and IP Enabled Smart Objects.

Keywords: Industrial Networks. Industrial Automation. Sensors. Actuators. Field buses. Programmable Logic Controllers. Smart Sensors.

LISTA DE ILUSTRAÇÕES

Figura 1	Hierarquia dos Sistemas de Automação	10
Figura 2	Controle de nível em um tanque de fluido	12
Figura 3	CLP Siemens Simatic S5	13
Figura 4	Comparação entre os sistemas de controle centralizado e SDCD's	14
Figura 5	Representação gráfica de um Sistema Integrado de Gestão Industrial	15
Figura 6	Circuito típico de monitoração remota 4-20mA.....	18
Figura 7	Transmissor Rosemount 644	19
Figura 8	Comparação entre os modos de comunicação unipolar e bipolar	20
Figura 9	Efeito da EMI em cabos paralelos versus par trançado	20
Figura 10	Rede multiponto com camada física EIA-485	21
Figura 11	Formato do quadro de mensagem ModBus	22
Figura 12	Camadas dos protocolos ModBus e hierarquias de aplicação	23
Figura 13	Formato do quadro de mensagem ModBus Plus	24
Figura 14	Topologias de redes Hart	26
Figura 15	Formato do quadro de mensagem Hart	26
Figura 16	Relação entre a modulação APM e a codificação Manchester-II	27
Figura 17	Formato de Telegrama na rede AS-i para chamadas e respostas	28
Figura 18	Topologia da rede DeviceNet	29
Figura 19	Quadro de dados da rede DeviceNet	29
Figura 20	Pilha de protocolos do padrão Profibus e seus perfis	32
Figura 21	Acesso híbrido ao meio físico do padrão Profibus	33
Figura 22	Várias conexões lógicas na rede Profibus Modbus/TCP	34
Figura 23	Modelo Foundation Fieldbus em comparação com o modelo OSI	36
Figura 24	Formato do quadro de dados Foundation Fieldbus	36
Figura 25	Informação através das camadas Foundation Fieldbus	37
Figura 26	Integração Ethernet / Foundation Fieldbus.....	38
Figura 27	Diagrama de blocos de um sensor no Sistema IEEE1451.....	39
Figura 28	NCAP (versão Ethernet) e TIM com interface RS-232	40
Figura 29	Redução do Backbone Ethernet	44

LISTA DE TABELAS

Tabela 1	Volume de dados e tempo de reação versus o nível de informação	16
Tabela 2	Características do padrão EIA-485A Conceção Profibus	21
Tabela 3	Padrões Ethernet que viabilizaram aplicações industriais	43

LISTA DE ABREVIATURAS E SIGLAS

100-BaseT	Padrão Ethernet de 100 Mbit em par trançado
ASCII	American Standard Code for Information Interchange
APM	Arbitration on Message Priority
ATM	Asynchronous Transfer Mode
AS-i	Actuator-Sensor Interface - Interface Sensor-Atuador
APM	Alternating Pulse Modulation
TI	Tecnologia da Informação
CAN	Controller Area Network
CPU	Central Processing Unit
CLP	Controlador Lógico Programável
CRC	Cyclic Redundancy Check
CSMA/CD	Carrier Sense Multiple Access with Collision
CSMA/NBA	Carrier Sense Multiple Access with Non Destructive Bitwise Arbitration
DLL	DAta Link Layer
DDL	Device Description Language
DDC	Direct Digital Control
DP	Distributed Peripheral
EEPROM	Electrically-Erasable Programmable Read-Only Memory
EIA	Electronics Industry Association
EMI	Eletromagnetic Interference
ERP	Enterprise Resources Planning - Sistemas de Planejamento Empresarial
EPS	Enterprise Production Systems
ERP	Enterprise Resource Planning
FMS	Fieldbus Message Especification
FMS	Fieldbus Message Specification
HART	Highway Addressable Remote Transducer
HDLC	High-Level Data Link Control
HTTP	Hypertext Transfer Protocol
IEEE	Institute of Electrical and Electronics Engineers
IHM	Interface Homem-Máquina
ISO	International Standards Organization

IS	Intrinsic Safety
LAS	Link Active Scheduler
LAN	Local Area Network
LD	Linking Device
LLI	Lower Layer Interface
MAC	Medium Access Control
MODEM	Modulação e Demodulação
NCAP	Network Capable Application Processor
NIST	National Institute of Standards and Technology
OSI	Open Systems Interconnection
OD	Object Dictionary
PA	Process Automation
QoS	Quality of Service
RO	Read Only
RFI	Radio Frequency Interference
RS-232	Recommended Standard 232
RS-485	Recommended Standard 485
RTU	Remote Terminal Unit
SCADA	Supervisory Control and Acquisition Data System
SCM	Supply Chain Management
SDCD	Sistema Digital de Controle Distribuído
STP	Shielded Twisted-Pair
TEDS	Transducer Electronic Data Sheet
TCP/IP	Transmission Control Protocol/Internet Protocol
TIA	Telecommunications Industry Association
TIM	Transducer Interface Module
UTP	Unshielded Twisted-Pair
XML	Extensible Markup Language
VFD	Virtual Field Devices

SUMÁRIO

1.	INTRODUÇÃO	10
2.	HISTÓRICO	12
3.	HIERARQUIAS DE REDES INDUSTRIAIS	15
4.	PADRÕES DE CAMADA FÍSICA	18
4.1	Loops de Corrente 4-20mA	18
4.2	O Padrão TIA/EIA-485	20
5.	PROTOCOLOS A CARACTERE	22
5.1	Protocolo Modbus	22
5.2	Protocolo Modbus Plus	24
6.	REDES COM ALIMENTAÇÃO SOBREPOSTA	25
6.1.	O protocolo HART	25
6.2	AS-Interface	26
6.3.	Redes Devicenet	28
7.	PROCESS FIELDBUS (PROFIBUS)	31
7.1	A Concepção Profibus	31
7.2	O Acesso Híbrido ao Meio Físico	33
7.3	Dispositivos de Campo Virtuais	34
8.	FOUNDATION FIELDBUS	35
8.1	A Concepção Foundation Fieldbus	35
8.2	O Agendamento de Links Ativos	36
8.2	O Padrão HSE	38
9.	NIST - IEEE 1451	39
10.	ETHERNET INDUSTRIAL	41
10.1	Fieldbus HSE	41
10.2	Rede ProfiNet	42
10.3	IEEE 1451	42
10.4	Modbus/TCP	42
10.5	Melhoramentos na Rede Ethernet	43
11.	CONCLUSÃO	46
	REFERÊNCIAS	47

1. INTRODUÇÃO

Com a evolução da automação¹ e a necessidade cada vez maior da troca de informações entre os setores das empresas, administradores de redes podem a qualquer momento ter necessidade de interligar redes envolvidas na supervisão e controle de processos com as redes administrativas. Esse fato é resultado da integração cada vez mais freqüente de sistemas automatizados utilizados na Indústria, na Domótica², em Segurança Eletrônica e em Geração e Conservação de Energia, com os sistemas tradicionalmente gerenciados pelos profissionais de TI.

Sistemas que operam dessa forma, chamados de Sistemas Integrados de Automação, têm por característica uma grade variedade de interfaces com o mundo real gerando e utilizando informações com formatos e requisitos específicos, com conseqüente diversidade de padrões e protocolos de comunicação. Esses sistemas são fortemente baseados em recursos de hardware, apresentando uma hierarquia semelhante a que é ilustrada na Figura 1 onde os mais sofisticados recursos de software estão nos níveis hierárquicos menos envolvidos diretamente com a automação. Como poderá ser visto ao longo deste trabalho, existe a tendência de deslocamento cada vez maior do software para os dispositivos de campo o que está alterando a geometria dessa tradicional hierarquia.

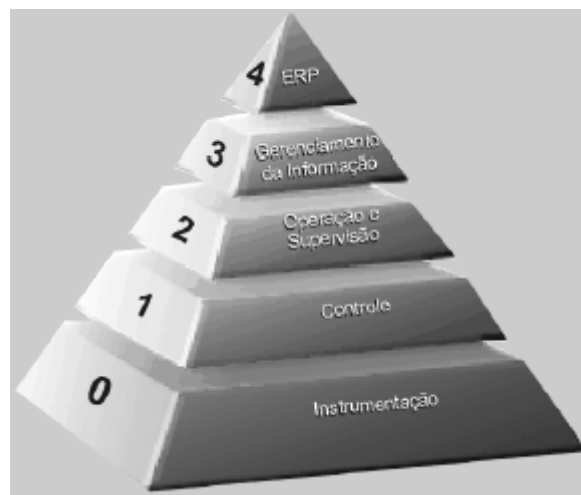


Figura 1. Hierarquia dos Sistemas de Automação com a relação hardware/software.

O profissional de TI envolvido em administração de redes não pode mais estar à margem da compreensão das Redes Industriais cujo tratamento atualmente é da competência apenas de engenheiros e técnicos de automação. Este trabalho pretende fornecer ao leitor uma

¹ Execução de tarefas por máquina ou sistema com a mínima interferência do operador humano.

² Gestão automatizada de recursos residenciais.

visão geral sobre Redes Industriais e uma introdução aos principais tipos de Redes existentes, apresentando suas características e justificativas de utilização. Um breve histórico da evolução da automação industrial é apresentado juntamente com fundamentos dos processos de automação e controle. A hierarquia de redes é abordada de forma a dar uma idéia básica do posicionamento das diversas redes dentro do sistema industrial. As comunicações de chão de fábrica são descritas, tentando-se manter uma ordem de cronológica e de complexidade, desde simples padrões até os protocolos mais complexos, sem o compromisso de detalhamento de protocolos ou avaliações de performance.

2. HISTÓRICO

Na indústria existem basicamente dois tipos de processos: Processos Contínuos e Processos Discretos. Nos Processos Contínuos o produto apresenta saída contínua como o caso de líquidos, gases e pós. Nos Processos Discretos a saída é contabilizada em unidades como peças ou equipamentos (SILVEIRA, 1998) (Ribeiro, 2005). O controle de processos contínuos geralmente envolve variáveis analógicas como pressão, temperatura, pH, ao passo que os processos discretos envolvem variáveis discretas como contagem de peças, estampa, soldagem, embalagem, etc. Uma indústria pode utilizar combinações dos dois tipos de processo como, por exemplo, uma indústria de refrigerantes que engarrafa o líquido produzido e acomoda garrafas em caixas.

A mecanização surgiu no século XVII com as máquinas a vapor, porém os primeiros mecanismos automáticos só surgiram no século XIX, junto com as linhas de montagem. Foram usados inicialmente sistemas puramente mecânicos. Depois surgiram os pneumáticos (que usam a energia do ar comprimido) e os hidráulicos (que usam a energia de fluidos, normalmente óleo). Com a introdução da energia elétrica, os processos discretos foram beneficiados pela introdução dos controles sequenciais baseados em temporizadores e relés, conectados a acionadores eletromecânicos.

Com o aparecimento dos sensores, transdutores, válvula de fluxo e reostatos, o controle de processos contínuos, tradicionalmente efetuados através da leitura de medidores e ajustes manuais, puderam ser substituídos por controles em malha fechada³ (OGATA,2006) usando controladores analógicos. Controles isolados com monitoração remota puderam substituir tarefas manuais como, por exemplo, manter a temperatura de um forno ou um nível pré-determinado em um reservatório conforme exemplificado na Figura 2.

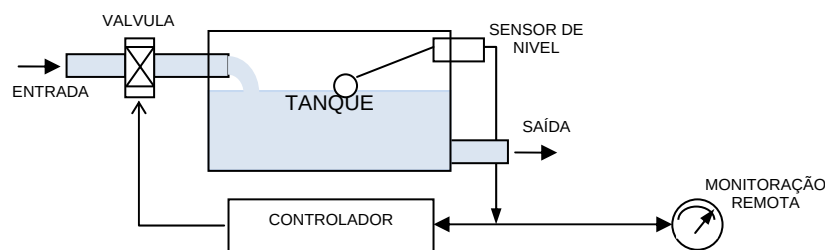


Figura 2. Controle de nível de um tanque de fluido com monitoração remota.

³ Forma de controle onde a diferença entre a amostragem da saída e um valor de referência corrige o comportamento do processo.

A monitoração remota possibilitou o acompanhamento de processos em locais de difícil acesso possibilitando melhor controle da produção (BEGA, 2006). Sensores e medidores analógicos passaram a se comunicar por meio de cabos instalados ao longo da planta industrial.

Com a introdução dos circuitos digitais no início da década de 60, os controles por relés foram sendo substituídos por circuitos lógicos. Grandes indústrias como a automotiva e a petroquímica investiram em computadores tipo *mainframe*, inicialmente para monitoração e posteriormente para controle dos processos. Mainframes podiam controlar vários processos simultaneamente, mas necessitavam de longos cabos para interligar suas salas refrigeradas com maquinário de produção.

O aumento da capacidade de processamento em tempo real e o desenvolvimento dos conversores A/D e D/A, possibilitou a criação dos sistemas DDC (*Direct Digital Control*). Os computadores passaram a substituir os controladores analógicos nos processos contínuos utilizando os mesmos sensores e atuadores já implantados. Executando digitalmente as funções dos controladores analógicos os computadores podiam facilmente otimizar seus parâmetros de funcionamento pela simples alteração do software.

Com a redução do tamanho das CPU's, placas processadoras e interfaces foram instaladas em rack's, próximo aos equipamentos de produção numa alternativa que beneficiou as indústrias de médio porte (Figura 3). Esse arranjo deu origem aos Controladores Lógicos Programáveis (CLP's) no início da década de 70. Inicialmente utilizados para seqüenciamento e intertravamento (BOLTOM, 2006), os CLP's evoluíram muito com a utilização dos microprocessadores. De controle de processos isolados os CLP's passaram a trabalhar através de conexões per to per ou em redes, com diversos níveis hierárquicos, formando sistemas descentralizados⁴.

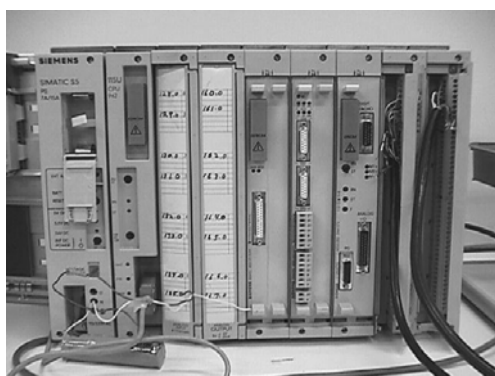


Figura 3. CLP Siemens Simatic S5

⁴ Controle implementado de forma distribuída com dados processados localmente.

A abordagem centralizada dos mainframes nos sistemas DDC apresentava várias desvantagens: a dependência de um sistema único, o alto custo de atualização do hardware, a quantidade de cabos e a distância do controle ao processo. Os Sistemas Digitais de Controle Distribuído (SDCD's) surgiram em 74 para resolver esses problemas a través de um modelo hierárquico de processamento distribuído com um controle centralizado (BEGA, 2006). Nesses sistemas os processadores de controle são instalados próximos aos equipamentos a serem controlados. Existem estações de operação, que comandam esses processadores, ligadas por barramento de alta velocidade a uma sala central onde se executa o controle supervísório (RIBEIRO, 1999). A Figura 4 apresenta um comparativo entre os sistemas centralizados e os SDCD's.

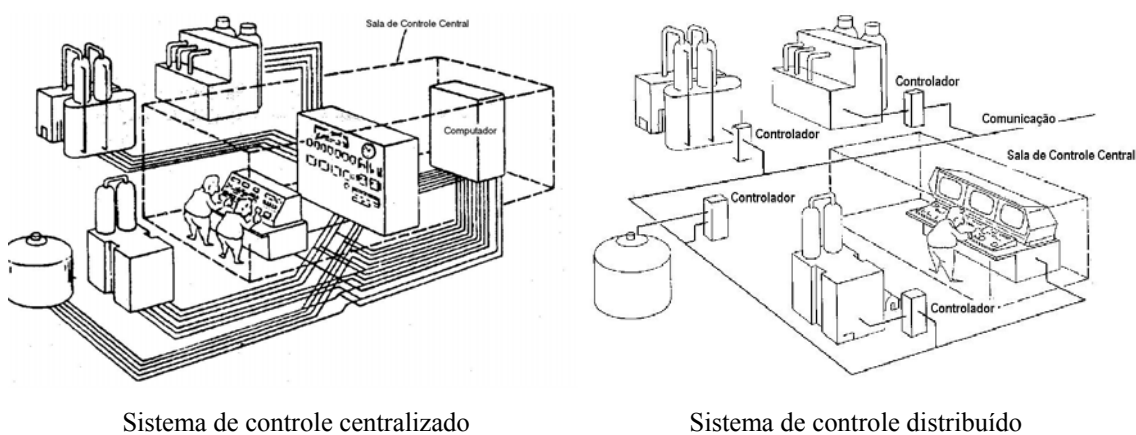


Figura 4. Comparação entre os sistemas de controle centralizado e SDCD's

Paralelamente ao desenvolvimento de controle, os controles supervísórios evoluíram de observadores a interventores dos processos de controle, possibilitando a re-programação de setores da produção através de avançadas interfaces homem-máquina (IHM). A utilização dos sistemas SCADA (*Supervisory Control and Data Acquisition*) na indústria possibilitou a integração de processos geograficamente distribuídos, atendendo principalmente a indústria petroquímica. Os sistemas SCADA utilizam bancos de dados distribuídos e uma grade variedade de redes e topologias (BAILEY, 2003)

Atualmente os sistemas industriais empregam tanto tecnologias recentes como heranças dos modelos que tiveram sucesso no passado. Ao contrário das redes de computadores onde a padronização chegou relativamente cedo, a automação industrial já estava em plena utilização quando a eletrônica digital começou a ser aplicada. Substituir equipamentos e processos sem prejudicar a produção, além de capacitar mão de obra para os avanços que se apresentavam foi uma tarefa difícil em muitos casos realizada gradualmente.

3. HIERARQUIAS DE REDES INDUSTRIAIS

Hierarquias de redes nas indústrias modernas incluem pelo menos três níveis de interligação: um a nível de equipamento no chão de fábrica, outro a nível do supervisor que interliga os equipamentos de controle e o último a nível de gerenciamento que é o que se interliga com os setores administrativo e comercial (SCHAEFFER, 2004). Um sistema de rede industrial de uma grande empresa pode se assemelhar ao esquema da Figura 5.

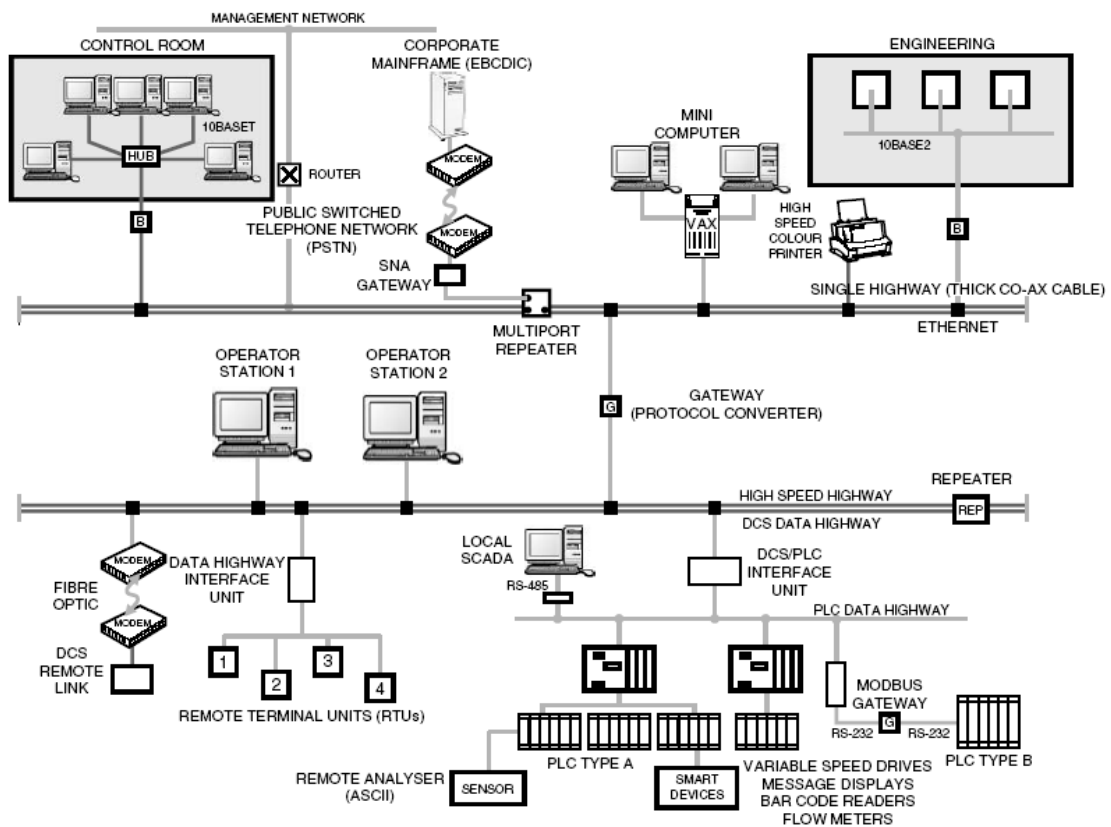


Figura5. Representação gráfica de um Sistema Integrado de Gestão Industrial (Mackay, 2004)

Os vários níveis hierárquicos de rede apresentam diferentes requisitos. No nível mais baixo estão as comunicações entre sensores e atuadores com diversos tipos de CLP's ou controladores. Neste nível as redes são chamadas de Barramentos de Campo (*Fieldbuses*), e são voltadas principalmente para comunicações ponto a ponto, muitas vezes realizadas de forma analógica (por loops de corrente). Sensores dotados de maior complexidade eletrônica são capazes de implementar comunicações digitais baseadas em padrões tipo RS-232 ou RS485, através de protocolos de barramentos de campo como Hart, ModBus, AS-i, etc. Mesmo a baixas taxas de comunicação (1200bps a 250Kbps) estas ligações são muito eficientes por serem ponto a ponto e com troca de pequena quantidade de dados.

No nível intermediário, ocorrem trocas de dados entre CLP's ou entre CLP's e supervisórios. Neste nível existem protocolos de comunicação de baixo *overhead*⁵ e estas redes devem garantir baixa latência e baixa taxa de erro. Muitas vezes equipamentos de diferentes origens possuem diferentes protocolos e padrões proprietários ou não podendo haver necessidade de gateways conversores de protocolos. Alguns dos protocolos mais comuns são: DeviceNet, ControNet, DF1, Data Highway 485 da Allen Bradley (antiga Rockwell); Profibus da Siemens e Modbus Plus e ModBus TCP/IP da Modicom (hoje Schneider Electric).

Os Sistemas Supervisórios oferecem uma interface entre o operador e o processo que não existe nas CLP's e nos Controladores. Os modernos supervisórios são programas que rodam em PC's industriais de alta confiabilidade e permite a operação e visualização através de telas gráficas elaboradas de acordo com o processo industrial monitorado. Os supervisórios se comunicam com centrais de controle ou com sistemas administrativos através de barramentos de alta velocidade.

O nível mais alto é representado pela rede de informação. Em grandes corporações é natural a escolha de um backbone de grande capacidade para interligação dos Sistemas Planejamento de Recursos (Enterprise Resource Planning - ERP), Sistemas de Gerenciamento da Cadeia de Suprimentos (Supply Chain Management - SCM) e os Sistemas de Controle de Produção (Enterprise Production Systems - EPS). Este backbone pode ser baseado em rede ATM ou GigaEthernet utilizando fibra ótica ou cabeamento STP nível 5 mas está cada vez mais popular o uso de redes Ethernet 100-BaseT com cabeamento UTP, devido à sua simplicidade e baixo custo.

A Tabela 1 apresenta uma idéia do que sejam os tempos de reação das aplicações em relação aos diversos níveis de informação em um ambiente industrial. Pode parecer um contra-senso que as comunicações de maior simplicidade esteja justamente nos níveis onde os requisitos de reação sejam de maior exigência.

Tabela 1. Volume de dados e tempo de reação versus o nível de informação em uma fábrica

	VOLUME	TEMPO de REAÇÃO	PERIODICIDADE
Gerenciamento	MByte	minutos a horas	dia / turno / hora
Supervisão	KByte	100ms a 1s	segundos a minutos
Operação	Byte	10ms a 100ms	milisegundos a segundos
Atuador-Sensor	Bit	milisegundos	milisegundos

⁵ Carga adicionada aos dados pelos serviços das diversas camadas de protocolos..

A resposta para a eficiência dessas redes de campo está na simplicidade de implementação, pequeno volume de dados e baixo *overhead*. Neste sentido foram desenvolvidos padrões de comunicação e protocolos de enlace que pudessem sustentar as aplicações com um mínimo de camadas intermediárias de endereçamento, roteamento e estabelecimento de seções, mas ainda assim atendendo as necessidades mais complexas do moderno instrumental industrial.

4. PADRÕES DE CAMADA FÍSICA

4.1 Loops de Corrente 4-20mA

Com a tecnologia de meados do século passado, era difícil a troca de sinais de controle e medição através do ambiente industrial. A resistência dos cabos de comunicação e as fortes interferências geradas pelo chaveamento de cargas, motores, e soldadores, tornavam impraticável a comunicação por sinais baseados em amplitudes de tensão. Desde o início do século entretanto, loops de corrente foram utilizados com sucesso por equipamentos de telex (teletipos) para comunicações em longas distâncias. Com um código de 5 bits (32 caracteres) também conhecido como código Baudot, os sinais de teletipo codificavam uns e zeros como correntes de 0 e 20mA.

Os loops de corrente usam variações de corrente ao invés de variações de tensão para transmitir informação. Nos loops de corrente o efeito da resistência da fiação e das conexões é anulado porque a corrente em todos os pontos do loop é a mesma (lei de Kirchhoff), e a baixa impedância e limitada banda passante da linha minimizam os efeitos das interferências eletromagnéticas (EMI) e de rádio frequência (RFI). Como na maioria dos processos a taxa de variação do sinal é baixa (menor que 100Hz) o loop de corrente passou a ser largamente empregado nas instalações industriais.

O Loop de Corrente 4-20mA não é um padrão oficial mas a sua ampla utilização o tornou um padrão de facto da indústria a partir dos anos 60 (MAKAY, 2004). A Figura 6 apresenta o diagrama de um circuito de medição utilizando Loop de Corrente 4-20mA.

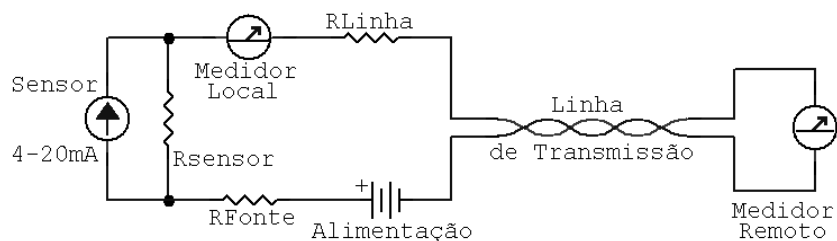


Figura 6. Circuito típico de monitoração remota de um sensor em Loop de 4-20mA.

A faixa de valores foi adotada de forma que a corrente tenha potência necessária para energizar pequenos dispositivos eletromecânicos no lado receptor ao mesmo tempo em que seja baixa o suficiente para ser controlada pelos sensores e transdutores no lado transmissor.

O valor 4mA representa 0%, garante um nível de sinal acima de possíveis ruídos e possibilita a detecção de circuito aberto (caso a corrente atinja valores próximos a zero).

Não existe limite imposto para a tensão utilizada, o que permite que vários instrumentos de medição possam ser inseridos no loop. No diagrama da Figura 5 estão instalados dois medidores. É importante observar que instrumentos com resistência ôhmica interna de 250Ω apresentam medida de 5V em fundo de escala.

A saída 4-20mA é atualmente encontrada em uma grande variedade de sensores e instrumentos industriais e está presente como opção de interface inclusive nos modernos instrumentos digitais. Instrumentos como o transmissor apresentado na Figura 7 podem ser programados digitalmente e produzir saídas em múltiplos formatos incluindo 4-20mA.



Figura 7. Transmissor Rosemount 644 para sensores de temperatura com saída em formatos 4-20mA, Hart e Foundation Fieldbus. Fonte: WE Instrumentation Limited

4.2 O Padrão TIA/EIA-485

Com a introdução dos equipamentos digitais, surgiu a necessidade de comunicação eficiente entre computadores e interfaces do processo, suficientemente robustos às perturbações presentes em chão de fábrica. O padrão de comunicação EIA-232 introduzido em 1962 e utilizado para conexões de computadores e periféricos e terminais remotos, não se mostrou suficientemente adequado para ambiente industrial. Apesar de utilizar níveis de tensão superiores aos encontrados nas placas lógicas sua principal fragilidade era o referencial comum ao terra. Os fortes loops de corrente de aterramento no chão de fábrica podem produzir diferenciais de tensão de vários Volts em poucos metros de distância.

Alguma vez referido como RS-485 (*Recommended Standard 485*), o padrão EIA-485, descrito pelas normas TIA/EIA-485 e ISO/IEC 8482.1993, atende as necessidades fabris com o emprego de sinalização diferencial sem referência ao terra e da utilização cabos de par

trançado. Uma comparação entre a sinalização unipolar e a sinalização diferencial é ilustrada na Figura 8. No modo unipolar de transmissão, as interferências induzidas no condutor com referencial terra são adicionadas ao sinal causando dificultando a recuperação da informação. No modo bipolar os sinais nos dois condutores têm fases opostas. As interferências induzidas nos dois condutores têm a mesma fase e conseqüentemente são eliminadas no receptor (AXELSON, 2000).

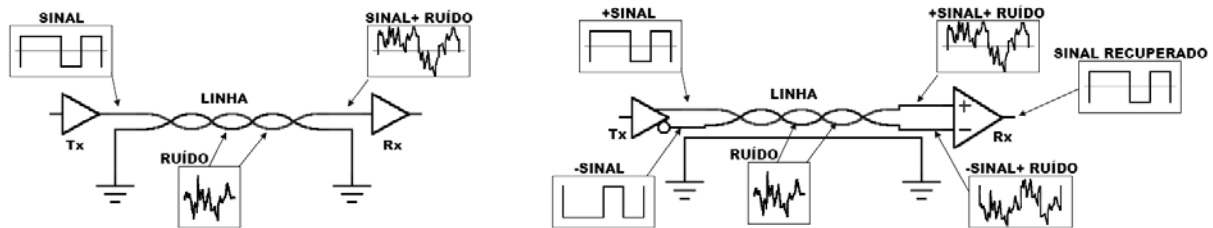


Figura 8. Comparação entre os modos de comunicação unipolar e bipolar.

Adicionalmente os condutores que transportam a informação podem ser trançados fazendo com que os campos magnéticos produzam correntes opostas em seções consecutivas do mesmo fio (Figura 9). Os cabos podem ainda ser blindados (STP) ou não blindados (UTP).

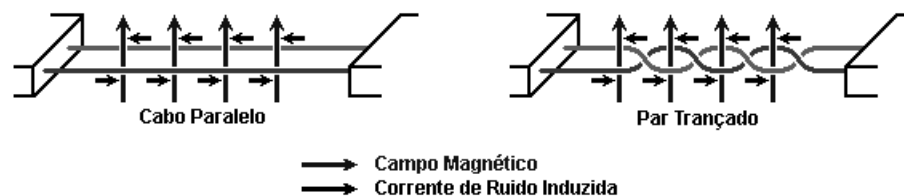


Figura 9. Efeito da EMI em cabos paralelos versus par trançado.

O padrão EIA-485 permite comunicação multiponto *half-duplex* recomendando-se a topologia em barra com a inserção de até 32 nós e utilização de terminadores de 120 Ohms. A Figura 10 apresenta uma rede típica com camada física EIA-485. A comunicação *full-duplex* pode ser obtida pela utilização de dois pares na comunicação possibilitando a implementação de uma grande variedade de protocolos. A Tabela 2 apresenta as características técnicas do padrão EIA-485.

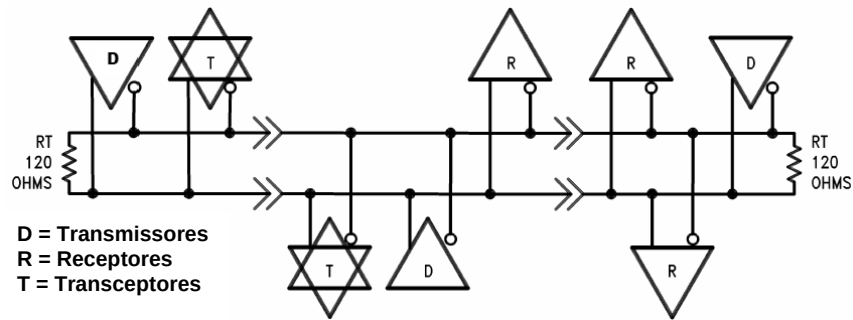


Figura 10. Rede multiponto com camada física EIA-485.

Tabela 2. Características do padrão EIA-485. Fonte: Maxim nota de aplicação AN736.

PARÂMETRO	VALOR
Comprimento máximo do cabo	1220m
Taxa de transmissão máxima	10Mbps
Tensão de sinalização mínima	$\pm 1,5V$
Tensão de sinalização máxima	$\pm 5,0V$
Corrente máxima de curto circuito	250mA
Impedância de Linha	120 Ohms
Impedância dos terminadores	120 Ohms
Forma de transmissão	Diferencial
Forma de comunicação	<i>Half-duplex</i>
Número máximo de transmissores e receptores	32

O padrão EIA-485 é atualmente utilizado com os protocolos de rede ModBus, ModBus Plus, Data Highway DH485 e ProfiBus e é suportado por um grande variedade de fabricantes de chips de interface e cabos de comunicação.

5. PROTOCOLOS DE CARACTERE

Alguns protocolos de redes industriais são conhecidos como protocolos de caracteres por transportar dados no formato ASCII, embora todos eles tenham a capacidade de também comunicar-se através de dados hexadecimais. A utilização de comandos tanto em formato ASCII como em hexadecimal provê um meio de visualizar a comunicação presente na rede através de terminais do tipo teletipo, muito usado na época dos *mainframes*, durante processos de manutenção ou calibração.

5.1 Protocolo Modbus

ModBus é uma protocolo de especificação aberta criado pela Gould Modicon (hoje Schneider Electric) em 1979 para estabelecer comunicação entre CLP's sensores e atuadores. O protocolo implementa apenas as camadas de aplicação e de enlace do modelo OSI operando com base na configuração mestre-escravo. Em uma rede ModBus o dispositivo mestre pode ser um CLP enquanto os escravos são sensores, válvulas, solenóides ou, em uma hierarquia de CLP's, o dispositivo máster pode ser um CLP que comanda um grupo de CLP's escravos.

No protocolo ModBus a camada física é baseada no padrão RS-485 (EIA-485) o que limita a rede a 32 nós em um mesmo segmento. Os enlaces são realizados entre o dispositivo mestre e até 246 escravos com endereços pré configurados em cada escravo entre 1 e 247, mas na prática o limite imposto pelo EIA-485 dificilmente é alcançado (MAKAY, 2004).

As trocas de dados podem ser feitas em dois modos: modo ASCII onde as mensagens são legíveis, usado principalmente para testes e no modo RTU com formato hexadecimal, mais compacto e rápido, usado nas operações normais. A verificação de erros é feita na camada física pela verificação de paridade e na camada de enlace pela verificação do LRC no modo ASCII e do CRC16 no modo RTU. A Figura 11 mostra os formatos do quadros de mensagem ModBus (MODICOM, 1996).

Formato ASCII

Start	Endereço	Função	Dados	LRC	END
: (0x3A)	2 Chars	2 Chars	N Chars	2 Chars	CRLF

Formato RTU

Start	Endereço	Função	Dados	CRC	END
Silêncio 3..5 chars	← 8 bits→	← 8 bits→	←N x 8 bits→	←16 bits→	Silêncio 3..5 chars

Figura 11. Formato do quadro de mensagem ModBus

O protocolo ModBus apesar de proprietário, tornou-se padrão de-facto adotado pela indústria. A Schneider incentivou essa adoção através do apoio a uma organização de usuários e desenvolvedores independentes chamada Modbus-IDA. O protocolo ModBus atualmente suporta outros protocolos de comunicação mestre-escravo como ModBus Plus e ModBus TCP/IP. A figura 12 relaciona as camadas dos protocolos ModBus com o modelo de referência OSI (KRUTZ, 2006) e ilustra a hierarquia de aplicações.

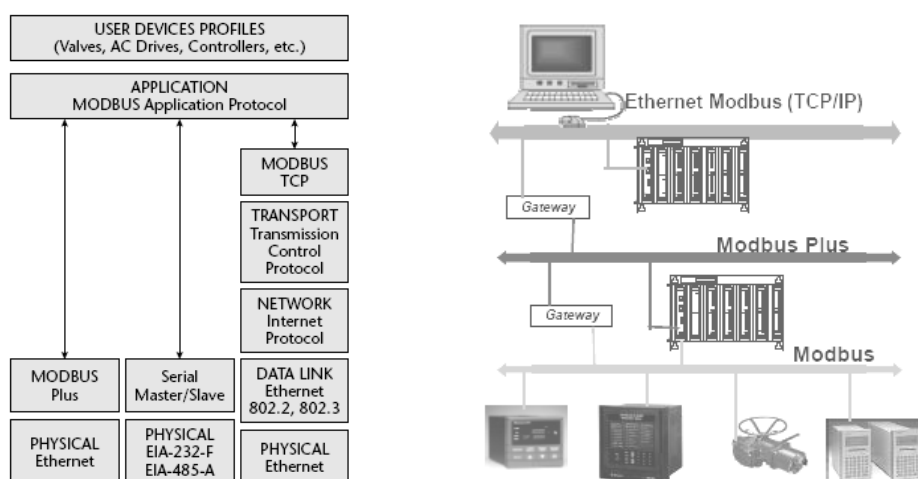


Figura 12. Camadas dos protocolos ModBus e hierarquias de aplicação.

5.2 Protocolo Modbus Plus

O protocolo ModBus Plus foi criado para contornar a limitação de mestre único do protocolo ModBus e ao contrário do ModBus clássico, não é um protocolo aberto. O ModBus Plus é um protocolo determinístico, baseado em passagem de ficha que permite até 64 dispositivos em um segmento rede ser conectado a outros segmentos até 5 níveis. Como no ModBus, os endereços são pré configurados em cada nó porém apenas na faixa entre 1 e 64 e o roteamento inclui agora o endereço do dispositivo e o endereço da rede ao qual está conectado. A Figura 13 apresenta o formato de quadro do protocolo ModBus Plus (MAKAY, 2004).

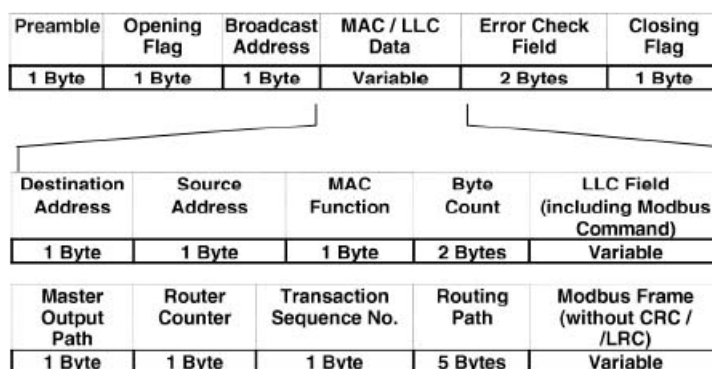


Figura 13. Formato do quadro de mensagem ModBus Plus

O protocolo ModBus Plus é usado para comunicação entre CLP's, CLP's e Supervisórios, módulos de controle, chaves de partida eletrônica de motores, interfaces homem máquina etc. O meio físico é o RS-485 com taxas de transmissão de 1 Mbps e controle de acesso ao meio por HDLC (*High Level Data Link Control*).

O protocolo ModBus TCP/IP é usado para comunicação entre sistemas de supervisão e controladores lógicos programáveis. O protocolo Modbus é encapsulado no protocolo TCP/IP e transmitido através de redes padrão ethernet com controle de acesso ao meio por CSMA/CD.

6. REDES COM ALIMENTAÇÃO SOBREPOSTA

É muito comum na indústria a instalação de instrumentos e dispositivos de campo em áreas remotas ou de difícil acesso. Prover alimentação para tais dispositivos através do mesmo cabeamento pelo qual é realizada a comunicação é uma forma de tornar mais prática e econômica de instalação de tais dispositivos. Embora existam sérias limitações de fornecimento de corrente nessas soluções, os equipamentos são projetados para funcionar com baixo consumo dispondo apenas das mínimas funções necessárias.

6.1 O Protocolo HART

O protocolo HART (*Highway Addressable Remote Transducer*) foi criado pela Rousemont (atualmente Emerson Process Management) para acomodar as técnicas de comunicação digital de instrumentos, sensores e atuadores na rede instalada de comunicação por loop de corrente possibilitando a convivência dos dispositivos analógicos com sensores providos de comunicação digital (PARK, 2002).

O protocolo HART funciona através da sobreposição do sinal de comunicação digital aos sinais analógicos de 4-20mA, usando modulação FSK (*frequency shift keying*) baseado no padrão de comunicações Bell 202 (MAKAY, 2004). As frequências chaveadas são 1200kHz referente ao nível lógico "1" e 2400kHz referente ao nível lógico "0". Os dispositivos na rede Hart podem ser alimentados individualmente ou pela energia transportada pelo loop de corrente mas o sinal FSK é transmitido de forma que a corrente média do sinal é zero e a do corrente do loop permanece dependente apenas dos dispositivos analógicos.

O protocolo Hart funciona de três formas (Figura 14): (1) junto com o sinal analógico de 4-20mA no modo ponto a ponto, (2) em conjunto com outros dispositivos de campo no modo *multi-drop* ou (3) com um dispositivo de campo único enviando sinal em *broadcast*. Nas formas (1) e (2) o protocolo opera em forma de varredura (*poll/response mode*) onde o mestre solicita de cada instrumento de campo as informações programadas. Na forma (3), modo *broadcast*, o instrumento de campo envia continuamente dados do processo sem a requisição do mestre.

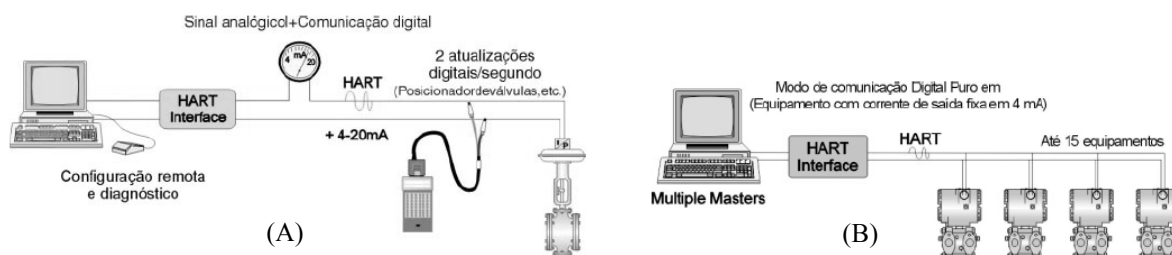


Figura 14. Topologias de redes Hart: (A) loop analógico e digital; (B) em barra com comunicação digital.

Fonte: <http://www.smar.com/hart.asp>

No protocolo Hart apenas as camadas de aplicação, de enlace e física do modelo OSI são implementadas. A camada de aplicação define os comandos, respostas, tipos de dados e decodifica os relatórios de status do dispositivo. A camada de enlace divide a informação a ser transmitida em pacotes, adiciona os bits de detecção de erros e controla o acesso ao meio. A camada física especifica como os dispositivos serão conectados mecanicamente e eletricamente (tipo de cabo, distâncias, aterramento) e define de que forma o sinal digital será codificado.

Em uma rede Hart pode haver dois dispositivos mestres e, do ponto de vista do protocolo, um número muito grande de escravos. Na prática o número de escravos é limitado em 15. Cada escravo tem um endereço único que pode ser de 4bits definidos em campo ou de 38 bits definidos na fabricação do instrumento, que são chamados de endereço curto (*short frame*) ou endereço longo (*long frame*). Um dispositivo Hart também pode ser endereçado por um Tag que é um identificador definido pelo software de rede. A Figura 15 ilustra um quadro da comunicação Hart.

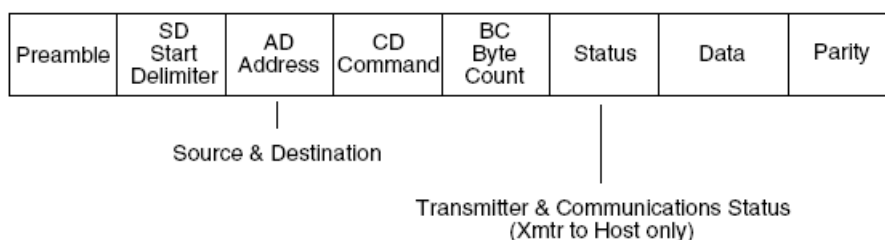


Figura 15. Formato do quadro de mensagem Hart.

6.2 AS-Interface

A interface AS-I (*Actuator Sensor interface*) é um sistema aberto desenvolvido por onze fabricantes e suportado pela AS-i Association atualmente com mais de 280 membros. Em 1998 a rede foi padronizada e recebeu o nome EN50295. A solução AS-Interface é um

sistema de cabeamento inteligente projetado para ligar sensores e atuadores simples entre si através de um barramento de dois fios e assim como nos loops de corrente, possibilitar a alimentação dos dispositivos através da própria linha de comunicação. (PARK, 2002).

A rede AS-i foi projetada para comunicações orientadas a bit, visando atender os processos industriais onde existem sensores e atuadores que operam de forma binária, isto é, ligado ou desligado, fechado ou aberto, energizado ou não, com o objetivo de aumentar a eficiência das mensagens para esses tipos de dispositivos.

A comunicação AS-i se dá no modelo mestre-escravo com mestre único. Na Camada Física, o padrão emprega cabo de par trançado com bitola de capacidade suficiente para alimentar com uma tensão de 30V até 31 nós escravos, cada um drenando um máximo de 65mA. Caso esse limite de corrente não seja suficiente para uma determinada aplicação, um segundo par conduzindo apenas alimentação pode ser usado em paralelo. A especificação atual V2.1 possibilita a instalação de até 62 dispositivos com 124 entradas e 124 saídas binária para cada um (REYNDERS, 2005).

A técnica de modulação usada em AS-i conhecida como APM (*Alternating Pulse Modulation*) e baseada na codificação Manchester-II reduz a banda passante necessária ao sinal e as reflexões nos extremos da linha. A figura 16 apresenta o formato do sinal APM comparado com os sinais binários banda base e Manchester-II. Pode-se observar que todo bit tem um pulso na segunda metade do intervalo e que a cada pulso a polaridade é invertida. Esta característica é explorada pela camada de enlace para verificação de erros de transmissão sem a inclusão de redundâncias, de modo a manter o quadro de dados pequeno.

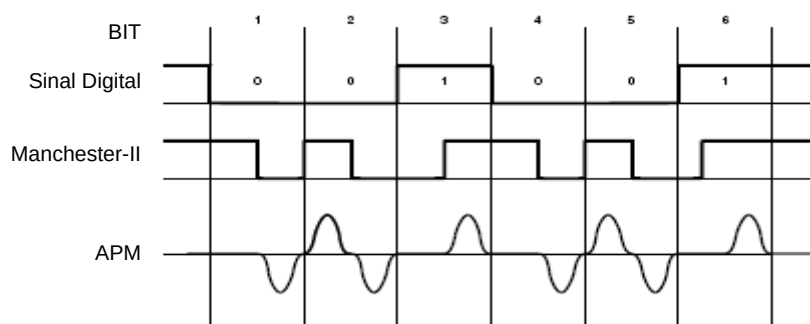


Figura 16. Relação entre a modulação APM e a codificação Manchester-II

As mensagens na Camada de Enlace das redes AS-i consistem em chamadas do mestre e respostas dos escravos. Esses quadros de dados (telegramas) têm respectivamente 14 e 7 bits com uma pausa entre cada transmissão para sincronização como apresentado na Figura 17. Algumas regras dos quadros estão diretamente relacionadas ao sinal APM: o bit de partida deve obrigatoriamente ser um pulso negativo e o bit de parada um pulso positivo; dois pulsos

seguidos devem sempre ter polaridades opostas; a pausa entre dois impulsos consecutivos deve ser de 3 microssegundos.

Pedido do Mestre														Pausa do Mestre	Resposta do Escravo							Pausa do Escravo
0	SB	A4	A3	A2	A1	A0	I4	I3	I2	I1	I0	PB	1		0	I3	I2	I1	I0	PB	1	
ST													EB		ST						EB	
Pedidos: 14 bits														3..10	Respostas: 7 bits							1..2

Figura 17. Formato de Telegrama na rede AS-i para chamadas e respostas

Os endereços de nós AS-i são armazenados em memória não volátil e podem ser designados tanto pelo máster como por uma unidade de endereçamento da rede. Tabelas de endereços armazenadas no máster contêm o perfil de cada dispositivo. O *start-bit ST* marca o início de um telegrama. O bit de controle *SB* em 1 define chamadas de comando e em 0 chamadas de dados/parâmetro/endereço. Existem 5 bits para endereçamento e 5 bits de informação. Os últimos dois bits são paridade par e o bit de parada *EB*. Na instalação cada instrumento recebe manualmente seu endereço de rede que armazenado em EEPROM.

Redes ASi são determinísticas. Como apenas um mestre pode estar presente e o acesso se dá por varredura cíclica, cada dispositivo é endereçado num tempo bem definido. Para uma rede completa de 31 escravos, o tempo de ciclo é de 5 ms. Este tempo será menor se menos escravos estiverem presentes. Tempos de até 500ms são possíveis. As redes AS-i são robustas, eficientes e de fácil manutenção. São utilizadas por um grande número de dispositivos simples nos processos de automação. Além de CLP's compatíveis com AS-i, existem também diversas placas de interface para PC's e conversores que possibilitam a conexão AS-i com interfaces RS-232 e RS-485.

6.3 Redes Devicenet

A rede Devivenet foi desenvolvida pela Allen Bradley (atualmente Rockwell Automation) com base no protocolo CAN (Controller Area Network) e sua especificação é aberta e gerenciada pela Devicenet Foundation. CAN é um protocolo de rede digital para a indústria automobilística desenvolvido pela empresa Robert Bosh Corp.

A rede Devicenet permite a conexão de até 64 nós com mecanismo de comunicação ponto a ponto com prioridade. O esquema de arbitragem é herdado do protocolo CAN e se realiza bit a bit. A transferência de dados se dá segundo o modelo produtor consumidor.

A camada física é caracterizada pela topologia em barra com derivações. Embora não conduza alimentação sobre o sinal, a rede Devicenet especifica cabos contendo pares separados para transmissão de dados e para alimentação de 24 Volts (Figura 18). Utilizando conectores moldados especiais, a rede permite a inserção e remoção de módulos em quanto em funcionamento (*hot swap*), e utiliza interface por foto-acopladores para possibilitar o compartilhamento do cabo com dispositivos alimentados externamente.

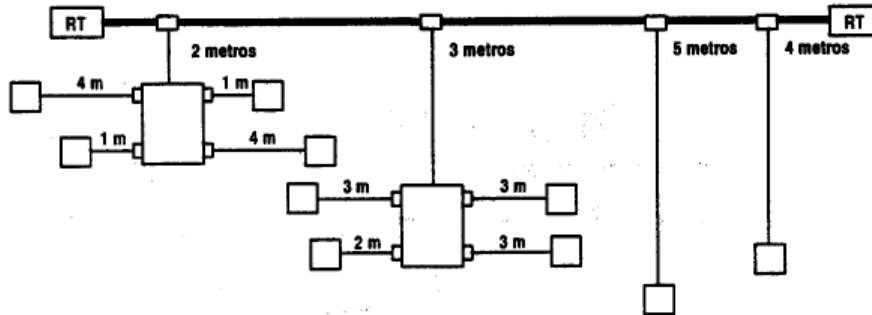


Figura 18. Topologia da rede DeviceNet.

A camada de enlace das redes DeviceNet Utiliza protocolo CSMA/NBA (*Carrier Sense Multiple Access with Non Destructive Bitwise Arbitration*) ou CSMA/CD + AMP (*Arbitration on Message Priority*). Através deste protocolo qualquer nó pode acessar o barramento quando este se encontra livre. Caso haja contenção, ocorrerá arbitragem bit a bit baseada na prioridade da mensagem que é função do identificador de pacote de 11 bits. O dispositivo vencedor prossegue na transmissão dos dados enquanto os demais dispositivos encerram a transmissão sem prejuízo aos dados sendo transmitidos. O identificador também determina como os escravos devem responder às solicitações: simultaneamente ou individualmente. Em respostas simultâneas o esquema de arbitragem do barramento define a sequência das respostas pela prioridade das mensagens.

A Figura 19 apresenta o quadro de dados do protocolo Devicenet. O processo de arbitragem pode ser visto em detalhes na especificação CAN V2.0 (ROBERT BOSCH GMBH).

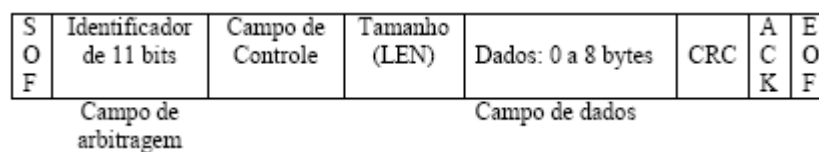


Figura 19. Quadro de dados da rede DeviceNet.

No modelo Produtor/Consumidor o Dado é identificado pelo seu conteúdo. A mensagem não necessita explicitar endereço da fonte e destino dos dados. Também não existe

o conceito de mestre. Qualquer nó pode iniciar um processo de transmissão que pode assumir os modelos Mestre-Escravo, Peer-to-Peer ou Multi-Mestre.

São definidos dois tipos de mensagens: Mensagens de Entrada e Saída e Mensagens Explícitas. As mensagens de Entrada/Saída são as informações do processo de controle. Elas permitem o trânsito de dados entre uma aplicação produtora e uma ou mais aplicações consumidoras em alta prioridade. As Mensagens Explícitas, de baixa prioridade, são utilizadas para transportar dados de configuração e diagnóstico ponto a ponto.

A especificação CAN não determina como a informação presente no campo de dados deve ser interpretada deixando essa formatação livre para os desenvolvedores do software de aplicação Devicenet. Qualquer dispositivo que necessite mais de oito bits de dados na comunicação poderá fragmentar a informação em múltiplos quadros. Neste caso o primeiro byte do campo de dados é utilizado para identificar a sequência de quadros e os sete bytes restantes parte da informação.

7. PROCESS FIELDBUS (PROFIBUS)

Profibus é hoje um dos padrões de rede industrial mais empregado na Europa e bastante popular em todo o mundo. Foi concebido em 1989 a partir de uma iniciativa conjunta de fabricantes, usuários e do governo alemão. A rede está padronizada através da norma DIN 19245 partes 1 e 2 e incorporada pela *European National* como padrão EN50170.

7.1 A Concepção Profibus

Profibus é uma rede multimestre. Sua especificação distingue dois tipos de dispositivos: Dispositivos Mestres, estações ativas capazes de enviar mensagens independente de solicitações externas, e Dispositivos Escravos, estações passivas que acessam o barramento apenas para confirmar ou responder mensagens enviadas por um mestre. Em ambos os casos, o acesso ao meio se dá quando existe permissão.

O padrão Profibus define uma família de três redes ou perfis de comunicação (*communication profiles*) no jargão Profibus:

1. Profibus DP (*Distributed Peripheral*) é uma rede especializada na comunicação entre sistemas de automação e periféricos distribuídos (sensores e atuadores). Neste perfil, múltiplos mestres podem ler dados de um dispositivo, mas apenas um mestre pode escrever dados neste dispositivo. Utilizando meio físico EIA-485 ou fibra ótica, o Profibus DP foi projetado para a transmissão de 1 kbyte de entrada ou saída em menos de 2 ms objetivando a utilização em controles com tempo crítico.
2. Profibus FMS (*Fieldbus Message Specification*) é uma rede *peer to peer* para comunicação de dispositivos inteligentes tais como computadores, CLPs ou outros sistemas inteligentes que impõem alta demanda de transmissão de dados. As mensagens FMS consomem mais overhead que as mensagens DP.
3. Profibus PA (*Process Automation*) é uma rede para a interligação de instrumentos analógicos de campo tais como transmissores de pressão, vazão, temperatura, etc. O perfil PA permite o envio de alimentação sobre as linhas de dados, a níveis de tensão e corrente reduzidos, de acordo com as especificações IEC61158-2 (*Intrinsic Safety*)⁶ para segurança de processos industriais em áreas de risco.

⁶ Intrinsic Safety é uma técnica de proteção para equipamentos eletrônicos operando em ambientes inflamáveis.

A pilha de protocolos Profibus pode ser vista na Figura 20. Todos os perfis, DP, FMS e PA, compartilham a mesma camada de enlace (camada 2). Os perfis FMS e DP usam camada física enquanto a versão PA usa IEC61158 para atender as exigências de segurança.

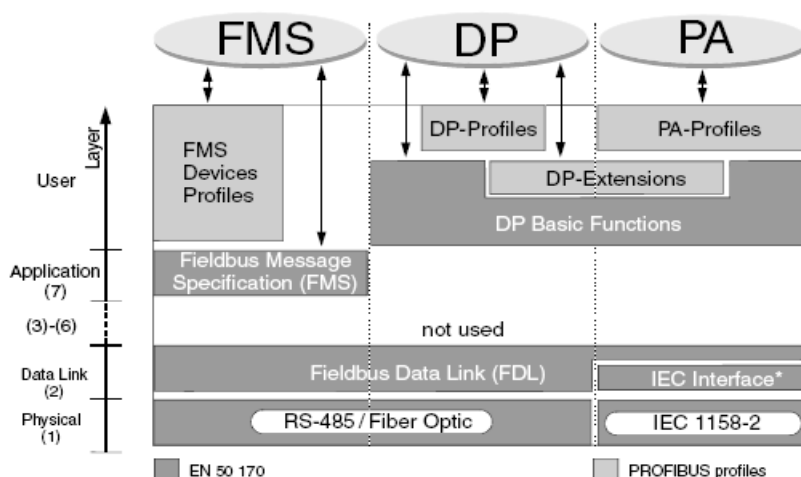


Figura 20. Pilha de protocolos do padrão Profibus e seus perfis

A Camada de Usuário (camada 8) acima da camada 7 do modelo OSI foi criada para possibilitar a máxima eficiência da rede nos perfis DP e PA. O significativo aumento da velocidade em comparação com o PROFIBUS-FMS deve-se principalmente ao uso do serviço SRD (*Send Receive Data*) da camada 2 para transmissão de entrada/saída de dados num único ciclo de mensagem (PROFIBUS Descrição Técnica).

A suite FMS possui as camadas 1, 2 e 7. A camada de aplicação é composta do FMS (*Fieldbus Message Specification*) e do LLI (*Lower Layer Interface*). O FMS define uma ampla seleção de serviços de comunicação mestre-mestre ou mestre-escravo. O LLI define a representação destes serviços FMS no protocolo de transmissão de dados.

A camada física utiliza três tipos de comunicação: (1) RS-485 para uso em todos os perfis, em especial em sistemas de automação da manufatura; (2) IEC 61158-2 para aplicações em sistemas de automação em controle de processo; (3) Fibra Ótica para aplicações em sistemas que demandam grande imunidade a interferências e grandes distâncias.

No padrão de transmissão assíncrona RS-485 as taxas de transmissão podem ser selecionadas entre 9.6 kbit/sec e 12 Mbit/sec. A transmissão síncrona em conformidade à norma IEC 61158-2 tem taxa de transmissão definida em 21,25 Kbits/s para atender aos requisitos das indústrias químicas e petroquímicas. Permite, além de segurança intrínseca, que os dispositivos de campo sejam energizados pelo próprio barramento.

7.2 O Acesso Híbrido ao Meio Físico

Os perfis de comunicação Profibus (*Communication Profiles*) usam o mesmo protocolo de acesso ao meio. Os serviços implementados pela camada 2 da rede Profibus incluem segurança de dados e a manipulação dos meios de transmissão e mensagens.

O Controle de Acesso ao Meio (MAC) especifica o procedimento quando uma estação tem a permissão para transmitir dados. O MAC deve assegurar que uma única estação tem direito de transmitir dados em um determinado momento. O protocolo do PROFIBUS foi projetado para atender os dois requisitos básicos do Controle de Acesso ao Meio: (1) assegurar que cada uma das estações tenha tempo suficiente para executar suas tarefas de comunicação dentro de um intervalo definido e preciso durante a comunicação entre sistemas complexos de automação (mestres); e (2) implementar de forma rápida e simples a transmissão cíclica de dados em tempo real entre um controlador programável complexo e seus dispositivos de I/O (escravos).

Para atender os dois requisitos, o protocolo Profibus provê duas formas de acesso ao barramento. A comunicação utilizada entre as estações ativas da rede (mestres) baseia-se no procedimento de passagem de ficha, formando um anel lógico entre os dispositivos mestres sobre a topologia em barra Profibus (Figura 21). A comunicação entre estações ativas (mestres) e passivas (escravos) ocorre da forma mestre-escravo, onde sensores e atuadores atendem e respondem as solicitações dos CLP's ou Controladores Digitais.

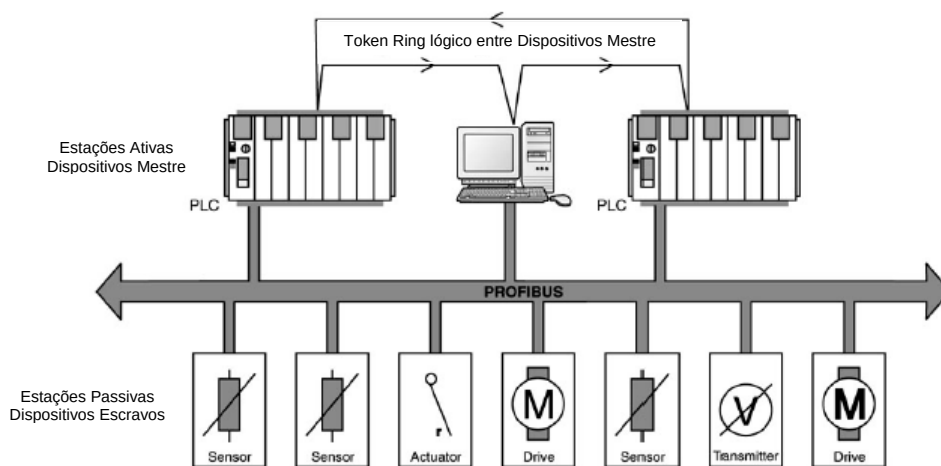


Figura 21. Acesso híbrido ao meio físico do padrão Profibus

Cada perfil de comunicação PROFIBUS utiliza um subconjunto específico dos serviços da camada 2 (veja tabela 8). Os serviços são acionados pelas camadas mais elevadas via Pontos de Acesso de Serviço (SAP's). No PROFIBUS-FMS estes pontos de acesso de serviço são utilizados para endereçar os relacionamentos lógicos de comunicação. No PROFIBUS-DP a cada função definida é associado um ponto de acesso de serviço. Vários

pontos de acesso de serviço podem ser usados simultaneamente por todas as estações passivas e ativas. Uma distinção é feita entre fonte (*SSAP – Source Service Access Point*) e destino dos pontos de acesso de serviço (*DSAP - Destiny Service Access Point*).

7.3 Dispositivos de Campo Virtuais

O modelo de comunicação Profibus permite a combinação de aplicações distribuídas com processos centralizados usando relacionamentos de comunicação. Instrumentos de campo são vistos pela comunicação como Dispositivos de Campo Virtuais (*Virtual Field Devices, VFD*). Todos os objetos de um dispositivo real que podem ser acessados como variáveis, programas e definições, são chamados de Objetos de Comunicação. O VFD é composto pelos Objetos de Comunicação que podem ser manipulados pelos serviços da Camada de Aplicação via o Profibus. Um dispositivo real pode se relacionar com mais de uma aplicação através do mapeamento de diferentes VFD's e diferentes conexões lógicas. A Figura 22 ilustra esse processo (REYNDERS, 2005).

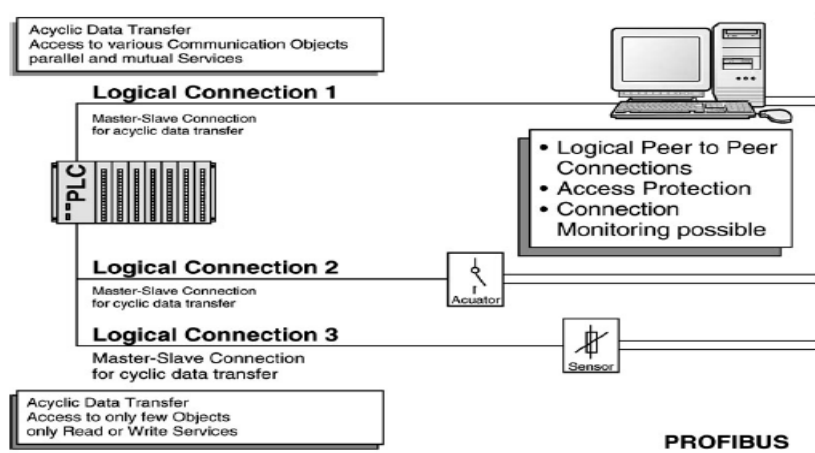


Figura 22. Várias conexões lógicas a um mesmo dispositivo na rede Profibus

Em cada estação Profibus os objetos são relacionados em um Dicionário de Objetos (*OD*) por entrada manual ou a partir de arquivos de configuração via rede. Eles podem ser endereçados pelo índice, por nome ou por endereço físico. Existe ainda a possibilidade de liberar um objeto apenas para leitura (*read only*) ou adicionar proteção por senha. Ao selecionar um objeto, uma aplicação já define a relação a ser utilizada com o dispositivo e a forma de comunicação aplicada.

8. FOUNDATION FIELDBUS

A rede Foundation Fieldbus⁷ (FF) assim como as redes Hart e Profibus, suas concorrentes mais próximas, é uma rede que preserva as vantagens do padrão 4-20mA como interface padronizada para o link de comunicação, alimentação sobre as linhas de comunicação e segurança intrínseca (*Intrinsic Safety*), ao mesmo tempo em que aproveita as modernas técnicas de comunicação digital.

8.1 A Concepção Foundation Fieldbus

A rede Foundation Fieldbus trouxe três grandes inovações ao controle industrial. A primeira foi estender a visão da área de processo além dos CLP's ou Controladores Digitais até os elementos de campo através da adoção de instrumentos com eletrônica integrada que apesar de denominados *smart sensors*⁸ correspondem na realidade a sensores e atuadores.

A segunda foi permitir a migração das estratégias de controle do controlador, antes representado por uma estação remota ou CLP para os elementos de campo (transmissores de temperatura, pressão, válvulas de controle etc), permitindo que dois ou mais instrumentos estabeleçam malhas de controle, que uma vez configuradas remotamente podem operar de forma independente do controlador externo. Estas estratégias de controle constituem os chamados Blocos de Controle.

A terceira é que a adoção do modelo Foundation Fieldbus associado à instrumentação inteligente permite a ligação direta entre os módulos de campo e estações de controle com a conseqüente redução de equipamentos necessários para instalar os instrumentos.

Os protocolos Foundation Fieldbus estão localizados em quatro camadas, três das quais correspondem às camadas 1, 2 e 7 do modelo OSI e a quarta chamada denominada Camada do Usuário posicionada acima da camada 7 não incluída no modelo OSI. A camada do usuário provê uma interface padronizada entre o software de aplicação e os dispositivos de campo. A Figura 23 apresenta o modelo Foundation Fieldbus em comparação com o modelo OSI.

Existem dois padrões de comunicação nas redes Foundation Fieldbus. O padrão H1, com taxa de comunicação de 31.25kbps e o padrão HSE operando a 100Mbps. A Camada Física H1 é baseada nas normas IEC61158-2 e ISA S50.02-1992 e foi planejada para utilizar a fiação já instalada na planta industrial com cabos STP #22 AWG. O esquema de codificação

⁷ Usa-se a expressão *Foundation Fieldbus* para diferenciar do termo genérico *fieldbus* (barramento de campo).

⁸ Smart Sensor é um dispositivo Plug and Play composto por um módulo transdutor (Transducer Interface Module - TIM) e um processador de rede (Network Capable Application Processor - NCAP)

de dados *Manchester Bi-Phase L* é usado sobre uma linha balanceada isolada, com terminadores de 100 Ohms desacoplados capacitivamente.

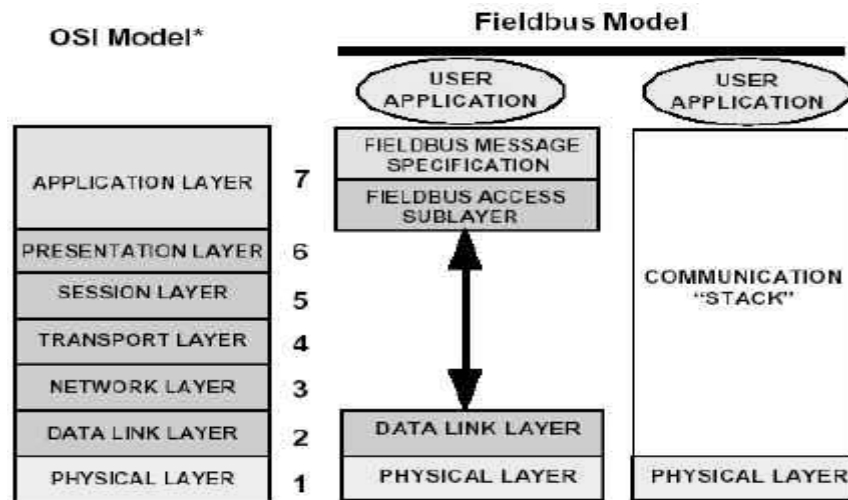


Figura 23. Modelo Foundation Fieldbus em comparação com o modelo OSI.

8.2 O Agendamento de Links Ativos

A camada de enlace controla o acesso ao barramento através de um esquema centralizado de agendamento chamado *Link Active Scheduler (LAS)*. O quadro de dados tem o formato apresentado na Figura 24.



Figura 24. Formato do quadro de dados Foundation Fieldbus.

O LAS controla o acesso ao barramento dando permissão a cada dispositivo de acordo com agendamentos pré-definidos dos tipos Cíclico ou Acíclico. Mensagens cíclicas são usadas para transmitir informações do processo que requerem atualização periódica. A transferência de informações é efetuada pelo método Editor-Assinante (*Publisher-Subscriber*). Baseado no agendamento do LAS, cada dispositivo que tem acesso ao barramento “publica” a sua informação (um sistema semelhante ao *broadcast*). Todos os dispositivos recebem a informação publicada mas apenas os dispositivos que necessitam da informação a registram e todos os demais descartam. Mensagens acíclicas são usadas para casos especiais que não ocorrem de forma regular que podem ser reconhecimento de alarmes

ou comandos especiais de diagnósticos. As mensagens acíclicas são encaixadas em espaços de tempo vagos (*time slots*) detectados pelo LAS.

A Camada de Aplicação na especificação Foundation Fieldbus é dividida em duas partes: a Subcamada de Acesso (FAS) e a Subcamada de Especificação de Mensagem (FMS). O agendamento na camada LAS permite a priorização de dispositivos com necessidades críticas de temporização. O esquema de agendamento via LAS permite implementar diferentes serviços entre a aplicação e os dispositivos de campo como cliente/servidor, editor/assinante e recepção e resposta a eventos especiais.

A Subcamada FMS mantém um dicionário de objetos, que permite o acesso aos dados por intermédio de *tags* ou número de índice. O dicionário de objetos contém uma listagem completa de todos os tipos de dados, descrições de tipos de dados e objetos de comunicação usados pela aplicação. As informações do dicionário de objetos podem ser atualizadas permitindo a manipulação da aplicação e dos serviços oferecidos.

A Camada do Usuário especificada pelo modelo Foundation Fieldbus é responsável pelo gerenciamento da rede, gerenciamento do sistema e descrições das funções dos dispositivos. A Figura 25 ilustra como os pacotes de informação são passados até o meio físico (MAKAY, 2004).

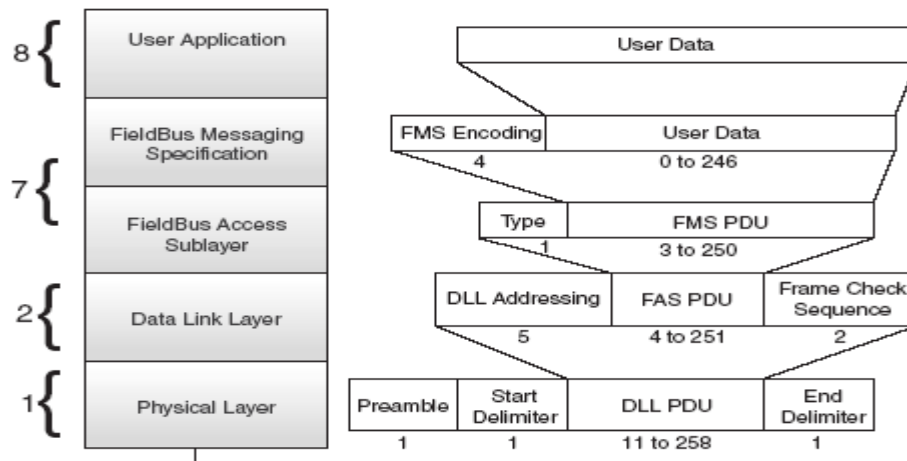


Figura 25. Informação através das camadas Foundation Fieldbus

Blocos de funções e descrições de dispositivos possibilitam a formação de blocos pré programados que podem ser usados pelo usuário para facilitar as configurações. Existem três tipos de blocos básicos: blocos de recursos e blocos de transdutores, utilizados para configurar os dispositivos e blocos de função, utilizados para construir a estratégia de controle. O conceito de blocos permite a seleção de funções genéricas, algoritmos e dispositivos genéricos de uma biblioteca de objetos durante a programação e configuração do sistema. O objetivo desta abordagem é prover um sistema aberto que suporte interoperabilidade e linguagem de

descrição de dispositivo (DDL) que permita dispositivos de múltiplos fornecedores serem descritos como blocos ou símbolos.

8.3 O padrão HSE

O padrão HSE mencionado no início desta seção é responsável pelo *backbone* de alta velocidade da rede Foundation Fieldbus. Múltiplos segmentos H1 podem ser conectados ao *backbone* HSE a uma taxa de 100Mbps padrão Ethernet (IEEE802) através de *HSE Linking Devices (LD)*. Switches HSE podem ser usados para conectar estações, pontes e outros barramentos HSE. Os HSE LD's podem ser configurados e monitorados por estações e cada segmento H1 tem seu próprio esquema de agendamento LAS residente no LD (Figura 26).

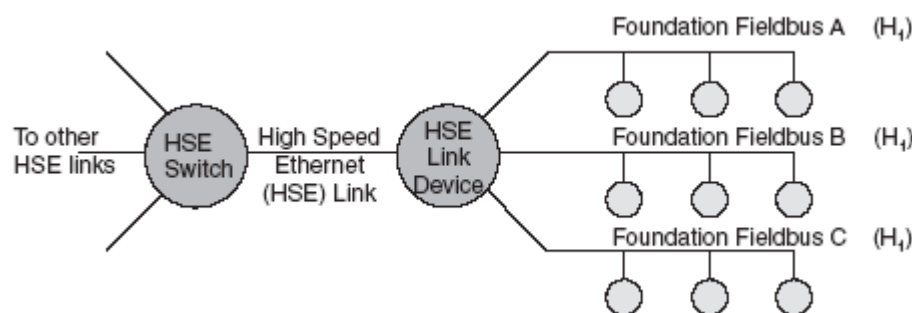


Figura 26. Integração Ethernet / Foundation Fieldbus.

Além de servir de gateway entre a rede HSE e a rede H1 os LD's podem ter pontos de I/O locais para permitir a interligação de sinais discretos oferecendo uma boa solução para aplicações de natureza híbrida. Alguns LD's possuem interfaces para outros protocolos como o Modbus para facilitar a interligação de inversores de frequência e outros tipos de dispositivos inteligentes orientados a byte.

A rede HSE suporta todas as funcionalidades das camadas de enlace de dados da especificação H1, permitindo o intertravamento de instrumentos localizados em diferentes segmentos de rede e a interligação de dispositivos que requerem grande capacidade de rede como CLPs, computadores *host* e instrumentos especializados que necessitam transferir grandes blocos de dados como espectrofotômetros.

9. NIST - IEEE 1451

O conjunto de padrões IEEE1451 foi desenvolvido para a geração dos novos dispositivos de campo (*Smart Sensors*) em uma tentativa de oferecer um protocolo base para unificar uma variedade de protocolos e padrões de barramentos de campo. Sua principal característica é prover um formato padrão para a comunicação de dados e configurações (*TEDs*) comum a todos os sensores e atuadores inteligentes para redes baseadas em cabo ou redes sem fio (NIST, 1999).

O padrão IEEE 1451, suportado pelo NIST é baseado em dois componentes conforme representado na (Figura 27): O Módulo de Interface do Transdutor (*TIM*) e um processador com capacidade para aplicações e acesso à rede *NCAP* (*Network Capable Application Processor*).

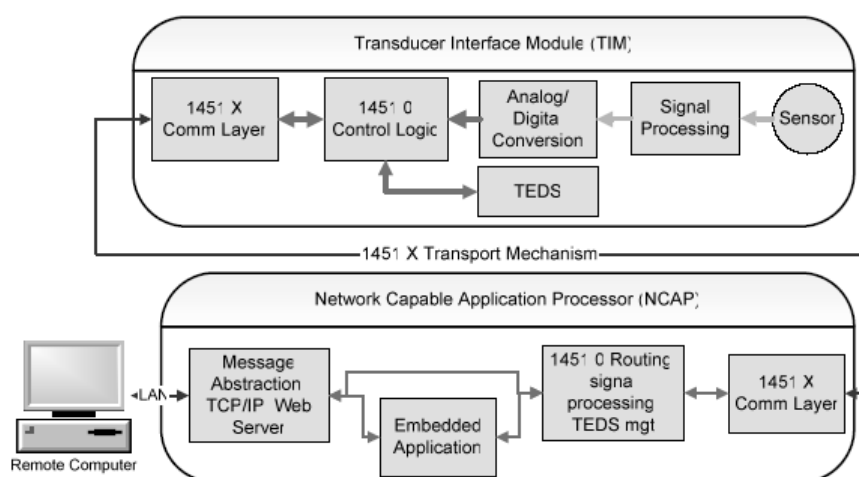


Figura 27. Diagrama de blocos de um sensor no Sistema IEEE1451 (*Smart Sensor Systems*).

O TIM incorpora as definições *TEDS* (*Transducer Electronic Data Sheet*), um dos elementos chave do padrão IEEE 1451. O *TEDS* contém informações de identificação do TIM e dados necessários para prover a interface com um outro instrumento ou sistema de controle. O *TEDS* pode estar gravado na eletrônica do próprio instrumento, em memória não volátil ou em algum ponto do sistema, acessível pelo instrumento e pelo sistema de controle associado (IEEE STANDARDS ASSOCIATION, 2004).

As informações são passadas entre o NCAP e o TIM por intermédio da interface de hardware e software do padrão IEEE 1451. O software padronizado simplifica as tarefas de adição de novas interfaces de transporte. As interfaces definidas no IEEE 1451 incluem

padrões como RS-232, RS485, USB, CAN, IEEE801.11, *Bluetooth* e *ZigBee* (802.15.4). A Figura 28 apresenta um par NCAP e TIM interconectados por interface RS-232.

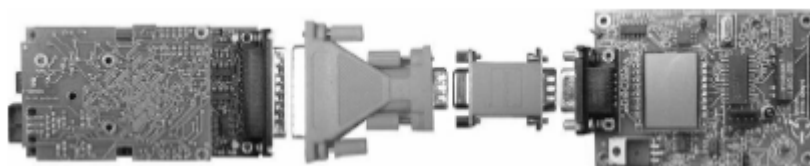


Figura 28. NCAP (versão Ethernet) e TIM com interface RS-232.

O NCAP gerencia os TIMs e processa os dados a serem usados pela aplicação. Um NCAP ao ser iniciado procura os TIM's conectados em suas interfaces e copia seus TEDS's para um banco de dados interno. Os TIM's trocam informações com os NCAP's em seu formato nativo, sem conversões de unidades. O NCAP aplica aos dados recebidos as informações do TEDS do instrumento efetuando as conversões necessárias para formatar os dados no Sistema Internacional. Os dados são então enviados à rede externa usando protocolo HTTP e XML. Smart Sensors são *plug-and-play*, o que significa que esses dispositivos podem entrar e sair da rede em pleno funcionamento. É função do NCAP manter uma referência atualizada dos dispositivos presentes nas suas interfaces.

Atualmente pequenos sensores ou atuadores podem ser instalados em quaisquer máquinas desde um simples reostato até complexos maquinários industriais. A união do padrão IEEE 1451 com as tecnologias *Wireless* e *Plug and Play* tornam esses pequenos dispositivos nós de rede capazes de transmitir dados críticos, atualizados em segundos, por redes locais e internet para controladores e supervisores geograficamente distribuídos. Esses dispositivos recentemente passaram a ser classificados como *IP Enabled Smart Objects* inaugurando a era da tecnologia de objetos inteligentes (*Smart-Object Technology*), uma nova classe de dispositivos de baixa potência e de alto poder de processamento, que se beneficia dos avanços dos microcontroladores e sensores para digitalizar e comunicar várias formas de dados e medições (MULLIGAN, 2010).

10. ETHERNET INDUSTRIAL

A rede Ethernet passou por rápida evolução nos últimos anos tornando-se a rede de melhor relação custo/desempenho para uma variada gama de aplicações. A Ethernet foi inicialmente concebida para ser uma rede de barramento *multidrop* (10Base-5) com conectores do tipo vampiro (*piercing*) em cabeamento coaxial. Características como custo de cabeamento e praticidade de instalação levaram a Ethernet a evoluir para uma topologia estrela com par trançado ao mesmo tempo em que as velocidades cresceram de 10 Mbps para 100 Mbps, 1 Gbps (IEEE802.3z IEEE802.3ab) e 10 Gbps (IEEE802.3ae). Atualmente a Gigabit Ethernet concorre diretamente com a tecnologia ATM nas aplicações em *backbones* de redes empresariais.

Como parte dessa evolução ocorreu também a adoção de cabos *full duplex* (pares separados para Tx e Rx), em substituição aos cabos half duplex mais comumente utilizados, e de hubs inteligentes com capacidade de comutação de mensagens. Isto fez com que a Ethernet se tornasse determinística, reduzindo a probabilidade de colisão de dados, característica de máxima importância para redes de controle de processos.

Vários padrões de redes industriais desenvolveram formas de incluir Ethernet como opção aos seus protocolos, procurando aproveitar as vantagens da Ethernet para utilização em seus *backbones* de alta velocidade, mas mantendo a compatibilidade com seus padrões originais.

10.1 Fieldbus – HSE

A especificação H2 da rede Foundation Fieldbus, destinada a estender o espectro de aplicação da especificação H1 para a interligação de dispositivos como CLPs e sistemas de supervisão, incorporou a camada Ethernet passando a ser conhecida como padrão HSE. A rede Foundation Fieldbus utiliza protocolos UDP/IP sobre as camadas de enlace Ethernet

A interligação entre uma rede H1 e a rede HSE se dá através de *Linking Devices* que convertem os dados de diversos segmentos H1 em mensagens, utilizando protocolos padrão da Internet. Instrumentos de campo especializados que necessitam transferir grandes blocos de dados também podem dispensar o protocolo H1 e transmitir diretamente sobre linhas Ethernet usando o protocolo HSE.

10.2 Rede ProfiNet

Em busca de uma comunicação mais uniforme entre aplicativos de alto nível e dispositivos de campo os desenvolvedores da rede Profibus procuram o acoplamento entre as redes Profibus e Ethernet através do desenvolvimento de um padrão denominado Profinet. Esse projeto tem por objetivo:

1. Mapear todos os serviços de engenharia do PROFIBUS para TCP/IP, incluindo acesso ao status das variáveis de processo, dados de diagnóstico, parametrização e a definição de interfaces relevantes de SW com base em OPC.
2. Roteamento direto de TCP/IP para Profibus permitindo o uso de web server em dispositivos de campo.
3. Representação de dispositivos de campo complexos como objetos de sistemas distribuídos orientados a objeto.

10.3 IEEE 1451

O padrão IEEE 1451 já foi concebido para ligar sensores e atuadores diretamente à redes de controle incluindo o padrão Ethernet. Os desenvolvedores apostam na produção de chips miniaturizados em alta escala como elemento principal para a redução substancial do custo do padrão quando comparado à outras redes. Um dos grandes suportadores desta solução é a HP que combina este tipo de conexão com *embedded Java* e o uso de um *web browser* por instrumento.

10.4 Modbus/TCP

Esta rede une o protocolo de camada de aplicação mais popular da indústria com a pilha de transporte/rede mais utilizada em redes. Uma das vantagens do protocolo TCP/IP é a facilidade de se usar diversas camadas de aplicação diferentes. Isso possibilita, por exemplo, a utilização de diferentes portas TCP para comunicar diferentes protocolos de rede industrial.

Este tipo de aplicação visa interligar dispositivos de campo orientados a byte, como equipamentos de laboratório, medidores de energia CA/CC, relés inteligentes, etc., com computadores do tipo PC. As empresas que atuam nesta área defendem que não se pode fazer uma revolução e trocar todos os padrões de uma só vez, como tentado sem sucesso no

passado. O que se deve fazer é procurar uma evolução gradativa do que é usado de fato em direção a padrões mais abrangentes e de melhor desempenho.

Outra tecnologia emergente nesta área é o que se chama “*Communication Port Redirection*”. Um dispositivo serial está ligado numa rede Ethernet TCP/IP. Um computador cliente acessa seus dados utilizando o protocolo Modbus através de um device driver rodando em Windows, que permite enxergar o dispositivo na rede como se estivesse ligado a uma porta serial do micro. Isto permite continuar utilizando aplicações do legado Modbus, por exemplo, um programador *Ladder*, mesmo utilizando uma conexão moderna em rede do instrumento.

10.5 Melhoramentos na Rede Ethernet

Para reduzir o número de colisões e a conseqüente degradação de desempenho da rede Ethernet, o que a inviabiliza para algumas aplicações industriais, muitos melhoramentos foram realizados e novos padrões (listados na Tabela 3) criados.

Tabela 3. Padrões Ethernet que viabilizaram aplicações industriais.

Nome do standard	Função	Comentários
IEEE 802.1p	Priorização de mensagens	256 níveis de prioridade
IEEE 802.12d	Redundância de links	Traz maior confiabilidade para a rede
IEEE 802.3x	Full Duplex	Comunicação bidirecional simultânea sobre link 10/100Base-T em cabo categoria 5.
IEEE 802.3z	Gigabit Ethernet	Uso como backbone corporativo. Afeta pouco a automação.

O simples aumento da banda de 10 Mbps para 100 Mbps foi um fator significativo. O uso de *switches* é o segundo ponto importante. Se cada dispositivo estiver ligado a um port de um switch que pode armazenar a mensagem antes de retransmiti-la a outro nó, as colisões são reduzidas ao caso em que um mesmo nó deseja transmitir e receber uma mensagem. Finalmente através de ligações full duplex entre o dispositivo e switch, o problema é completamente solucionado.

As deficiências da rede Ethernet compartilhada são:

1. Largura de banda compartilhada e não dedicada
2. Compartilhamento necessita de arbitragem do barramento sem o conceito de prioridade

3. Compartilhamento resulta em colisões quando 2 ou mais dispositivos desejam transmitir simultaneamente.
4. Colisões bloqueiam a rede e impedem outros dispositivos de transmitir.
5. Mais dispositivos em um segmento aumenta a probabilidade de colisão.
6. Broadcast de mensagens consomem grande banda
7. Não existe como diferenciar o tráfego de alta e de baixa prioridade.
8. Não existe como assegurar um caminho de baixo atraso para o tráfego de tempo real.

As modificações a serem efetuadas na rede compartilhada estão ilustradas na Figura 29. Na rede A todos os dispositivos compartilham o mesmo meio físico. Para aumentar o desempenho três providências foram tomadas na rede B: (1) o backbone foi reduzido com a utilização um switch, (2) os links com servidores foram reforçados com maior taxa e menor latência, e (3) a rede foi micro segmentada ligando-se cada segmento de rede a uma porta do switch. Quando os requisitos por banda são baixos, podem-se ligar vários dispositivos em um mesmo segmento.

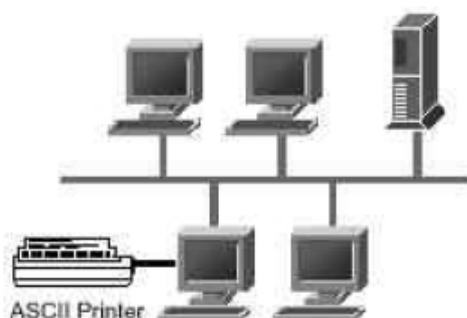


Figura 29-A. Backbone tradicional

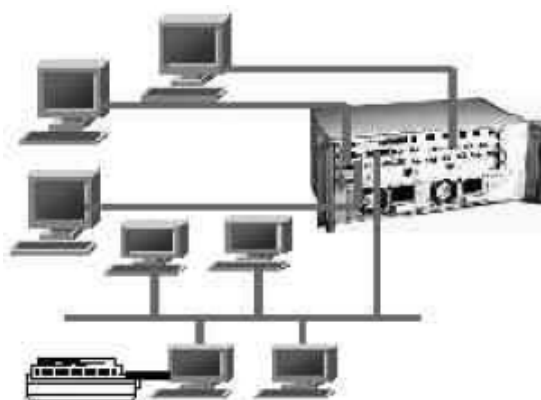


Figura 29-B. Backbone segmentado

Com a adoção da arquitetura cliente servidor, tornou-se necessário utilizar canais *Fast Ethernet full duplex*, propiciando largura de faixa de até 200 MHz para cada servidor. Os usuários passaram a utilizar canais com auto-detecção de 10/100 Mbps. A micro segmentação implica em dar a cada usuário um canal dedicado, sem compartilhamento com outros dispositivos. Com a micro segmentação tornou-se possível o uso de interfaces full duplex também para os usuários, o que permite eliminar a arbitragem do barramento, possibilitando a comunicação na velocidade nominal da rede. Isto equivale a duplicação da velocidade do barramento de 10/100Mbps para 20/200Mbps.

Outro fator que proporciona melhorias sensíveis para aplicações de tempo crítico é a seleção de prioridades com base no conteúdo transportado. O *QoS (Quality of Service)* é uma

maneira de alocar recursos em switches e roteadores de tal forma que os dados cheguem ao seu destino de forma rápida, consistente e confiável.

Sintetizando, os seguintes fatores contribuíram para a adequação da rede Ethernet às aplicações industriais:

1. Uso de switches para evitar a arbitragem de barramento
2. Uso de canais dedicados de 10 Mbps e 100 Mbps.
3. Padrão IEEE802.1p/Q que acrescenta campos de prioridade e QoS ao frame Ethernet tradicional.
4. Canais full duplex para eliminar colisões.
5. Rede Fast Ethernet no backbone levando a velocidade a até 200 Mbps.

11. CONCLUSÃO

Como pode ser verificado as redes industriais evoluíram de simples barramentos de campo para hierarquias sofisticadas e protocolos elaborados. Mesmo assim novas e antigas tecnologias ainda convivem no ambiente industrial. Muitos dispositivos usados nos sistemas de automação operam apenas com informação binária (ligado/desligado, energizado ou não) sendo demasiadamente simples para necessitarem de eletrônica associada. Existe contudo a tendência de que parte do processamento se desloque em direção aos dispositivos de campo, localizando-se mais próximos aos processos.

Foi visto que as redes industriais, de forma geral, procuram usar protocolos com baixo *overhead* o que muitas vezes é conseguido suprimindo-se as camadas de transporte, seção e apresentação e criando mecanismos para que uma oitava camada, acima da camada de aplicação do modelo OSI, geralmente denominada Camada do Usuário, possa lidar com o encaminhamento das mensagens de acordo com a aplicação.

Pode ser visto que existe uma tendência de se adequar os protocolos das redes industriais que obtiveram sucesso, à camada física Ethernet através da criação de padrões que sejam compatíveis com os modelos existentes dessas redes. Com a capacitação dos dispositivos na ponta das redes (sensores e atuadores) através de miniaturização e maior poder de processamento, existe uma tendência para o tratamento de dispositivos de campo como objetos distribuídos e a utilização de protocolos da internet (como HTTP e XML) para a comunicação com esses objetos.

O tema, entretanto é vasto e a abordagem aqui apresentada visou apenas fornecer uma introdução ao assunto. As referências relacionadas oferecem maiores detalhes sobre essas redes, protocolos e sistemas de automação.

REFERÊNCIAS

1. SILVEIRA, PAULO R.; SANTOS, WINDERSON, E., **Automação e Controle Discreto 2ª edição**. Ed. Erica, São Paulo, 1998.
2. BEGA, EGÍDIO ALBERTO ET AL., **Instrumentação Industrial 2ª edição**. Editora Interciência, Rio de Janeiro – RJ, 2006.
3. OGATA, KATSUHIKO, **Engenharia de Controle Moderno 4ª edição**. Ed. Pearson Brasil, São Paulo, 2006.
4. RIBEIRO, MARCO ANTÔNIO, **Automação Industrial 4ª edição**. Tek Treinamento & Consultoria Ltda, Salvador 1999.
5. RIBEIRO, MARCO ANTÔNIO, **Automação Industrial 5ª edição**. Tek Treinamento & Consultoria Ltda, Salvador 2005.
6. BOLTON, W., **Programmable Logic Controllers 4th edition**. Ed. Elsevier-Newnes, Oxford, England, 2006.
7. MAKAY, STEVE AT AL., **Practical Industrial Data Networks: Design Instalation and Troubleshooting**. Ed. Elsevier-Newnes, Oxford, England, 2004.
8. REYNDERS, DEON AT AL., **Practical Industrial Data Communications: Best Practice Techniques**. Ed. Elsevier-Newnes, Oxford, England, 2005.
9. PARK, JOHN ET AL, **Practical Data Communications for Instrumentation and Control**. Ed. Elsevier-Newnes, England, 2002.390p.
10. GROOVER, MIKELL P., **Automation, Production Systems and Computer-Integrated Manufacturing. 3nd ed**. Ed. Prentice-Hall, Upper Saddle River - NJ, 2001.
11. CLARKE, GORDON ET AL., **Practical Modern SCADA Protocols DNP3, 60870.5 and Related Systems**. Ed. Newnes, Oxford, England, 2004.
12. BAILEY, DAVID; WRIGHT, EDWIN, **Practical SCADA for Industry**. Ed. Elsevier-Newnes, Oxford, England, 2003.
13. AXELSON, JAN, **Serial Port Complete: Programming and Circuits for RS-232 and RS-485 Links and Networks**. Ed. Lakeview Research, Madison – WI, USA, 2000.
14. KRUTZ, RONALD L., **Securing SCADA Systems**. Wiley Publishing, Inc., Indianapolis, Indiana, 2006.
15. MODICOM, **Modicon Modbus Protocol Reference Guide PI-MBUS-300Rev.J**. Modicon, Inc., Industrial Automation Systems, Massachusetts-USA, 1996.
16. AS-I FAC, **AS-i - Frequently Asked Questions**. AS-interface Experts Forum. Disponível em <http://as-interface.net/System/Experts>.

17. ROBERT BOSCH GMBH, **CAN Specification Version 2.0**. Robert Bosch GmbH, Stuttgart, 1992. Disponível em <http://www.semiconductors.bosch.de/pdf/can2spec.pdf>
18. PROFIBUS BRASIL. **PROFIBUS - Descrição Técnica**. Associação PROFIBUS Brasil, outubro 2000. Disponível em <http://www.profibus.org.br/>.
19. REYNDERS, DEON; WRIGHT, EDWIN, **Practical TCP/IP and Ethernet Networking**. Ed. Elsevier-Newnes, Oxford, England, 2003.
20. NIST - NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. **IEEE P1451 Draft Standard for a Smart Transducer Interface for Sensors and Actuators**. National Institute of Standards and Technology - NIST, 1999. Disponível em <http://ieee1451.nist.gov/intro.htm>.
21. IEEE STANDARDS ASSOCIATION. **IEEE 1451.1 Standard for a Smart Transducer Interface for Sensors and Actuators**. IEEE Xplore Digital Library, 1999. Disponível em http://ieeexplore.ieee.org/xpl/freeabs_all.jsp?arnumber=5494713.
22. IEEE STANDARDS ASSOCIATION. **IEEE 1451.4 Mixed-Mode Communication Protocols and Transducer Electronic Data Sheet (TEDS) Formats**. IEEE Xplore Digital Library, 2004. Disponível em http://ieeexplore.ieee.org/xpl/freeabs_all.jsp?arnumber=1405786.
23. MULLIGAN, GEOFF. **A New Revolution: IP Enabled Smart Objects**. A New Revolution Part 1: IP Enabled Smart Objects. Sensors Magazine, August 20, 2010
24. TURK, ROBERT J. **Cyber Incidents Involving Control Systems**. US-CERT Control Systems Security Center, Idaho National Laboratory - INL, USA, October, 2005.