PTC3421 – Instrumentação Industrial

Aspectos Gerais III
Redes de Processo e Comunicação Digital

V2018B

PROF. R. P. MARQUES

Comunicação Analógica

Possivelmente ainda o meio de transmissão mais utilizado, transmissão por corrente (4mA – 20mA) possui limitações evidentes:

- Um único sinal é transmitido: a leitura do sensor ou o comando para o atuador;
- A comunicação é unidirecional;
- Há limitações na distribuição: cada receptor adicional usualmente exige um aumento de tensão para que a corrente se mantenha no valor desejado;
- Cada instrumento exige um par de fios independente, que deve se estender desde o instrumento até o painel de controle;
  OBS. Em algumas situações o retorno pode ser comum a vários sensores;
- O sinal elétrico pode ser afetado por ruídos.
- Não é possível fazer configurações remotamente, diagnósticos ou verificar o status do instrumento.

Sinais pneumáticos também possuem limitações semelhantes.

Comunicação Digital

Comunicação analógica era perfeitamente adequada a instrumentos analógicos, porém com o surgimento de instrumentos baseados em tecnologia digital, novas possibilidades surgiram, especialmente.

- A possibilidade de usar comunicação digital (elétrica, ótica, etc.);
- A possibilidade de integrar os instrumentos em rede;
- A possibilidade de configurar remotamente os instrumentos;
- A possibilidade de consolidar o cabeamento em um único cabo de rede;

Comunicação Digital

O uso de instrumentos com comunicação digital deverá se tornar predominante no futuro e comunicação analógica deve ser reduzida a nichos específicos dadas as vantagens de seu uso, porém comunicação digital apresenta as seguintes desvantagens:

- A comunicação é mais complexa;
- Garantia de comunicação em tempo real pode ser problemática;
- A comunicação é menos robusta;
- Deixa os instrumentos mais vulneráveis a ataques computacionais.

O Protocolo HART

O protocolo HART (Highway Addressable Remote Transducer) foi desenvolvido originalmente pela Rosemount, atualmente Emerson, no início dos anos 1980, tornando-se um padrão aberto em 1986.

A indústria estabeleceu um organismo para gerenciar o padrão, a HCF (HART Communications Foundation).

A HCF eventualmente incorporou o gerenciamento de outros protocolos abertos e hoje denomina-se FieldComm Group.

http://www.fieldcommgroup.org

O Protocolo HART

A ideia geral do protocolo é superpor um sinal digital bidirecional ao sinal analógico de 4mA-20mA no mesmo par de fios.

Com isso é possível aproveitar instalações concebidas para sinais analógicos e manter a compatibilidade entre instrumentos e sistemas de controle tradicionais e seus equivalentes compatíveis com HART.

É um dos mais simples e populares protocolos de comunicação digital para processos industriais.

O Protocolo HART

Padrão

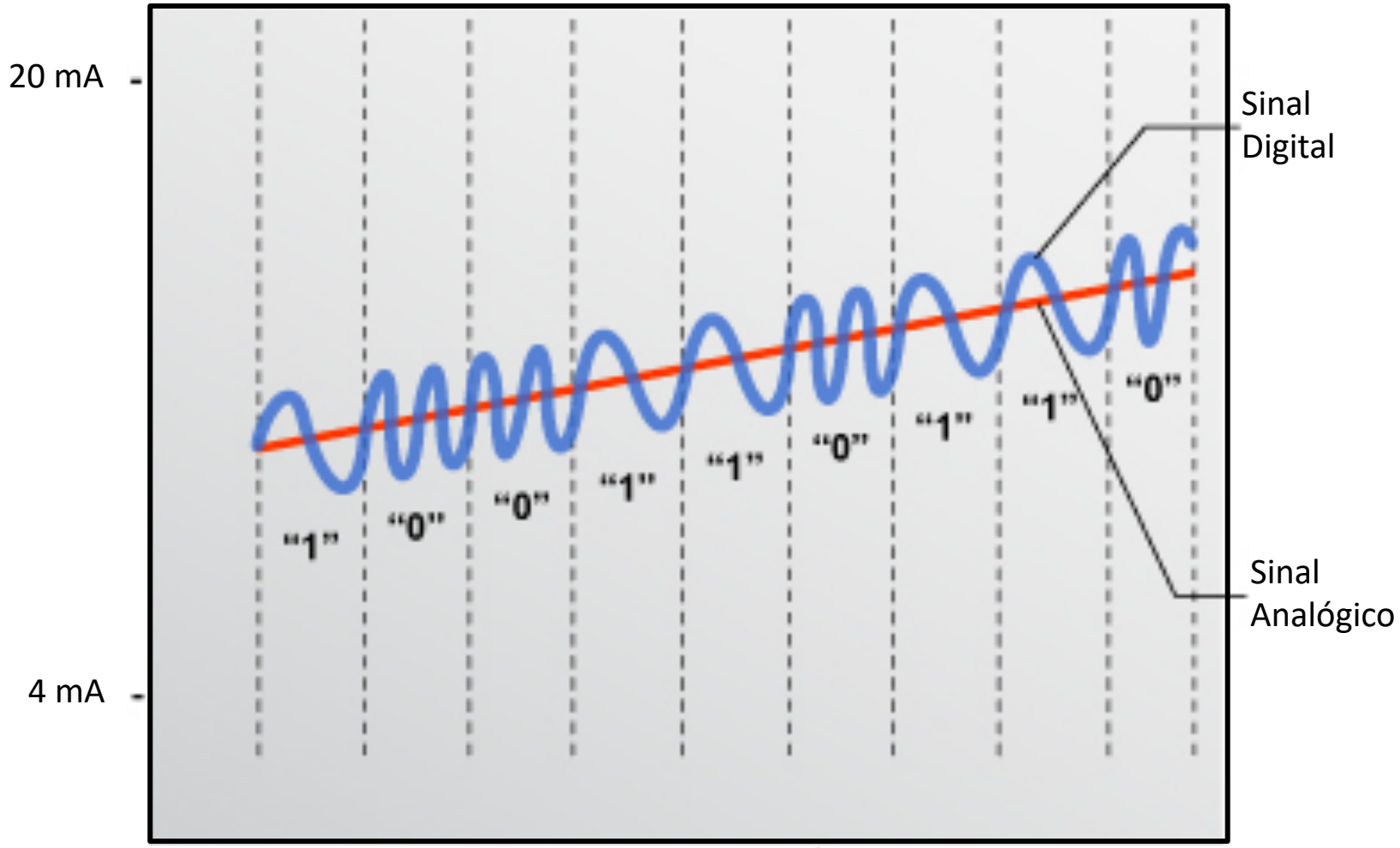
O padrão utilizado é baseado no **Bell 202 modem** (dos anos 1970), que consiste em modulação por deslocamento de frequência (FSK – Frequency Shifting Keying) transmitindo a uma taxa de 1200 bps em modo half-duplex (somente uma direção de cada vez).

Tom de 1200Hz	(mark)	“1” digital
Tom de 2200Hz	(space)	“0” digital

Como o sinal analógico é de frequência muito mais baixa que o sinal digital, é muito simples separá-los.

O Protocolo HART

Padrão



O Protocolo HART

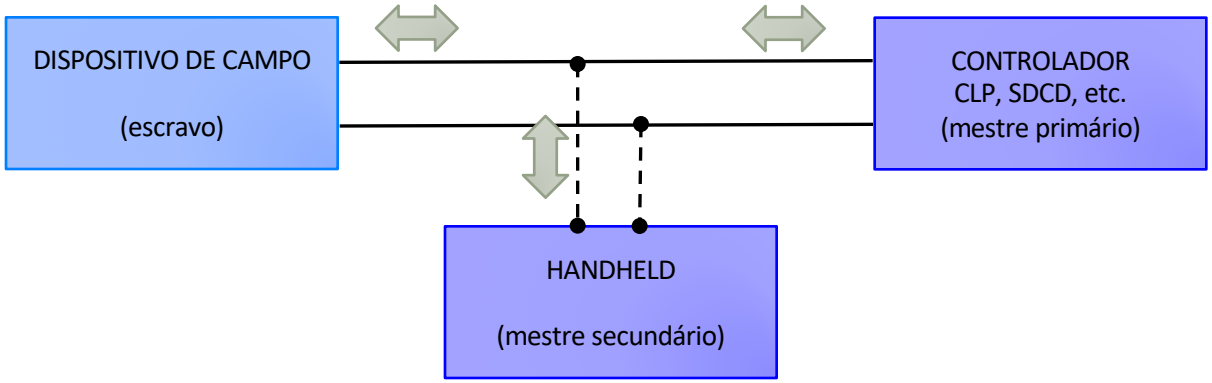
Comunicação Ponto a Ponto

A troca de mensagens pode ser feita de dois modos principais sem interferir no sinal analógico:

1. MODO MESTRE - ESCRAVO (*master–slave* ou *poll response*)

O instrumento de campo é o único escravo (não inicia comunicação e apenas responde a comandos de algum mestre).

Podem haver até dois mestres (primário e secundário) ligados em paralelo que podem iniciar comunicação e enviar comandos ao escravo. Usualmente um dos mestres é o sistema de controle e o segundo algum dispositivo portátil para testes ou configuração.



O Protocolo HART

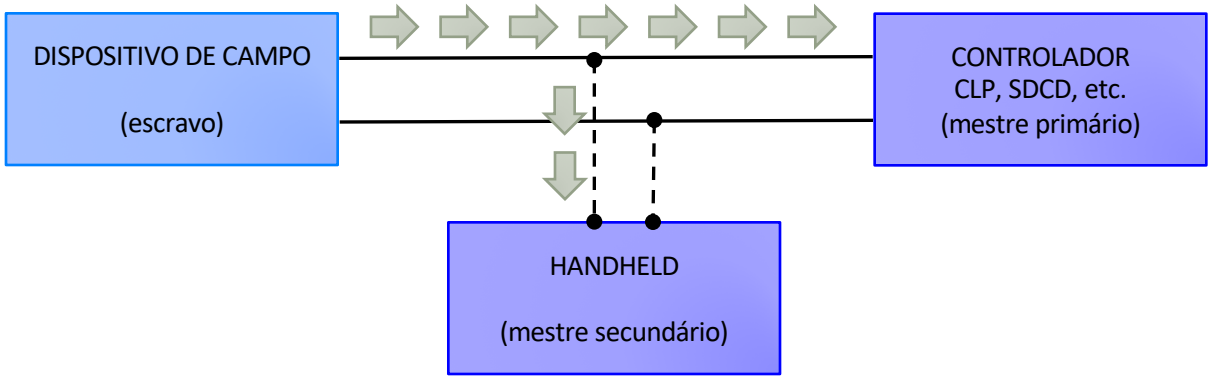
Comunicação Ponto a Ponto

2. MODO TRANSMISSÃO (broadcast ou burst)

O servidor instrui o escravo a transmitir continuamente uma resposta padrão até ser instruído a parar. A resposta padrão é usualmente o valor da variável de processo.

Este modo é utilizado sempre que é necessário ter atualizações rápidas de um sinal.

OBS: Entenda-se “rápido” como algumas mensagens por segundo.



O Protocolo HART

Estrutura da Mensagem

Há três tipos de comandos:

1. Comandos universais (que todo dispositivo compatível deve reconhecer)

Exemplos: ler identificador do dispositivo;
ler variável e unidades;
ler range; etc.

2. Comandos de prática comum (implementados por muitos dispositivos, mas que não são obrigatórios)

Exemplos: calibrar;
iniciar auto-teste; etc.

3. Comandos específicos de dispositivo (comandos específicos de um dado modelo de dispositivo, definidos pelos fabricantes)

O Protocolo HART

Mais Detalhes

A especificação completa do protocolo HART desde a camada física até a descrição de cada comando encontra-se em

https://fieldcommgroup.org/hart-specifications

(US$ 975,00 para não membros do consórcio)

O Protocolo HART
Limitações

O Protocolo HART apresenta as seguintes limitações importantes:

- É lento.
  A taxa de transmissão é de 150 byte/s e as mensagens têm entre 14 e 272 bytes.
- Não reduz o cabeamento (exceto em modo multiponto).
- A capacidade de conexão é relativamente pequena.
- Sua fundamentação é baseada em tecnologia e princípios antigos.

O Protocolo HART
Variações e Extensões

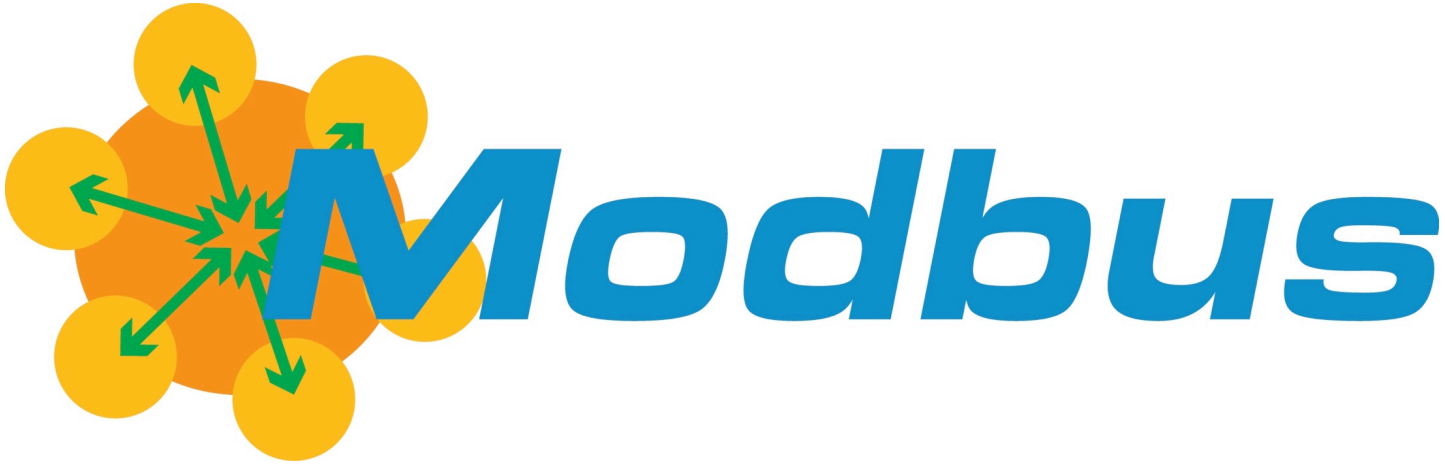
As seguintes variações e extensões foram criadas mais recentemente:

WirelessHART
Extensão wi-fi para o protocolo HART. Útil para instrumentos instalados temporariamente ou em localizações remotas sem cabeamento.

HART-IP
Protocolo HART sobre IP. Permite a transmissão de mensagens sobre meios que suportem o protocolo internet (e.g. Ethernet, Rádio, GPRS, 3G, 4G, fibra ótica, etc.).
Permite mais flexibilidade e maior velocidade.

(converter protocolos de natureza serial em IP é uma tendência da indústria)

O Protocolo MODBUS



O protocolo MODBUS (Modicon Bus) foi desenvolvido originalmente pela Modicon, atualmente Schneider Eletric, em 1979. Em 2004 a Schneider transferiu o gerenciamento do protocolo para um organismo independente, a **Modbus Organization**.

É um protocolo serial aberto (posteriormente estendido para ethernet e outros protocolos), possivelmente o mais popular dentre os protocolos de comunicação industrial.

O Protocolo MODBUS

Protocolo Serial

O protocolo foi originalmente concebido para comunicação serial entre CLPs, mas hoje é bastante utilizado também para comunicação entre dispositivos de campo (sensores e atuadores) e mesmo sistemas SCADA.

O protocolo é aberto e isento de taxas de licenciamento o que, aliado à sua flexibilidade, o tornou num dos protocolos industriais mais bem sucedidos.

O protocolo não está definido para a camada física, então os modos usuais de comunicação serial podem ser utilizados. Os mais comuns são RS-232 e RS-485

RS-232: ponto a ponto; taxa limitada.
RS-485: multiponto; taxas maiores; maior alcance.

OBS. Não há superposição com o sinal analógico como no HART.

O Protocolo MODBUS
Protocolo Serial

Há dois protocolos seriais principais:

MODBUS RTU
A implementação mais comum. As mensagens contêm dados binários seguidos de um checksum CRC. Os frames são separados por períodos de silêncio.

MODBUS ASCII
As mensagens contêm dados codificados em ASCII seguidos de um checksum LRC. Os frames contêm “:” no início e <CR/LF> no final.

O Protocolo MODBUS

Outras Implementações

MODBUS TCP/IP (ou MODBUS TCP)
Para uso sobre redes TCP/IP. Não contém checksums (são utilizados os checksums das camadas inferiores).

MODBUS sobre TCP/IP (ou MODBUS sobre TCP ou MODBUS RTU/IP)
Para uso sobre redes TCP/IP. Inclui checksums como o MODBUS RTU (trata-se do MODBUS RTU implementado em TCP/IP).

MODBUS sobre UDP
Para redes locais. Exclui o overhead do protocolo TCP para se obter maior desempenho (não tem confirmação de chegada dos pacotes).

Outras implementações abertas e proprietárias: MODBUS+, etc.

O Protocolo MODBUS
Comunicação

A comunicação utiliza o esquema Mestre/Escravo.

Na versão serial, podem haver diversos nós, porém somente um pode atuar como Mestre (inicia comunicação e envia comandos).

Na versão TCP qualquer nó pode enviar comandos, porém o usual é que haja apenas um mestre.

Comandos e mensagens são enviados a nós específicos ou a todos simultaneamente (cada nó tem um endereço de 1 a 247 e o endereço 0 é utilizado para broadcast).

O Protocolo MODBUS

Estrutura da Mensagem - RTU

START	ADDR	FUNCTION	[DATA]	CHK	END
3 ½ bytes (mark)	1 byte	1 byte	n bytes	1 byte	3 ½ bytes (space)
Início Sincronização Período de silêncio.	**Endereço** Endereço de destino da mensagem (1 a 247)	**Função** Comando, tipo da mensagem, etc.	**Dados** Dados relacionados ao comando/mensagem. (depende de FUNCTION)	**Checksum CRC**	**Fim** Sincronização Período de silêncio.

O Protocolo MODBUS

Estrutura da Mensagem - ASCII

START	ADDR	FUNCTION	[DATA]	CHK	END
1 byte	2 bytes	2 bytes	2n bytes	2 bytes	2 bytes
Início Caractere ":" (3Ah)	**Endereço** Endereço de destino da mensagem (1 a 247).	**Função** Comando, tipo da mensagem, etc.	**Dados** Dados relacionados ao comando/mensagem. (depende de FUNCTION)	**Checksum LRC**	**Fim** Caracteres <CR/LF> (0Dh + 0Ah)

OBS. Bytes são convertidos em hexadecimais (255 equivale a "FF")

O Protocolo MODBUS

Estrutura da Mensagem - TCP

TRANSACTION ID	PROTOCOL ID	LENGTH	[DATA]	CHK	END
2 bytes	2 bytes	2 bytes	n bytes	1 byte	3 ½ bytes (space)
Identificador de transação Sincronização entre mestre e escravo.	**Identificador de protocolo** (MODBUS TCP = 0)	**Comprimento** Comando, tipo da mensagem, etc.	**Dados** Dados relacionados ao comando/mensagem. (depende de FUNCTION)	**Checksum CRC**	**Fim** Sincronização Período de silêncio.

O Protocolo MODBUS
Especificações

As especificações completas do protocolo podem ser encontradas em

http://www.modbus.org/specs.php

(documentação gratuita)

Foundation Fieldbus

No final dos anos 1980 e início dos anos 1990, surgiram diversos padrões concorrentes para redes industriais de tempo real. Um dos principais é o FOUNDATION FIELDBUS (FF).

É um protocolo aberto, atualmente gerenciado pela FieldComm Group e regulado pela norma IEC 61158 (junto com outros padrões).

Foundation Fieldbus

Há duas implementações principais:

FOUNDATION FIELDBUS H1 (1996)
Protocolo serial operando a 31,25 kbit/s no mesmo cabo em que é feita a alimentação dos instrumentos.
Vantagens incluem comunicação isócrona, download de firmware através do protocolo, endereçamento automático, etc.

FOUNDATION FIELDBUS HSE (1999)
HSE significa High Speed Ethernet. Utiliza os padrões ethernet e IP (sem alterações) até 1Gbit/s.

Foundation Fieldbus

O protocolo foi concebido para prover controle em malha fechada através de uma rede.

As mensagens são trocadas entre quaisquer nós (não há uma estrutura mestre/escravo), de modo que múltiplos dispositivos de campo e controladores podem compartilhar a mesma rede.

O protocolo possui esquemas de priorização para sinais e instrumentos críticos (isso é importante quando a comunicação possui taxa baixa).

Foundation Fieldbus

A especificação completa do FF encontra-se em

https://fieldcomm-group.myshopify.com/products/ff-spec

(US$ 4.500,00 para não membros do consórcio)

O Protocolo PROFIBUS

O protocolo PROFIBUS (Process Field Bus) foi desenvolvido pelo governo alemão e pela Siemens no final dos anos 1980.

Atualmente o protocolo é gerenciado pela PROFIBUS & PROFINET International (PI).

http://www.profibus.com

É um protocolo similar ao FOUNDATION FIELDBUS H1.

O Protocolo PROFIBUS

Há duas implementações principais:

PROFIBUS DP
(Decentralised Peripherals)
Como no FF, alimentação também é provida pelo mesmo cabeamento da comunicação. É a implementação normalmente utilizada.

PROFIBUS PA
(Process Automation)
É o mesmo protocolo com alterações no meio físico para operar em zonas seguras nível 0 e 1 (vide próxima apresentação). Possui recursos para limitação de corrente para minimizar o risco de explosão (com isso o número de dispositivos que pode ser ligado ao barramento é menor que numa implementação equivalente do tipo DP)

É um dos padrões, juntamente com FF, regulado pela IEC 61158.

O Protocolo PROFINET

O protocolo PROFINET (Process Field Network) é um protocolo simular ao FOUNDATION FIELDBUS HSE e também é gerenciado pela PROFIBUS & PROFINET International (PI).

http://www.profibus.com

Comparação dos Protocolos

HART, MODBUS são mais adequados para comunicação entre instrumentos e controladores (são protocolos mais simples), seja ponto a ponto ou multiponto.
HART mantém a compatibilidade com instrumentos 4mA – 20mA.

FF H1, PROFIBUS DP são protocolos mais sofisticados, que podem ser utilizados para interligação também entre controladores.

HART-IP, MODBUS TCP, FF HSE, PROFINET são protocolos baseados em ethernet que devem se tornar preponderantes a médio e longo prazo, tanto para comunicação entre controladores como também entre instrumentos e controladores.

MODBUS ainda é o mais utilizado dos protocolos, e tem sido incluído também em dispositivos baseados em FF ou PROFIBUS como “segunda língua” por compatibilidade.

PROFIBUS / PROFINET aparenta estar se tornando predominante no mercado em comparação a FF.

Deficiências Comuns

Algumas deficiências comuns aos protocolos no atual estágio tecnológico:

- A comunicação é lenta, especialmente em implementações seriais com grande número de dispositivos.
  Esse problema tem sido extremamente minimizado com o uso de redes ethernet de alta velocidade.

- A confiabilidade da comunicação, devido à complexidade de hw+sw, ainda é um problema.
  Esquemas de redundância melhoram a disponibilidade do sistema, mas o problema é atacado efetivamente aumentando-se a complexidade do sistema.

- Vulnerabilidade a ataques. Nenhum dos protocolos é suficientemente maduro ou possui recursos de segurança realmente suficientes (e.g. criptografia e autenticação).

O Futuro

Os protocolos são relativamente simples e pouco flexíveis principalmente pelas limitações tecnológicas da época em que foram concebidos.
Instrumentos de campo especialmente tinham capacidades de comunicação e processamento limitadas.

Atualmente isso está mudando, portanto se espera que cada vez mais haja comunicação via redes sofisticadas. Os padrões ethernet e TCP devem se tornar dominantes.
Tendo isso em vista, os seguintes pontos ainda merecem atenção:

- Comunicação em tempo real (efetivamente conseguida no padrão ethernet graças à subutilização dos canais);
- Segurança (cybersecurity).