Rede Wireless em Sistemas de Automação Industrial

Éder da Silva Lourenço[1]
Emerson Rogério Alves Barea[2]

Resumo
A comunicação de dados sem a utilização de meios físicos como portadora para transferência do sinal é realidade atualmente. As redes sem fio (wireless) são utilizadas em casas, escritórios, bancos, nas pequenas, médias e grandes empresas, sempre com a finalidade de transmitir mensagens instantâneas, arquivos, dados de sistemas e outras informações que se fizerem necessárias. As tecnologias e topologias empregadas são capazes de garantir um grau de segurança satisfatório à comunicação, tanto em relação ao roubo de informação, modificação ou até mesmo a interceptação de seu conteúdo. O presente estudo expõe a aplicação da tecnologia *wireless* em sistemas de automação industrial, abordando seus princípios, relatando alguns de seus componentes e tipos de redes utilizadas. Apresenta as características e diferenças entre os principais protocolos já desenvolvidos para utilização em ambientes industriais, o WirelessHART, ISA-SP100.11a e o ZigBee. Também discute as deficiências e problemas enfrentados no âmbito da segurança.
Palavras chaves: ISA-SP 100; WirelessHART; ZigBee.

Abstract
Data communication without using physical methods as a carrier, for signal transfer, nowadays is a reality. Wireless Networks, are used at homes, offices, banks, small, medium and large companies, always aiming to transmit instant messages, files, system data and other information that may be necessary. The topologies and technologies used are able to ensure a satisfactory level of security communications, both for information theft, unauthorized changes or even the interception of their content. This article, shows the use of wireless technology, for industrial automation systems, explaining its principles, reporting some of its components and types of networks used. It discusses features and differences between the main

[1]Graduado Análise de Sistemas e Tecnologias da Informação da Fatec Ourinhos, e-mail: eder@shw.com.br
[2]Especialista em Redes de Computadores, professor da Fatec Ourinhos, e-mail: emerson.barea@fatec.sp.gov.br

protocols, already developed for use in industrial environments, the WirelessHART, ISA-SP100.11a and ZigBee. It also discusses the deficit and problems faced in providing safety.
Key-words: ISA-SP 100. WirelessHART. ZigBee.

1 INTRODUÇÃO

Um sistema de automação industrial compreende um sistema operacional em tempo real com equipamentos de alta confiabilidade e desempenho, dedicados ao controle de processos. Basicamente composto por um CLP, IHM, atuadores e dispositivos.

O CLP, Controlador Lógico Programável, é o elemento de valor mais agregado em um sistema de automação, pois, concentra todas as instruções lógicas desenvolvidas para processamento dos controles de processo. A IHM, Interface Homem Máquina, é o meio utilizado para interação direta do usuário com o sistema de automação. Os atuadores, são equipamentos reagentes para mudar o estado das variáveis de processo enviadas pelos dispositivos. Já os dispositivos são sensores que enviam informações do processo, são utilizados no monitoramento de variáveis e podem ser discretos - sensores de duplo estado (ligado ou desligado); discretos em rede - com o mesmo princípio de estado citado anteriormente, porém há diferenças quanto a sua integração com o CLP; e os analógicos - que fornecem informações de variáveis mensuráveis como temperatura, vazão e pressão.

É grande a variedade de dispositivos existentes, podendo tanto estarem relacionados à aplicações simples ou às que envolvem áreas classificadas[3], nesse caso, devendo ser resistentes a explosão ou intrinsecamente seguros. Em comum, necessitam de cabos para interligá-los ao CLP, sendo assim, uma automação de grande porte pode conter quilômetros de cabos, aumentando o custo à medida que esses dispositivos se afastam do CLP, necessitando até mesmo de repetidores para amplificar o sinal.

O objetivo é apresentar e discutir as características e diferenças entre

[3] Local ou ambiente sujeito à probabilidade de formação ou existência de atmosfera explosiva.

o WirelessHART, ISA-SP100.11a e o ZigBee, de forma a tornar mais clara a viabilidade ou não da utilização do *wireless* em redes de automação industrial, tratando também dos quesitos de segurança a serem considerados.

2 REDES DE COMUNICAÇÃO INDUSTRIAL

A tecnologia da informação tem contribuído muito no desenvolvimento de novas tecnologias na área da automação industrial, chegando a indústria nos mais diversos setores (processos, manufatura, logística). Levando-se em consideração o orçamento máximo disponível para um projeto, pode-se elaborar uma combinação de diferentes sistemas de comunicação em redes com protocolo aberto, como por exemplo, *AS-Interface*, *PROFIBUS* e *Ethernet*. (CASSIOLATO et al., 2010).

Segundo a *Virtual Academy of As-Internacional Association* (2010), usuários de uma rede *AS-Interface* não necessitam deter conhecimentos profundos sobre protocolos e sistemas digitais, diferentemente de outros tipos de redes industriais que necessitam de arquivos de configuração e terminadores[4] de rede, ela apenas requer um único cabo onde são conectados os módulos de entrada e saída. Esta rede provê uma redução de custos de 50% em cabeamento e instalação.

A rede PROFIBUS DP foi desenvolvida para comunicação com dispositivos de campo em alta velocidade utilizando comunicação serial. Nesse processo de comunicação, o mestre da rede, normalmente um CLP, lê e escreve ciclicamente as informações de entrada e saída nos dispositivos. Já a rede PROFIBUS PA, foi desenvolvida em conjunto com usuários da indústria de processos que teve como principais requisitos a padronização, intercambiabilidade entre dispositivos de diferentes fabricantes, mobilidade, alimentação pelo próprio barramento e possibilidade de uso em áreas classificadas. "As definições e opções do perfil de aplicação PA, tornam o PROFIBUS um conveniente substituto para transmissão analógica com 4 a 20mA ou HART[5]". (CASSIOLATO et

[4]Terminadores: Elemento instalado no final do barramento da rede utilizado para casamento de impedância.

[5]HART: Protocolo utilizado para comunicação entre sistemas em tempo real.

al., 2010, p. 53).

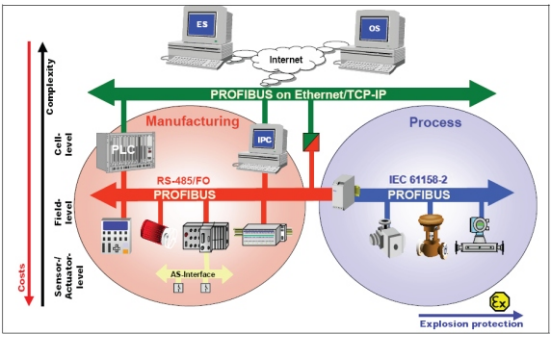

Figura 1 - Comunicação Industrial
Fonte: Cassiolato et al. (2010, p. 3)

Conforme a Siemens (2010), a Ethernet é o padrão mais utilizado no mercado mundial de redes de comunicação, com uma participação estimada em 80%. Destina-se a comunicação de células e área aberta, baseada no padrão *IEEE 802.3* e está adequada ao uso em ambiente industrial, permitindo comunicação entre Sistemas de Automação operando na faixa de 100 Mbps.

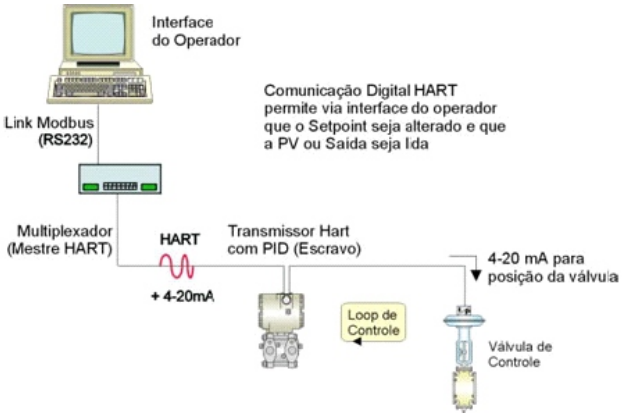

Figura 2 - HART em um Controle de Malha Fechada
Fonte: HELSON, 2010

A associação PROFIBUS internacional, por meio de grupos de trabalhos em conjunto com a *HART Foundation* e *Fieldbus Foundation*, vem desenvolvendo um padrão para suportar a comunicação sem fio *WirelessHART* baseado no padrão *IEEE 802.15.4*. (CASSIOLATO et al.,

2009). Esse padrão utiliza sinal de chaveamento por deslocamento de frequência, provendo comunicação nos dois sentidos e tornando possível a transmissão e recepção de dados e da informação da variável de processo pelo mesmo par de cabos. A taxa de comunicação do protocolo é 1,2 Kbps, sem causar qualquer interrupção no sinal analógico de 4 a 20mA, provendo também uma aplicação tipo "mestre/escravo" com duas ou mais atualizações por segundo. (HELSON, 2010).

Ainda segundo Helson (2010), o mestre normalmente é um SDCD - Sistema Digital de Controle Distribuído, um CLP e um controle central baseado em um computador ou sistema de supervisão. A aplicação típica da arquitetura é o controle em malha fechada, que se baseia em executar um algoritmo usando as variáveis proporcional, integral e derivada, sendo que, com um sinal de *feedback* e uma variável de saída, obtêm o controle da malha independente de operação manual.

3 TECNOLOGIA WIRELESS

A diferença entre as redes cabeadas e redes *wireless* é que fatores externos ocasionam muito mais interferências. Isso acontece, porque, não há uma proteção física com relação ao meio de transmissão, no entanto sua vantagem com relação às redes baseadas em cabos são que elas podem alcançar facilmente locais de difícil acesso ou distantes. (RUFINO, 2007).

Presente no dia-a-dia, os sinais de radiofrequência são utilizados pelos mais diversos serviços (TV, radio, telefonia celular, etc.), porém a maior parte das frequências comumente utilizadas não é padronizada internacionalmente, o que significa que uma frequência com fins militares em um país, pode ser de uso comercial em outro. Dentro dessas faixas de frequências definidas no espectro[6] ainda existem subdivisões em frequências menores denominados canais, com isso, é possível a transmissão em paralelo de sinais diferentes na mesma frequência. Uma grande desvantagem dessa comunicação fixa pode ser apontada como o fato de ser mais suscetível à interferências.

[6]Espectro: Intervalo completo da radiação eletromagnética.

Na tentativa de resolver o problema das interferências, foram desenvolvidas novas tecnologias, como por exemplo, *Spread Spectrum* - SS (Espalhamento Espectral), que visa distribuir o sinal uniformemente por toda faixa de frequência, garantindo dessa forma maior integridade no tráfego dos dados, porém consumindo mais banda. Se o receptor não conhece o código do espelhamento espectral, tudo o que receber pode ser entendido como ruído. "O padrão de comunicação para todos os tipos de redes sem fio atuais utiliza essa tecnologia". (RUFINO, 2007).

Rufino(2007) ainda descreve que outra tecnologia, a *Frequency-Hopping Spread-Spectrum* – FHSS (Salto de Frequência com Espalhamento Espectral) utiliza a banda de 2,4 GHz e divide a frequência em 75 canais, sendo seus dados transmitidos de forma randômica utilizando todos os canais. Uma vez sincronizados o receptor e emissor, é estabelecido o canal lógico e os receptores que não conhecem a sequência de saltos entendem a transmissão como ruído. Essa tecnologia limita-se a transmissão de 2 Mbps.

Direct Sequence Spread Spectrum – DSSS, consiste na separação de cada bit de dados em 11 sub bits, sendo enviados por um mesmo canal e de forma redundante, a banda de 2,4 GHz é dividida em 3 canais.

Finalizando, Rufino(2007) explica que a tecnologia *Orthogonal Frequency Division Multiplexing/Modulation* – OFDM, garante transmissão mais eficiente e pode ser utilizada tanto em redes sem fio como em cabeadas (ex: ADSL). Capaz de identificar uma interferência ou ruído, sendo assim, permite a troca ou isolamento da faixa de frequência, podendo até mudar a velocidade de transmissão.

3.1. Topologias de Redes Wireless

As redes *wireless* têm um *layout* ou topologia que geralmente é determinado através da localização e capacidade lógica de seus nós e componentes. (CARO, 2008, p. 21). Malha, Estrela e Árvore são exemplos dessas topologias.

Segundo Caro (2008, p. 23), a arquitetura de Malha (Mesh), tem cada elemento da rede trabalhando tanto como um dispositivo de extremidade como de retransmissão. As redes *mesh* são naturalmente *self-*

healing[7] e redundantes, exatamente as características necessárias para redes de automação industrial. Em uma rede *mesh*, cada estação também é responsável pelo encaminhamento da mensagem (roteamento) dentro de sua faixa de frequência. Com isso, a rede se torna mais redundante, tolerante a falhas, e com maior alcance.

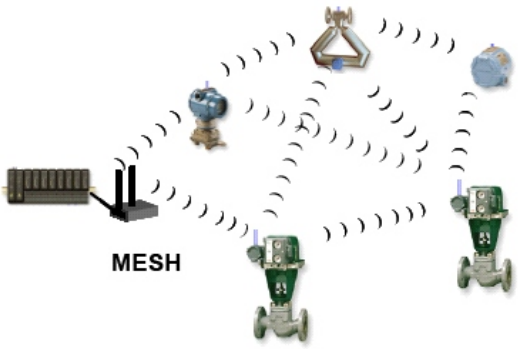

Figura 3 - Topologia em Malha para rede Wireless.
Fonte: *Caro (2008, p.25)*

A topologia Estrela (Star), na qual o ponto de acesso sem fio está no centro, é caracterizada por permitir somente que cada dispositivo sem fio comunique-se com o ponto de acesso comum, normalmente ligado através de cabos a um *switch*[8] da rede. (CARO, 2008, p. 21; FARAHANI, 2008, p.10).

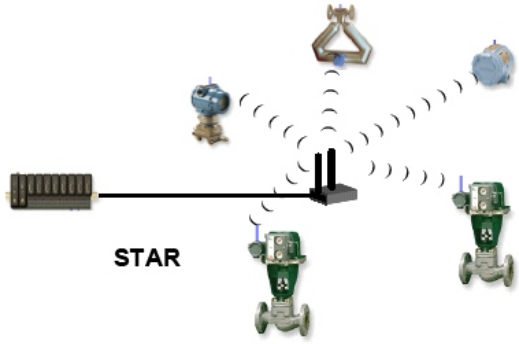

Figura 4 - Topologia em Estrela para rede Wireless.
Fonte: *Caro (2008, p.22)*

[7]Self-healing: Característica de auto adaptação para redes sem fio.
[8]Switch: Dispositivo utilizado em redes para reencaminhar mensagens entre os diversos nós.

Na topologia de Árvore (*Tree*), cada unidade de campo é configurada para uma rede que está ligada a um ponto de acesso específico. Esse ponto de acesso é então, hierarquicamente ligado a outro ponto de acesso mais próximo da rede cabeada. (CARO, 2008, p. 23).

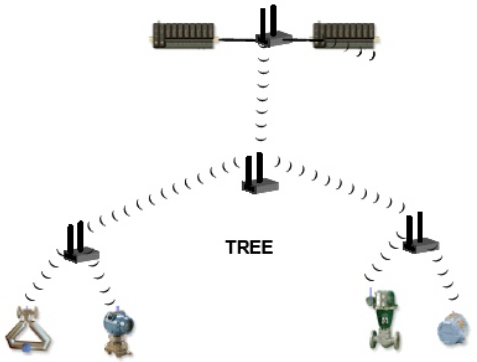

Figura 5 - Topologia em Arvore para rede Wireless.
Fonte: *Caro (2008, p.24)*

Conforme Farahani (2008, p. 11) apresenta, a topologia de rede em árvore é composta por um coordenador – que estabelece a rede inicial – roteadores – que são como os galhos da árvore e são os responsáveis por retransmitir as mensagens – e os dispositivos – que são como as folhas, recebem as mensagens, porém não tem participação no seu encaminhamento.

4 PADRONIZAÇÃO

Alguns padrões de comunicação para a utilização de *wireless* em ambiente industrial foram desenvolvidos de forma a possibilitar a aplicação dessa tecnologia de transmissão de dados em ambientes industriais. São exemplos o WirelessHART, a norma ISA SP-100 11.a e o ZigBee, sendo os três tecnologias independentes que utilizam o mesmo protocolo nas camadas baixas, o IEEE 802.15.4.

4.1 IEEE – Institute of Electrical and Electronics Engineers

A fim de definir padrões para redes sem fio, o IEEE elaborou grupos de trabalho, como por exemplo 802.11, cuja função é definir como deve ser

a comunicação entre dispositivos clientes e concentradores (WLAN – *Wireless Local Area Network*). (RUFINO, 2007). Segundo Heile e Alfvin (2010), o grupo de trabalho 802.15 define como deve ser a comunicação em redes pessoais de curta distância (WPAN – *Wireless Personal Area Network*). O padrão 802.15.4, resultado desse trabalho, encontra-se em uma banda de frequência internacional, que não necessita licença de uso e opera na frequência de 2,4GHz. As aplicações potenciais interativas para esse padrão são sensores, brinquedos, dispositivos de controle remoto residenciais e automação industrial. Utiliza uma taxa de transmissão de dados baixa para solucionar problemas de consumo de bateria.

4.2. WirelessHART

De acordo com *The Official Source For Hart Communication Technology* (2010), o WirelessHART é o elemento essencial do protocolo de comunicação HART, revisão 7. Tanto um quanto o outro são compatíveis com os atuais dispositivos HART existentes em aplicações. Sua camada física baseia-se principalmente no *IEEE* STD 802.15.4-2006, operando na faixa de 2,4GHz em DSSS. Nessa camada são definidas as características rádio elétricas do equipamento, tais como: método de sinalização, intensidade do sinal e sensibilidade do dispositivo. (CHEN et al.,2010).

Ainda segundo Chen et al. (2010), o WirelessHART opera na faixa de 2400 ~ 2483,5 MHz, com canais numerados de 11 a 26 em intervalos de 5 MHz entre dois canais adjacentes. Essa banda faz parte do ISM (*Industrial, Scientific and Medical)*, e não necessita de licenciamento dos órgãos de telecomunicação para sua utilização, bem como a transmissão é realizada a 250 Kbps. Possui características distintas no momento de sincronização de dados em sua camada de enlace, pois, define um rigoroso tempo de 10ms e utiliza tecnologia TDMA (Time Division Multiple Access) para fornecer colisão livre[9] e comunicações deterministas. O conceito de superframe é introduzido ao grupo numa sequência de horários consecutivos, sendo que todos os superframes iniciam a partir do ASN

[9]Colisão Livre: Não existem mecanismos para evitar colisão de pacotes de dados quando duas estações tentam transmitir simultaneamente.

(*Absolution Slot Number*) “0” no momento em que a rede é criada pela primeira vez.

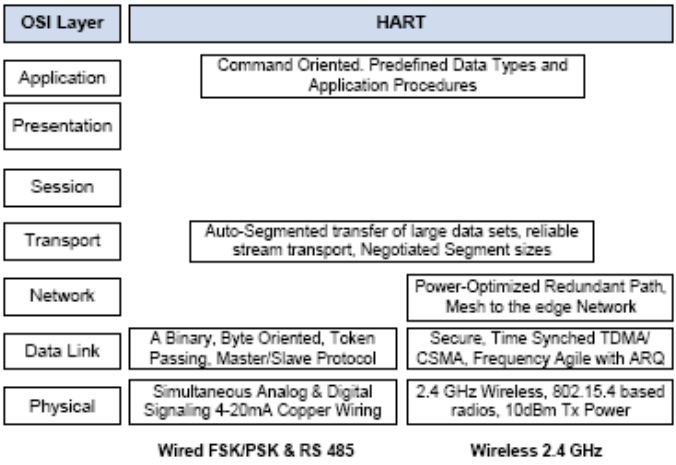

Figura 6 - Arquitetura do protocolo HART
Fonte: Chen et al. (2010, p. 7)

No WirelessHART a transação em uma faixa de tempo é descrita pelo vetor: {frame_id, index, type, src_addr, dst_addr, channel offset} no qual frame_id, identifica o superframe, index a faixa de tempo do índice do superframe, type indica o tipo de operação (transmissão/recebimento/consumo), src_addr e dst_addr são os endereços de origem e destino do dispositivo e channel offset fornece o canal lógico a ser utilizado na operação. Para ajuste fino do canal utilizado, o WirelessHART emprega o conceito de de canal em lista negra, onde, canais afetados por interferências consistentes podem ser colocados nessa lista. Para suporte a mudança de canal, cada dispositivo mantém uma tabela canais ativos. Devido aos canais em lista negra, a tabela pode ter menos de 16 entradas.

Para determinar a faixa de canais de offset, o canal atual é determinado pela formula: ActualChannel = (ChannelOffset + ASN) % NumChannels, onde, o número atual do canal é utilizado como índice dentro do canal ativo na tabela para obter as características físicas do canal. Uma vez que o ASN aumenta constantemente, o mesmo canal de offset pode ser mapeado para diferentes canais físicos em diferentes faixas,

assim, provendo uma diversidade de canais e melhorando a confiança da comunicação.

Ainda segundo Chen et al (2010, p. 10), as camadas de rede e de transporte trabalham para assegurar uma comunicação fim-a-fim confiável entre os dispositivos. Para dar suporte a tecnologia de comunicação Mesh, os dispositivos WirelessHART são requeridos para transmitir pacotes de dados em nome de outros dispositivos. Existem dois protocolos de roteamento definidos no WirelessHART:

Graph Routing: é uma coleção de caminhos que conectam nós de rede. Os caminhos em cada gráfico, expressamente criado pelo gestor da rede, são descarregados para cada dispositivo individualmente. Para enviar um pacote, o dispositivo especifica o gráfico id (determinando o destino) no cabeçalho da rede.

Source Routing: é um suplemento do Graph Routing com objetivo de obter diagnósticos na rede para enviar um pacote ao seu destino. O dispositivo de roteamento inclui no cabeçalho uma lista ordenada de dispositivos pelo qual o pacote deve percorrer. Através da tabela de diagnóstico do dispositivo, que é uma espécie de histórico, pode-se encurtar o caminho até o destino.

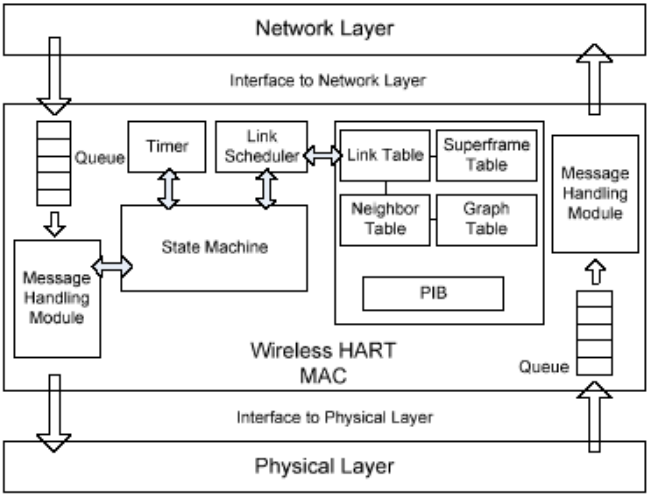

Figura 7 - Arquitetura da camada de *Data Link* - WirelessHART
Fonte: Chen et al. (2010, p. 9)

A camada de aplicação é o alto nível do protocolo WirelessHART. Nela são definidos vários comandos, respostas a dispositivos, tipos de dados e elaboração de relatórios. A comunicação entre os dispositivos de acesso se baseia nos comandos e nas respostas. (CHEN et al., 2010, p. 11).

4.3 ISA SP100 11.a

Em 2005, foi criado o comitê 100 da ISA *Standard and Practices* com a finalidade de desenvolver um padrão de redes sem fio para aplicações industriais. Esse comitê contava com os fabricantes de equipamentos de automação como principais colaboradores. A primeira versão da norma foi designada como ISA SP100 11.a e foi orientada às necessidades da indústria de processos. (CARO, 2008, p.65). Sua principal preocupação foi o desenvolvimento de uma rede universal sem fio que suportasse o FOUNDATION™ Fieldbus, HART e Profibus PA, de forma que todos fabricantes de dispositivos para automação industrial pudessem seguir.

A norma ISA100.11a, assim como o ZigBee e o WirelessHART, também se baseia no protocolo IEEE 802.15.4 em suas camadas inferiores. Seus equipamentos operam na faixa de frequência de 2,4GHz, em ciclos muito baixos para permitir vida longa às baterias. Buscando maximizar ainda mais sua utilização, os dispositivos ISA100.11a ficam a maior parte do tempo em *standby*, sendo possível configurar esse tempo de forma a permitir um melhor tempo de latência com mínimo consumo de bateria nos equipamentos da rede. (CARO, 2008, p. 67).

Em meados de 2007 a *Foundation Fieldbus* aceitou basear sua versão sem fio do FOUNDATION™ Fieldbus na norma SP100 11.a; já a HART *Communications Foundation* decidiu lançar sua própria e única interface sem fio (WirelessHART), porém está trabalhando com o comitê ISA100 para buscar algum tipo de compatibilidade. (CARO, 2008, p. 66)

De acordo com Caro (2008, p. 66), a ISA SP100.11a está sendo projetado para suportar aplicações não-críticas em indústrias de processo, mas não será voltada exclusivamente a isso. Essa primeira versão oferece suporte a malhas de controle fechadas de baixa velocidade, com tempos de ciclo mais rápidos que um segundo, e as latências não inferiores a 100ms.

Futuras versões serão alvo de malhas de controle com velocidades maiores e latências mais baixas, sendo mais apropriadas para controles discretos em automação de fábrica.

A camada de Aplicação da norma ISA100.11a, não apenas fornece todas as habituais funções de leitura/escrita e *upload/download*, mas também adiciona um objeto baseado no acesso a camada de aplicação superior através de parâmetros de dados usando EDDL (*Electronic Device Description Language*) que é padronizado pela IEC 61804. Com o EDDL presente na norma ISA100.11a, torna-se possível a compatibilidade com o FOUNDATION ™ Fieldbus, HART 4~20mA, PROFIBUS e todos os que têm acesso a dados EDDL compatíveis com suas redes cabeadas. Além disso, o OPC (*OLE for Process Control*) também adotou EDDL para seu acesso a objetos de dados baseados em rede. (CARO, 2008, p. 68).

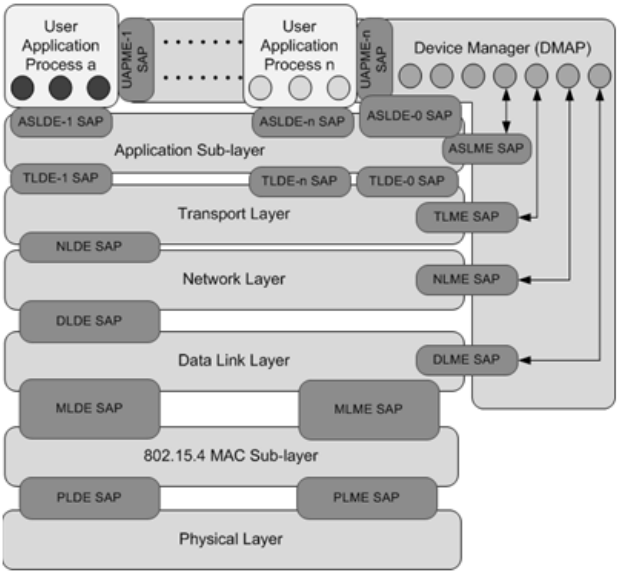

Figura 8 - Arquitetura do protocolo ISA SP100.11a
Fonte: ZigBee, ISA SP100.11a AND 802.15.4 (2010)

Espera-se utilizar a ISA100 11.a tanto em novos dispositivos de campo como em módulos que conectem dispositivos com fio existentes e que utilize o protocolo HART 4-20mA, permitindo o acesso aos dados digitais disponíveis, obtidos pela especificação HART *Device*

Description. Esses módulos serão capazes de extrair energia da fiação do dispositivo HART 4-20mA e os dados poderão então ser recuperados em um dispositivo portátil compatível com a norma ISA100.11a, ou até mesmo serem encaminhadas através de uma rede a um dispositivo de *gateway* conectado a um sistema *host*. (CARO, 2008, p. 66).

4.4. ZigBee

O ZigBee é um padrão de rede sem fio que define um conjunto de protocolos de comunicação com baixa taxa de transmissão de dados e curto alcance. Operando nas frequências de 868 MHz, 915 MHz e 2,4 GHz têm taxa máxima de dados definida em 250 Kbps. Foi desenvolvido principalmente para aplicações que requerem transmissão de dados em baixa velocidade, baixo custo de implementação e longa duração da bateria. Em muitas aplicações ZigBee, o tempo total que o dispositivo sem fio está envolvido em qualquer tipo de atividade é muito limitado, o dispositivo passa a maior parte de seu tempo, cerca de 97%, em *standby*. Assim um dispositivo pode permanecer em operação por vários anos sem a necessidade de substituir sua bateria. (FARAHANI, 2008, p. 1).

Exemplos de aplicação do ZigBee podem ser o monitoramento da pressão sanguínea e a frequência cardíaca de um paciente em sua própria casa, através de dispositivos portáteis. Outro exemplo é a aplicação em automação predial, onde são instalados vários sensores formando uma única rede sem fio que visa coletar dados que poderão ser utilizados em avaliação da integridade estrutural do prédio. Isso seria muito útil após um terremoto antes de liberá-lo para entrada de pessoas. (FARAHANI, 2008, p. 2).

Segundo Farahani (2008, p.2), o padrão ZigBee foi desenvolvido pela ZigBee Alliance com centenas de empresas associadas, que são indústrias de semicondutores a desenvolvedores de software para fabricantes de equipamento e instaladores. A ZigBee Alliance foi formada em 2002 como uma organização sem fins lucrativos, aberta a todos que queiram participar. O padrão ZigBee adotou como sua Camada Física (PHY) e de Acesso ao Meio Control (MAC) o protocolo IEEE 802.15.4.

O ciclo de trabalho em relação ao tempo total que o dispositivo fica

ativo é definido para garantir baixo consumo de energia. Por exemplo, se um dispositivo sai de *standby* a cada um minuto e permanece ativo por 60 ms, então o ciclo desse dispositivo será de 0,001, ou 0,1%. Em muitas aplicações ZigBee, os dispositivos têm ciclos de menos de 1% para garantir anos de vida útil da bateria.

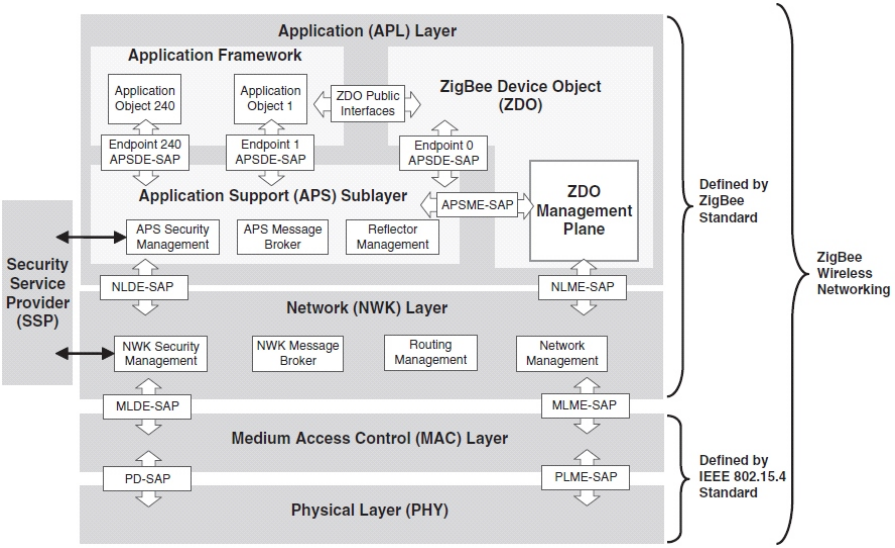

Figura 9 - Arquitetura do protocolo ZigBee
Fonte: Farahani (2008, p. 34)

As camadas de protocolo ZigBee são baseados no *International Standards Organization* (ISO) e *Open System Interconnect* (OSI) como modelo de referência em sua base. Há sete camadas do modelo ISO/OSI, porém ZigBee implementa apenas as camadas que são essenciais para a baixa potência e baixa transmissão de dados em rede sem fio. As duas camadas inferiores (PHY e MAC) são definidas pela norma IEEE 802.15.4. As camadas de Rede (NWK) e Aplicação (APL) são definidos pela norma ZigBee. Os recursos de segurança são definidas em ambos os padrões. Uma rede que implementa todas estas camadas pode ser considerada uma rede sem fio ZigBee. (FARAHANI, 2008, p. 34).

Farahani (2008, p. 247), defende que os nós de dispositivos ZigBee operam em faixas de frequências que são comumente utilizadas por outros padrões *wireless*. O ZigBee, IEEE 802.11, Bluetooth, entre outros padrões

de rede sem fio foram desenvolvidos para operar em uma faixa de frequência compartilhada, por isso devem ter algum nível de tolerância para a presença de outros sistemas.

4.5. Relação: ZigBee, WirelessHART e ISA SP100 11.a

Três tecnologias diferentes desenvolvidas com a mesma finalidade, a utilização em sistemas de automação predial, residencial e industrial, cada qual com suas características particulares. São tecnologias diferentes que sustentam em suas bases o protocolo padrão 805.15.4.

O protocolo padrão 802.15.4 de 2006, desenvolvido pelo IEEE (*Institute of Eletrical and Eletronics Engineers*) tem a finalidade de definir o comportamento da camada física e de controle de acesso ao meio (MAC). Com taxa de transmissão baixa, de 20 a 250 Kbps denominada Low-Rate Wireless Personal Area Network (LR-WPAN). Seu alcance é classificado como curto e esse padrão trata das necessidades de sistemas com pouca transmissão de dados, vida útil da alimentação muito alta, com gerenciamento de energia para garantir baixo consumo. (CARO, 2008, p.43).

O endereçamento dos rádios podem ser definidos em 16 ou 64 bits, admitindo reconhecimento para garantir confiabilidade na transmissão das mensagens e estabilização automática da rede pelo coordenador. Esse padrão define 16 canais na banda ISM na faixa de 2,4 GHz, 10 canais na faixa de 915 MHz (América do Norte) e 01 canal na faixa de 868 MHz (Europa). Os acessos aos canais são feitos através do mecanismo CSMA-CA (*Carrier Sense Multiple Access with Collision Avoindance*). (CARO, 2008, p. 44).

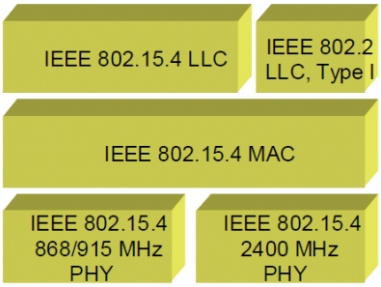

Figura 10: Protocolo padrão IEEE 802.15.4
Fonte: Caro (2008, p. 43)

A tecnologia ZigBee se comparado ao modelo OSI tem quatro camadas: Física, Acesso ao Meio (MAC), de Rede e Aplicação. Suas aplicações são voltadas a automação predial, residencial e sistemas de medição, pois não oferece salto de frequência - FHSS (*Frequency Hopping Spread Spectrum*) que tem sido utilizado com sucesso em dispositivos com fins de automação industrial. A taxa de transmissão de dados moderada e a largura da banda foram projetadas para manter baixo consumo de energia durante a transmissão, não suportando altas taxas de dados e funções de rede *backbone*. Essa tecnologia não fornece suporte a comunicação FOUNDATION™ *Fieldbus*, *Profibus*, *DeviceNet*, *LonWorks*. (CARO, 2008, p. 64).

De acordo com Labiod et al (2007, p. 109), a arquitetura de rede para tecnologia ZigBee pode ser definida como estrela, malha ou par a par. Em relação ao gerenciamento da rede, tem desvantagem em relação aos seus concorrentes, pois não oferece diversidade de caminhos, ou seja, não há mestres redundantes e o mestre da rede sempre precisa estar ativo antes dos escravos, o que acaba sendo um grande problema em aplicações complexas, pois se o mestre cair, há necessidade de desligar todos os escravos para que eles se reconectem novamente.

A arquitetura do protocolo de comunicação WirelessHART, se comparado ao modelo OSI, possui cinco níveis: camada Física, camada de data link, camada de rede, camada de transporte e camada de aplicação, não contendo as camadas de sessão e apresentação. (CHEN et al., 2010, p. 7).

Conforme Caro (2008, p. 71), o protocolo privado e fechado dessa comunicação, denominado HART 7, está limitado ao gerenciamento de 250 dispositivos de campo. A camada de rede é a responsável pelo encaminhamento gráfico usando a tecnologia de roteamento proporcionando caminhos redundantes para aumentar a confiabilidade e otimizar para o mínimo de latência. A transmissão pode ser em modo broadcast, multicast ou unicast.

Sua topologia pode ser definida como estrela, malha ou par a par. Há requisição de retransmissão no caso de transmissão de dados não bem sucedida e utiliza FHSS (*Frequency Hopping Spread Spectrum*) para

evitar congestionamentos. Todos os 15 canais, tal como definido no IEEE 802.15.4, são utilizados em paralelo; WirelessHART FHSS usa um "salto" através desses canais. Canais que já estão em uso são adicionados a uma lista negra para evitar colisões com outros sistemas de comunicação sem fio. (CHEN et al., 2010, p. 8).

A tecnologia ISA, norma SP100.11a, se comparado ao modelo OSI tem seis camadas: Física, Link de Dados, Rede, Transporte, Sub-Aplicação e Aplicação. (ZIGBEE, ISA SP100.11a, 802.15.4, 2010). Suas aplicações são voltadas ao monitoramento, controle e segurança em sistemas de automação industrial. Teve seu desenvolvimento focado na criação de uma rede industrial sem fio para ser aplicada de forma consistente e unificada tanto para indústrias de processo como manufatura discreta. Além disso, a comissão ISA100 reconheceu a necessidade de suportar múltiplos protocolos fieldbus para dispositivos inteligentes de campo, como por exemplo, FOUNDATION™ Fieldbus e Profibus PA. Diferente do WirelessHART, as aplicações com a norma SP100.11a podem conter milhares de dispositivos de campo. A versão do protocolo de Internet 6 ou IPv6 (6LoWPAN, IETF draft standard RFC4944), pode ser utilizada na camada de rede, oferecendo acesso IP para dispositivos de campo. A Camada de Rede fornece compatibilidade e roteamento fora da rede ISA100. Por razões de eficiência, a camada de rede define endereços curtos de 16 bits que são utilizados para troca de dados entre dispositivos ISA100.11a. (CARO, 2008, p. 66-67).

5 SEGURANÇA

Segurança em uma rede de automação industrial significa também proteger a rede contra espionagem, sabotagem ou ataque. A palavra segurança, muitas vezes, é utilizada para referenciar privacidade, confiabilidade e autenticidade; mas disponibilidade, alimentação dos dispositivos e algoritmos de segurança e a criptografia dos dados também devem ser considerados.

5.1 Privacidade

A privacidade pode ser descrita como manter uma rede livre de

acessos não autorizados, tanto internos quanto externos. Bloqueio de acessos à rede geralmente são atribuídos a dispositivos chamados *firewalls*. convencionalmente utilizados para isolar uma rede de negócios da Internet ou setores de uma empresa. Os *firewalls* bloqueiam o acesso a endereços IP e portas de comunicação. Além disso, eles podem autenticar usuários, exigindo uma credendial. (CARO, 2008, p. 57).

5.2. Confiabilidade

A ocorrência de falhas em uma rede, muitas vezes significa o fracasso de um sistema de automação em que o controle do processo ou da máquina depende. Quando uma rede ou sistema não tem resposta do dispositivo, geralmente é necessário conduzir o processo ou a máquina a um estado seguro, dependendo da natureza dos dados que estão trafegando pela rede. Por exemplo, se todo o controle ocorre apenas em dispositivos de campo e eles não dependem da rede, uma falha na rede não deve interromper o controle, no entanto deve produzir um alarme para notificar os operadores de tal anomalia. Se o processo não puder ser executado quando ocorrer uma falha na rede, então um mecanismo à prova de falhas deve ser implementado para trazer o processo ou a máquina a um estado seguro. (CARO, 2008, p. 57).

Em redes cabeadas, maior confiabilidade muitas vezes pode ser conseguida utilizando cabos melhores, conectores e terminações, bem como componentes eletrônicos de melhor qualidade ou maior robustez. Rádios com maior poder de transmissão poderiam muitas vezes ser utilizados para superar interferências, porém, algumas vezes, a potência irradiada é limitada por regulamentações governamentais. Redes que são tolerantes a falhas têm capacidade de fornecer mais de um caminho para comunicação entre os dispositivos. As redes *mesh* são uma solução especificamente tolerante a falhas para redes sem fio. (CARO, 2008, p. 58).

5.3 Alimentação dos Dispositivos

Redes industriais com fio geralmente são responsáveis por alimentar cada um dos dispositivos nos nós de rede, assim como transportar os sinais da rede. Em muitas automações de processo, espera-se que a rede também

seja intrinsecamente segura, o que significa que uma ruptura do cabo em ambientes com gases inflamáveis não irá causar uma explosão. As redes sem fio definitivamente têm a vantagem de não usar o fio e são inerentemente seguras, mas alimentar nós sem fio continua sendo um problema.

Dispositivos sem fio geralmente utilizam baterias para estarem ativos na rede, porém a bateria não é uma fonte de energia bem aceita para dispositivos de controle primário, exceto para fornecer energia de emergência. Essa atitude pode eventualmente mudar, mas uma fonte melhor de energia primária deve ser fornecida para dispositivos sem fio. Uma vez que as fontes de energia locais estão geralmente disponíveis, alimentação DC ou às vezes AC, podem ser uma opção, pois o cabeamento com fins de alimentação tem muito menor custo do que os utilizados para comunicação e transmissão de dados. (CARO, 2008, p. 58).

5.4. Tecnologias e Algoritmos de Segurança

De acordo com Farahani (2008), o ZigBee, utiliza criptografia de chaves simétricas AES (*Advanced Encryption Standard*[10]) de 128 bits com autenticação do remetente e destinatário da mensagem e a sincronização dos dados em tempo variável, utilizando tecnologia TDM (*Time Division Multiplexing)*. Já o WirelessHART, possui sincronização de dados fixada em 10ms utilizando acesso múltiplo por divisão de tempo (TDMA - *Time Division Multiple Access*). Em relação ao algoritmo de segurança utiliza criptografia de chaves simétricas AES de 128 bits e chaves estáticas. (CARO, 2008, p.69).

A tecnologia ISA, norma SP100.11a, tem sincronização dos dados em tempo variável utilizando TDMA, porém podem ser configurados também para tempo fixo de 10ms. Em relação ao algoritmo de segurança utiliza criptografia de chaves simétricas AES-128 ou 256 bits ou chaves assimétricas pública/privada. (CARO, 2008, p.68).

[10]Algoritmo desenvolvido por Rijmen e Daemen com chaves de 128 e 256 bits, conhecido como Rijndael. Utiliza chaves simétricas que processa dados em blocos de 128, 192 ou 256 bits. (TANENBAUM, 2003, p.790).

6 APLICAÇÕES INDUSTRIAIS

Automatizar processos industriais significa fazer uso de dispositivos comumente utilizados para medição de variáveis (temperatura, pressão, vazão), dispositivos de controle como válvulas e inversores de frequência, com a finalidade de substituir o trabalho humano. A utilização de dispositivo *wireless* vem crescendo cada vez mais, no entanto, essa tecnologia ainda é novidade em dispositivos para automação industrial. (AZEVEDO, 2009, p. 27).

A transmissão de dados é feita por transmissores acoplados ou integrados aos instrumentos que enviam os sinais a estações base e retransmitem aos sistemas de monitoramento e controle. A grande vantagem é a eliminação da fiação que, em alguns casos, pode ser um fator complicador ou até mesmo tornar uma instalação inviável. Em uma embarcação petroleira, por exemplo, considerando-se o peso total do navio, 12% equivalem somente a cabos. Com o uso da tecnologia sem fio essa massa poderia ser diminuída, porém, os cabos não deixariam de existir, principalmente quando relacionado a automação industrial. (AZEVEDO, 2009, p. 27).

"A nova tecnologia não substitui completamente os sistemas cabeados tradicionais, pois se dedica a um tipo de aplicação muito específico, principalmente em locais da planta onde é difícil passar a fiação" (PEREIRA apud AZEVEDO,2009, p.27).

Segundo Azevedo (2009), quando se trata de automação em indústrias químicas e petroquímicas, existe uma série de riscos, pois a falha de comunicação ou perda de sinal poderia causar sérios danos em equipamentos de natureza crítica como reatores que estão sujeitos a altas pressões e temperaturas.

"A comunicação sem fio, em seu estágio atual de desenvolvimento, ainda requer uma série de cuidados na fase de projeto da rede, mas é o futuro". (PEREIRA apud AZEVEDO,2009, p.27).

Outra questão que levanta suspeitas refere-se a padronização dos protocolos, pois ainda que utilizem a mesma frequência de rádio, 2,4GHz, dispositivos de fabricantes diferentes ainda não se comunicam. Essa padronização é um processo semelhante ao que ocorreram com os

celulares, todos se comunicam independente das operadoras. Uma das vertentes desta padronização é o WirelessHART. (AZEVEDO, 2009, p. 27).

A simples desconfiança que muitos técnicos têm pelo *wireless* também atrapalha na sua utilização em ambientes industriais. "BlueTooth é interessante, mas não é adequado ao ambiente industrial". (PELUSO apud JUNIOR, 2007, p.42). Apesar de vários protocolos utilizarem o ar como meio de comunicação de dados, não significa que todos têm são iguais. Cada um tem características distintas, portanto, cada um tem seu direcionamento de utilização correta.

6.1. Mais que Redução de Cabos

De acordo com Azevedo (2009, p. 28), a redução de custos quando se fala em automação utilizando dispositivo *wireless*, não significa apenas menos cabos, mas também se refere à economia com infra-estrutura, mão de obra e projetos de encaminhamento elétrico. Uma rede cabeada custa em média 6% do total da obra. Uma aplicação característica para esse tipo de instrumento é na medição de temperatura em um tambor giratório de um equipamento de incineração, outra aplicação é em medições provisórias com objetivos específicos para testes com finalidade temporária.

"É muito complicado passar novos cabos em instalações industriais. Exige-se um novo projeto e uma série de medidas que precisam ser levadas em consideração". (PEREIRA apud AZEVEDO, 2009, p.28).

Aplicações *wireless* no Brasil são relativamente novas, a Petrobras e indústrias do setor siderúrgico tiveram as primeiras aplicações dessa tecnologia. É importante destacar que o monitoramento é diferente do controle, sendo o primeiro referente a medição de grandezas e transmissão destas informações, já o segundo envolve dispositivos de ação para correção de desvio de valores pré determinados. A tecnologia *wireless* em ambiente industrial, como qualquer outra tecnologia, possui suas desvantagens. A mais clara é a falta de garantia da comunicação em 100% do tempo, fato relacionado diretamente à necessidade de diminuir o consumo de bateria, mas, com a utilização das baterias atuais que têm duração de cinco anos com medição média de uma vez por minuto, torna

um atrativo muito grande em monitoramento. (AZEVEDO, 2009, p. 28).

Figura 11 - Dispositivo Wireless aplicado a medição de fluídos em tanques

Possibilidades de falhas dos dispositivos podem ser eliminadas tomando algumas medidas de segurança, em outras os próprios dispositivos podem utilizar recursos para evitar falhas, como é o caso de interferências com outros comprimentos de onda. Para isso tanto as estações base quanto os dispositivos podem utilizar FHSS, alterando suas frequências automaticamente. (AZEVEDO, 2009, p. 27).

6.2 WirelessHART e ISA SP100

Grande parte dos dispositivos *wireless* disponíveis no mercado utilizam o protocolo WirelessHART, porém a ISA, em abril de 2009 publicou a norma ISA SP100 aprovada pela ANSI (*American National Standards Institute*), que tem como principal objetivo estabelecer um padrão global para comunicação *wireless* industrial, padrão este que não é compatível com WirelessHART.

Uma das empresas mais tradicionais no segmento de automação, a Yokogawa, empresa japonesa fabricante de transmissores de pressão e temperatura, se mostrou conservadora e optou por esperar a publicação da norma SP100 da ISA, acreditando que no futuro esta norma venha

englobar o protocolo WirelessHART. A Yokogawa acredita que o WierelessHART foi destinado originalmente para aplicações de monitoramento, enquanto o ISA SP100 pode ser utilizado também para o controle. Ainda, para Yokogawa, quem prega a filosofia de que a comunicação *wireless* não é adequada a controle é usuário de WirelessHART, no entanto a limitação não se aplica ao protocolo desenvolvido pela ISA. (AZEVEDO, 2009, p. 33).

Conforme Azevedo (2009, p.33), a estatal brasileira de petróleo, Petrobras, tem equipamentos em testes da Yokogawa, devido ao fato dela oferecer menos resistência a entrada de novas tecnologias. Existem pátios com quase cem tanques a uma distancia considerável entre eles, tornando muito caro a utilização de cabos, por isso a empresa opta pela medição manual.

Com a utilização da tecnologia sem fio, é possível diagnosticar se uma válvula enrosca, se há agarramento de gaxeta[11] ou bloqueio, fato que a instrumentação tradicional a cabo não suporta. No início os instrumentos possuíam somente protocolos analógicos com propósito único, enviar um sinal proporcional a variável de medição entre 4 a 20 mA, sem tráfego de informações. Logo surgiram os protocolos digitais como o Fieldbus e o PROFIBUS que permitiam maior envio de informações, porém tem limitações de distância dos cabos. A tecnologia sem fio contorna esses dois problemas. (AZEVEDO, 2009, p. 33).

7 CONSIDERAÇÕES FINAIS

Apesar das redes sem fio apresentarem algumas características não vantajosas em determinadas aplicações, o futuro do *wireless* na indústria ainda tem um grande horizonte a ser explorado. Com o contínuo avanço tecnológico, proporcionando protocolos digitais cada vez mais robustos e seguros, bem como equipamentos cada vez mais completos e a um menor custo, permitirão inevitavelmente sua utilização em ambientes industriais.

O protocolo ZigBee foi o primeiro padrão criado. Em conjunto com o protocolo do IEEE 802.15.4, foi desenvolvido para ser utilizado em

[11] Junta de separação entre duas peças montadas uma na outra.

aplicações de automação predial e residencial, pois se destina a um volume de dados pequeno e tem curto alcance.

O padrão WirelessHART, revisão 7 do protocolo HART, é proprietário. Esse padrão saiu na frente quanto à adoção por fabricantes de dispositivos e hoje existe um grande disponível no mercado e até mesmo já instalados em indústrias. No entanto, redes utilizando tecnologia WirelessHART não se destinam a aplicação em malhas de controle, estão voltadas ao monitoramento de variáveis do processo, como por exemplo, temperatura, nível e pressão. O fator taxa de atualização dos dados e a vida útil da bateria são as limitações quanto a aplicação em controles, principalmente os que exigem uma ação rápida do sistema, como por exemplo, reações químicas.

A ISA criou um comitê responsável por desenvolver um padrão de comunicação *wireless* a ser utilizado em aplicações industriais. Esse comitê desenvolveu a norma ISA SP100.11a, protocolo não proprietário que tende a ser um padrão global, fornecendo suporte a outras redes cabeadas, como por exemplo o PROFIBUS, HART, FOUNDATION™, entre outras. Ainda não é possível afirmar que o padrão da ISA englobará WirelessHART, sendo assim, não se sabe se serão compatíveis.

Um mercado potencial para utilização dessa tecnologia são os parques de tancagem das refinarias de petróleo, onde a área de cobertura é muito grande, onde seriam necessários quilômetros de cabos, para uma completa interligação, o que torna praticamente inviável.

8 REFERÊNCIAS

AZEVEDO, M. Comunicação sem cabos avança na indústria e chega a instrumentação de processos. **Revista Química e Derivados**. São Paulo: Dezembro, ed. 492, dez. 2009, p. 26-34.

CARO, D. Wireless Networks for Industrial Automation. 3. ed. US, 2008.

CASSIOLATO, C. et al. **PROFIBUS Process Field Bus**: Descrição Técnica. Disponível em: <http://www.profibus.org.br/files/DescricaoTecnica/PROFIBUS_DESCTEC2009.pdf>. Acesso em: 16 abr 2010.

CHEN, D.; NIXON, M.; MOK, A. **WirelessHART Real-Time Mesh Network for Industrial Automation.** 1. ed. Springer, 2010.

FARAHANI, S. **ZigBee Wireless Networks and Transceivers.** 1. ed. US: Elsevier, 2008.
HEILE, R. F.; ALFVIN, R. **Working Group Wireless Personal Area Networks**. Disponível em: < http://www.ieee802.org/15/ >. Acesso em: 26 mai 2010.
HELSON, R. **Os Benefícios do Protocolo HART em Sistemas de Instrumentação Inteligentes**. Disponível em: < http://www.smar.com/brasil2/hart.asp>. Acesso em: 25 abr 2010.
JUNIOR, W. Wireless - E se pudesse...?. **Revista Petro e Química**. São Paulo: Abril, ed. 294, abr. 2007, p. 40-44.
KIELBLOCK, L. Integridade de Sinal de Rede Wireless Industriais. **Revista InTech America do Sul**. São Paulo: 200, ed. 111, 2009, p. 17.
LABIOD, H.; AFIFI, H.; DE SANTIS, C. **Wi-Fi, Bluetooth, ZigBee e WiMax.** 1. ed. Springer, 2007.
PEREIRA, S. B; ALIPERTI, J. **Normas da ISA: O Mundo da Instrumentação, Automção e Controle na Palma das Mãos**. Disponível em:< http://www.brazilautomation.com.br/painel/normas_isa.html>. Acesso em: 21 nov 2010a.
RUFINO, Nelson Murilo de Oliveira. **Segurança em Redes sem Fio**: Aprenda a proteger suas informações em ambientes Wi-Fi e Bluetooth. 2ª ed. São Paulo: Novatec Editora, 2007.
SIEMENS. **Industrial Ethernet**. Disponível em:< http://www.siemens.com.br/templates /produto.aspx?channel=3674&channel_ter_nivel=3680&produto=4500 >. Acesso em: 20 mai 2010.
TANENBAUM, A. S. **Redes de Computadores.** 4. ed. Campus, 2003.
The Official Source For Hart Communication Technology. Disponível em: < http://www.cds.caltech.edu/~shiling/wirelesshart_datasheet.pdf >. Acesso em: 12 abr 2010.
Virtual Academy of As-Internacional Association. Disponível em: < http://www.as-interface.net/academy/content/sys/start/start.en.html >. Acesso em: 10 mai 2010.
ZigBee, ISA SP100.11a and 802.15.4. Disponível em: < http://cio.nist.gov/esd/emaildir/lists /i2g_interop/doc00014.doc >. Acesso em: 11 set 2010.