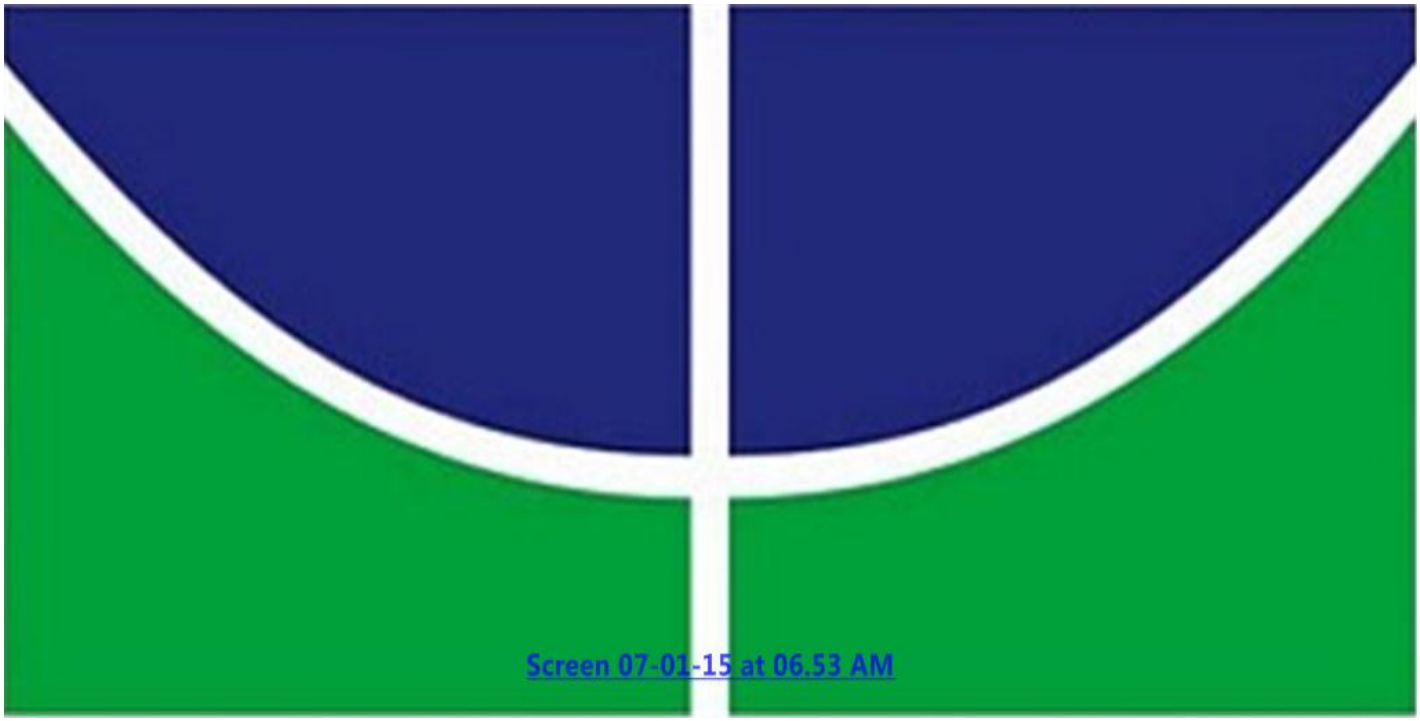

ESTUDO DA TECNOLOGIA RFID: APLICAÇÃO E POTENCIAL EM DIVERSAS ÁREAS DE ATIVIDADE HUMANA

EDUARDO SOARES BASTOS

ORIENTADOR: PROF. Ph.D. MARCO ANTÔNIO BRASIL TERADA

TRABALHO DE CONCLUSÃO DE CURSO

BRASÍLIA/DF: MARÇO – 2015

PROJETO DE GRADUAÇÃO

RFID – Identificação por radiofrequência aplicação e potencial em diversas áreas de atividade humana

Por **Eduardo Soares Bastos**

Monografia de graduação submetida ao Departamento de Engenharia Elétrica da Faculdade de Tecnologia da Universidade de Brasília, como requisito parcial para obtenção do grau de Engenheiro Eletricista.

Banca Examinadora

Marco Antonio Brasil Terada (Orientador) _____

Paulo Henrique Sales Wanderley _____

Leonardo R.A.X de Menezes _____

Brasília, 24 de Novembro de 2015

Dedicatória

A DEUS por ter me proporcionado a força necessária para a conclusão do curso, a meu irmão Alessandro por ter me permitido manter o entusiasmo pelo curso, a minha mãe Márcia, a meu pai Cesar e a minha irmã Carla.

Agradecimentos

Agradeço a toda minha família e meus amigos, que me apoiaram, me estimulam a crescer como profissional e como pessoa e que me proporcionaram condições para que eu alcance meus objetivos; ao meu orientador, Marco Antônio Terada que desde a primeira matéria cursada com ele me fez desenvolver um interesse ela área em que atua e por me servir como estímulo profissional; Ao Hugo meu amigo que desde quando se formou me passou dicas fundamentais para a vida profissional, aos colegas da UFG que me proporcionaram momentos de coleguismo e crescimento social e pessoal e aos colegas da Unb que me proporcionaram exelentes momentos de crescimento pessoal e profissional com um ambiente desafiador e estimulante.

TRABALHO DE CONCLUSÃO DE CURSO I SUBMETIDO AO DEPARTAMENTO DE ENGENHARIA ELÉTRICA DA FACULDADE DE TECNOLOGIA DA UNIVERSIDADE DE BRASÍLIA COMO PARTE DOS REQUISITOS NECESSÁRIOS PARA A CONCLUSÃO DO CURSO DE ENGENHARIA ELÉTRICA.

RESUMO

Este trabalho versa sobre o uso da tecnologia RFID(***Radio Frequency Identification***), suas aplicações atuais nos diversos campos de atividades humana e sobre seu potencial de uso em diversos setores. Tendo em vista a agilidade, a segurança e outros benefícios que podem ser obtidos, o uso do RFID tende a ser mundialmente expandido. Levando-se em consideração a aplicabilidade da tecnologia na vida cotidiana, é possível verificar que praticamente tudo poderá ser facilitado com seu uso, como, por exemplo, o RFID substituindo as chaves de casa, do carro, do escritório, o controle remoto do portão da garagem, extinguindo a necessidade de parar na cabine de pedágio, auxiliando no controle de quantidade e da validade de produtos na despensa, ou na geladeira, elaborando e enviando, automaticamente, a lista de compras ao supermercado, assim que algum produto é retirado de um armário ou prateleira de casa, dentre várias outras facilidades que a tecnologia poderá proporcionar. Este trabalho apresentará também uma visão de futuro, para que rumo poderá nos levar o uso desta tecnologia, e o que podemos esperar como mudanças em nosso cotidiano.

SUMÁRIO

1 FUNCIONAMENTO DA TECNOLOGIA RFID (acrônimo para Radio-Frequency IDentification ou, em português, Identificação por Rádio Frequência).

1.1 CARACTERISTICAS DE UMA SISTEMA RFID.

1.1.1 CARACTERISTICAS FUNDAMENTAIS DE SISTEMAS RFID.

Os sistemas RFID existem em inúmeras variantes de aplicação, produzido por um número quase igualmente elevado des fabricantes. Se quisermos manter uma visão geral dos sistemas RFID devemos procurar as características que podem ser usadas para diferenciar um sistema RFID de outro. Os sistemas RFID operam de acordo com um dos dois procedimentos básicos: sistemas full duplex (FDX) / half-duplex (HDX) e sistemas seqüenciais (SEQ). [1]

Em sistemas do tipo full e half duplex a resposta do transponder é transmitida quando o campo de RF do leitor esta ligado. Uma vez que os sinais dos transponders para a antena do receptor pode ser extremamente fraca em comparação com o sinal emitido a partir do próprio leitor, procedimentos de transmissão apropriados devem ser utilizados para diferenciar o sinal emitido do transponder do sinal emitido a partir do leitor. Na prática, a transferência de dados a partir do transponder até o leitor é feita utilizando modulação de carga, a modulação de carga usada utiliza uma subportadora, mas também pode ser utilizado (sub)harmônicos da freqüência de transmissão do leitor. [1]

Em contraste, os procedimentos sequenciais empregam um sistema através do qual o campo do leitor é desligado brevemente em intervalos regulares. Essas lacunas são reconhecidas pelo transponder e usadas para o envio de dados do transponder para o leitor. A desvantagem do procedimento seqüencial é a perda de energia pelo transponder durante a pausa na transmissão, estas perdas devem ser suavizadas pelo fornecimento auxiliar de energia, através de condensadores ou baterias, que seja suficiente para manter o funcionamento do sistema. [1]

A capacidade de armazenamento de dados dos transponders RFID normalmente variam de poucos bytes para várias kilobytes. Os chamados transponders de 1 bit representam uma exceção a esta regra. Uma quantidade dados de exatamente 1-bit é apenas o suficiente para sinalizar dois estados para o leitor: 'transponder está no campo "ou" transponder não está no campo'. No entanto, isso é perfeitamente adequado para cumprir funções de monitoramento ou de sinalização simples. Uma vez que um transponder de 1-bit não precisa de um chip eletrônico, esses transponders podem ser fabricados por uma fração de centavos. Por esse motivo, um grande número de transponders de 1-bit são utilizados em Electronic Article Surveillance (EAS) para proteger bens em lojas e empresas. Se alguém tenta deixar a loja com produtos que não tenham sido pagos, o leitor instalado na saída

indicará o estado 'transponder está no campo' e inicia a reação apropriada. O transponder de 1-bit é removido ou desativado no plantio direto, quando as mercadorias são pagos. [1]

A seguir, figura 1, um diagrama mostrando os diversos tipos de classificação de um sistema *RFID*.

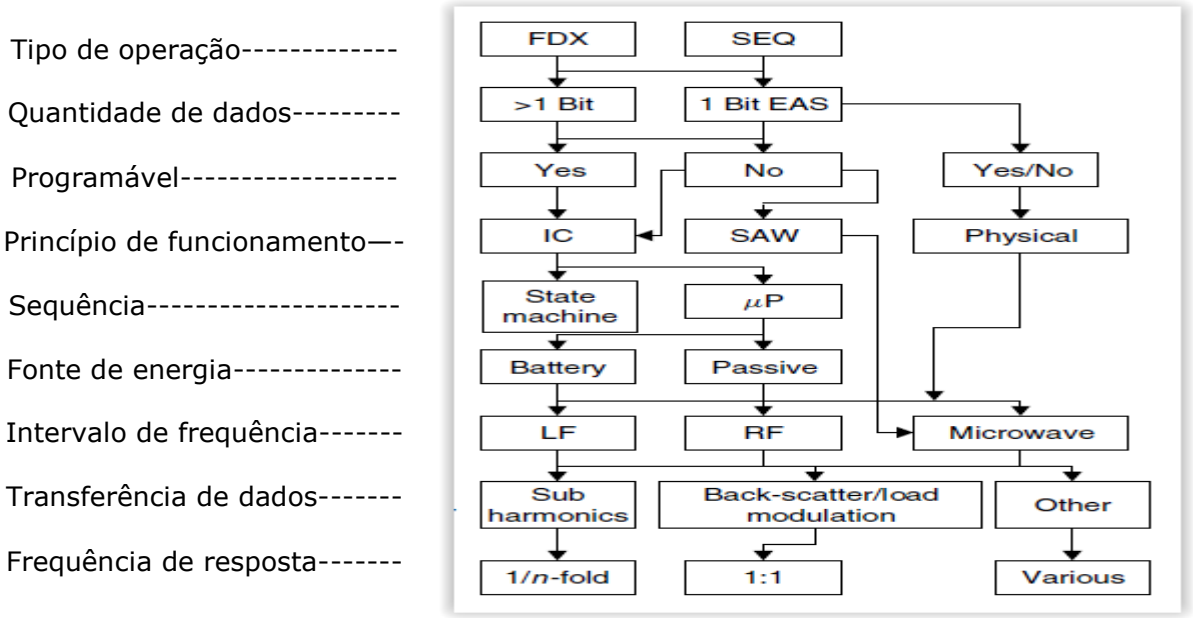

Figura 1 – As diferentes características de um sistema RFID.

A possibilidade de gravação de dados no transponder nos fornece outra forma de classificar os sistemas RFID. Em sistemas muito simples o registro de dados no transponder é normalmente uma série de números simples, quando incorporados no chip durante a fabricação os dados não podem ser alterados posteriormente. Em respondedores graváveis, por outro lado, o leitor pode escrever dados no transponder. Os três procedimentos principais são usados para armazenar os dados: sendo indutivamente acoplados EEPROMs sistemas RFID (eletricamente apagável programável memória somente leitura) são de uso dominante. No entanto, estes apresentam as seguintes desvantagens: alto consumo de energia durante a operação de escrita e número limitado de ciclos de escrita (tipicamente da ordem de 100 000 a 1 000 000). Frams (memória de acesso aleatório ferromagnético) têm sido usado recentemente, em casos isolados. O consumo de energia de leitura de frams é menor do que a de EEPROM por um fator de 100 e o tempo de escrita é 1000 vezes mais baixo. Problemas de fabricação têm impedido a sua introdução generalizada no mercado. [1]

Particularmente comum em sistemas de microondas, as memórias SRAM (memória estática de acesso aleatório) também são utilizadas para armazenamento de dados em sistemas RFID, facilitando os ciclos de escritas tornando-os muito rápido. Contudo, os dados de retenção requer uma fonte de alimentação ininterrupta através bateria auxiliar. [1]

Em sistemas programáveis, escrever e ler, ter acesso à memória e quaisquer pedidos de autorização para gravação e leitura deve ser controlado pela lógica interna do suporte de dados. No caso mais simples dessas funções pode ser realizada por uma máquina de estado. Muitas seqüências complexas podem ser realizadas usando máquinas de estado. No entanto, a desvantagem do uso de máquinas de estado é a sua inflexibilidade sobre alterações a funções programadas, porque tais mudanças exigem alterações no circuito do chip

de silício. Na prática, isto significa redesenhar o layout do chip, com toda a despesa associada. [1]

O uso de um microprocessador nesta situação trás melharas consideraveis. Um sistema operacional de gestão de dados de aplicativo é incorporado ao processador durante a fabricação, usando-se uma máscara. As alterações são mais barata de se implementar e, além disso, o software pode ser adaptado para executar aplicações muito diferentes. [1]

No contexto dos cartões inteligentes que dispensão contacto com o leitor, os suportes de dados graváveis com uma máquina de estado também são conhecidos como "cartões de memória", para distingui-los dos cartões de processador. [1]

Neste contexto, devemos mencionar também transponders que podem armazenar dados, utilizando efeitos físicos. Isso inclui um transponder de onda de superfície usado somente para leitura de 1 bit, transponders que normalmente podem ser desativados (definido como 0), mas raramente podem ser reativados. [1]

Uma característica muito importante dos sistemas RFID é o fornecimento de energia para o transmissor-respondedor. Transponders passivos não têm a sua própria fonte de alimentação e, portanto, toda energia necessária para o funcionamento do transponder passivo deve ser retirado do (campo magnético/elétrico) do leitor. Por outro lado, os transponders ativos têm uma bateria incorporada, que fornece toda ou parte da energia para a operação de um circuito integrado. [1]

Uma das características mais importantes de um sistema RFID é a freqüência de operação a qual influencia no alcance do sistema resultante. A freqüência de operação de um sistema RFID é a freqüência com que o leitor transmite. A frequência de transmissão do transponder é desconsiderada. Na maioria dos casos, é a mesma que a frequência de transmissão do leitor (modulação de carga, retroespalhamento). No entanto, a capacidade de tranmissão do transponder pode ser ajustada para transmitir em uma potência dez vezes menor que a do leitor. [1]

As diferentes freqüências de transmissão são classificadas nas três faixas básicas, LF (baixa freqüência, 30-300 kHz), HF (alta frequência) / freqüência de rádio RF (3-30MHz) e UHF (Ultra High Frequency, 300 MHz-3 GHz) / microondas (> 3 GHz). Uma outra subdivisão de sistemas RFID é feita de acordo com a faixa de frequência e nos permite diferenciar entre sistemas de acoplamento próximo (0-1 cm), de acoplamento de controle remoto (0-1 m), e de acoplamento de longo alcance (> 1m). [1]

Os diferentes procedimentos para o envio de dados do transponder de volta para o leitor podem ser classificados em três grupos: (i) o de uso de reflexão ou backscatter (A frequência da onda refletida corresponde à frequência de transmissão do leitor → proporção de frequência 1:1) ou (ii) de modulação de carga (o campo do leitor é influenciado pela proporção de frequência do transponder → 1:1), e (iii) o de uso de sub-harmonicos (1 / N vezes) e a geração de ondas harmónicas de (n vezes) no transponder. [1]

1.1.2 Formatos de construção dos Transponders

1.1.2.1 Discos e moedas

O formato mais comum usado na construção dos transponders são os chamados discos (moedas), que é um transponder em formato arredondado (ABS) moldado por injeção habitação, com um diâmetro que varia entre alguns milímetros a 10 cm. Geralmente, há um

furo para o uso de um parafuso de fixação no centro do transponder. Como alternativa a este tipo de molde (ABS) por injeção existe o polistirol ou mesmo o de resina epoxi que podem ser usados para atingir uma gama de temperatura de funcionamento mais ampla. [1]

A seguir, figura 2, diferentes formatos de transponder antes e depois do encapsulamento.

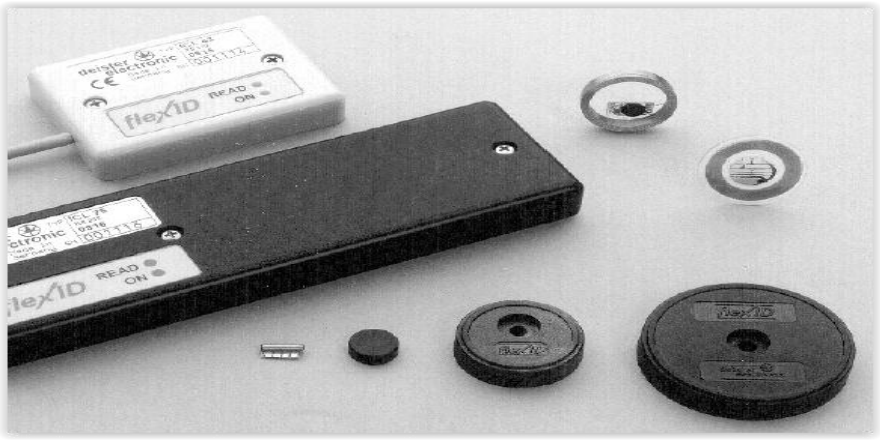

Figura 2-Diferentes formatos de transponders de disco. À direita, transponders de bobina e chips antes do encapsulamento; à esquerda, diferentes formatos de antenas do leitor. [1]

1.1.2.2 Encapsulamento de vidro

Transponders de vidro foram desenvolvidos para que pudessem ser injetados sob a pele de um animal para fins de identificação. Tubos de vidro de apenas 12-32mm contêm um microchip e um chip com capacitor, usado para facilitar a obtenção da corrente de alimentação montados sobre uma pequena placa de circuito impresso (PCB). A bobina do transponder contém fios de apenas 0,03 milímetros de espessura enrolados em um núcleo de ferrite. Os componentes internos são incorporados em um adesivo suave para alcançar a estabilidade mecânica. [1]

A seguir, figura 3, uma imagem de um transponder com encapsulamento de vidro.

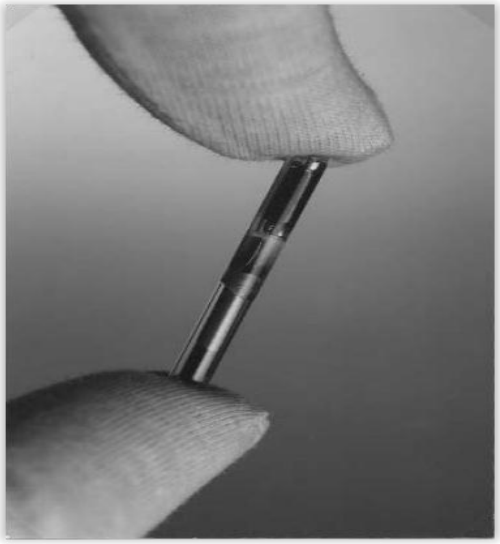

Figura 3 – Imagem próxima de um transponder de vidro 32 milímetros usado para a identificação dos animais ou ainda para a transformação em outros formatos de construção. [1]

A segui, figura 4, uma vista interna dos componentes de um transponder com encapsulamento de vidro.

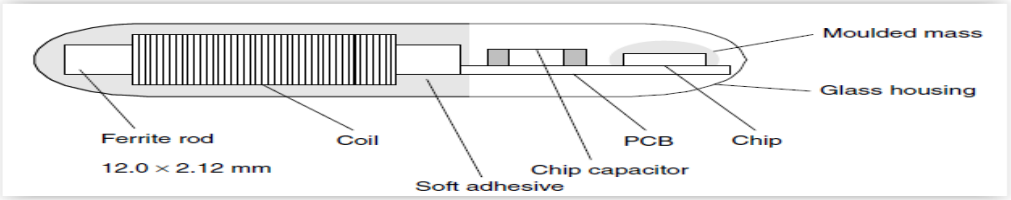

Figura 4 – Layout dos componentes de uma transponder de vidro: da esquerda para a direita, haste de ferrite, bobina, adesivo macio, chip com capacitor, PCB(Printed circuit board) ou placa de circuito impresso, microchip, invólucro(cápsula) de vidro, massa moldada. [1]

1.1.2.3 – Encapsulamento de plástico

O encapsulamento de plástico (embalagem de plástico, PP) foi desenvolvido para aplicações que envolvam solicitações mecânicas particularmente elevadas. Este revestimento pode ser facilmente integrado a outros produtos, por exemplo em chaves do carro para os sistemas electrónicos de imobilização. A cunha feita de substância moldável contém quase os mesmos componentes que o transponder de vidro, mas a sua bobina maior lhe confere um maior intervalo de funcionamento. Outras vantagens são sua capacidade de aceitar microchips maiores e sua maior tolerância a vibrações mecânicas, que é um dos requisitos exigidos pela industria automotiva. O transponder PP provou ser capaz de satisfazer outros requisitos de qualidade, tais como ciclos de temperatura e testes de queda. [1]

A seguir, figura 5, uma imagem de um transponder com encapsulamento de plástico. E , na figura 6, uma visão interna dos componentes deste tipo de transponder.

Figura 5 – Transponder em um encapsulamento de plástico. [1]

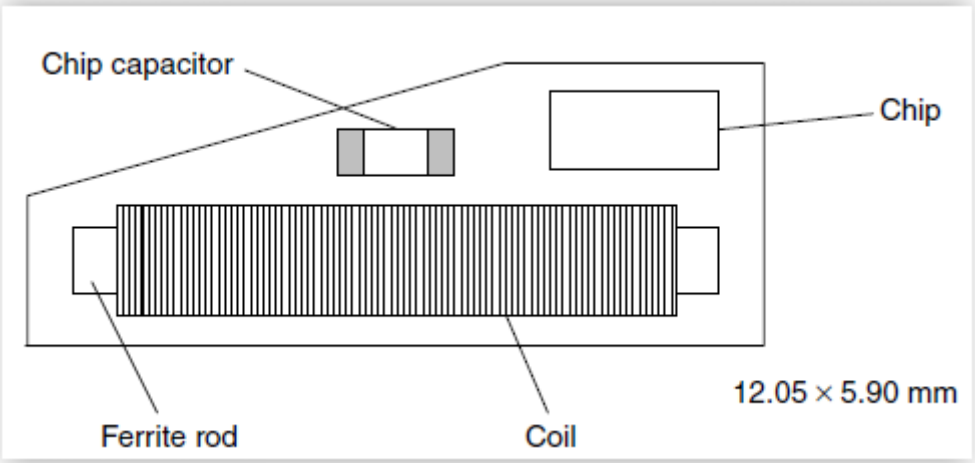

Figura 6 – Layout dos componentes de um transponder com encapsulamento de plástico, em sentido anti-horário: haste de ferrite, bobina, Chip e Chip com capacitor. [1]

1.1.2.4 – Instrumento e frasco gasoso de identificação

Formatos especiais de construção foram desenvolvidos para instalar transponders indutivamente acoplado em superfícies de metal. A bobina do transponder é enrolada em um núcleo de ferrite em forma de recipiente. O chip do transponder é montado no reverso do núcleo de ferrite em forma de recipiente e conectado com a bobina do transponder. [1]

A fim de obter uma tolerância suficiente para o funcionamento estável, em relação à vibração mecânica e ao calor, o chip do transponder e o núcleo de ferrite em formato de recipiente são revestidos por uma espécie de concha de PPS1(polímero, sulfeto de p-fenileno) usando resina epóxi. As dimensões externas do transponder e a sua zona de encaixe foram padronizados na ISO 69873 para incorporação em um botão de retenção ou

em uma fita de liberação rápida para a identificação de uma ferramenta. Diferente[1]s modelos são usados para a identificação de frascos de gás. [1]

A seguir, figura 7, imagem da montagem de um transponder em superfície de metal.

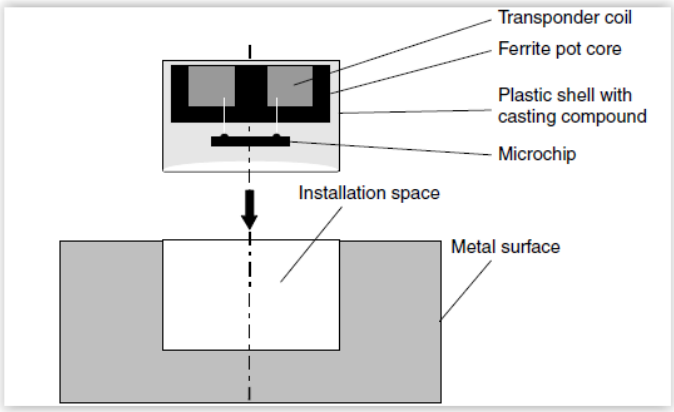

Figura 7 – Layout dos componentes de um transponder para a montagem em superfícies metálicas. A bobina do transponder é enrolada em torno de um núcleo de ferrite em forma de U e depois lançado em um reservatório de plástico. É instalado com a abertura do núcleo em forma de U na parte superior. De cima para baixo: bobina do transponder, núcleo de ferrite, reservatório de plástico com composto fundido, microchip, espaço de instalação e superfície de metal. [1]

2.1.2.5 – Chaves e porta-chaves

Transponders são também integrados em chaves mecânicas usadas por imobilizadores ou em portas de bloqueio, estas aplicações exigem requisitos de segurança particularmente elevados. Estes dispositivos são constituídas geralmente por um transponder num invólucro de plástico, que é moldado ou injetado no chaveiro. O modelo de chaveiro transponder provou ser muito útil para sistemas que fornecem acesso a áreas de escritório e de trabalho. [1]

A seguir, figura 8, uma imagem de um *transponder* do tipo Anel-chave.

1- PPS(sulfet o de p-fenileno) –Apresenta uma estrutura rígida resultante de seu alto grau de estabilidade molecular, elevada resistência à degradação térmica

Figura 8 – Anel-chave transponder para um sistema de acesso [1]

1.1.2.6 – Relógios inteligentes

Este formato de construção foi desenvolvido no início da década de 1990 pela empresa austríaca Ski-Data e foi usado pela primeira vez em passes de esqui. Estes relógios de identificação sem contato ganharam terreno também em sistemas de controle de acesso. Conforme a figura 9. O relógio contém uma antena de quadro com um pequeno número de voltas impressas sobre uma fina placa de circuito impresso, que se segue à carcaça do relógio, tanto quanto possível para maximizar a área delimitada pela bobina de antena - e, portanto, o intervalo de funcionamento. [1]

Figura 9 – Relógio com transponder integrante sendo usado em sistema de autorização de acesso sem contato. [1]

2.1.2.7 – Formato ID-1, cartões inteligentes de uso sem contato

O formato ID-1 conhecido em cartões de crédito e cartões de telefone (85,72 milímetros × 54.03mm × 0,76 milímetros ± tolerâncias) está se tornando cada vez mais importante para cartões inteligentes de funcionamento sem contato em sistemas RFID. Uma vantagem deste formato para acoplamento indutivo em sistemas de RFID é a grande área da bobina, o que aumenta a gama de funcionamento dos cartões inteligentes. Cartões inteligentes sem contato são produzidos pela laminação d e um transponder entre quatro folhas de PVC. As folhas individuais são cozidas em alta pressão e temperaturas superiores 100 ◦C para produzir um vínculo permanente. [1]

Cartões inteligentes sem contato do projeto ID-1 são perfeitamente adequados para o transporte de anúncios e muitas vezes têm overprints artísticos, como aqueles em cartões de telefone, por exemplo. No entanto, isso nem sempre é possível de aderir à espessura máxima de 0,8 milímetros especificados para cartões ID-1 em ISO 7810. Os transponders de microondas, em particular, exigem um desenho mais espesso, porque neste projeto o transponder geralmente é inserido entre dois escudos de PVC ou embalado utilizando um processo de moldagem por injecção. [1]

A seguir, figura 10, imagem de um cartão inteligente com um desenho impresso

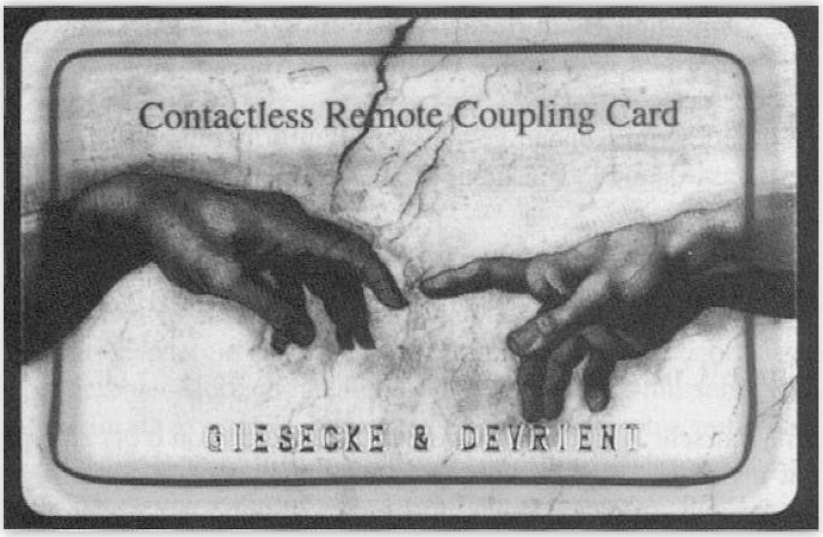

Figura 10 - Cartão inteligente Semitransparente, sem contato. A antena do transponder pode ser claramente vista ao longo da borda da placa. [1]

1.1.2.8 – Etiqueta inteligente

Etiqueta inteligente é um termo que se refere a um formato de transponder de papel fino. Em respondedores deste formato a bobina do transponder é aplicada a uma folha de plástico de apenas 0,1 milímetros de espessura por serigrafia ou gravação. Esta folha é muitas vezes laminada com uma camada de papel e a sua volta é revestida com adesivo. Os transponders são fornecidos sob a forma de etiquetas auto-adesiva em um rolo sendo finas e flexíveis o suficiente para ser presa a bagagens, embalagens e bens de todos os tipos. Uma vez que as etiquetas adesivas podem facilmente serem sobrepostas, o que permite facilmente ligar os dados armazenados a um código de barras adicional sobre a parte da frente do rótulo. [1]

A seguir, figura 11, imagem de uso de uma etiqueta inteligente. E, na figura 12, imagem interna de um transpoder do tipo etiqueta inteligente.

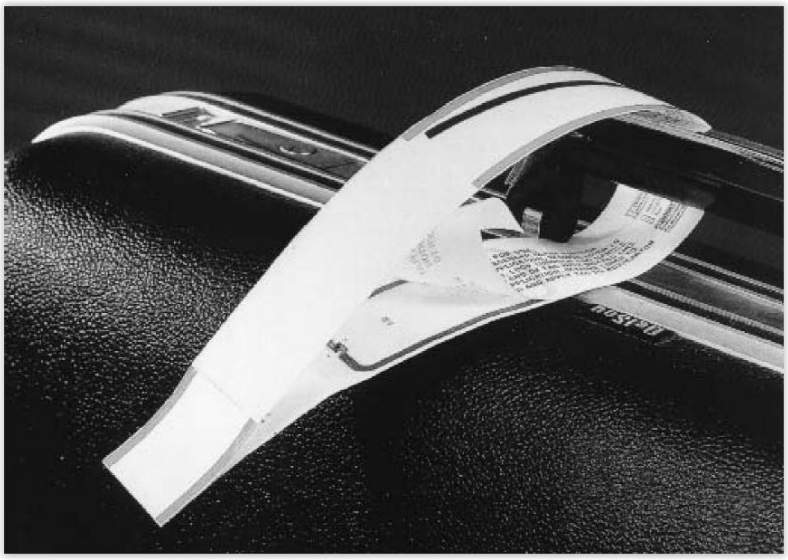

Figura 11 - Transponders de etiquetas inteligentes são finos e flexíveis o suficiente para ser anexados a bagagens sob a forma de uma etiqueta auto-adesiva. [1]

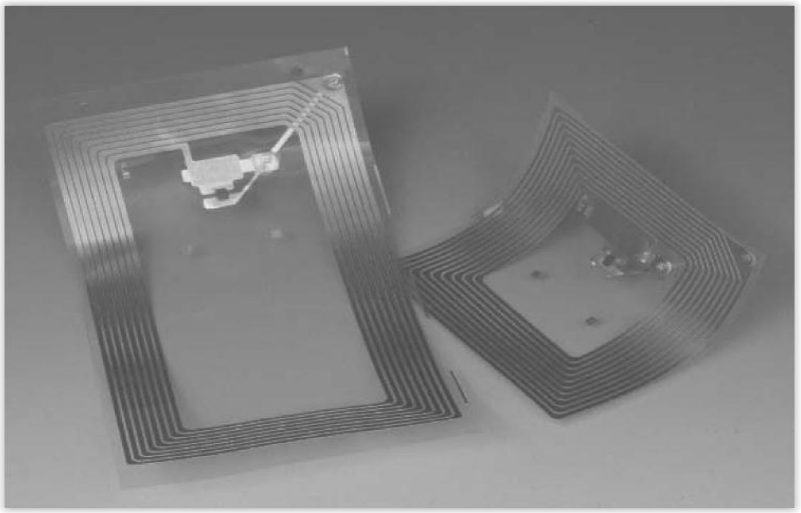

Figura 12 - Uma etiqueta inteligente consiste principalmente em um papel fino ou folha de plástico sobre a qual a bobina do transponder e o chip do transponder pode ser colocados. [1]

1.1.2.9 – Bobina no chip

Nos formatos de construção anteriormente citados os transponders consistem em um bobina de transponder que funciona como uma antena e um chip de transponder separados (tecnologia híbrida). A bobina de transponder está ligada ao chip de transponder de maneira convencional. Um passo óbvio o caminho da miniaturização é a integração da bobina no chip (bobina-on-chip). Isto é possível graças a um processo microgalvanico especial que pode ocorrer em uma pastilha de CMOS normal. A bobina é colocada diretamente num isolador do chip de silício sob a forma de um plano (camada única) em um arranjo espiral e em contacto com o circuito a seguir por meio de aberturas convencionais na passivação camada de passivação. As larguras de faixa do condutor alcançadas estão compreendidas no intervalo de 5-10µm com uma espessura de camada de 15-30µm. A passivação final em uma base de poliamida é realizada para garantir a capacidade de carga mecânica do módulo de contato de memória com base em tecnologia de bobina-on-chip. [1]

O tamanho da pastilha de silício, e,assim, praticamente todo o transponder, têm apenas 3 mm x 3 mm. Estes transponders são frequentemente incorporados a um reservatório de plástico de conveniência de aproximadamente 6 mm x 1,5 mm e estão entre os menores transponders RFID disponíveis no mercado. [1]

A seguir, figura 13, exemplos de transponder em miniatura usando a tecnologia da bobina no chip.

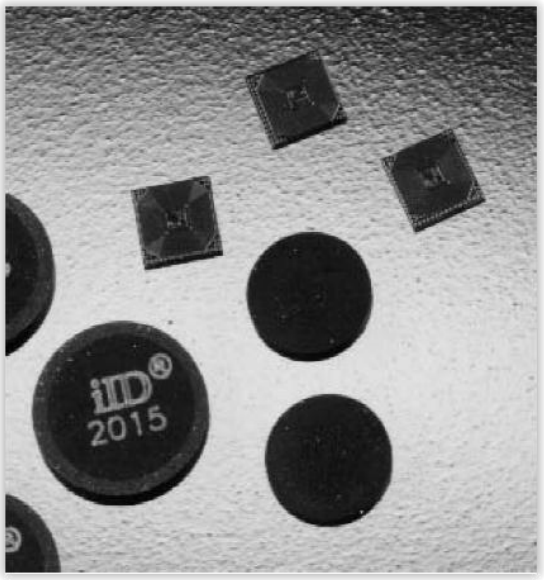

Figura 13 - Miniaturização extrema de transponders é possível usando a tecnologia de bobina-on-chip [1]

1.1.2.10 – Outros formatos

Além desses projetos principais, vários outros projetos especiais específicos de aplicação são também fabricados. Exemplos disso são o 'columbofilia transponder' ou o

'chip de campeão' para o sincronismo de esportes. Os transponders podem ser incorporados em qualquer desenho exigido pelo cliente. As opções preferidas são o de vidro ou de PP transponders, que são transformados ainda mais para obter a forma final.

1.1.3 – Frequência, alcance e acoplamento

Os critérios de diferenciação mais importantes para os sistemas RFID são a freqüência de operação do leitor, o método de acoplamento físico e o alcance do sistema. Sistemas RFID são operados em frequências muito diferentes, que vão desde 135 kHz em ondas longas até 5,8 GHz no intervalo de microondas. Os campos elétricos, magnéticos e eletromagnéticos são utilizado para o acoplamento físico. Finalmente, o alcance possível do sistema varia entre alguns milímetros para acima de 15 m. [1]

Sistemas RFID com alcance muito pequeno, tipicamente na distância de até 1 cm, são conhecidos como sistemas de acoplamento próximo. Para o funcionamento do transponder ou deve ser inserido no leitor ou posicionado sobre uma superfície prevista para o efeito. Sistemas de acoplamento próximo são acoplados usando ambos campos elétricos e magnéticos e pode ser teoricamente operados em qualquer frequência desejada entre DC e 30 MHz porque a operação do transponder não conta com a radiação de campos. A estreita ligação entre suporte de dados e leitor também facilita a disponibilização de maiores quantidades de potência e por isso mesmo um microprocessador com o consumo de energia não-ótima, por exemplo, pode ser operado. Sistemas de acoplamento próximo são usados principalmente em aplicações que estão sujeitas a requisitos de segurança rigorosos, mas não exigem um grande intervalo de frequência. Exemplos são eletrônicos de sistemas de fechamento de portas ou sistemas de cartões inteligentes sem contato com funções de pagamento. Transponders de sistemas de acoplamento próximo são atualmente utilizados exclusivamente no formato ID-1 cartões inteligentes sem contato (ISO 10536). No entanto, o papel de sistemas de acoplamento próximo no mercado têm se tornado cada vez menos importante. [1]

Sistemas com capacidade de escrever e ler que atigem alcance de operação de ate 1m são conhecidos como sistemas de acoplamento remoto(na vizinhança). Quase todos os sistemas acoplados remotamente baseiam-se num acoplamento indutivo (magnético) entre o leitor e o transponder. Por conseguinte, estes sistemas são também connhecidos como sistemas de rádio indutivo. Além disso, há também alguns sistemas com acoplamento capacitivo (elétrico). Pelo menos 90% de todos os sistemas RFID vendidos atualmente são indutivamente acoplados. Por esta razão, há agora um enorme número de tais sistemas no mercado. Há também uma série de padrões que especificam os parâmetros técnicos de transponders e leitores para vários tipos de aplicação, tais como cartões inteligentes de uso

sem contato, identificação de animais ou automação industrial. Estes sistemas incluem também acoplamento próximo (ISO 14443, cartões inteligentes de uso sem contato) e sistemas de acoplamento na vizinhança (ISO 15693, etiquetas inteligentes e cartões inteligentes sem contato). Frequências abaixo de 135 kHz ou 13,56 MHz são usadas como frequências de transmissão. Em algumas aplicações especiais (por exemplo, Eurobalise) também são usados frequências de operação no intervalo de 27 a 125 MHz. [1]

Os sistemas RFID com alcances significativamente maiores que 1m são conhecidos como sistemas de longo alcance. Todos os sistemas de longo alcance funcionam utilizando ondas eletromagnéticas na faixa de UHF e na faixa de microondas. A grande maioria desses sistemas são também conhecidos como sistemas de retrodispersão devido ao seu princípio físico de funcionamento. Além disso, há também sistemas de longa distância que utilizam ondas acústicas da superfície do transponders na faixa de micro-ondas. Todos esses sistemas são operados nas freqüências UHF de 868MHz (Europa) e 915MHz (EUA) e nas freqüências de microondas de 2,5 GHz e 5,8 GHz respctivamente. Valores típicos de até 3m podem ser conseguidos usando transponders passivos de retroespalhamento (sem bateria), enquanto que alcances de operação acima de 15m podem ser conseguidos usando transponders ativos do tipo backscatter (apoiada por bateria). A bateria de um transponder ativo não fornece a energia necessária para a transmissão de dados entre o transponder e o leitor, porém serve exclusivamente para abastecer o microchip e para a retenção de dados armazenados. A energia do campo eletromagnético recebido pelo transponder vindo do leitor é a única energia usada para a transmissão de dados entre transponder e leitor. [1]

A fim de evitar a referência equivocada aos intervalos de operação, este trabalho usa para classificação dos sistemas apenas termos como indutivamente acoplado ou capacitivamente acoplado e também a expressão sistema de microondas ou sistema *backscatter*. [1]

1.1.4 – Processamento de Informação no Transponder

Se classificarmos os sistemas RFID de acordo com a gama de informações e processamento de dados funções oferecidas pelo transponder e o tamanho da sua memória de dados, obtém-se um amplo espectro de variantes. Os extremos deste espectro são representados por sistemas de baixo (*low-end*) e alto nível (*high-end*).

1.1.4.1 Sistemas de baixa nível

Sistemas de EAS (sistemas de vigilância eletrônica de artigos) representam a extremidade inferior de sistemas *low-end*. Estes são sistemas de verificar e monitorar a possível presença de um transponder na zona de interrogação de um leitor de unidade de detecção usando simples efeitos físicos. [1]

Transponders de somente leitura com um microchip também são classificados como sistemas *low-end*. Nestes transponders temos um conjunto de dados codificados de forma permanente, que geralmente consiste apenas de um número de série único (número exclusivo) composto de vários bytes. Se um só Transponders de somente leitura é colocado

no campo de HF de um leitor, o *transponder* começa a continuamente transmitir seu próprio número de série. Não é possível que o leitor se comunique com apenas um transponder de somente leitura - há um fluxo unidireccional de dados do transponder para o leitor. Na pratica, para o funcionamento adequado de um sistema de somente leitura, é necessário assegurar que exista apenas um transponder na zona de interrogação do leitor, caso contrário, os outros transponders presentes nesta zona transmitirão simultaneamente, o que levará a uma colisão de dados. Sendo assim o leitor não seria mais capaz de detectar o transponder. Apesar desta limitação, transponders de somente leitura são bastante adequados para muitas aplicações em que é suficiente a leitura de um único número. Por causa da função simples de um transponder de somente leitura, a área do chip pode ser minimizada, conseguindo-se assim um consumo de energia baixo e um baixo custo de fabricação. [1]

Sistemas de somente leitura são operados em todas as frequências disponíveis para sistemas RFID. A gama de frequência realizável é geralmente muito alta, graças ao baixo consumo de energia do microchip. Sistemas de somente leitura são utilizados quando apenas uma pequena quantidade de dados é necessária ou onde este sistema pode substituir a funcionalidade dos sistemas de código de barras, por exemplo no controle de fluxo de produto, na identificação de paletes, recipientes e garrafas de gás (ISO 18000), mas também pode ser usados na identificação de animais (ISO 11785). [1]

1.1.4.2 Sistemas de médio nível

O nível médio é ocupado por uma variedade de sistemas com memória de dados gravaveis, que significa que esta classe de sistemas tem de longe a maior diversidade de tipos. Os tamanhos das memórias variam de alguns bytes a mais de 100 Kbyte EEPROM (transponder passivo) ou SRAM (transponders ativos, isto é transponder com backup de bateria). Estes transponders são capazes de processar simples comandos de leitor para uma leitura seletiva e escrita de dados na memória em uma permanente máquina de estado codificada. Em geral, estes transponders suportam procedimentos anti-colisão, de modo que vários transponders localizados na zona de interrogação do leitor respondam ao mesmo tempo sem interfir umas nas outras e permitindo também que os transponders possam ser abordados de forma seletiva pelo leitor. [1]

Procedimentos criptológicos de autenticação, entre transponder e leitor, ou seja, criptografia de fluxo de dados também são comuns nesses sistemas. Estes sistemas são operados em todas as frequências disponíveis para sistemas RFID. [1]

1.1.4.3 Sistemas de Alto nível (de ponta)

A classe sistemas de ponta é composta de sistemas com um microprocessador e um sistema operacional de cartão inteligente (OS smart card). O uso de microprocessadores facilita a realização de criptografias significativamente mais complexas e algoritmos de autenticação que seriam possíveis, utilizando a lógica por *hardware* de uma máquina de estado. A extremidade superior de sistemas de ponta é ocupada por cartões inteligentes de moderna interface dupla, que têm um co-processador criptográfico. A enorme redução do tempo de processamento que resulta da utilização de um co-processador permite que os

cartões inteligentes sem contato possam ser usados em aplicações que impõem exigências elevadas de criptografia para uma transmissão de dados mais segura, tais como sistemas de bolsa ou de emissão de bilhetes eletrônicos para os transportes públicos. Sistemas alto nível são quase exclusivamente operados na freqüência 13,56MHz. O padrão de transmissão de dados entre transponder e leitor está descrito na norma ISO 14443. [1]

1.1.5 - Critérios de seleção para Sistemas RFID

Tem havido um enorme aumento na popularidade de sistemas RFID nos últimos anos. O melhor exemplo desse fenômeno são os cartões inteligentes sem contato usados como bilhetes eletrônicos para transportes públicos. A poucos anos atrás, era inconcebível que dezenas de milhões de bilhetes sem contato estariam hoje sendo usados. Os possíveis campos de aplicação para sistemas de identificação sem contato também se multiplicaram recentemente. [1]

Os desenvolvedores de sistemas RFID têm tomado conta desta evolução, com isso, inúmeros sistemas estão atualmente disponíveis no mercado. Os parâmetros técnicos destes sistemas são otimisados para diversas áreas de aplicação - ticketing, identificação animal, automação industrial ou controle de acesso. Os requisitos técnicos destes campos de aplicação muitas vezes se sobrepõem, o que significa que a classificação precisa de sistemas de funcionamento adequado não é uma questão simples. Para tornar as coisas ainda mais difíceis existem alguns casos especiais (identificação animal, de acoplamento perto e cartões inteligentes). [1]

É difícil, mesmo para um especialista, manter uma visão geral da gama de sistemas RFID atualmente em oferta. Por isso, nem sempre é fácil para os usuários selecionar o melhor sistema adequado para suas necessidades. [1]

Na sequência são apresentados alguns pontos a se considerar ao selecionar um sistema RFID.

1.1.5.1 Frequência de operação

Os sistemas RFID que usam freqüências entre aproximadamente 100 kHz e 30 MHz operam utilizando acoplamento indutivo. Em contrapartida, os sistemas de microondas na faixa de freqüência de 2.45 a 5.8 GHz são acoplados usando campos eletromagnéticos. [1]

A taxa de absorção específica (amortecimento) para substâncias de água ou não condutoras é inferior por um fator de 100 000 para uma frequência de 100 kHz do que é para uma frequência de 1 GHz. Portanto, praticamente nenhuma absorção ou amortecimento ocorre. Sistemas HF de baixa frequência são principalmente usados por permitir a uma melhor penetração nos objetos. Um exemplo disto é a bólus, um transponder colocado no

omaso[2] do gado, que pode ser lido a de fora do animal, com uma frequência de interrogação maior do que 135 kHz. [1]

Sistemas de microondas apresentam um alcance significativamente maior do que os sistemas indutivos, tipicamente de 2 a 15m. No entanto, em contraste com sistemas indutivos, sistemas de microondas requer uma bateria de reserva adicional. A potência de transmissão do leitor é geralmente insuficiente para fornecer a energia necessária para o funcionamento do transponder. [1]

Outro fator importante é a sensibilidade aos campos de interferência eletromagnética, como os gerados por robôs de soldagem ou motores elétricos fortes. Transponders indutivos estão em desvantagem significativa nesse aspecto. Sistemas de microondas têm, portanto, se estabelecidos nas linhas de produção e em sistemas de pintura da indústria de automóvel. Outros fatores a se considerar de sistemas de microondas são a alta capacidade de memória (até 32 Kbyte) e a alta resistência à temperatura. [1]

1.1.5.2 – Alcance

O alcance necessário para cada aplicação dependente de vários fatores:

- a precisão do posicionamento do transponder;
- a distância mínima entre vários transponders em funcionamento real;
- a velocidade do transponder na zona de interrogação do leitor.

Por exemplo, nos pedidos de pagamento sem contato – como em bilhetes de transporte público – a velocidade de posicionamento é muito baixa, uma vez que o *transponder* é guiado para o leitor pela mão. A distância mínima entre os vários transponders, neste caso, corresponde a distância entre dois passageiros que entram num veículo. Para tais sistemas, há uma faixa ideal de 5-10 cm de alcance. Um alcance maior só iria dar origem a problemas nesta aplicação, uma vez que várias passagens dos passageiros iriam poder ser detectadas pelo leitor simultaneamente. Isso tornaria impossível alocar de forma confiável o bilhete para o passageiro correto. [1]

Modelos de veículos diferentes de dimensões variáveis são muitas vezes construídos simultaneamente nas linhas de produção de uma indústria automotiva. Assim, grandes variações na distância entre o transponder no veículo e o leitor são pré-programados. A distância de gravação/leitura do sistema RFID utilizado deve, portanto, ser concebida para o alcance máximo requerido. A distância entre os transponders deve ser tal

[2] Omaso: compartimento gástrico dos mamíferos ruminantes.

que apenas um transponder esteja na zona de interrogação do leitor de cada vez. Nesta situação, os sistemas de microondas, em que o campo tem a possibilidade de irradiação direcional apresenta uma grande vantagem sobre campos não direcionais de sistemas acoplados indutivamente. [1]

A seguir, figura 14, uma imagem de comporação das zonas de interrogação dos diferentes sistemas *RFID*, acoplamento indutivo, acoplamento eletomagnetico não direcional e acoplamento eletromagnetico direcional.

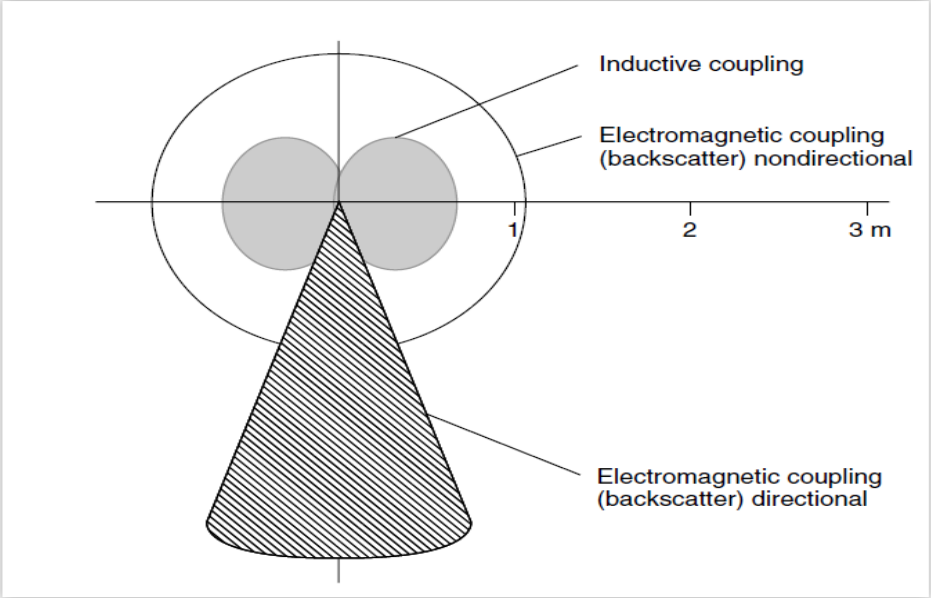

Figura 14 - Comparação das zonas de interrogação dos diferentes sistemas; de cima para baixo, acoplamento indutivo, acoplamento eletromagnético não direcional e acoplamento magnético direcional.

A velocidade do transponder, em relação ao leitor, em conjunto com a distância máxima de escrita/leitura, define o tempo de permanência na zona de interrogação do leitor. Para a identificação de veículos, o alcance requerido do sistema RFID é concebido de tal forma que a velocidade máxima do veículo e o tempo de permanência na zona de interrogação sejam suficientes para a transmissão dos dados necessários. [1]

1.1.5.3 Requisitos de segurança

Os requisitos de segurança a serem impostos a uma aplicação RFID planejada, isto é, a criptografia e a autenticação, deve ser avaliada de forma muito precisa para afastar quaisquer surpresas desagradáveis na fase de implementação. Para este objetivo, o incentivo que o sistema representa para um invasor em potencial como um meio de obter dinheiro ou bens materiais através de sua manipulação deve ser avaliado. A fim de ser capaz de avaliar este poder de atração, dividimos as aplicações em dois grupos: [1]

- aplicações industriais ou fechadas;
- aplicações públicas relacionadas com dinheiro e bens materiais.

Isto pode ser ilustrado com base em dois exemplos de contraste de aplicação.

Vamos mais uma vez considerar uma linha de montagem na indústria automotiva como um típico exemplo de uma aplicação industrial ou fechada. Somente pessoas autorizadas têm acesso a este sistema RFID, assim o círculo de potenciais atacantes permanece razoavelmente pequeno. Um ataque malicioso no sistema pela alteração ou falsificação dos dados em um transponder pode provocar um mau funcionamento crítico na sequência operacional, mas o invasor não ganharia qualquer benefício pessoal. A probabilidade de um ataque pode ser assim considerada zero, o que significa que mesmo um sistema baixo nível (*low-end*) barato sem lógica de segurança pode ser usado. [1]

Nosso segundo exemplo é um sistema de bilhete para uso em transportes públicos. Em tal sistema, o suporte de dados é feito principalmente na forma de cartões inteligentes sem contato, acessíveis a qualquer pessoa. O círculo de potenciais atacantes é assim enorme. Um ataque bem sucedido em tal sistema poderia representar um prejuízo financeiro em larga escala para a empresa de transportes públicos em questão, por exemplo, no caso de venda organizada de passagens de viagens falsificadas, para não falar nos danos à imagem da empresa. Para essas aplicações um transponder de alto nível (*high-end*) com procedimentos de autenticação e criptografia é indispensável. Para aplicações com requisitos de segurança máxima, tais como em aplicações bancarias com um porta-moedas eletrônico, deve ser usado apenas transponders com microprocessadores. [1]

1.1.5.4 Capacidade de memória

O tamanho do chip do portador de dados - e, assim, a classe de preços - é definida principalmente pela sua capacidade de memória. Portanto, suportes de dados de somente leitura codificados permanentemente são utilizados em aplicações de massa sensíveis ao preço com um baixo requisito de informação local. No entanto, apenas a identidade do objeto pode ser definida usando este tipo de suporte de dados. Além disso os dados são armazenados na base de dados de uma central de computador de controle. Se houver dados a

serem escritos de volta no transponder, um transponder com EEPROM ou memória RAM será necessário. [1]

Memórias EEPROM são encontradas principalmente em sistemas indutivamente acoplados. Memórias de capacidade que vão de 16 bytes a 8 kbytes estão disponíveis no mercado. [1]

Dispositivos de memória SRAM com uma bateria de reserva, por outro lado, são predominantemente utilizados em sistemas de microondas. As capacidades de memória oferecidas no mercado variam de 256 bytes a 64 kbytes. [1]

1.1.6 Princípios fundamentais de operação

Este tópico descreve a interação básica entre transponder e leitor, em particular o fornecimento de energia para o transponder e a transferência de dados entre o transponder e o leitor.

1.1.6.1 1-Bit Transponder

Um bit é a menor unidade de informação que pode ser representado e tem apenas dois estados: 1 e 0. Isto significa que apenas dois estados podem ser representados através de sistemas baseados em 1-bit transponder: 'transponder na zona de interrogação "e" não transponder na zona de interrogação'. Apesar desta limitação, os transponders de 1-bit são muito difundidos no mercado – seu principal campo de aplicação é em dispositivos anti-roubo em lojas de eletrônicos (EAS, eletrônico vigilância artigo). [1]

Um sistema EAS é composto dos seguintes componentes: a antena de um "leitor" ou interrogador, o elemento de segurança ou etiquetas, e um dispositivo opcional de desativação para desativar a etiqueta após o pagamento. Em sistemas modernos a desativação ocorre quando o código de preço é registrado no caixa registrador. Alguns sistemas também incorporam um ativador, que é usado para reativar o elemento de segurança após a desativação. A principal característica de desempenho de todos os sistemas é a taxa de reconhecimento ou de detecção em relação à largura do portal (distância máxima entre transponder e a antena do interrogador). [1]

O procedimento para a inspeção e teste de sistemas instalados de vigilância de artigos é especificado na diretriz *VDI 4470*, intitulada "Sistema Anti-roubo de mercadorias - portas de detecção. Diretrizes de inspeção para os clientes". Esta diretriz contém definições e procedimentos de teste para o cálculo da taxa de detecção e taxa falsa de alarme. Ele pode ser usado pelo comércio varejista como base para contratos de venda ou para monitorar o desempenho dos sistemas instalados em uma base contínua. Para o fabricante do produto, as regras de controle de clientes representa uma eficaz referência no desenvolvimento e otimização de soluções integradas para projetos de segurança. [1]

A seguir, figura 15, diagrama dos diferentes princípios de funcionamento dos sistemas RFID.

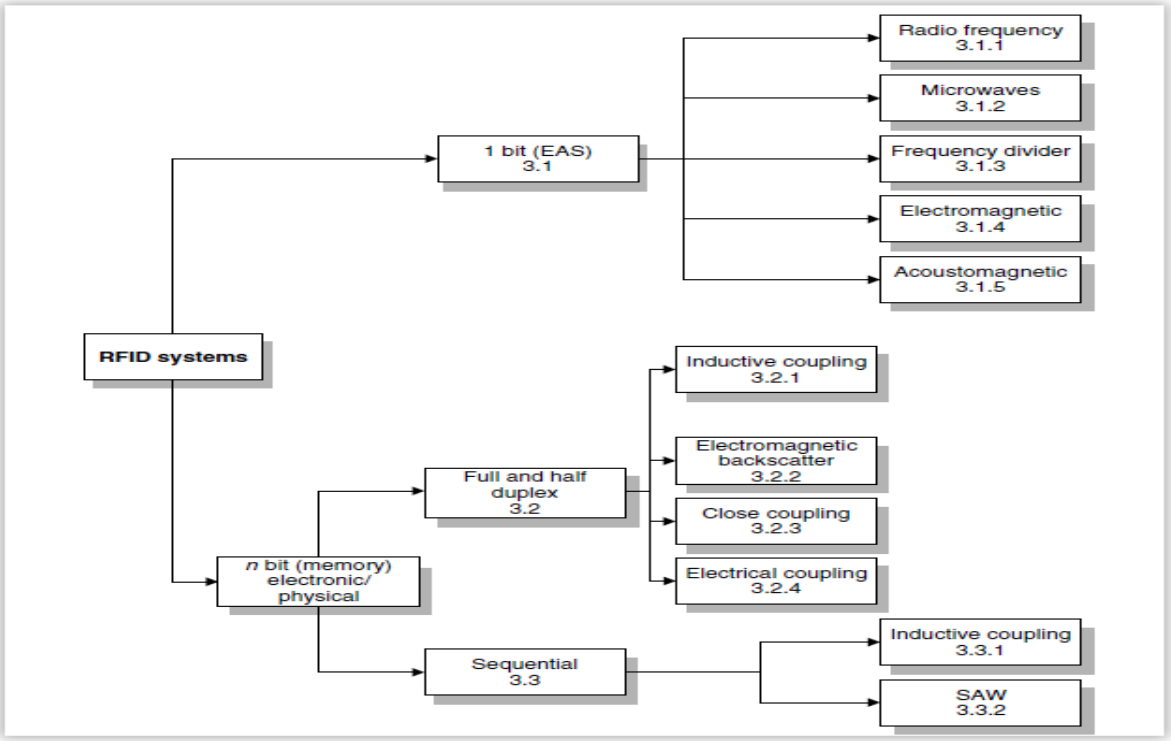

Figura 15 - A distribuição dos diferentes princípios de funcionamento de sistemas RFID [1]

1.1.6.1.1 Frequência de rádio

O processo de radiofrequência (RF) é baseado em circuitos ressonantes LC, ajustados a uma freqüência de ressonância definida fR. As primeiras versões empregava resistências indutivas feitas de lascas esmaltadas de fio de cobre soldados a capacitor em uma caixa de plástico (tag duro). Os sistemas modernos empregam bobinas gravadas entre folhas em forma de autocolantes. Para garantir que a resistência de amortecimento não se torne demasiado grande e assim reduzir a qualidade do circuito ressonante para um nível inaceitável, a espessura dos caminhos de alumínio para condução presentes sobre a lâmina de polietileno de espessura de 25 µm devem ter pelo menos 50 µm. Lâminas intermediarias de espessura de 10 µm são usadas para fabricar as placas do capacitor. [1]

O leitor (detector) gera um campo magnético alternado na faixa de rádio freqüência. Se o circuito ressonante LC for deslocado para a vizinhança do campo magnético alternado, uma energia alternada pode ser induzida no circuito ressonante, a partir desse campo, através das suas bobinas (Lei de Faraday). Se a frequência *f*G do campo alternado corresponder à frequência de ressonância *f*R do circuito ressonante LC isso produzirá uma oscilação simpática. A corrente que circula no circuito ressonante, como resultado de uma ação contra a sua causa, ou seja, ela age contra o campo magnético alternado externo. Este efeito é perceptível como uma pequena variação na tensão do

gerador ligado à bobina do transmissor a qual cai a um valor abaixo do valor medido antes do efeito e, finalmente, leva a um enfraquecimento da intensidade do campo magnético mensurável. Uma alteração na tensão induzida pode ser igualmente detectada numa bobina de sensor opcional, logo que um circuito oscilante ressonante é trazido para o campo magnético da bobina do gerador. [1]

A magnitude relativa desta imersão é dependente da diferença entre as duas bobinas (bobina de gerador - elemento de segurança, elemento de segurança - bobina sensor) e a qualidade Q do circuito ressonante induzida (no elemento de segurança). [1]

A magnitude relativa das mudanças na tensão no gerador e sensor de bobinas é geralmente muito baixa e, portanto, difíceis de detectar. No entanto, o sinal deve ser tão claro quanto possível, de modo que o elemento de segurança pode ser detectado de forma confiável. Isto é conseguido usando um pouco de um truque: a frequência do campo magnético gerado não é constante, essa é "varrida". Isto significa que a frequência do gerador atravessa continuamente o intervalo entre mínima e máxima. A faixa de frequência disponível para os sistemas varrerem é 8.2 MHz ± 10%. [1]

Sempre que a freqüência do gerador varrida corresponder exatamente à freqüência de ressonância do circuito ressonante (no transponder), o transponder começa a oscilar, produzindo uma nítida diminuição das tensões no gerador e no sensor de bobinas. Tolerâncias freqüência do elemento de segurança, que dependem da tolerância de fabricação, variam na presença de um ambiente metálico, ou seja, não apresentam o mesmo desempenho quando do "varrimento" de toda a gama de frequências. [1]

Porque as etiquetas não são removidas no caixa registrador, elas devem ser alteradas de modo a que não façam a ativação do sistema anti-roubo. Para conseguir isso, o caixa coloca o produto protegido num dispositivo - o desativador - que gera um campo magnético suficientemente elevado para que a tensão induzida destrua a placa do capacitor do transponder. Os capacitores são concebidos com intencionais pontos de curto-circuito, chamados de ondulações. O dano causado no capacitor é irreversível e dessintoniza o circuito ressonante a um grau tal que este pode deixar de ser acionado com o sinal de varredura. [1]

Grandes áreas de antenas em forma de moldura são utilizadas para gerar o necessário campo magnético alternado que atuará na área de detecção. As antenas em forma de moldura são integradas em colunas e combinadas de modo a formar um portal. O design clássico comumente visto em grandes departamentos de loja está ilustrado na Figura 19. Portais de larguras de até 2 m podem ser conseguidos utilizando o procedimento RF. A taxa de detecção relativamente baixa de 70% é influenciada por certos materiais do produto. Metais em particular (por exemplo, latas de alimentos) afetam a frequência de ressonância das etiquetas e o acoplamento com a bobina e, assim, tem um efeito negativo sobre a taxa de detecção do detector. Etiquetas de 50 milímetros × 50 milímetros devem ser usadas para obter a largura do portal e a taxa de detecção mencionados acima. [1]

A seguir, figura 16, um exemplo de leitor do tipo moldura. E , na figura 17, um diagrama mostrando o princípio de funcionamento de um sistema de rádiofrequência EAS.

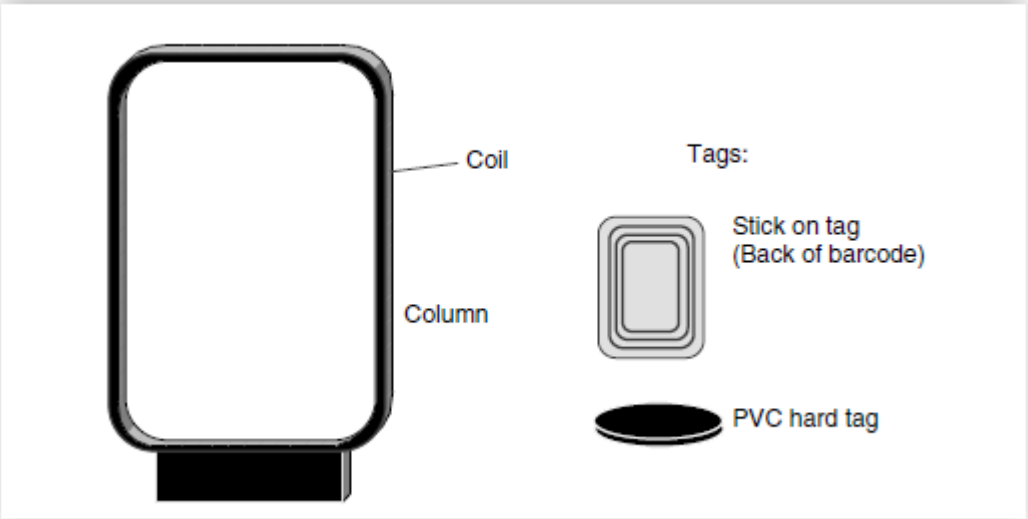

Figura 16 – À esquerda, típica antena em forma de moldura de um sistema de RF (altura 1.20-1.60m); à direita, modelos de tags(etiqueta). [1]

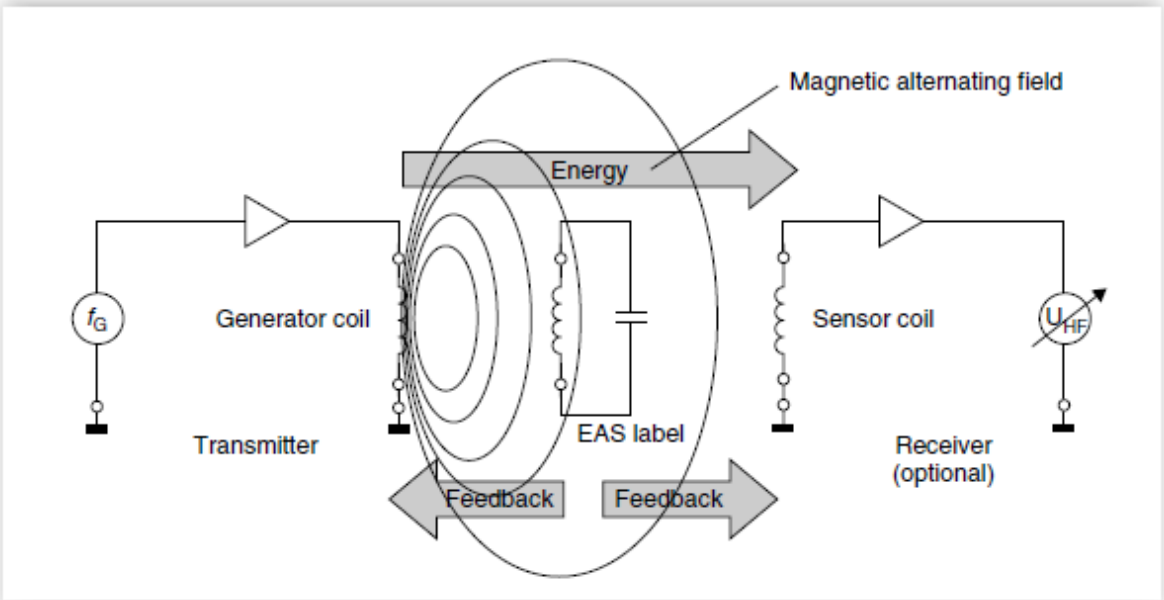

Figura 17 - Princípio de funcionamento de um sistema de radiofreqüência EAS. [1]

Tabela 2 - Os parâmetros típicos para um sistema de RF	
Fator de qualidade Q de um elemento de segurança	>60–80
Desativação mínima intensidade do campo H_D	1.5 A/m
Força máxima do campo no intervalo de desativação	0.9 A/m

A gama de produtos que têm as suas próprias frequências ressonantes, representa uma grande desafio para os fabricantes de sistemas. Se estas frequências ressonantes errarem 8.2 MHz na freqüência de varredura ± 10% eles sempre iram disparar falsos alarmes. [1]

TRANSFERÊNCIA NÃO RADIATIVA DE ENERGIA SEM FIO

EFICIÊNCIA DE TRANSFERÊNCIA MELHORADA

A energia não radiativa transferida sem fio mais simples ligações consiste de transferência de um par de antenas de quadro em estreita proximidade uns dos outros. Um fluxo magnético emanado da antena de transmissão de laço induz uma tensão no circuito de recepção, como previsto pelas leis de Ampère e Faraday. A eficiência de transferência com uma carga ótima é derivado da equação a seguir: [1]

$$\eta_{\text{opt}} = \frac{k^2 Q_t Q_r}{\left(1+\sqrt{1+k^2 Q_t Q_r}\right)^2}, \qquad (1)$$

onde k é o coeficiente de acoplamento entre as duas antenas, que é definido como

$$k = \frac{M}{\sqrt{L_t L_r}}, \qquad (2)$$

em que M é a indutância mútua entre as antenas loop emparelhadas. Os fatores Q da antena, Qt e Qr, são definidos como[10]

$$Q_{t,r} \approx \frac{\omega_{0_{t,r}} L_{t,r}}{R_{t,r}}, \quad (3)$$

Onde: Lt,r e Rt,r são a auto-indutância equivalente e os valores da resistência das antenas. A eficiência de transferência é assim depende de dois fatores-chave, o coeficiente de acoplamento e os Q-factores da antena, como mostrado na Figura 18. Os modelos têm, consequentemente, focado em aumentar os Q-fatores e os coeficientes de acoplamento para aumentar a eficiência de transferência de energia. [1] A seguir, figura 18, curva de eficiencia de um transmissão de energia sem fio.

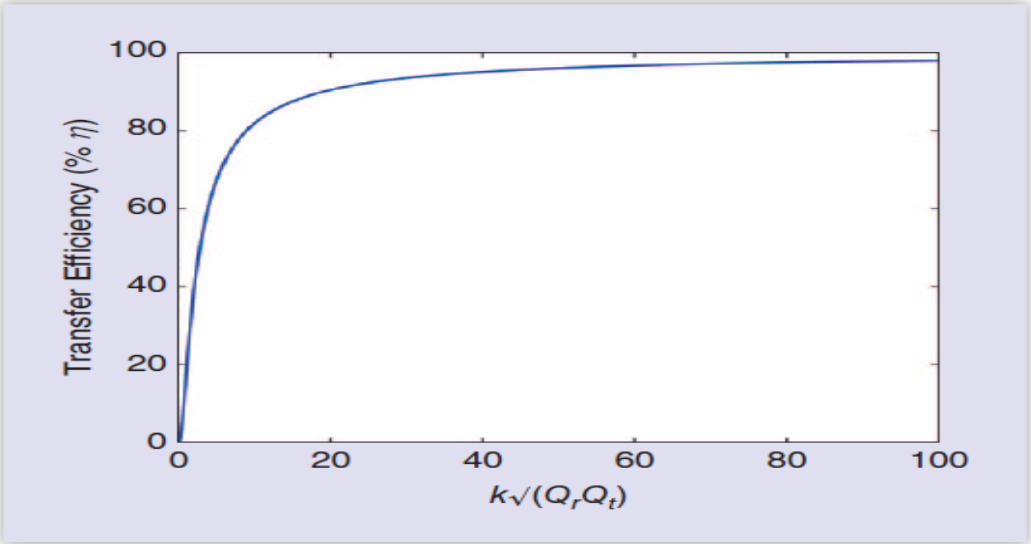

Figura 18 - O efeito do coeficiente de acoplamento e
dos Q fatores na eficiência de transferência de energia. [1]

1.1.6.1.2 Microondas

Sistemas EAS na faixa de microondas exploram a geração de harmônicos em componentes com curvas características não-lineares (por exemplo, díodos). A harmônica de uma tensão A senoidal com uma frequência definida *f*A é uma tensão B senoidal, cuja frequência *f*B é um múltiplo inteiro da frequência *f*A. Os harmônicos da freqüência *f*A são, portanto, as frequências 2 *f*A, 3 *f*A, 4 *f*A, etc. O N múltiplo da frequência de saída é

denominado o N harmônico (enésima onda harmônica) em engenharia de rádio; a própria frequência de saída é denominada a onda portadora ou primeira harmónico. [1]

Em princípio, cada rede de dois terminais com uma característica não-linear gera harmônicos a partir do primeira harmônico. No caso das resistências não lineares, no entanto, a energia é consumida, de modo que apenas uma pequena parte da potência do primeiro harmônico é convertida nas oscilações harmônicas. Sob condições favoráveis, a multiplicação de f por n, ou seja, $n \times f$ ocorre com uma eficiência de $\eta = 1 / n^2$. No entanto, se o armazenamento de energia não-linear é usado para multiplicação, então, no caso ideal já não existem perdas. [1]

Diodos de capacitância são reservas de energia não-lineares particularmente adequadas para a multiplicação de frequência. O número e a intensidade dos harmônicos que são gerados dependem da capacidade do diodo, perfil dopante e gradiente da curva característica. O expoente n (também γ) é uma medida para o gradiente (= curva característica de capacitância-tensão). Para diodos difusos simples, ele é de 0,33 (por exemplo, BA110), para diodos-ligados ele assume o valor de 0,5 e para diodo sintonizador com uma junção P-N hiper-abrupta ele é em torno de 0,75 (por exemplo, BB 141; ITT, 1975). [1]

A curva característica de capacitância-voltagem de diodos de capacitância ligados tem uma trajetória quadrática e é, portanto, mais adequado para a duplicação de frequências. Diodos difusos simples podem ser usados para produzir harmônicos mais altos. [1]

O esquema de um transponder de 1-bit para a geração de harmónicos é extremamente simples: um diodo de capacitância está ligado à base de um dipolo ajustado para a frequência da onda portadora (Figura 21). Dado uma frequência da onda portadora de 2,45 GHz, o dipolo tem um comprimento total de 6 cm. As frequências de onda portadora utilizadas são 915 MHz (fora da Europa), 2,45 GHz ou 5,6 GHz. Se o *transponder* está localizado dentro do alcance do transmissor, então o fluxo de corrente no díodo gera e emite novamente harmônicos da onda portadora. Particularmente sinais característicos são obtidos em duas ou três vezes a frequência da onda portadora, dependendo do tipo de díodo utilizado. [1]

Transponders deste tipo moldados em plástico (etiquetas rígidas) são usadas principalmente para proteger têxteis. As tags(etiquetas) são removidas no caixa registrador, quando as mercadorias são pagas, sendo posteriormente reutilizados. [1]

A Figura 22 mostra um transponder que está sendo colocado dentro do alcance de funcionamento de um transmissor de microondas transmitindo a 2,45 GHz. A segunda harmônica de 4,90 GHz gerado por causa da característica do diodo do transponder é retransmitida e detectada por um receptor, que é ajustado a esta frequência precisa. A recepção de um sinal na frequência da segunda harmônica pode então acionar um sistema de alarme. [1]

A seguir, figura 19, circuito básico e formato de etiqueta de microondas. E, na figura 20, imagem de funcionamento de um sistema usando por etiquetas de microondas.

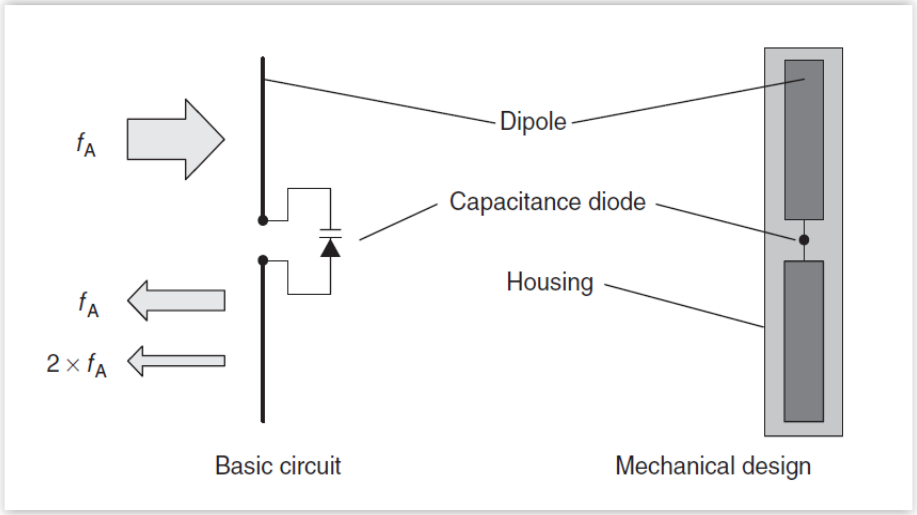

Figura 19 – À esquerda, circuito básico e à direita, típico formato de uma etiqueta de microondas[1]

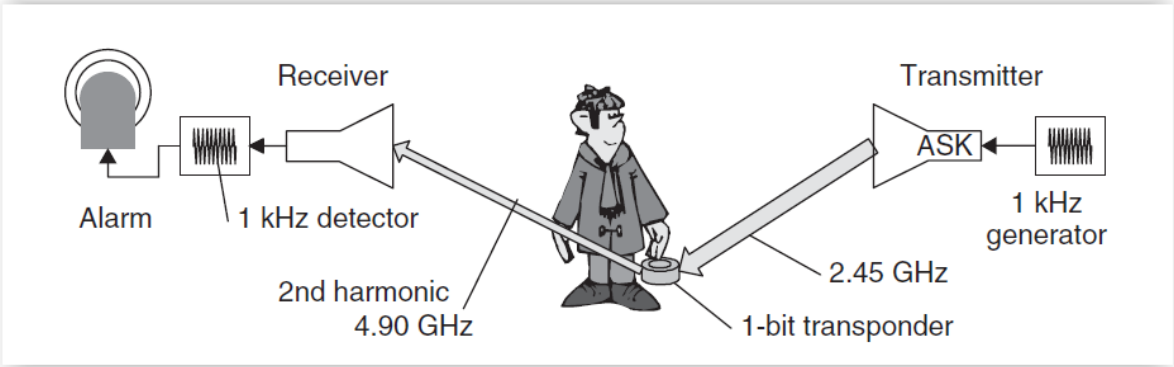

Figura 20 – Tag(etiqueta) de Microondas na zona de interrogação de um detector [1]

Se a amplitude ou a frequência da onda portadora é modulada (ASK, FSK), então todas as harmônicas incorporam a mesma modulação. Isso pode ser usado para distinguir entre "interferência" e sinais "úteis", evitando falsos alarmes provocados por sinais externos. No exemplo acima, a amplitude da onda portadora é modulada com um sinal de 1 kHz (100% ASK). O segundo harmônico gerado pelo transponder também é modulado em 1 kHz ASK. O sinal recebido no receptor é demodulado e encaminhado para um detector de 1 kHz. Sinais de interferência que venham a ser recebidos na freqüência de 4,90 GHz não podem acionar falsos alarmes, porque estes não são modulados normalmente e, se forem, eles terão uma modulação diferente. [1]

1.1.6.1.3 Divisor de frequência

Este processo opera na faixa de ondas longas em 100-135,5 kHz. As etiquetas de segurança contêm um circuito semicondutor (microchip) e um circuito ressonante feito de bobina de cobre esmaltado de feridas. Ao circuito ressonante é feito este entrar em ressonância com a frequência de funcionamento do sistema EAS usando um capacitor soldado. Estes transponders podem ser obtidos sob a forma de etiquetas rígidas (plástico) e são removidas dos produtos quando estes são adquiridos. [1]

A seguir, figura 21, diagrama do circuito básico do procedimento de divisão de frequência EAS.

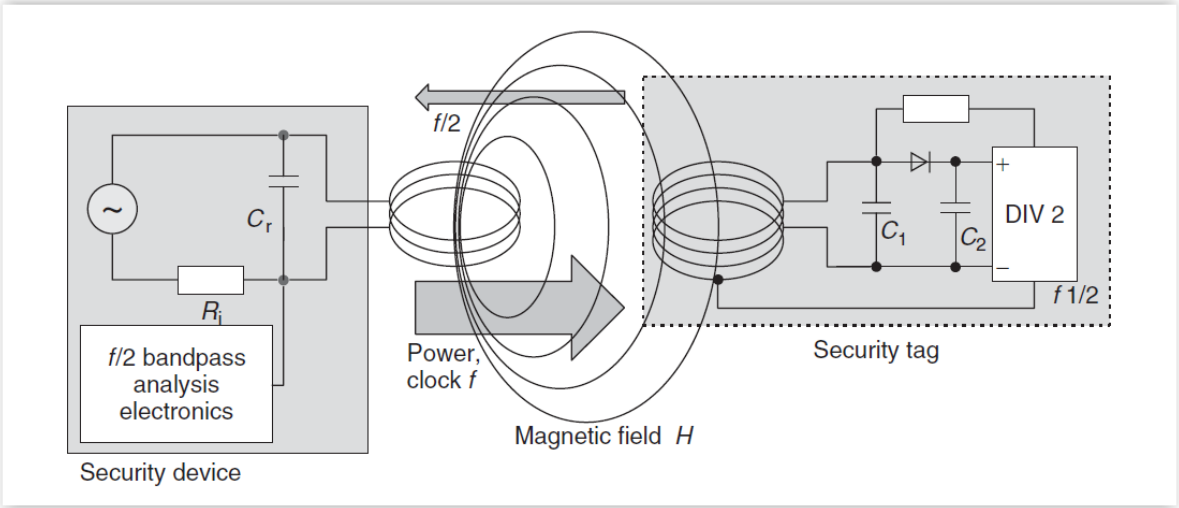

Figura 21 - Diagrama do circuito básico do procedimento de divisão de frequência EAS: tag de segurança (transponder) e detector (dispositivo de avaliação),da esquerda para a direita; análise eletrônica da banda passante *f*/2; dispositivo de segurança; potência, relógio f; campo magnético *H* e tag de segurança. [1]

Tabela 3 - Os parâmetros típicos do sistema	
Frequência	130 kHz
Tipo de modulação	100% ASK
Frequência de modulação/Sinal modulante	12.5 ou 25 Hz, retangular 50%

O microchip no transponder recebe a sua alimentação de energia a partir do campo magnético do dispositivo de segurança. A freqüência na bobina auto-indutiva é dividida por dois no microchip e enviada de volta para o dispositivo de segurança. O sinal com metade da frequência original é alimentado por uma fonte na bobina do circuito ressonante. [1]

O campo magnético do dispositivo de segurança é pulsado a uma frequência mais baixa (ASK modulado) para melhorar a taxa de detecção. De modo semelhante ao procedimento para a geração de harmônicos, as modulações da onda portadora (ASK ou

FSK) são mantidas à metade da frequência (subharmonica). Este artifício é usado para diferenciar entre os sinais 'úteis' e os sinais de interferência. Este sistema exclui quase inteiramente os falsos alarmes. [1]

Antenas de quadro, semelhantes aos conhecidos sistemas de RF, são utilizadas como antenas de sensores.

1.1.6.1.4 Tipos eletromagnéticos

Tipos eletromagnéticos operam utilizando campos magnéticos fortes na faixa NF de 10 Hz a cerca de 20 kHz. Os elementos de segurança contém uma tira de metal amorfo suave magneticamente com uma curva de histerese abrupta-ladeada. A magnetização destas tiras é invertida periodicamente e as tiras são tomadas por uma saturação magnética através de um campo magnético alternado forte. A marcante relação não linear entre a força do campo aplicado H e a densidade de fluxo magnético B perto da saturação, mais a variação súbita da densidade de fluxo B na vizinhança do cruzamento pelo zero do forte campo aplicado H, gera harmônicos na freqüência básica do dispositivo de segurança, estes harmônicos podem ser recebidos e avaliados pelo dispositivo de segurança. [1]

O tipo eletromagnético é otimizado pela sobreposição de trechos de sinais adicionais com freqüências maiores, acima do sinal principal. A não-linearidade acentuada da curva de histerese das tiras geram não apenas harmônicos, mas também partes do sinal com a soma e a diferença das freqüências dos sinais fornecidos. Dado um sinal principal de frequência fS = 20 Hz e os sinais adicionais com frequências f1 = 3,5 e f2 = 5,3 kHz, os seguintes sinais são gerados (primeira ordem): [1]

$$f_1 + f_2 = f_{1+2} = 8.80 \text{ kHz} \quad (1)$$

$$f_1 - f_2 = f_{1-2} = 1.80 \text{ kH} \quad (2)$$

$$f_S + f_1 = f_{S+1} = 3.52 \text{ kHz} \quad (3)$$

e assim por diante

Neste caso, o dispositivo de segurança não reage com a harmônica da frequência de base, mas sim com a frequência da soma ou da diferença dos sinais extras.

As etiquetas estão disponíveis sob a forma de tiras auto-adesivas com comprimentos que variam desde alguns centímetros até 20 centímetros. Devido à frequência de funcionamento ser extremamente baixo, sistemas eletromagnéticos são os únicos sistemas adequados para produtos que contenham metal. No entanto, estes sistemas têm a

desvantagem de que a função das tags(etiquetas) depende de sua posição: para uma detecção confiável as linhas do campo magnético do dispositivo de segurança devem passar verticalmente através da tira de metal amorfo. [1]

Para a desativação, as etiquetas são revestidas com uma camada de metal magnético duro ou parcialmente coberta por placas magnéticas duras. No caixa registrador, o operador passa um forte ímã permanente ao longo da tira de metal para desativar os elementos de segurança. Este magnetizado é uma placa dura de metal magnético. As tiras de metal são concebidas de tal modo que a intensidade do campo remanência da placa seja suficiente para manter as tiras metálicas amorfas em ponto de saturação para que o campo magnético alternado do sistema de segurança não possa ser ativado. [1]

A seguir, figura 22, formato típico de antena para um sistema de segurança.

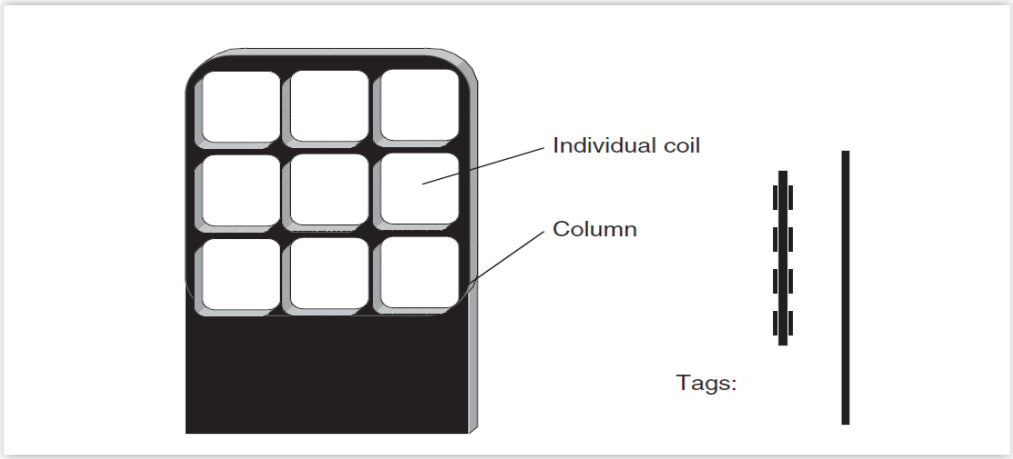

Figura 22 - Esquerda, formato típico de antena para um sistema de segurança (altura de aproximadamente 1,40 m); direita, possível formato de tags. [1]

As tags podem ser reativadas a qualquer momento por desmagnetização. O processo de desativação e reativação pode ser realizado por enumeras vezes. Por esta razão, a proteção de bens em sistemas eletromagnéticos foi originalmente usada, principalmente, em bibliotecas de emprestimo. Uma vez que as etiquetas são pequenas (mínimo, tiras de 32mm) e baratas, estes sistemas estão atualmente sendo cada vez mais utilizados no setor de mercearia. [1]

A fim de conseguir a força necessária para o campo de desmagnetização das tiras de permalloy, o campo é gerado por sistemas de duas bobinas em colunas em cada lado de uma passagem estreita. Várias bobinas individuais, tipicamente 9 a 12, estão localizadas nos dois pilares, e estes geram um campo magnético fraco no centro e campos magnéticos mais fortes na parte externa. Larguras de portal de até 1,50 m podem atualmente serem realizadas utilizando este método, enquanto ainda alcançar taxas de deteção de 70%. [1]

A seguir, figura 23, imagem de uso de etiquetas eletromagnéticas.

Figura 23 - Etiquetas eletromagnéticas em uso. [1]

Na figura 24, um tipo de leitor para sistemas de vigilância. E na figura 25, um esquema mostrando um sistema magnético acústico.

Figura 24 - Formato prático de uma antena para um sistema de vigilância de artigos. [1]

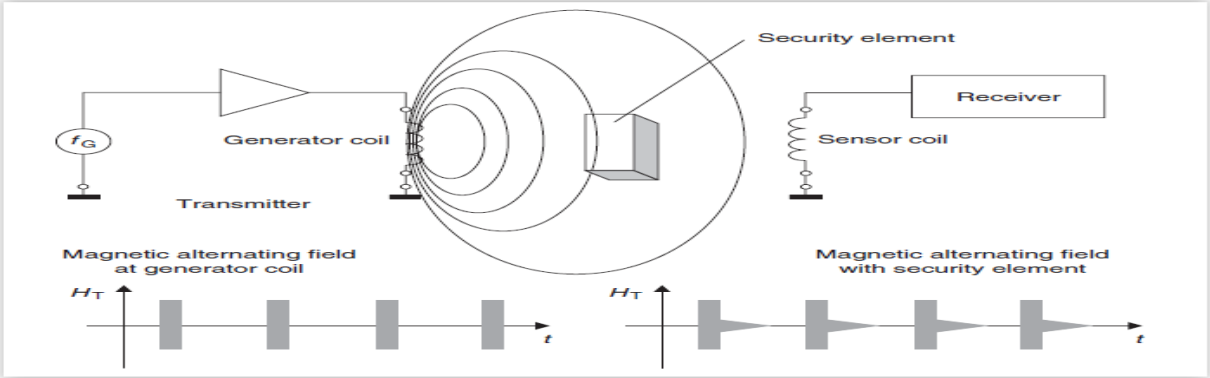

Figura 25 - Sistema magnético acústico compreendendo transmissor e dispositivo de detecção (receptor). Se um elemento de segurança está dentro do campo da bobina do gerador este oscila como um diapasão no tempo com os impulsos da bobina do gerador. As características transitórias podem ser detectadas por uma unidade de análise [1]

Tabela 4 - Parâmetros típicos do sistema	
Frequência	70 Hz
Combinação opicional de frequências de sistemas diferentes	12 Hz, 215 Hz, 3.3 kHz, 5 kHz
Força de campo Heff na zona de detecção	25–120 A/m
Intensidade mínima de campo para desativação	16 000 A/m

1.1.6.1.5 Acustomagnéticos

Elementos de segurança para sistemas acustomagnéticos consistem em caixas de plástico extremamente pequenas em torno de 40 milímetros de comprimento, 8-14mm de largura, dependendo do formato, e apenas 1 mm de altura. As caixas contêm duas tiras de metal, uma tira de metal duro magnétizado permanentemente conectado à caixa de plástico, além de uma tira feita de metal amorfo, posicionado de tal modo que fique livre para vibrar mecanicamente. [1]

Metais ferromagnéticos (níquel, ferro etc.) alteram ligeiramente seus comprimentos quando submetidos a um campo magnético sob a influência da força do campo H. Este efeito é chamado magnetoestricção e resulta de uma pequena mudança na distância interatômica como consequência da magnetização. Em um campo magnético alternado uma tira de metal magnetostritivo vibra em sua direcção longitudinal na frequência do campo. A amplitude da vibração da tira metalica torna-se especialmente elevada, se a frequência do campo magnético alternado corresponder à (acústico) frequência de ressonância desta tira de metal. Este efeito é particularmente marcante em materiais amorfos. [1]

O fator decisivo neste fenômeno é que o efeito magnetoestritivo é reversível. Isto significa que uma tira de metal magnetoestrictivo oscilante emite um campo magnético alternado. Sistemas de segurança acustomagnéticos são concebidos de tal modo que a frequência do campo magnético alternado gerado coincide precisamente com as frequências

de ressonância das tiras de metal do elemento de segurança. A tira de metal amorfo começa a oscilar sob a influência do campo magnético. Se o campo magnético alternado é desligado depois de algum tempo, a tira magnética excitada continua a oscilar por um tempo, como um diapasão, e desse modo, gera um campo magnético alternado, que pode ser facilmente detectado pelo sistema de segurança. [1]

A grande vantagem deste modo de atuação é que o sistema de segurança não está transmitindo enquanto o elemento de segurança está respondendo, assim a detecção do receptor pode ser concebida com um grau de sensibilidade apropriado. [1]

Tabela 5 – Parâmetros típicos de funcionamento de sistemas acustomagnéticos	
PARÂMETROS	VALORES TÍPICOS
Frequência de ressonância *f*0	58 kHz
Tolerância de frequência	±0.52%
Fator de qualidade *Q*	>150
Intensidade minima do campo *H*A para ativação	>16 000 A/m
Duração do campo ligado	2ms
Pausa do campo (duração do campo desligado)	20 ms
Processo de decaimento do elemento de segurança	5 ms

Em seu estado ativado, elementos de segurança acustomagnéticos estão magnetizados, ou seja, a tira de metal magnético rígido, citada anteriormente, tem uma força de campo remanence elevada e, portanto, forma um ímã permanente. Para desactivar o elemento de segurança a tira de metal magnético rígido deve ser desmagnetizada. Este dessintoniza a frequência de ressonância da tira de metal amorfo para que, assim, ele não possa mais ser excitado com a freqüência de operação do sistema de segurança. A tira metal magnético duro só pode ser desmagnetizada por um campo magnético alternado forte com uma força de campo lentamente decadente. É assim absolutamente impossível que o elemento de segurança seja manipulado por um ímã permanente trazido para dentro da loja pelos clientes. [1]

1.1.6.2 Modo de comunicação *Full* e *Half-Duplex*

Em contraste com os transponders de 1 bit, que exploram normalmente efeitos físicos simples (métodos de estimulação e oscilação, processo de estimulação de harmónicos pela característica não-linear de díodos ou a curva de histerese não linear dos metais), os

transponders descritos neste e em tópicos subsequentes usam um microchip eletrônico como dispositivo que carrega os dados. Este microchip tem uma capacidade de armazenamento dados de um entre alguns bytes e mais de 100 kilobytes. Para ler ou escrever no dispositivo que transporta os dados deve ser possível transferir dados entre o leitor e o transponder e, em seguida, de volta a partir do transponder para o leitor. Essa transferência ocorre de acordo com um dos dois principais modos de comunicação: full-duplex e half-duplex, que são descritos nesta seção, e sistemas sequenciais, que estão descrito na seção seguinte. [1]

No modo de comunicação *half-duplex* (HDX) a transferência de dados do transponder para os leitores alternam com a transferência de dados do leitor para o transponder. Em freqüências abaixo de 30 MHz esse método é mais utilizado junto com o processo de modulação de carga, com ou sem uma subportadora, a qual envolve circuitos muito simples. Intimamente relacionado com este é o método de seção transversal refletida modulada que é familiar para a tecnologia de radar e é usado em frequências acima de 100 MHz. Modulação de carga e método de seção transversal refletida modulada influenciam diretamente o campo magnético ou o campo eletromagnético gerado pelo leitor e estão, portanto, entre os procedimentos harmônicos. [1]

No modo de comunicação *full-duplex* (FDX) o transferência de dados do transponder ao leitor (*up-link*) tem lugar ao mesmo tempo que a transferência de dados do leitor para o transponder (*down-link*). Este inclui métodos nos quais os dados são transmitidos a partir do transponder numa fracção da frequência do leitor, ou seja, uma subharmonica, ou numa totalmente independente, isto é, frequência, não harmônica. [1]

No entanto, ambos os métodos têm em comum o fato de a transferência de energia a partir do leitor para o transponder ser contínua, isto é, está independente da direção do fluxo de dados. Em um sistema seqüencial (SEQ), por outro lado, a transferência de energia proveniente do transponder para o leitor acontece somente por um período de tempo limitado (operação de pulso → sistema pulsado). A transferência de dados a partir do transponder para o leitor ocorre nas pausas de fornecimento de energia da fonte de alimentação para o transponder. [1]

A seguir, figura 26, uma representação dos modos de comunicação *full-duplex, half-duplex* e sistemas sequências.

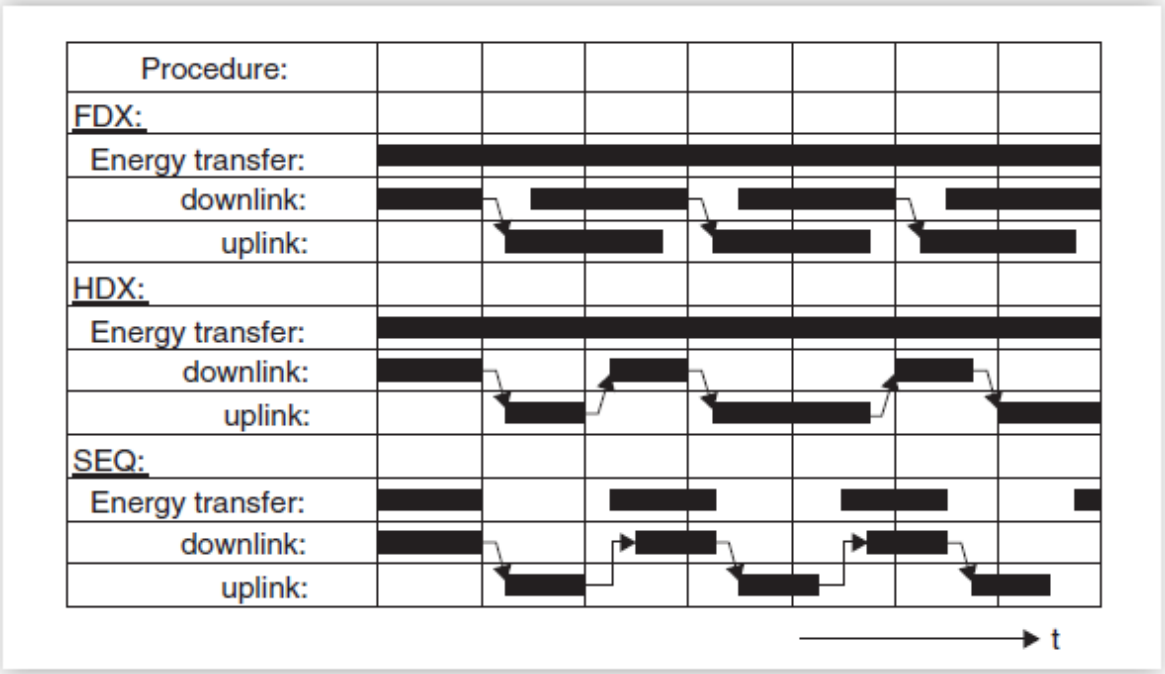

Figura 26 - Representação dos modos *full-duplex, half-duplex* e de sistemas seqüenciais ao longo do tempo. A transferência de dados do leitor para o *transponder* é denominada ligação descendente(*down-link*), enquanto que a transferência de dados do *transponder* para o leitor é denominado ligação ascendente (*up-link*). [1]

Infelizmente, a literatura relativa à RFID ainda não foi capaz de concordar com uma nomenclatura consistente para estas variantes do sistema. Em vez disso, tem havido uma classificação confusa e inconsistente de sistemas individuais em modo *full* e *half-duplex*. Assim sistemas pulsados são frequentemente denominados sistemas *half-duplex* - isso é correto do ponto de vista da transferência de dados - e todos os sistemas não pulsados são falsamente classificados como sistemas *full-duplex*. Por esta razão, neste trabalho sistemas pulsados – por diferenciação de outros métodos, são denominados sistemas seqüenciais (SEQ). [1]

TIPOS DE ACOPLAMENTO

1.1.6.2.1 Acoplamento indutivo

1.1.6.2.1.1 Fonte de alimentação para Transponders passivos

Um transponder indutivamente acoplado compreende um dispositivo de transporte de dados eletrônicos, geralmente um único microchip, e uma bobina ou condutor circular de grande área que funciona como antena.

Transponders indutivamente acoplados são quase sempre operados de forma passiva. Isto significa que toda a energia necessária para o funcionamento do circuito integrado tem de ser fornecida pelo leitor (Figura 29). Para este fim, a bobina do leitor que atua como elemento de acoplamento gera, um campo eletromagnético forte de alta

frequência, que penetra na seção transversal da área da bobina e da área em torno da bobina. Porque o comprimento de onda na faixa de freqüência utilizada (<135 kHz: 2400 m, 13,56 MHz: 22,1 m) é várias vezes maior do que a distância entre a antena do leitor e o transponder, o campo eletromagnético pode ser tratado como um campo magnético alternado simples no que diz respeito à distância entre transponder e a antena. [1]

Obs.: Cabe ressaltar que nas literaturas encontradas no mercado sobre a tecnologia RFID tratam as bobinas dos transponders e dos leitores de sistemas de acoplamento indutivo como sendo antenas o que pode ser considerado um erro conseitual, sendo assim neste trabalho consideraremos estes componetes como sendo elementos de acoplamento, o qual permite a comunicação sem contato dos transponders e leitores.

Uma pequena parte do campo emitido penetra na bobina do transponder, o qual está a pouca distância da bobina do leitor. A tensão Ui é gerada na bobina do transponder por indutância. Esta tensão é retificada e serve como fonte de alimentação para o dispositivo de transporte de dados (microchip). [1]

Um capacitor Cr está ligado em paralelo com a bobina do leitor, a capacitância deste capacitor é selecionada de tal modo que ele funciona com a indutância da bobina de modo a formar um circuito ressonante paralelo com uma frequência ressonante que corresponda à frequência de transmissão do leitor. Correntes muito elevadas podem ser geradas na bobina do leitor por ressonância *step-up* no circuito ressonante paralelo, podendo ser usadas para gerar as forças de campo requeridas para o funcionamento do transponder de forma remota. [1]

A seguir , figura 27, um esquema mostrando como ocorre o acoplamento indutivo.

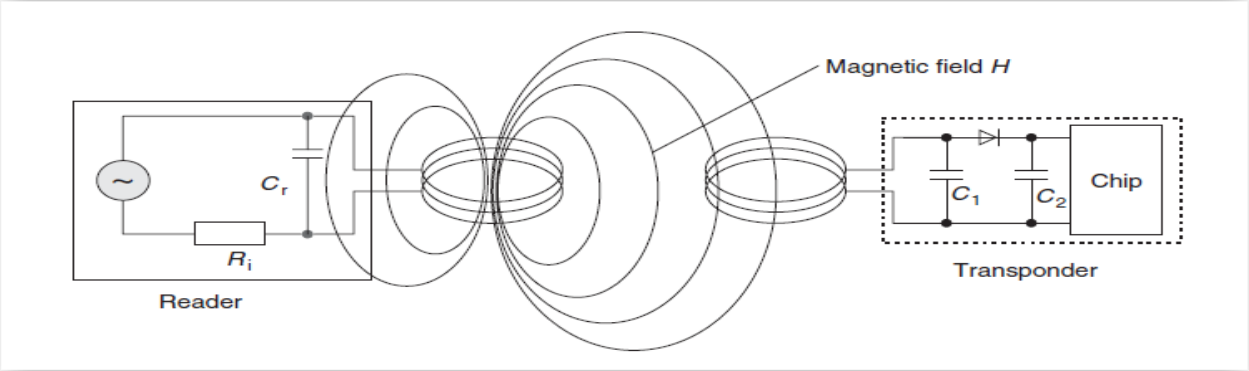

Figura 27 - Fonte de alimentação para um *transponder* acoplado indutivamente a partir da energia do campo magnético alternado gerado pelo leitor. [1]

A bobina do *transponder* e o capacitor C1 formar um circuito ressonante sintonizado com a frequência da transmissão do leitor. A tensão U na bobina do

transponder atinge um máximo devido à ressonância *step-up* no circuito ressonante paralelo. [1]

A seguir, figura 28, diferentes formatos de *transponders* indutivamente acoplado. E, na figura 29, uma imagem de da parte interna de um leitor de *transponder* indutivamente acoplado.

Figura 28- Os diferentes formatos de *transponders* indutivamente acoplados. A foto mostra *transponders* meio-acabados, ou seja, antes dos *transponders* serem inseridos em um encapsulamento de plástico. [1]

A disposição das duas bobinas também pode ser interpretada como um transformador (acoplamento de transformador), no caso em que existe apenas um acoplamento muito fraco entre os dois enrolamentos. A eficiência da transferência de energia entre a bobina do leitor e o transponder é proporcional à frequência operação f, o número de enrolamentos N, a área A delimitada pela bobina do transponder, o ângulo entre as duas bubinas e a distância entre as duas bobinas. [1]

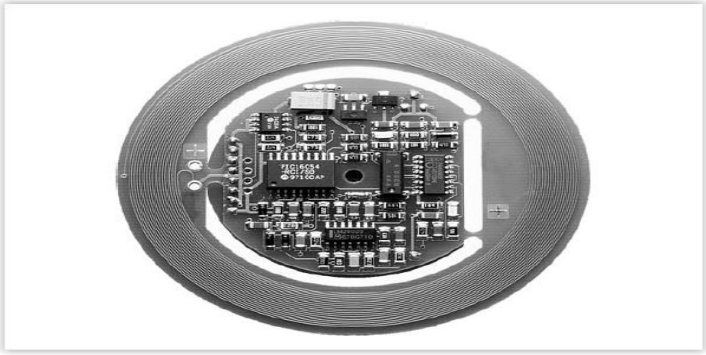

Figura 29 - Leitor para transponders indutivamente acoplados na faixa de freqüência <135 kHz com uma bobina integrante. [1]

Tabela 6 - Visão geral do consumo de energia de vários blocos de construção RFID-ASIC					
	Memória (bytes)	Distância de leitura/escrita (cm)	Consumo de energia	Frequência	Aplicação
ASIC#1	6	15	10 µA	120 kHz	Identificação animal
ASIC#2	32	13	600 µA	120 kHz	Fluxo de mercadorias, verificação de acesso
ASIC#3	256	2	6 µA	128 kHz	Transporte público
ASIC#4	256	0.5	<1mA	4MHz∗	Fluxo de mercadorias, o transporte público
ASIC#5	256	<2	~1mA	4/13.56 MHz	fluxo de mercadorias
ASIC#6	256	100	500 µA	125 kHz	verificação de acesso
ASIC#7	2048	0.3	<10mA	4.91 MHz∗	Cartões com chip sem contato
ASIC#8	1024	10	~1mA	13.56 MHz	Transporte público
ASIC#9	8	100	<1mA	125 kHz	fluxo de mercadorias

ASIC#10	128	100	<1mA	125 kHz	verificação de acesso

*Sistema de acoplamento próximo

No que frequência f aumenta, a indutância necessária da bobina do *transponder* e, portanto, o número de voltas n diminui (135 kHz: típicos 100-1000 enrolamentos, 13,56 MHz: típico 3-10 enrolamentos). Uma vez que a tensão induzida no transponder é proporcional à frequência f, um número reduzido de enrolamentos quase não afeta a eficiência da transferência de energia se for usado frequências maiores. [1]

1.1.6.2.1.2 Transferência de dados Transponder → Leitor

1.1.6.2.1.2.1 Modulação de carga

Como descrito acima, os sistemas acoplados indutivamente baseiam-se num acoplamento do tipo transformador entre a bobina primária, no leitor e a bobina secundária no *transponder*. Isso é verdade quando a distância entre as bobinas não excede $(\lambda / 2\pi)$ 0.16λ, de modo a que o *transponder* esteja localizado no campo próximo da "antena" (elemento de acoplamento – bobina) do transmissor. [1]

Se um transponder de ressonância (isto é, um transponder com uma frequência de auto-ressonante correspondente com a frequência de transmissão do leitor) é colocado dentro do campo magnético alternado da bobina do leitor, o *transponder* extrai energia desse campo magnético. A reação resultante do transponder na bobina ("antena") do leitor pode ser representada como uma impedância ZT modificada na bobina do leitor. O chaveamento da resistência de carga ligando e desligando a bobina do transponder, provoca uma mudança na impedância ZT, e, portanto, variações de tensão na bobina do leitor. Isto tem o efeito de uma modulação de amplitude da tensão UL na bobina do leitor pelo repetidor remoto. Se o intervalo de tempo com que a resistência de carga é ligada e desligada é controlado pelos dados, estes dados podem ser transferidos do transponder para o leitor. Este tipo de transferência de dados é chamado de modulação de carga. [1]

Para recuperar os dados no leitor, a tensão drenada na bobina do leitor é retificada. Este efeito representa a demodulação de um sinal de amplitude modulada. Um circuito de exemplo é mostrado na figura 32. [1]

A seguir, figura 30, um exemplo de circuito de retificação de tensão.

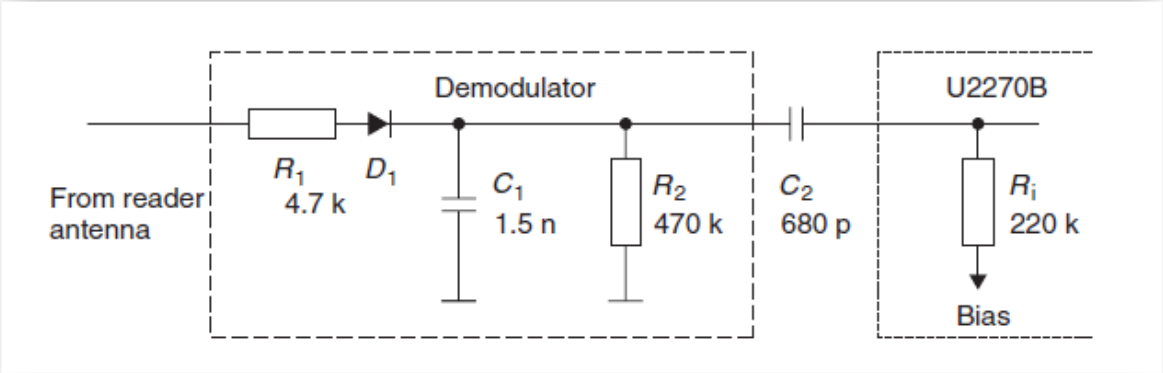

Figura 30 - Rectificação da tensão de amplitude modulada na bobina do leitor. [1]

Se o transponder deixa a região do campo próximo, isto é, a região de distância <λ / 2π (0,16 λ), o acoplamento de transformador entre a bobina do leitor e a bobina do transponder irá ser perdido. Assim, com a transição para o campo distante, a modulação de carga não é mais possível. Isso não significa, porém, que a transmissão de dados desse transponder para no leitor não é, em princípio, mais possível. Com a transição para a região de campo distante, o mecanismo de acoplamento backscatter torna-se eficaz. Na prática, a transmissão de dados para no leitor normalmente falha devido a baixa eficiência das "antenas"do *transponder* (ou seja, por causa do baixo ganho da "antena") na região de campo distante. [1]

1.1.6.2.1.2.2 Modulação de carga com subportadora

Devido ao acoplamento fraco entre a antena do leitor e a antena do transponder, as flutuações de tensão na antena do leitor que representam o sinal útil são menores em várias ordens de grandeza do que a tensão de saída do leitor. Na prática, para um sistema de 13,56 MHz, uma dada tensão de bobina de aproximadamente 100V (tensão de *step-up* por ressonância) um sinal útil de cerca de 10mV pode ser esperado (razão = 80 dB de sinal / ruído). Como detectar esta ligeira mudança de voltagem requer circuitos muito complicados, as bandas laterais de modulação criadas pela modulação de amplitude da tensão da bobina são utilizadas. [1]

Se a resistência de carga adicional no transponder for chaveada, isto é, ligada e desligada a uma frequência elementar fS muito elevada, então duas linhas espectrais são criadas a uma distância de ± fS em torno da frequência de transmissão do leitor fREADER, e estes espectros podem ser facilmente detectados (no entanto fS deve ser menor que fREADER). Na terminologia de tecnologia de rádio a nova frequência fundamental é chamada: uma subportadora. A transferência de dados é feita através da modulação ASK, FSK ou PSK da subportadora no tempo com o fluxo de dados. Isso representa uma modulação em amplitude da subportadora. [1]

Modulação de carga com uma subportadora cria duas bandas laterais de modulação na bobina do leitor com uma distância *f*S ,frequência da subportadora, em relação à frequência de transmissão do leitor fREADER, estando a frequ ência da subportadora em

torno da frequência do leitor fREADER. Estas bandas laterais de modulação podem ser separadas a partir de um sinal significativamente forte do leitor passando por um filtro banda-passante (BP) com frequência central sendo uma das duas frequências fREADER ± fS. Uma vez que tenha sido amplificado, o sinal da subportadora passa a ser muito simples de demodular. [1]

A seguir, figura 31, um exemplo de circuito gerador de modulação de carga. E , na figura 32, esquema mostrando as bandas laterais criados pela modulação de carga. Na figura 33, um exemplo de circuito para a geração de modulação de carga com subportadora.

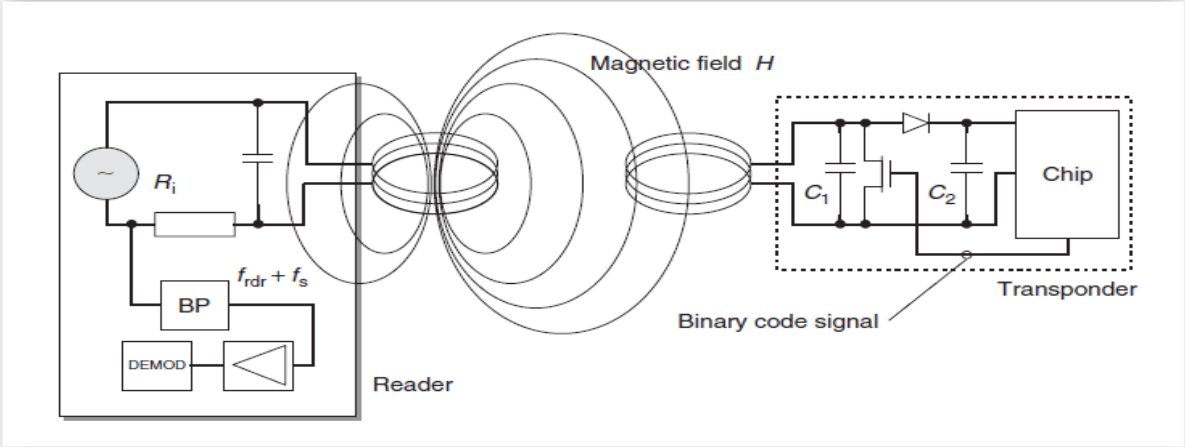

Figura 31 - Geração de modulação de carga no transponder, alternando a resistência dreno-fonte de um FET no chip. O leitor ilustrado é concebido para a detecção de uma subportador. [1]

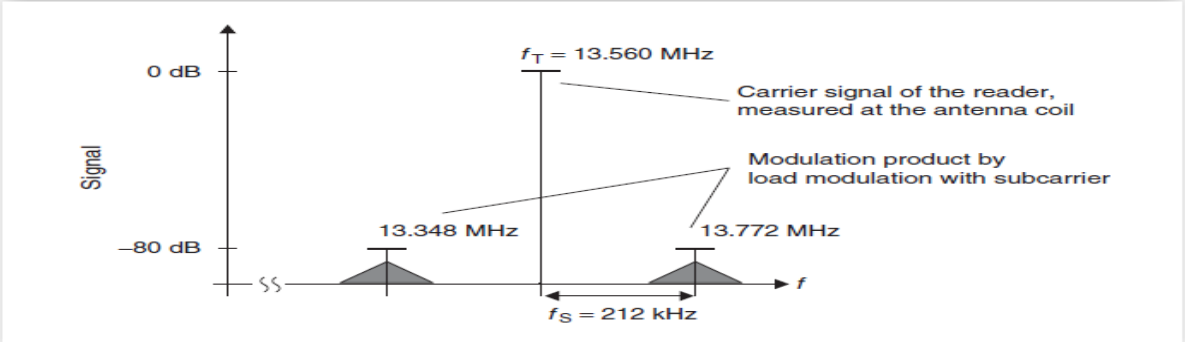

Figura 32 - Modulação de carga cria duas bandas laterais, a uma distância de fS,frequência da subportadora, em relação à frequência de transmissão do leitor. A informação real é transportada nas bandas laterais da subportadora, duas bandas laterais, que são criadas pela própria modulaçaõ da subportadora. [1]

Modulações de carga com subportadora são limitadas à faixa de freqüência de 13,56 MHz. Freqüências Típicas de subportadoras são 212 kHz, 424 kHz (por exemplo, ISO/IEC 15 693) e 848 kHz (por exemplo, ISO / IEC 14443). [1]

Exemplo de Circuito de carga com motulação de subportadora

A Figura 34 apresenta um exemplo de circuito para um transponder usando modulação de carga com uma subportadora. O circuito é projetado para uma freqüência operacional de 13,56 MHz e gera uma subportadora de 212 kHz. [1]

A tensão induzida na bobina L1 por onde passa o campo magnético alternado do leitor é retificada utilizando a ponte rectificadora (D1-D4) e depois de uma suavização adicional (C1) essa está disponível para o circuito como tensão de alimentação. O regulador paralelo (ZD 5V6) impede que a tensão de alimentação seja submentida a um aumento não controlado, quando o transponder se aproxima da bobina do leitor. [1]

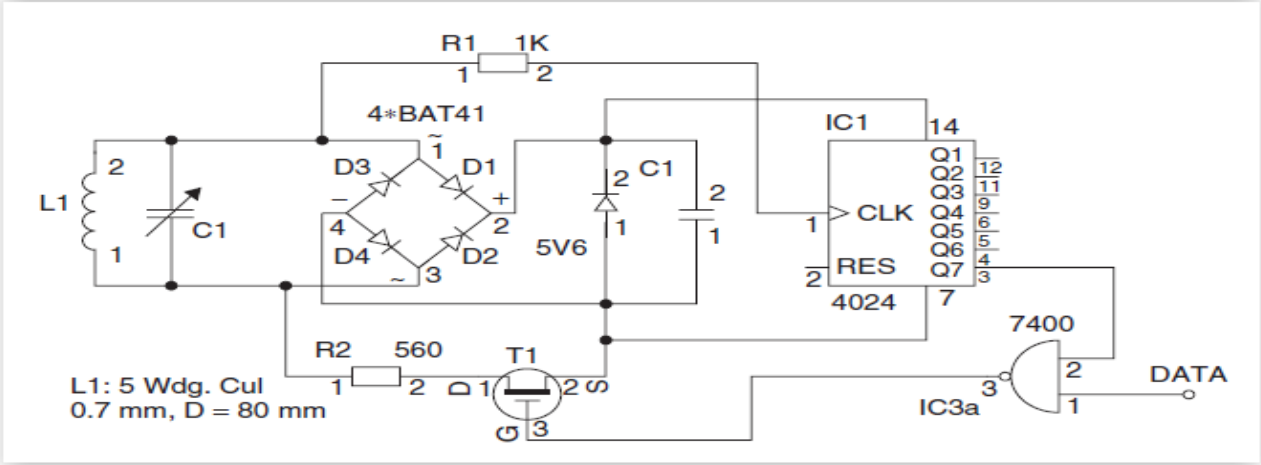

Figura 33 – Exemplo de circuito para a geração de modulação de carga com subportadora em uma transponder acoplado indutivamente. [1]

Parte da tensão de alta frequência da bobina (13,56 MHz) chega até a entrada de relógio (CLK) do divisor de freqüência através da resistência de proteção (R1) e fornece ao transponder a base para a geração de um sinal de relógio interno. Após a divisão por 26 (= 64) um sinal de *clock* da subpotadora de 212 kHz está disponível na saída Q7. O sinal de relógio da subportadora, controlado por uma série de dados que flui pela entrada de dados (DATA), é transmitido para o interruptor (T1). Se um sinal lógico alto (bit 1) atravessa na entrada de dados (DATA), então o sinal de relógio da subportadora é transmitido para o interruptor (T1). A resistência de carga (R2) é então chaveada, ligada e desligada, no tempo, de acordo com a frequência da subportadora. [1]

Opcionalmente, no circuito ilustrado, o circuito ressonante do *transponder* pode ser posto em ressonância com o capacitor C1 a 13,56 MHz. O alcance deste "*transponder* mínimo' pode ser significativamente aumentado desta maneira.

2.1.6.2.1.2.3 – Processo de comunicação por sub-harmônicas

Uma sub-harmônica de uma tensão senoidal A com uma frequência definida fA é uma tensão senoidal B, cuja frequência fB é derivada de uma divisão da frequência fa. Os sub-harmonicos da frequência fA são, portanto, as frequências fA / 2, fA / 3, fA / 4. . . . [1]

Na transferência por processo de sub-harmônica, uma segunda frequência fB, que é geralmente inferior por um fator de dois, é obtido pela divisão digital por dois da frequência de transmissão do leitor fA. O sinal de saída fB de um divisor binário pode agora ser modulado com o fluxo de dados vindos do *transponder*. O sinal modulado é em seguida alimentado de volta para a bobina do transponder por meio de um condutor de saída. [1]

Uma frequência de funcionamento comum para sistemas que usam sub-harmônicas é de 128 kHz. Isso dá origem uma frequência de resposta do transponder de 64 kHz. [1]

A "antena" do transponder consiste em uma bobina com uma ligação no centro, através da qual a energia de alimentação é retirada a partir de uma das extremidades. Um sinal de retorno do transponder é alimentado na segunda conexão da bobina (Figura 36). [1] A seguir, figura 34, um Circuito básico de um transponder com freqüência de retorno sub-harmônica.

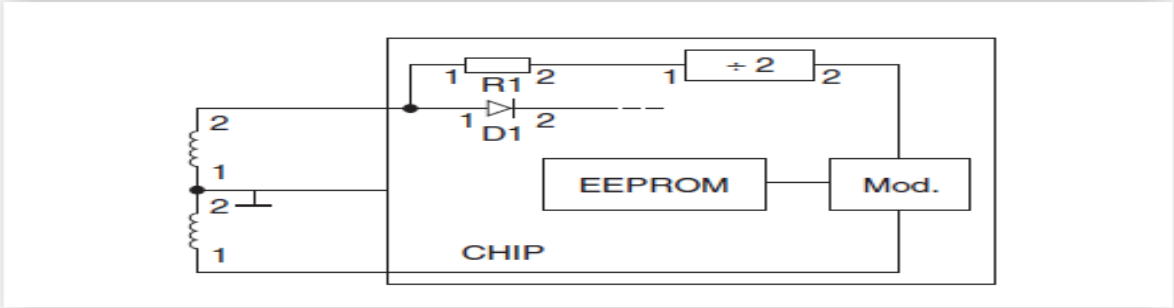

Figura 34 - Circuito básico de um transponder com freqüência de retorno sub-harmônica. O sinal de clock recebido é dividido em dois, os dados são modulados e alimentados para a bobina do transponder através de uma ligação. [1]

1.1.6.2.2 – Acoplamento eletromagnético *Backscatter(*por retrodifusão)

1.1.6.2.2.1 - Fonte de alimentação para o *Transponder*

Os sistemas RFID em que a disância de funcionamento entre o leitor e o transponder é superior a 1m são chamados de sistemas de longo alcance. Estes sistemas são operados nas freqüências UHF de 868MHz (Europa) e 915MHz (EUA), e nas freqüências de microondas de 2,5 e 5,8 GHz. Os comprimentos de onda curtos dessas faixas de freqüência facilitam a construção de antenas com dimensões muito menores e maior eficiência do que seria possível utilizando faixas de frequências abaixo de 30 MHz. [1]

A fim de poder avaliar a energia disponível para a operação de um transponder nós primeiro calculamos o espaço livre perdido de percurso a_F em função da distância r entre o transponder e a antena do leitor, do ganho GT e GR da antena do transponder e da antena do leitor e da frequência de transmissão f do leitor: [1]

$$a_F = -147.6 + 20\log(r) + 20\log(f) - 10\log(G_T) - 10\log(G_R) \qquad (1)$$

A perda em espaço livre é uma medida da relação entre a potência de RF emitida por um leitor em "espaço livre" e a potência de RF recebida pelo transponder.

Usando a tecnologia atual de baixa potência de semicondutores, chips de transponder pode ser produzido com um consumo de energia de não mais do que 5 mW. Uma eficiência de um retificador integrado pode ser assumida como sendo de 5-25% na faixa de microondas e de UHF. Dada uma eficiência de 10%, nós, portanto, necessitamos de uma potência recebida de Pe = 50 mW no terminal da antena do *transponder* para a operação da chip do *transponder*. Isto significa que onde a potência de transmissão do leitor é Ps = 0.5W a perda de percurso no espaço livre não pode exceder 40 dB (Ps / Pe = 10 000/1) quando a potência a ser obtida na antena do transponder for suficiente elevada. Um olhar sobre Tabela 3.7 mostra que em uma frequência de transmissão de 868 MHz um alcance de um pouco mais de 3m seria realizável; a 2,45 GHz um pouco mais de 1 m poderia ser alcançado. Se o chip do *transponder* tiver um maior consumo de energia o alcance realizável cairia em conformidade. [1]

A fim de atingir longos alcances de até 15 metros ou de ser capaz de operar com chips de transponder com maior consumo de energia em uma faixa aceitável, transponders de retroespalhamento muitas vezes têm uma bateria de backup para fornecer energia para o chip do transponder (Figura 36). Para evitar que esta bateria seja descarregada desnecessariamente, os microchips têm, geralmente, um modo 'desligado' ou modo 'standby' para a economia de energia. [1]

Tabela 7 Perda de percurso em espaço livre aF em diferentes frequências e distâncias. O ganho da antena do transponder foi assumido o como sendo 1,64 (dipolo), o ganho da antena do leitor foi assumido como um (emissor isotrópico)

Distância r (m)	868 Mhz (dB)	915 Mhz (dB))	2.45 GHz (dB)
0.3	18.6	19.0	27.6
1	29.0	29.5	38.0
3	38.6	39.0	47.6
10	49.0	49.5	58.0

A seguir, figura 35, a imagem interna de um *transponder* ativo.

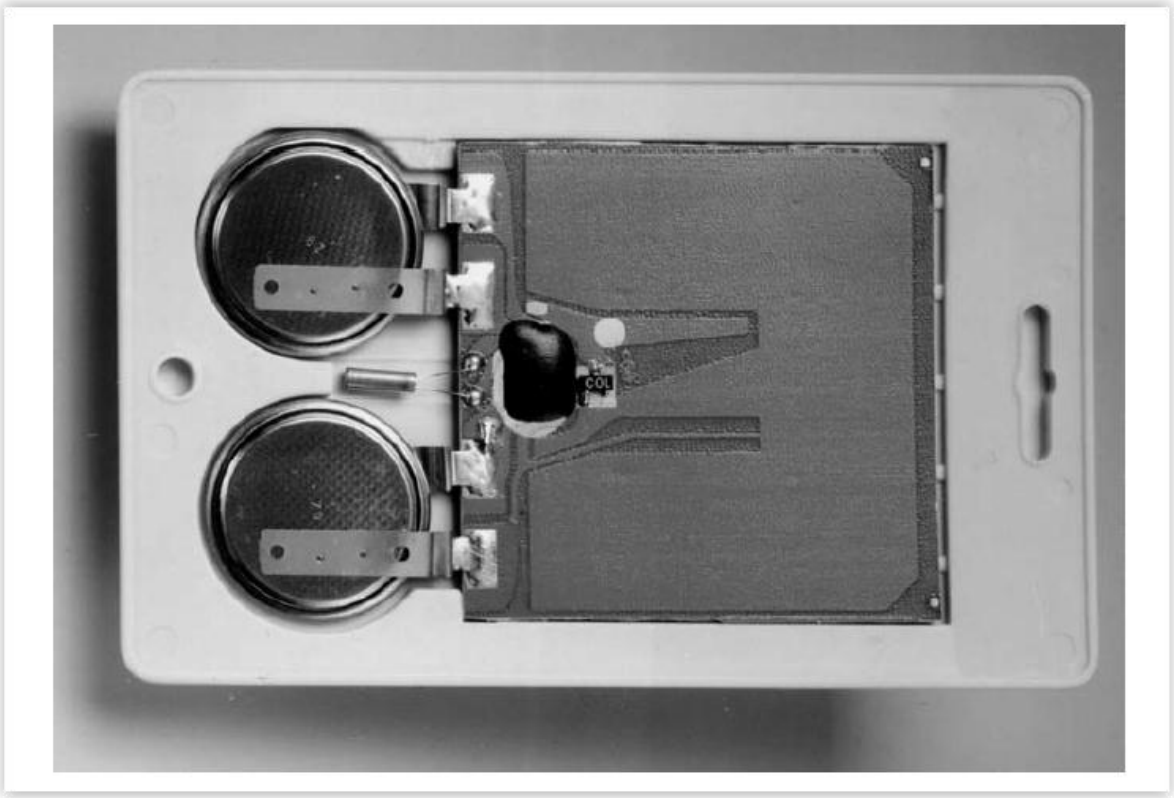

Figura 35 - Transponder ativo para a faixa de freqüências de 2,45 GHz. O portador dos dados é alimentado com energia por duas baterias de lítio. A antena de microondas do *transponder* é visível na placa de circuito impresso com forma de uma área em forma de U. [1]

Se o transponder se move para fora do alcance de um leitor, então o chip automaticamente chaveia (muda) para o modo de economia de energia ou 'baixa potência'. Nesse estado, o consumo de energia está a poucos μA no máximo. O chip não é reativado até que um sinal suficientemente forte é recebido no alcance de leitura de um leitor, após o que, o *transponder* volta para a operação normal. No entanto, a bateria de um transponder ativo nunca fornece energia para a transmissão de dados entre transponder e leitor, mas serve exclusivamente para a alimentação do microchip. A transmissão de dados entre *transponder* e leitor baseia-se exclusivamente na energia do campo eletromagnético emitido pelo leitor. [1]

1.1.6.2.2.2 Transferência de dados Transponder → Leitor

1.1.6.2.2.2.1 Reflexão de seção transversal modulada

Sabemos a partir do campo de tecnologia de radar que as ondas eletromagnéticas são refletidas por objetos com dimensões maiores do que cerca de metade do comprimento da onda. A eficiência com que um objeto reflete as ondas eletromagnéticas é descrita pela

sua seção transversal de reflexão. Objetos que estam em ressonância com a frente de onda que os atinge, como é o caso para as antenas na frequência adequada, por exemplo, ter uma secção transversal de reflexão particularmente grande.

A potência P1 é emitida a partir da antena do leitor, uma pequena porção desta (atenuação no espaço livre) atinge a antena do *transponder* (Figura 38). A potência P1' é fornecida às conexões da antena como voltagem de RF e após a retificação por díodos D1 e D2 esta pode ser utilizada como tensão de comutação para a desativação ou ativação do modo de economia de energia 'baixa potência'. Os diodos usados aqui são diodos Schottky de baixa barreira, que têm uma tensão de limiar particularmente baixa. A tensão obtida pode também ser suficiente para servir como uma fonte de alimentação para distâncias curtas.

A seguir , figura 36, um esquema monstrando o princípio de funcionamento de um transponder *backscatter*.

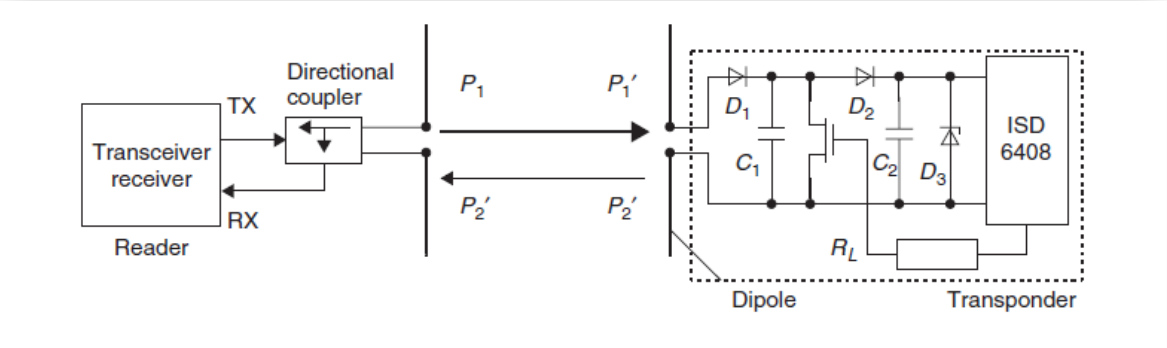

Figura 36 Princípio de funcionamento de um *transponder backscatter*. A impedância do chip é "modulada" pela comutação do chip de FET. [1]

A porção da potência de entrada P1' é refletida pela antena e devolvida como potência P2. As características de reflexão (= secção transversal de reflexão da antena) podem ser influenciadas alterando a carga ligada à antena. A fim de transmitir dados do transponder ao leitor, uma R_L resistência de carga conectada em paralelo com a antena é ligada e desligada em sincronismo com o fluxo de dados a ser transmitido. A amplitude da energia refletida P2 a partir do transponder pode ser assim modulada (modulação por retrodifusão - *backscatter*). [1]

A potência P2 refletida a partir do transponder é irradiada para o espaço livre. Uma pequena porção desta (atenuação no espaço livre) é captada pela antena do leitor. O sinal refletido, por conseguinte, viaja para a antena do leitor em sendo captado percorre a direção para trás desta até onde possa ser dissociado utilizando um acoplador direcional e transferido para a entrada do receptor do leitor. O sinal diante do transmissor, que é mais forte por potências de dez, é em grande parte suprimida pelo acoplador direcional. [1]

A relação de potência transmitida pelo leitor e a potência de retorno do transponder (P1/P2) pode ser estimada usando a equação radar.

1.1.6.2.3 Acoplamento próximo.

1.1.6.2.3.1 Fonte de alimentação para o Transponder

Sistemas de acoplamento próximo são projetados para alcances entre 0,1 cm e um máximo de 1 cm. O *transponder* é inserido no leitor ou colocado em uma superfície marcada ("*touch and go* ') para operação. Inserindo o transponder ou colocando o no leitor, permite que a bobina do transponder seja precisamente posicionada no espaço de ar do núcleo em forma de anel ou em forma de U. Disposição funcional da bobina do transponder e da bobina do leitor corresponde com a de um transformador (Figura 38). O leitor representa o enrolamento primário e a bobina do transponder representa o enrolamento secundário de um transformador. A corrente alternada de alta frequência no enrolamento primário gera um campo magnético de alta frequência no núcleo e no espaço de ar do arranjo, que também flui através da bobina do *transponder*. Esta energia é retificada para proporcionar uma fonte de energia para o chip. [1]

A seguir, figura 37, uma imagem de um *transponder* de acoplamento próximo em funcionamento.

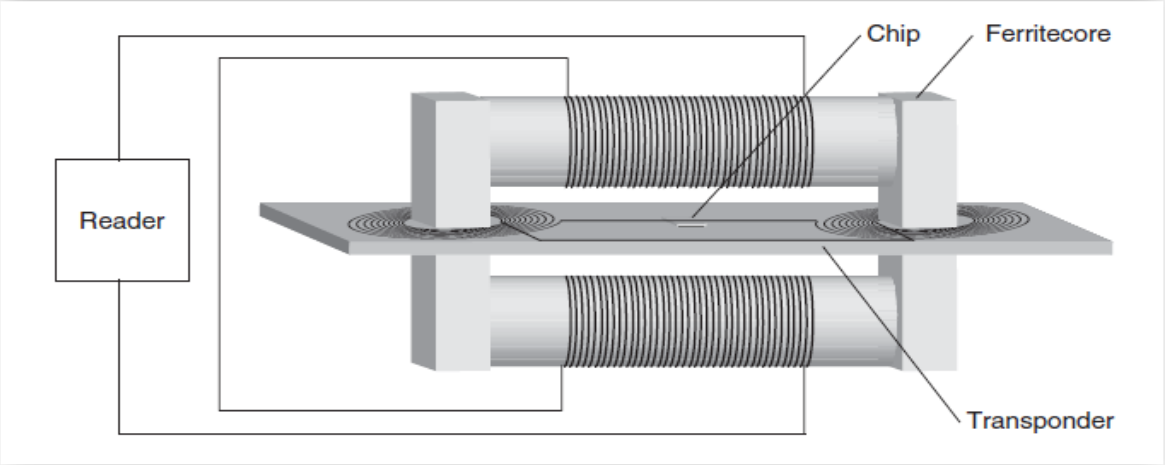

Figura 37 – Transponder de acoplamento próximo em um leitor de inserção com bobinas de acoplamento magnético. [1]

Uma vez que a tensão *U* induzida na bobina de transponder é proporcional à frequência f da corrente de excitação, a frequência seleci onada para a transferência de energia deve ser tão alta quanto possível. Na prática, frequências na faixa de 1-10MHz são usadas. A fim de manter baixas as perdas no núcleo do transformador, um material de ferrite que é adequado para esta frequência deve ser seleccionado como sendo o material do núcleo. [1]

Devido, em contraste com sistemas de acoplamento por indução ou de microondas, à eficiência na transferência de energia do leitor para o *transponder* ser muito boa, sistemas de acoplamento próximo são perfeitamente adequado para a operação de chips com um alto consumo de energia. Isto inclui microprocessadores, que ainda requerem alguma potência de 10mW para a operação. Por esta razão, o chip para

acoplamento próximo de sistemas de cartões no mercado, todos contêm microprocessadores. [1]

Os parâmetros mecânicos e elétricos de sistemas de acoplamento próximo para cartões sem contato com chip são definidos em seu próprio padrão, ISO 10536.

1.1.6.2.3.2 Transferência de dados Transponder → Leitor

1.1.6.2.3.2.1 Acoplamento magnético

Modulação de carga com subportadora também é utilizada para a transferência de dados a partir do transponder para o leitor em sistemas de acoplamento próximo acoplados magneticamente. Frequência e modulação da subportadora são especificadas na ISO 10536 para acoplamento próximo de cartões com chip.

1.1.6.2.3.2.2 Acoplamento capacitivo

Devido à curta distância entre o leitor e o transponder, sistemas de acoplamento próximo pode também empregar o acoplamento capacitivo para transmissão de dados. Capacitores de placa são construídos a partir do acoplamento de superfícies isoladas umas das outras, e essas estão dispostas no *transponder* e no leitor tais que quando um transponder é inserido elas ficam exatamente paralelas um com a outra. [1]

Este método também é usado em cartões inteligentes de acoplamento próximo. As características mecânicas e elétricas destes cartões são definidas na ISO / IEC 10536.

A seguir, figura 38, um exemplo de acoplamento capacitivo em sistemas de acoplamento próximo.

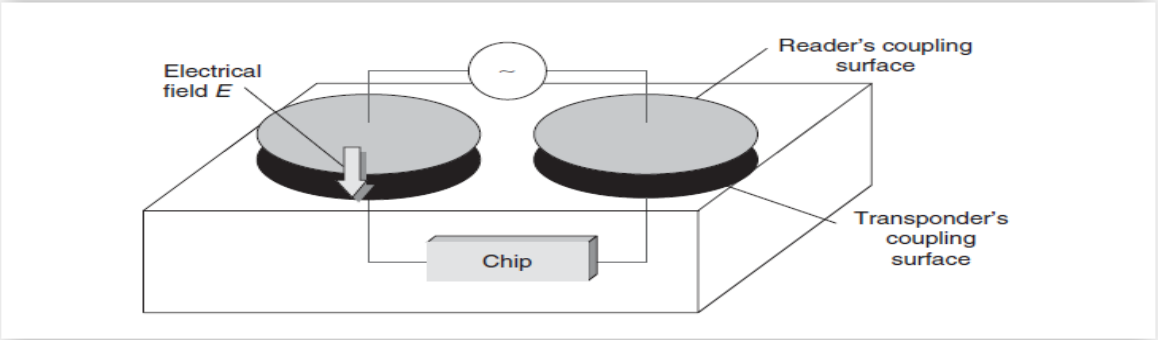

Figura 38 - Acoplamento capacitivo em sistemas de acoplamento próximo ocorre entre duas superfícies metálicas paralelas posicionadas a uma curta distância entre elas. [1]

Tipos de modulação em Sistemas de Comunicação *full* e *half-duplex*

Todas as técnicas de modulação digital conhecidas são usadas na transferência de dados do leitor para o transponder em sistemas de *full* e *half-duplex*, independentemente da freqüência de operação ou o tipo de acoplamento. Há três técnicas básicas: [1]

• ASK: amplitude shift keying;

• FSK: frequency shift keying;

• PSK: phase shift keying;

Devido à simplicidade na demodulação, a maioria dos sistemas usam a modulação ASK.

1.1.6.2.4 Acoplamento elétrico

1.1.6.2.4.1 Fonte de Alimentação de *transponders* passivos

Em sistemas eletricamente acoplados (ou seja, capacitivo) o leitor gera um forte campo eléctrico de alta freqüência. A antena do leitor consiste em uma grande área eletricamente condutiva (eletrodo), geralmente uma folha de metal ou uma placa de metal. Se uma tensão de alta frequência é aplicada ao elétrodo, um campo elétrico de alta frequência é formado entre o elétrodo e o potencial do solo (terra). As tensões requeridas para isso, variando entre algumas centenas de volts e alguns milhares de volts, são gerados no leitor pelo aumento de tensão em um circuito ressonante formado por uma bobina L1 no leitor, mais a ligação em paralelo de um capacitor C1 interno e a capacitância ativa entre o eletrodo e o potencial de terra GND-CR. A frequência de ressonância do circuito corresponde com a frequência de transmissão do leitor. [1]

A antena do transponder é constituída por duas superfícies condutoras situadas num plano (eletrodos). Se o *transponder* é colocado dentro do campo elétrico do leitor, em seguida, uma tensão elétrica surge entre os dois eletrodos do transponder, que é usada para fornecer energia para o chip do *transponder*. [1]

Uma vez que um capacitor é ativado tanto entre o transponder e a antena de transmissão (CR-T) e quanto entre a antena do transponder e o potencial de terra (GND-CT) o diagrama de circuito equivalente de um acoplamento eléctrico pode ser considerado de uma forma simplificada como sendo um divisor de tensão com os elementos CR-T, RL (resistência de entrada do transponder) e CT-GND (Figura 40). Tocando um dos eletrodos do *transponder* resulta em uma capacitância CT-GND, e, portanto, também em um alcance de leitura apropriado significativamente maior. [1] A seguir, figura 39, diagram do circuito equivalente, sistema *RFID*.

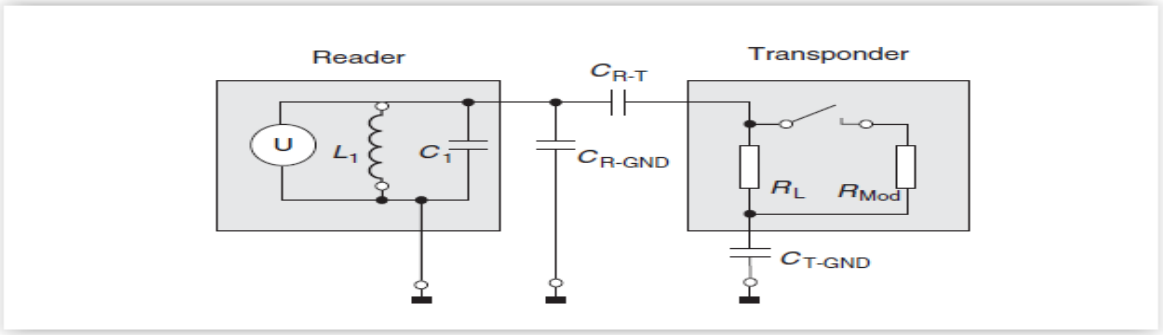

Figura 39- Diagrama do circuito equivalente de um sistema RFID acoplado eletricamente. [1]

As correntes que correm nas superfícies dos eletrodos do transponder são muito pequenas. Por isso, nenhum requisito particular é imposto em relação à condutividade do material do eletrodo. Além das superfícies de metal normais dos eletrodos (folhas de metal) seu efeito pode assim ser também obtido através do uso de cores condutoras (por exemplo, uma pasta condutora de prata) ou um revestimento de grafite. [1]

1.1.6.2.4.2 Transferência de dados Transponder → Leitor

Se um *transponder* acoplado eletricamente é colocado na zona de interrogação de um leitor, a resistência de entrada RL do *transponder* atua sobre o circuito ressonante do leitor por meio do acoplamento do capacitor ativo CR-T entre os eletrodos do leitor e do transponder, amortecendo o circuito ressonante ligeiramente. Este amortecimento pode ser comutado entre dois valores pelo chaveamento de um resistor de modulação R_{MOD} no *transponder*, sendo este ligado e desligado. Mudar o resistor de modulação R_{MOD} ligado e desligado gera, assim, uma modulação de amplitude da tensão presente em L1 e C1 através do *transponder* à distância. Do chaveamento do resistor de modulação R_{MOD} ligando e desligando, no tempo, em sincronismo com os dados, estes dados podem ser transmitidos para o leitor. Este procedimento é chamado de modulação de carga. [1]

A seguir, figura 40, um diagrama de um sistema acoplado eletricamente usando campos elétricos.

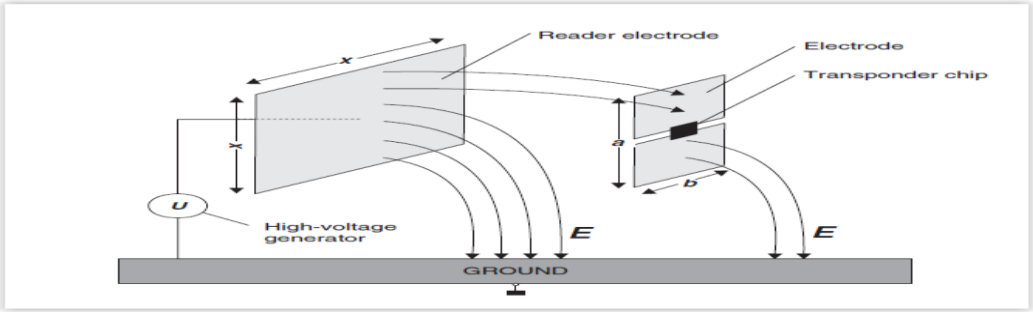

Figura 40 - Um sistema acoplado eletricamente usa campos elétricos (eletrostáticos) para a transmissão de energia e de dados. [1]

1.1.6.3 Modo de comunicação sequencial

Se a transmissão de dados e energia do leitor para o suporte de dados alterna com a transferência de dados do transponder para o leitor, então falamos de um modo de comunicação sequencial (SEQ).

1.1.6.3.1 Acoplamento indutivo

1.1.6.3.1.1 Fonte de alimentação para o *Transponder*

Sistemas seqüenciais de acoplamento indutivo são operados exclusivamente em freqüências abaixo de 135 kHz. Um acoplamento do tipo transformador é criado entre a bobina do leitor e a bobina do *transponder*. A tensão induzida gerada na bobina do *transponder* pelo efeito de um campo alternado do leitor é rectificada e pode ser usada como uma fonte de alimentação. [1]

A fim de conseguir uma maior eficiência na transferência de dados, a frequência do *transponder* deve corresponder precisamente com aquela do leitor, e a qualidade da bobina do *transponder* deve ser cuidadosamente especificada. Por esta razão, o transponder contém um capacitor de corte no chip para compensar a tolerância da frequência de ressonante de fabricação. [1]

No entanto, ao contrário dos sistemas *full* e *half-duplex*, em sistemas seqüenciais o transmissor do leitor não opera de modo contínuo. A energia transferida para o transmissor durante a operação de transmissão carrega um capacitor de carga para proporcionar um acumulador de energia. O chip do transponder é comutado para o modo de espera (*standby*) ou para o modo de economia de energia durante a operação de carregamento, de modo que quase toda a energia recebida é usada para carregar o capacitor de carga. Depois de um período de carregamento fixado o transmissor do leitor é de novo desligado. [1]

A energia armazenada no transponder é usada para enviar uma resposta para o leitor. A capacitância mínima do capacitor de carga pode ser calculada a partir da tensão de funcionamento necessária e do consumo de energia do chip: [1]

$$C = \frac{Q}{U} = \frac{It}{[V_{\max} - V_{\min}]} \qquad (4)$$

Onde: *V*max e *V*min são os valores-limite para a tensão de funcionamento que não podem ser excedidos; *I* é o consumo de energia do chip durante a operação; *t* é o tempo necessário para a transmissão dos dados do transponder para o leitor.

1.1.6.3.1.2 Transmissão de Dados Transponder → Leitor

Em sistemas sequenciais um ciclo de leitura completo consiste em duas fases, a fase de carregamento e a fase de leitura.

O fim da fase de carregamento é detectada por um detector de fim da ruptura, que monitora o caminho da tensão na bobina do transponder e, assim, reconhece o momento em que o campo do leitor está desligado. No final da fase de carregamento de um oscilador no chip, o qual usa o circuito ressonante formado pela bobina do *transponder* como um componente de frequência que determina, seja ativado. Um campo magnético alternado fraco é gerado pela bobina do *transponder*, e este pode ser recebido pelo leitor. Este apresenta uma distância de sinal-interferência melhorada de tipicamente 20 dB em comparação com o pleno de sistemas full/half-duplex , o que tem um efeito positivo sobre os intervalos que podem ser conseguidos usando sistemas sequenciais. [1]

A frequência de transmissão do transponder corresponde à frequência de ressonância da bobina do *transponder*, a qual foi ajustada para a frequência de transmissão do leitor quando era gerada. [1]

A fim de ser capaz de modular o sinal de RF gerado na ausência de uma fonte de alimentação, um capacitor de modulação adicional está ligado em paralelo com o circuito ressonante em sincronismo com o fluxo de dados. A Frequency Shift Keying resultante fornece uma modulação FSK 2. [1]

Após todos os dados terem sido transmitidos, o modo descargar é ativado para descarregar totalmente a capacitor de carga. Isto garante uma força de restauração segura no início do próximo ciclo de carregamento. [1]

A seguir, figura 41, diagrama de blocos de um transponder seguencial. E, na figura 42, gráfico da tensão do capacitor de carga de um transponder SEQ

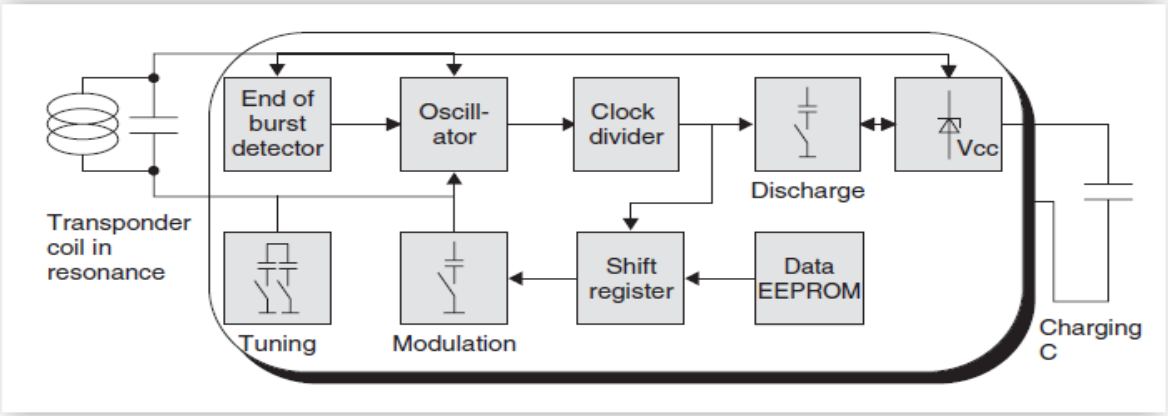

Figura 41 - Diagrama de blocos de um transponder sequencial, usando acoplamento indutivo. [1]

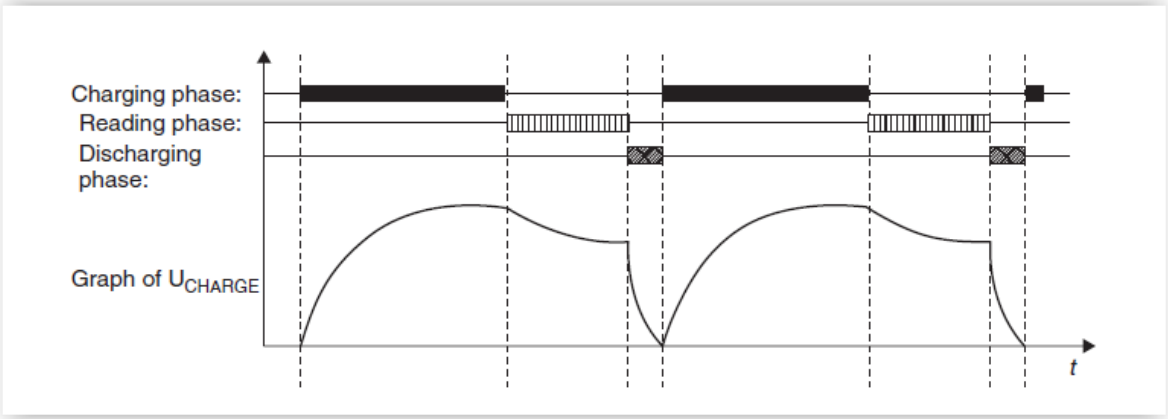

Figura 42 - Trajeto da tensão do capacitor de carga de um *transponder* SEQ indutivamente acoplado durante a operação. [1]

1.1.6.4 Uma comparação entre sistemas FDX/HDX e SEQ.

Figura 43 ilustra as diferentes condições decorrentes de um sistema *full/half-duplex* e sistemas seqüenciais (SEQ).

Porque a fonte de alimentação do leitor para o transponder em sistemas *full-duplex* ocorre ao mesmo tempo que a transferência de dados em ambas as direções, o chip esta permanentemente no modo operacional. Para uma maior correspondencia de energia entre a antena do transponder (fonte de corrente) e o chip (corrente consumida) é desejável utilizar a energia transmitida de forma óptima. No entanto, em caso de correspondência exata da energia é usada apenas metade da tensão da fonte (= tensão de circuito aberto da bobina). A única opção para aumentar a tensão de operação disponível é aumentar a impedância (= resistência de carga) do chip. No entanto, esta é a mesma operação para diminuir o consumo de energia. [1]

Portanto, o projeto de sistemas *full-duplex* é sempre um compromisso entre potência correspondente (consumo máximo de energia no Pchip para Uchip = 1 / 2U0) e tensão correspondente (potência mínima Pchip consumo na tensão máxima Uchip = U0). [1]

A situação é completamente diferente em sistemas seqüenciais: durante o processo de carregamento do chip o transponder está em modo de espera ou o modo de economia de energia, o que significa que quase nenhuma energia é puxada através do chip.

O capacitor de carga fica completamente descarregado no início do processo de carregamento e, por conseguinte, representa uma carga muito baixa ohmica para a fonte de tensão (Figura 44: começar a carregar). Neste estado, a quantidade máxima de corrente flui para o capacitor de carregar, ao passo que a tensão se aproxima de zero (= corrente correspondente). Como o capacitor de carga é carregado, a corrente de carga começa a diminuir de acordo com uma função exponencial, e chega a zero quando o capacitor está totalmente carregado. O estado do capacitor carregado corresponde com uma tensão na bobina do *transponder*. [1]

Este alcança as seguintes vantagens para o fornecimento de energia do chip em relação a um sistema *full*/*half-duplex*:

- Toda a tensão da fonte da bobina do transponder está disponível para a operação do chip. Assim a tensão de funcionamento disponível é de até o dobro de um sistema *half-duplex*/*full* comparável.
- A energia disponível para o chip é determinado apenas pela capacitância do capacitor de carga e pelo período de carregamento. A ambos os valores podem (em teoria) ser dados qualquer magnitude necessária. Dentro do sistema *full*/*half-duplex* o consumo máximo de energia do chip é fixado pelo ponto de energia correspondente (ou seja, a geometria da bobina e força do campo H). [1]

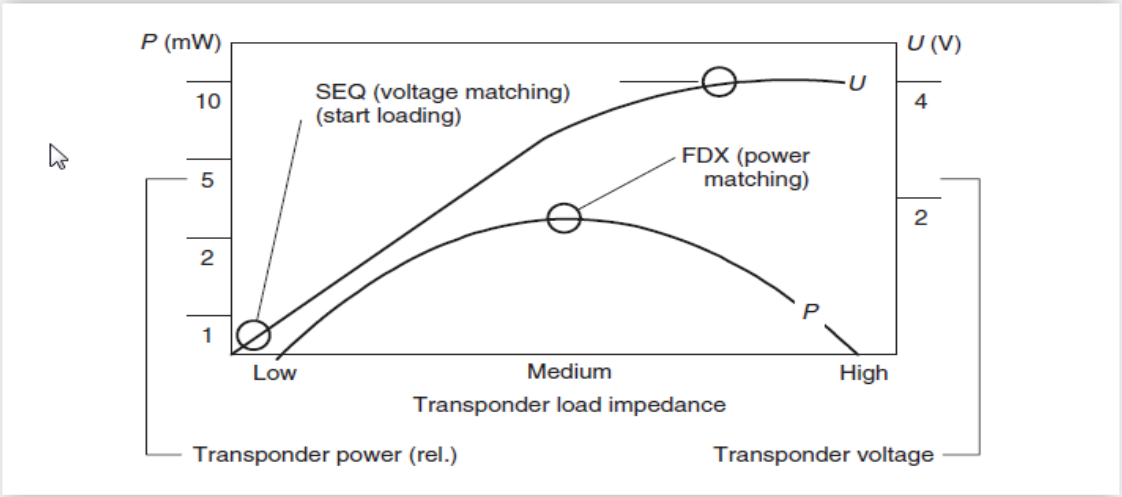

Figura 43 - Comparação da tensão induzida no *transponders de* sistemas FDX/HDX e SEQ.

1.2 Faixas de freqüência Usadas

Como os sistemas RFID geram e irradiam ondas eletromagnéticas, eles são legalmente classificados como sistemas de rádio. O funcionamento do outros serviços de rádio não deve, em circunstância alguma, ser interrompidos ou prejudicados pela operação dos sistemas RFID. É particularmente importante para garantir que os sistemas RFID não interfiram com rádio e televisão nas proximidades, serviços de rádio móveis (polícia, serviços de segurança, indústria), os serviços de rádios da marinha e aeronáutica e telefones móveis. [1]

A necessidade de ter cuidado com relação a outros serviços de rádio restringe significativamente a gama de frequências de funcionamento adequados disponíveis para um sistema de RFID. Durante o início da tecnologia RFID apenas frequências ISM disponíveis internacionalmente e a faixa de freqüência abaixo de 135 kHz poderiam ser utilizados devido ao *nonassignment* das frequências separadas. ISM significa "industriais, científicos e Médico ', ou seja, para aplicações de alta frequência industriais, científicas e médicas. Frequências ISM são internacionalmente reservadas para aplicações que utilizam dispositivos de alta freqüência. Exemplos são máquinas elétricas de descarga, fornos de microondas ou médico de radioterapia de ondas curtas. [1]

Além destas aplicações, as frequências ISM também podem ser usadas para a transmissão de rádio. Devido a interferência de radiação inevitavelmente causadas pela aplicação «efectiva» ISM, freqüências ISM de rádio de aplicações fechadas para dispositivos de alta frequência são propensas a interferências. Em nossa comunicação da sociedade moderna, as radiofrequências são um bem valioso que deve ser utilizado de forma eficiente. Portanto parecia sensato reservar frequências ISM para aplicações de rádio que são capazes de temporariamente tolerar interferências e que tem que cobrir distâncias curtas. A idéia original era que qualquer pessoa, incluindo aplicações RFID, poderia usar dispositivos de rádio - sem quaisquer custos e localização separada de frequência - em freqüências ISM. Hoje em dia, as bandas de frequência ISM são utilizadas por inúmeras instalações de rádio de baixo preço (por exemplo, a 27 MHz, 433 MHz e 2,45 GHz intervalo). [1]

Duas frequências ISM clássicas - 13,56 e 2,45 GHz - ainda são usadas intensamente para sistemas RFID atualmente. Provavelmente, a disponibilidade mundial destas frequências ISM e a possibilidade de usar transponders e leitores internacionalmente, sem alterações, em muitos países tem decisivamente contribuiu para o triunfo internacional de sistemas RFID. [1]

Devido à crescente importância comercial dos sistemas RFID e a frequência cada vez mais liberal na regulação na Europa e outras regiões, em torno do ano 2000, novas faixas de freqüência para os sistemas RFID foram criadas ou as condições de (ISM) freqüências existentes têm sido melhoradas. Assim, na Europa, a faixa de freqüência entre 865 e 868 MHz foi reservada para Sistemas UHF de retroespalhamento. Sistemas RFID com uma intensidade de campo de até 60 dB uA/m, medida a uma distância de 10 m, pode ser

operado na freqüência ISM clássica 13,56 MHz. Outras aplicações só podem usar 42 dB mA/m nesta frequência. Sistemas RFID não são mais classificados como aplicações ISM, mas são tratados na Europa como um aplicativo separado de dispositivos de curto alcance (SRD). [1]

Dispositivos de curto alcance são dispositivos versáteis para uso profissional e privado, como modelo de controle remoto, abridores de portas de garagem, sistemas de travamento central, termômetros ao ar livre, detectores de movimento, avalanche transceptores, dispositivos de rádio de baixa capacidade para implantes médicos, artigos de vigilância, Bluetooth, identificação do veículo para veículos ferroviários, telemática de tráfego e de sinais de distância, rádio sensores de movimento, instalações de rádio alarme, aplicações de rádio indutivo, microfones sem fio, RFID sistemas WLAN, e muitos mais. [1]

A utilização do dispositivo de curto alcance, oferece várias vantagens para o usuário: freqüências SRD são alocadas para o uso do público em geral. Isso significa que o uso a SRD não vem nem a ser registrado, nem autorizados e não há custos associados à utilização dessas frequências. Finalmente, SRD pode ser usado em vários países europeus nas mesmas condições. [1]

Além de freqüências ISM e SRD, toda a gama de frequências abaixo de 135 kHz (no Norte e do Sul e no Japão <400 kHz) é também apropriado, porque é possível trabalhar com campo magnética alto intensidade nesse intervalo, em particular quando operam sistemas RFID indutivamente acoplado. [1]

As faixas de frequência mais importantes para os sistemas RFID são, portanto, 0-135 kHz, a clássica frequência ISM em torno de 6,78 MHz, 13.56 MHz, 27,125 MHz, 40.68 MHz, 869.0 MHz, 2,45 GHz, 5.8 GHz e 24.125 GHz, bem como as frequências SRD Europeia entre 865 e 868 MHz (915MHz em os EUA). [1]

Um requisito muito importante com relação ao RFID é a escolha da freqüência de operação. Sistemas RFID utilizam diversas bandas para comunicação, como mostra a figura 47. [1]

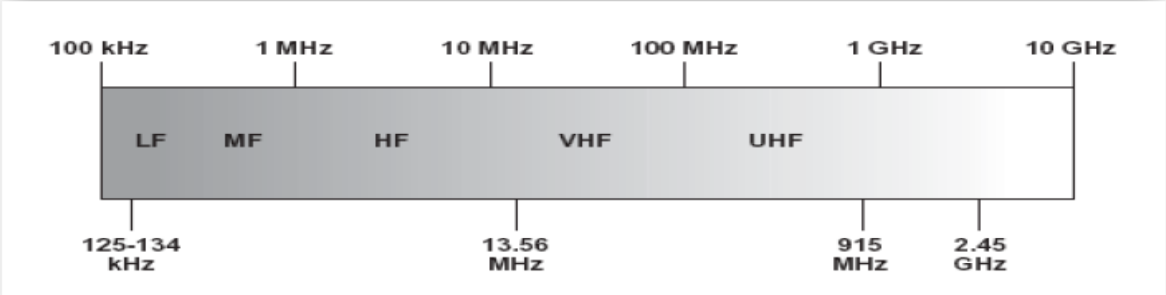

Figura 47 – Bandas de frequências [1]

Basicamente são consideradas as seguintes faixas de freqüência para aplicações de RFID: LF, HF, UHF e Microondas. A escolha da freqüência de operação depende de várias variáveis, bem como afeta várias características do sistema a ser implantado, como segue:

- **Alcance de leitura**: Nas freqüências de operação mais baixas o alcance de leitura de tags passivos não passa de 50-60 cm (Tal alcance é extremamente restrito devido, principalmente, ao baixo ganho das antenas, visto que em baixas freqüências os comprimentos de onda são muito grandes, logo, muito maiores que as dimensões das antenas integradas nos tags. Como o ganho de uma antena é diretamente proporcional ao seu comprimento, que, por sua vez, é relacionado com o comprimento de onda, o ganho em baixas freqüências é muito baixo.) Em altas freqüências o alcance de leitura é muito maior, especialmente quando se utiliza tags ativos. No entanto, devido a possíveis danos que as altas freqüências possam causar à saúde humana, os órgãos reguladores impuseram limites de potência aos sistemas que utilizam UHF e Microondas, o que reduziu a distância de leitura, em sistemas RFID que utilizam essas freqüências, para algo em torno de 3-9 m, no caso de se usar tags passivos. [2]

- **Utilização de tags ativos ou passivos:** Normalmente, tags passivos são usados nas faixas LF e HF, enquanto que os tags ativos são usados em UHF e em Microondas. O motivo pelo qual se utiliza os tags dessa forma é histórico. Os primeiros sistemas RFID usavam as bandas HF e LF com tags passivos, devido ao alto custo da tecnologia na época. Porém hoje isso está sendo alterado. Os recentes avanços tornam possível usar tags ativos em bandas de alta freqüência, e essa tem sido a tendência do mercado de RFID. [2]

- **Interferência de outros sistemas de rádio**: Sistemas de RFID são naturalmente propensos à interferência de outros sistemas de rádio. Particularmente, os sistemas RFID que operam na banda LF são muito vulneráveis, devido ao fato de que baixas freqüências não sofrem muitas perdas, ou atenuam muito pouco quando propagadas em curtas distâncias, se comparadas com altas freqüências. Ou seja, os sinais de rádio de outros sistemas de comunicação que estiverem operando aproximadamente na mesma freqüência LF criarão altos campos eletromagnéticos na antena do leitor RFID, ou seja, gera interferência. Já os sistemas que utilizam a banda de Microondas estão muito menos susceptíveis a interferências externas, visto que as perdas nessas freqüências são muito maiores, e, geralmente, é necessário ter visada entre os irradiadores de microondas para que interfiram. [2]

- **Líquidos e metais:** A performance de um sistema RFID é severamente afetada pela água ou por superfícies úmidas. Sinais HF são mais eficientes na penetração da água do que sinais UHF e Microondas, devido ao comprimento de onda de um sinal HF ser maior do que o de um sinal UHF ou de um em Microondas. Sinais em bandas de altas freqüências são mais absorvidos pelos líquidos do que os de baixas freqüências. Com isso, tags HF são uma melhor escolha para contêineres que contenham líquidos. Os metais têm como característica a reflexão de ondas eletromagnéticas, logo, sinais de rádio não podem penetrá-lo. Sendo assim, um metal pode não apenas obstruir uma comunicação, se postado entre o tag e o leitor, como também afetará a operação do sistema, visto que quando um metal é colocado próximo a uma antena, as características da antena são modificadas. É importante ressaltar que as bandas de freqüências mais altas são mais afetadas por metais do que as de freqüências mais baixas. Logo, quando há a necessidade de instalar tags em objetos feitos de metal, contêineres que portem líquidos ou materiais com alta permissividade dielétrica, algumas precauções especiais tem de serem tomadas, o que, invariavelmente, elevará o custo da solução. [2]

- **Taxa de transmissão dos dados:** Quanto menor a freqüência de operação do sistema RFID, menor a taxa de transmissão. Sendo assim, sistemas que operam na banda LF têm taxas da ordem de Kbits/s, enquanto que na banda de Microondas essa taxa pode atingir Mbits/s. [2]

- **Antenas – Tamanhos e Tipos:** Como sinais de rádio de freqüências mais baixas possuem comprimentos de onda maiores, as antenas para sistemas que operam em LF e HF são maiores do que as que operam em sistemas de UHF e Microondas, mantendo-se o mesmo ganho de sinal, para efeito de comparação. Entretanto, essa diferença no tamanho das antenas conflita com o constante objetivo da indústria de produzir tags RFID cada vez menores e mais baratos. A fim de evitar elevar muito os custos dos tags, a maioria dos designers de sistemas ignoram o ganho das antenas, o que tem resultado em um baixo alcance de leitura para sistemas que utilizam as bandas LF e HF. Sendo assim, as antenas precisam ser maiores quando são usadas freqüências LF e HF, o que traz como resultado que tags LF e HF são tipicamente maiores do que tags para UHF e Microondas. Além do tamanho, a freqüência de operação do sistema também irá ditar o tipo de antena a ser utilizada. Sistemas LF e HF exigem antenas indutivas e por acoplamento indutivo, que, normalmente, são antenas em forma de loop. Enquanto que sistemas UHF e Microondas exigem antenas por acoplamento capacitivo, que são do tipo dipolo. [2]

- **Nulos de Antenas e problemas de orientação:** As antenas indutivas, tais como as utilizadas em LF e em HF, operam inundando a zona de leitura com sinais RF. Além disso, para os grandes comprimentos de onda dos sinais LF e HF, elas trabalham para inundar a zona de leitura com um sinal uniforme, que não tenha diferença de potência de um extremo a outro. Entretanto, as antenas dipolo, como as que são utilizadas nas freqüências UHF e Microondas, operam emitindo sinais do transmissor até o receptor diretivamente. Isso, considerando-se o pequeno comprimento de onda dos sinais UHF e Microondas, dá oportunidade a pequenas ondulações na zona de leitura, o que não permite que a força do sinal, de um extremo a outro da zona de leitura, seja uniforme. Esse fato pode, inclusive, chegar a diminuir a potência do sinal, gerando pontos de nulidade de sinal, ou regiões de sombra. As *tags* RFID que estiverem posicionados nessas regiões estarão efetivamente invisíveis para o leitor, o que pode, obviamente, causar problemas nos sistemas de UHF e Microondas. Tais regiões de sombra também podem ocorrer com uma desintonização dos tags, que ocorre quando dois tags são colocados em uma distância muito pequena entre si, ou quando são colocados próximos a líquidos, metais e outros materiais com alta permissividade dielétrica. Os sistemas que utilizam UHF e Microondas são mais sensíveis a diferenças na orientação das antenas. Antenas indutivas têm pouco ganho direcional, o que significa que a força dos campos em uma dada distância é a mesma acima, abaixo, na frente ou atrás da antena. Já antenas dipolo são mais diretivas, o que significa que há diferenças na força dos campos em uma dada distância entre os pontos à frente do dipolo e sobre ele. Para tags que usam UHF ou Microondas inundarem o leitor, a força do sinal pode não ser suficiente para estabelecer a comunicação. Todos esses problemas requerem que sistemas RFID que usam UHF ou Microondas estejam programados com uma modulação mais complexa, chamada frequency hopping, para superar tais defeitos. [2]

- **Tamanho e preço dos tags:** Os sistemas de RFID atuais usam principalmente a banda LF, devido ao fato dos tags LF serem os mais fáceis de serem fabricados. Todavia,

eles têm muitas desvantagens, como o grande tamanho, o que se traduz em um alto preço. Os tags HF são mais baratos de se produzir do que os LF, por isso sistemas RFID que usam a banda HF são, atualmente, os mais utilizados no mundo. A banda UHF representa o que há de mais evoluído em se tratando de RFID. Recentes avanços na tecnologia têm derrubado os preços dos tags UHF a ponto de poderem competir com os tags HF. Já os tags que funcionam por microondas são semelhantes aos tags UHF, no que tange a possibilidade de serem menores e mais baratos. [2]

1.2.1 - *Low Frequency* (LF) – 125kHz & 134kHz

A faixa de freqüências chamada de Low Frequency compreende sinais entre 30kHz e 300kHz. Sistemas RFID normalmente utilizam freqüências entre 125kHz e 134kHz. Um sistema LF RFID típico opera ou em 125kHz ou em 134.2kHz. Sistemas nessa faixa de freqüências geralmente utilizam tags passivos (apesar de ser possível a utilização de tags ativos, devido à maturidade desse tipo de tag), têm baixa taxa de transferência de dados do tag para o leitor, devido à baixa freqüência, e são especialmente bons para quando o ambiente operacional contém metais, líquidos, sujeira, neve ou barro. Atualmente os sistemas LF RFID compreendem a maior parte das aplicações instaladas no mundo, até mesmo porque a faixa de freqüências LF é aceita no mundo todo. [2]

1.2.2 - *High Frequency* (HF) - 13.56MHz

A faixa de freqüências compreendida entre 3MHz e 30MHz é chamada de High Frequency. A freqüência típica utilizada em sistemas de RFID é 13.56MHz. Tais sistemas que utilizam essa freqüência, normalmente, usam tags passivos, tem uma baixa taxa de transferência entre o tag e o leitor e tem um bom desempenho diante de materiais como metais e líquidos. Sistemas HF RFID são amplamente utilizados, principalmente pela faixa de HF ser regulamentada no mundo todo. Suas aplicações englobam várias áreas, mas destaca-se a implantação em hospitais, pois a freqüência de 13.56MHz não interfere no funcionamento dos equipamentos médicos.

1.2.3 - *Ultra High Frequency* (UHF) - 300MHz < f < 1GHz

A faixa de freqüências compreendida entre 300MHz e 1GHz é chamada de Ultra High Frequency, ou, simplesmente, UHF. Sistemas UHF RFID passivos normalmente operam nas freqüências 915MHz, nos Estados Unidos, e 868MHz, na Europa. Já os sistemas ativos operam, geralmente, em 315MHz e 433MHz. Um sistema UHF RFID pode utilizar tanto tags ativos quanto passivos e tem uma alta taxa de transferência de dados entre o tag e o leitor, mas seu desempenho é fraco quando da proximidade com metais e líquidos, salvo quando se utiliza as freqüências baixas do UHF, como 315MHz e 433MHz. Os sistemas UHF RFID começaram a ser amplamente utilizados por causa do recente incentivo de

empresas públicas e privadas, bem como do U.S. Department of Defense. Apesar disso, a banda UHF não é aceita mundialmente para aplicações de RFID. [2]

1.2.4 - *Microwaves Frequency* – 2.45GHz & 5.8GH

As freqüências que estão acima de 1GHz são consideradas microondas. Os sistemas Microwave RFID operam normalmente ou em 2.45GHz ou em 5.8GHz, sendo que a primeira é a mais comum. Tais sistemas podem utilizar tags semi-ativos ou passivos, tendo uma alta taxa de transmissão de dados entre o tag e o leitor, apesar do desempenho diante de materiais como metais e líquidos ser muito fraco. Devido ao comprimento da antena ser inversamente proporcional à freqüência, a antena de um tag passivo operando na banda de Microondas tem o seu tamanho extremamente reduzido, o que resulta em um tag muito pequeno, visto que o microchip também tem um tamanho muito pequeno. A freqüência de 2.4GHz também é chamada de *Industry, Science, and Medical* (ISM) Band e é aceita no mundo todo. [2]

A tabela 8 a seguir compara as diversas bandas de operação dos sistemas de RFID:

Frequency Band	LF 125 KHz	HF 13.56 MHZ	UHF 860–960 MHZ	Microwave 2.5 GHz and Up
Read Range (Passive Tags)	<2 Feet	<3 Feet	<10–30 Feet	–10 Feet
Tag Power Source	Generally passive	Generally passive	*Generally active* but Passive Also	*Generally active* but Passive Also
Tag Cost	Relatively expensive	*Expensive*, but less So Than LF	Potential to Be very cheap	Potential to Be very cheap
Typical Applications	Keyless entry, animal tracking, vehicle immobilizers, POS	"Smart" cards, item-level track such as baggage handling, libraries	Pallet tracking, electronic toll collection, baggage handling	Electronic toll collection
Data Rate	Slower			Faster
Performance Near Metal or Liquids	Better			Worse
Passive Tag Size	Larger			Smaller

Tabela 8 - Bandas de freqüência dos sistemas RFID. [2]

Existem restrições internacionais para definir quais as freqüências que podem ser utilizadas nos sistemas de RFID. Logo, algumas das freqüências citadas acima podem não serem válidas no mundo todo. A tabela 9 a seguir mostra algumas das restrições para as freqüências do RFID, bem como a máxima potência permitida.

Country/Region	LF	HF	UHF	Microwave
United States	125134 KHz	13.56 MHz 10 watts effective radiated power (ERP)	902-928 MHz, 1 watt ERP or 4 watts ERP with a directional antenna with at least 50-channel hopping.	24002483.5 MHz, 4 watts, ERP 57255850 MHz, 4 watts ERP
Europe	125134 KHz	13.56 MHz	865865.5 MHz, 0.1 watts ERP, Listen Before Talk (LBT). 865.6867.6 MHz, 2 watts ERP, LBT. 867.6868 MHz, 0.5 watts ERP, LBT.	2.45 GHz
Japan	125134 KHz	13.56 MHz	Not allowed. MPHPT (Ministry of Public Management, Home Affairs, Posts and Telecommunications) has opened up 950956 MHz band for experimentation.	2.45 GHz
Singapore	125134 KHz	13.56 MHz	923925 MHz. 2 watts ERP.	2.45 GHz
China	125134 KHz	13.56 MHz	Not allowed. Future possibility: 840843 MHz and/or 917-925 MHz. SAC (Standardization Administration of China) is entrusted to formulate the RFID regulations.	24462454 MHz, 0.5 watts ERP

Tabela 9 - Restrições para freqüências do RFID. [2]

Já a tabela 10 mostra exemplos das propriedades de alguns materiais diante de ondas de RF. Materiais RF-lucent permitem que as ondas de RF passem por eles, já os RF-opaque e os RF-absorbent não, o que dificulta, mas não impossibilita, a aplicação do RFID em sistemas com objetos que possuam esses materiais

Material	LF	HF	UHF	Microwave
Clothing	RF-lucent	RF-lucent	RF-lucent	RF-lucent
Dry wood	RF-lucent	RF-lucent	RF-lucent	RF-absorbent
Graphite	RF-lucent	RF-lucent	RF-opaque	RF-opaque
Liquids (some types)	RF-lucent	RF-lucent	RF-absorbent	RF-absorbent
Metals	RF-lucent	RF-lucent	RF-opaque	RF-opaque
Motor oil	RF-lucent	RF-lucent	RF-lucent	RF-lucent
Paper products	RF-lucent	RF-lucent	RF-lucent	RF-lucent
Plastics (some types)	RF-lucent	RF-lucent	RF-lucent	RF-lucent
Shampoo	RF-lucent	RF-lucent	RF-absorbent	RF-absorbent
Water	RF-lucent	RF-lucent	RF-absorbent	RF-absorbent
Wet wood	RF-lucent	RF-lucent	RF-absorbent	RF-absorbent

Tabela 10 - Propriedades de materiais diante de ondas de RF. [2]

2 Padronização dos sistemas de RFID

O RFID é uma tecnologia de comunicação via rádio, portanto necessita de regulamentação em vários países. A regulamentação governamental no caso do RFID se faz necessária, por exemplo, para organizar o espectro eletromagnético, através da alocação e do licenciamento de segmentos do mesmo para cada tecnologia; para estabelecer as melhores práticas e os níveis de segurança para cada aplicação, protegendo a saúde das pessoas, como, por exemplo, estabelecendo o nível máximo de exposição de uma pessoa à radiação eletromagnética; bem como para definir o máximo permitido de interferência entre bandas de freqüência. [2]

2.1 Órgãos e Normas aplicáveis

O mundo é organizado em três regiões regulatórias, conforme a figura 45:

- Região 1: Compreende a Europa;
- Região 2: Compreende as Américas;
- Região 3: Compreende a Ásia e a Austrália.

Figura 45 - Regiões regulatórias, segundo o ITU. [1]

Como as maiores empresas que lidam com o RFID estão situadas nos Estados Unidos, na Europa e no Japão, os principais órgãos reguladores mundiais estão situados nesses lugares e têm grande influência no futuro da tecnologia de RFID. No Japão o Ministério do

Gerenciamento Público, Assuntos Regionais, Correios e Telecomunicações (MPHPT) é quem regula o espectro de freqüências. Nos Estados Unidos o FCC (*Federal Communications Commission*) é quem executa essa tarefa. Já na Europa cada país tem seu próprio órgão regulador. Porém a maioria delas está unida em duas organizações – a *European Radiocommunications Commitee* (ERO) e o European *Telecommunications Standards Institute* (ETSI)-, através das quais as responsabilidades são divididas, e ambas estão ligadas à Conferência Européia de Administração de Correios e Telecomunicações (CEPT). [2]

Os as reguladores mundiais são citados na tabela 11 a seguir:

Organização	*Função*
International Telecommunication Union (ITU)	É uma organização internacional estabelecida para padronizar e regular mundialmente o rádio e as telecomunicações. Para o RFID ela divide o mundo em três regiões regulatórias.
European Telecommunications Standards Institute (ESTI), criado pela *European Conference of Postal and Telecommunications* (CEPT)	Regula o RFID na Europa
Federal Communications Commission (FCC)	Regula o RFID nos Estados Unidos
Ministry of Public Management, Home Affairs, Posts and Telecommunications (MPHPT)	Regula o RFID no Japão
Office of the Telecommunications Authority (OFTA)	Regula o RFID em Hong Kong
Standardization Administration of China (SAC)	Regula o RFID na China
EPCglobal	Desenvolve padrões para a rede EPCGlobal
International Organization for Standardization (ISO)	Desenvolve padrões para o RFID e para algumas outras aplicações
Agência Nacional de Telecomunicações (ANATEL)	Regulamenta o uso das freqüências, bem como certifica e homologa todos os produtos que podem ser utilizados no Brasil

Tabela 11 - Órgãos reguladores [1]

Muitos dos sistemas RFID são projetados para utilizarem as bandas ISM (*Industrial-Scientific-Medical*). Inicialmente criadas para o uso não-comercial industrial, científico e

médico, elas vêm sendo utilizadas em várias aplicações comerciais, como em *WLANs*, *Bluetooth* e nos próprios sistemas de RFID. Sendo assim, quem usa essas bandas de freqüências pula as etapas licenciatórias, que seriam obrigados a passar se utilizassem outra banda, visto que as ISM não são reguladas. [2]

Entretanto, como mencionado anteriormente no trabalho, a maioria dos sistemas RFID utiliza as bandas LF, HF, UHF e Microondas. A alocação no espectro dessas bandas não é a mesma no mundo todo. Entre Estados Unidos, Japão, Europa e China existem várias diferenças com relação a esta alocação.

- A banda LF (125kHz – 134kHz) está disponível para uso nos EUA, na Europa e no Japão. O RFID compartilha essa banda com aplicações de navegação da aeronáutica e da marinha.

- Já para a banda UHF há várias diferenças na regulação nos EUA, na Europa e no Japão. No momento o foco das atenções está nessa banda, visto que as principais aplicações em RFID que têm surgido utilizam freqüências nessa faixa.

- A banda de Microondas está disponível em muitos lugares, porém com muitas divergências com relação às regulamentações. Por exemplo, o limite de potência transmitida, em vários lugares, é de 4W, entretanto, no Japão é de apenas 1W. [2]

Padrões ISO

O ISO é uma organização padronizadora internacional, composta por representantes de organizações padronizadoras nacionais. Fundada em 1947, a ISO define padrões industriais e comerciais no mundo todo. A ISO desenvolveu padrões para o RFID nas seguintes áreas:

- Padrões de identificação relacionados à codificação do ID Number ou outras informações contidas nos tags;

- Protocolos de interface aérea que definem as regras de comunicação entre tags e leitores;

- Protocolos de dados para o middleware;

- Padrões para testes, tendências e segurança. [2]

Alguns dos padrões desenvolvidos pela ISO para aplicações RFID estão na tabela 12 a seguir:

Padrão ISO	*Descrição*
ISO/IEC 15961	Troca de informações em um sistema RFID para gerenciamento de itens (Protocolo de dados para interface de aplicação)
ISO/IEC 15962	Regras de codificação dos dados e de funções para memória lógica, para gerenciamento de itens
ISO/IEC 15963	Identificação única para tags RFID
ISO/IEC 18000-*i*	Parâmetros para interface de comunicação aérea em diferentes freqüências de operação
ISO/IEC 18047-*i*	Métodos de teste de equipamentos RFID para diferentes freqüências de operação
ISO/IEC 19762-3	Vocabulário para técnicas de Identificação Automática e Captura de Dados (AIDC)
ISO/IEC 24730-1	Application Program Interface (API) para sistemas de RTLS (Real-Time Locating Systems)

O valor da variável i depende da freqüência de operação do sistema.

Tabela 12 - Padrões ISO para RFID. [1]

Os protocolos de interface aérea definem as regras para comunicação entre leitores e tags. Isto inclui regras sobre:

- Codificação dos dados, modulação e demodulação;
- Comandos de comunicação para executar operações no tag, como leitura, escrita, modificação dos dados, bloqueio das informações, bem como para destruir o tag.
- Algoritmos anti-colisão.

A ISO também desenvolveu padrões para as aplicações do RFID, como:

- **Rastreamento Animal (Utilizando a banda LF):** A ISO desenvolveu dois padrões para esse fim: o ISO 11784 e o ISO 11785. O ISO 11784 define a estrutura do código pra tags utilizados em animais. Os animais podem ser identificados pelo código do país e um único ID nacional. O ISO 11785 define os parâmetros técnicos para a comunicação entre tag e leitores;
- **Cartões de identificação e dispositivos relacionados (Utilizando a banda HF):** Foram desenvolvidos três padrões para tal fim: o ISO 10536, o ISO 14443 e o ISO 15693. Esses são os padrões ISO mais utilizados atualmente, entretanto, são aplicáveis apenas a sistemas HF RFID.

O ISO 10536 define os parâmetros para contactless smart cards, com alcance de leitura de 7-15cm, utilizando 13.56MHz. Esse padrão está dividido em quatro partes. A parte 1 versa acerca das características físicas do cartão; a parte 2, acerca das dimensões e da localização das áreas de acoplamento; a parte 3, acerca dos sinais eletrônicos e dos procedimentos de reset do cartão; e a parte 4, acerca da resposta ao reset e dos protocolos de transmissão.

O ISO 14443 é aplicado a *proximity smart cards*. Esse padrão está dividido em quatro partes. A parte 1 versa acerca das características físicas do cartão; a parte 2, acerca da potência e da interface dos sinais; a parte 3, acerca da inicialização e do sistema anti-colisão; e a parte 4, acerca dos protocolos de transmissão.

O ISO 15693 é aplicado a *vicinity smart cards*. Esse padrão está dividido em quatro partes. A parte 1 versa acerca das características físicas do cartão; a parte 2, acerca da inicialização e da interface aérea; a parte 3, acerca dos protocolos; e a parte 4, acerca dos comandos e de funções de segurança.

- **RFID AIDC (Automatic Identification and Data Capture) e Tecnologias de Gerenciamento de Itens:** Para essas aplicações foram desenvolvidos os padrões ISO 15961, o ISO 15962, o ISO 15963, o ISO 18000 e o ISO 18001.

O ISO 15961 define padrões para a interface de aplicação e para os protocolos de dados. O ISO 15962 define especificações para regras de codificação, funções de memória e protocolos de dados. O ISO 15963 define um sistema de numeração único para os tags. O ISO 18000 está dividido em sete partes, conforme a tabela 13. O ISO 18001 define padrões para a tecnologia de endereçamento de informações.

Parte 1	Parâmetros genéricos para interface de comunicação aérea, para todas as freqüências aceitas mundialmente
Parte 2	Parâmetros para interface de comunicação aérea em 125KHz
Parte 3	Parâmetros para interface de comunicação aérea em 13.56MHz
Parte 4	Parâmetros para interface de comunicação aérea em 2.45GHz
Parte 5	Parâmetros para interface de comunicação aérea em 5.8GHz
Parte 6	Parâmetros para interface de comunicação aérea em 860-930MHz
Parte 7	Parâmetros para interface de comunicação aérea em 433MHz

Tabela 13 - Divisão da norma ISO 18000 [2]

A ISO determina padrões para várias outras áreas. Mas a tecnologia RFID possui um órgão padronizador específico: a EPCglobal. A EPCglobal Inc. é uma joint-venture entre a GS1 (formalmente conhecida como EAN International) e a GS1 US (formalmente conhecido como Uniform Code Council Inc.). A organização EPCglobal foi criada para conseguir a adoção e a padronização da tecnologia EPC no mundo inteiro, de uma forma ética e responsável. A EPCglobal desenvolveu um padrão, aprovado em dezembro de 2004, que pode revolucionar a tecnologia RFID: o EPCglobal Gen 2 (popularmente chamado de Gen 2). Esse padrão é, provavelmente, a forma de avançar no sentido de obter uma padronização dos tags RFID, que é um dos principais problemas atualmente. [2]

2.2 **EPCglobal *Network***

O Auto-ID Center, situado no *Massachusetts Institute of Technology* (MIT), trabalhando em conjunto com líderes da indústria e instituições acadêmicas de várias partes do mundo, desenvolveu um sistema para trazer os benefícios do RFID para a cadeia mundial de suprimentos. Esse sistema compreende o *Electronic Product Code* (EPC), tecnologia RFID e o *software* de suporte baseado nos padrões EPCglobal. Esse sistema é conhecido como *EPCGlobal Network*. A EPC Network é composta, basicamente, por quatro componentes: um objeto com uma etiqueta EPC, um computador rodando Savant, um servidor ONS (*Object Name Service*) e um servidor PML (*Product Markup Language*). O computador Savant e os servidores ONS e PML são conectados à internet e situados bem distantes uns dos outros. A figura 46 ilustra o funcionamento da EPC *Network*.

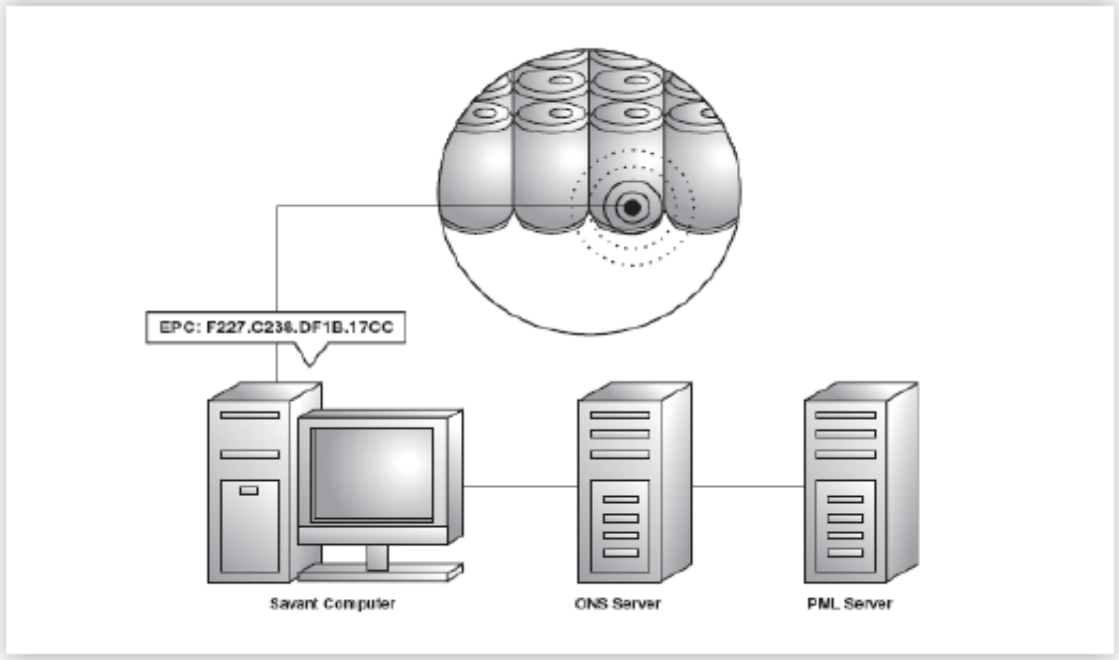

Figura 46 - Funcionamento da *EPC Network* [2]

Em um objeto, como uma lata de refrigerante, é colocada uma etiqueta EPC. Essa etiqueta grava um número, um identificador único, que indica qual o fabricante da lata de refrigerante, bem como um número de série para cada lata em particular. O computador *Savant*, que é, necessariamente, uma rede de leitores e um cliente rodando uma aplicação ou um *software*, lê a etiqueta EPC na embalagem. Esse processo pode ocorrer em qualquer local da cadeia de suprimentos. Vários computadores *Savant* e leitores podem ser instalados

na fábrica, em centros de distribuição, em mercearias ou em grandes redes de varejo. Vamos assumir que esse computador *Savant* esteja instalado em um varejista. Uma vez que ele tenha lido a etiqueta EPC da lata, ele fornece o número dela para o servidor ONS, que atua como o inverso de uma lista telefônica. Ele pega o número EPC e fornece o nome e o endereço da empresa que fabricou a lata de refrigerante, enviando, então, esses dados de volta ao computador *Savant*. O computador *Savant* pode usar esses dados para contatar diretamente o servidor PML da empresa. Se todas as empresas tiverem um site e um servidor web na *EPC Network*, todas elas terão um site PML e um servidor PML. Supondo que o fabricante da lata de refrigerante seja a empresa Soda. O computador *Savant* no varejista irá contatar o servidor PML da Soda, com o número de série único da lata de refrigerante. O servidor PML da Soda, por sua vez, deve conter todos os tipos de informação acerca daquela lata em particular, como a data e o local de fabricação, se o produto foi ou não passado por um *recall*, por quais lugares ele passou ao longo da cadeia de distribuição, etc. O computador *Savant* deve consultar essas informações para estar certo de que a lata de refrigerante está apropriada para venda. Além disso, se ela for a última lata de Soda na prateleira, o computador *Savant* deve solicitar mais produtos. Tudo isso pode ser feito com pouca ou sem qualquer intervenção humana. Esse é, basicamente, o funcionamento da *EPC Network*. [2]

A EPCglobal está desenvolvendo padrões e especificações para os seguintes componentes da *EPC Network*:

- Especificações dos dados de um tag EPC;
- Interface de comunicação para sistema HF e UHF;
- Protocolos de leitura;
- Savant;
- ONS (Object Name Service);
- PML (Physical Markup Language);

2.3 **EPC (*Electronic Product Code*)**

2.3.1 Descrição

EPC é uma família de esquemas de códigos para *tags*. Ele foi projetado para sanar as necessidades de várias indústrias, enquanto, ao mesmo tempo, garante singularidade para todos as *tags* compatíveis com o EPC, chamados *EPC tags*.

2.3.2 Características

Os esquemas dos códigos do EPC tipicamente contêm um número serial único, chamado de *EPC number*, que pode ser utilizado para identificar um objeto. O *EPC number* é estruturado em quatro partes, conforme a figura 48.

A primeira parte é o cabeçalho, composta por 8 bits. O cabeçalho serve para que se identifique o comprimento, o tipo, a estrutura, a versão e a geração do EPC. No caso da lata de refrigerante, citada anteriormente, estaria, por exemplo, a versão do EPC.

A segunda parte é o *EPC Manager*, composta por 28 bits. Ela serve para que se identifique o "*manager*", que, normalmente, é o fabricante do produto. Novamente fazendo a analogia com a lata de refrigerante, o *EPC Manager* seria a "Soda".

A terceira parte é o *Object Class*, composto por 24 bits. Ela serve para identificar precisamente o tipo de produto. Continuando a analogia com o caso da lata, o *Object Class* seria, por exemplo, Diet Soda, 12oz. Can, *U.S. version*.

A quarta e última parte do *EPC Number* identifica o número de série do produto. No caso, seria o número de série da lata de Soda na qual a tag está colocada.

Existem duas versões de tags: uma versão que possui uma memória de 64 bits e outra, que possui uma memória de 96 bits. Tags com maior capacidade de memória podem até serem utilizadas, mas 96 bits já tem se mostrado suficiente para as atuais necessidades mundiais. Um tag de 96 bits, como o mostrado na figura 48, com 28 bits para o *Manager Number*, 24 bits para o *Object Class* e 36 bits para o *Serial Number*, podem identificar 268 milhões de empresas diferentes, cada uma delas tendo mais de 16 milhões de produtos diversos e 68 milhões de números de série para cada tipo de produto. Esses números são mais do que suficientes para cobrir todos os fabricantes mundiais, durante muitos anos. As *tags* de 64 bits foram desenvolvidas para preencher uma necessidade da indústria de produtos mais baratos, visto que tais tags possuem um custo de produção muito mais barato do que as *tags* de 96 bits, e para colaborar com a manutenção do custo inicial da implantação baixo [2]. A seguir, figura 47, um exemplo de um EPC do tipo 1.

Figura 47 - EPC (*Electronic Product Code*) Tipo 1 [2]

2.3.3 **Classificação**

Além das versões em 64 bits e em 96 bits, os *EPC tags* são divididos também em classes, de acordo com a sua funcionalidade, ou se possui, pela alimentação própria. A figura 48 ilustra as classes dos *EPC tags*.

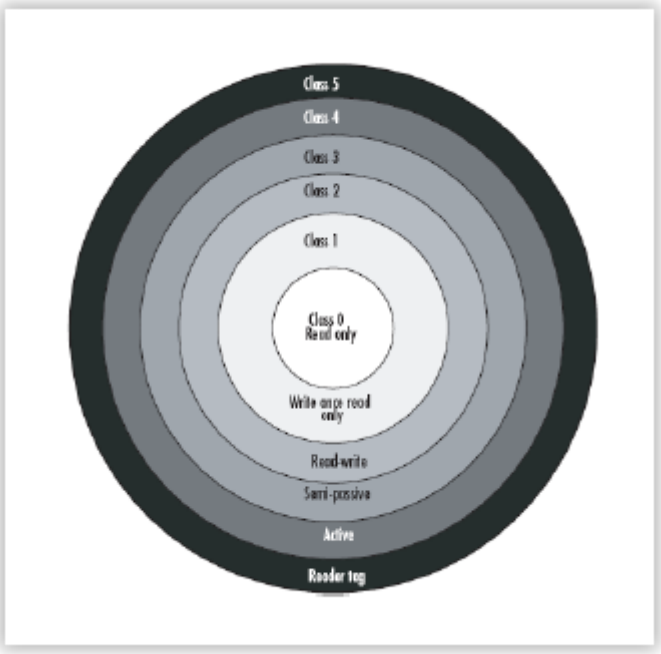

Figura 48 – Classes dos *EPC tags* [2]

As principais características de cada classe estão mostradas na tabela 14.

Classe do tag	*Tipo*	*Memória*	*Comunicação*	*Propriedades*
Classe 0	Passivo	Read-Only	Não inicia comunicação	*EPC Number* é programado durante o processo de fabricação
Classe 0+	Passivo	Write-Once-Read-Many	Não inicia comunicação	Programado uma única vez, pelo usuário final, utilizando o mesmo protocolo da Classe 0
Classe 1	Passivo	Write-Once-Read-Many	Não inicia comunicação	*EPC Number* é programado pelo usuário final
Classe 2	Passivo	Write-Once-Read-Many	Não inicia comunicação	Codificação
Classe 3	Semi-Passivo	Re-Writable	Não inicia comunicação	Capacidades dos Classe 2 mais extras, como sensores integrados
Classe 4	Ativo	Re-Writable	Pode iniciar comunicação; alimenta sua própria comunicação; é possível uma comunicação tag-to-tag	Capacidades dos Classe 3 mais extras
Classe 5	Ativo	Re-Writable	Pode iniciar comunicação; alimenta sua própria comunicação; é possível uma comunicação tag-to-tag	Capacidades dos Classe 4 mais extras

Tabela 14 - Características das classes do EPC[2]

2.3.4 Futuro do EPC

Deve-se notar que as tags EPC não comportam muito mais dados do que símbolos de códigos de barra UPC. Alguns argumentam que o EPC não tira total vantagem dos benefícios oferecidos pela tecnologia RFID. A *EPCglobal* argumenta que esse projeto serve para que se tenha um *tag* EPC de baixo custo. Agora existe a segunda geração das etiquetas EPC, conhecida como *Generation* 2, ou

simplesmente Gen 2, considerando-se que a anterior era a EPC Gen 1. A estrutura de classes das *tags*, a princípio, permanecerá no Gen 2, entretanto as funcionalidades dos mesmos serão aumentadas. Esse remanejamento é motivado, em parte, pelo *Wal-Mart*, *DoD* (US Department of Defense) e outros grandes *players* do mercado, para que hajam estruturas de dados mais flexíveis e seções de memória regraváveis, ao contrário dos números de produtos estáticos existentes na *Gen 1*. O padrão *Gen 2* foi publicado e adotado pela ISO e suas implantações pertencem em sua maioria à banda UHF. A tabela 15 compara algumas características dos padrões *EPC Gen1* e *EPC Gen2*.

Característica	*Generation 1*	*Generation 2*
Freqüência de operação	860-930MHz	860-960MHz
Capacidade de memória	64 ou 96 bits	96-256 bits
Outras características	-	Leitura mais veloz e confiável do que no Gen1

Tabela 15 - Comparação entre *EPC Gen1* e *EPC Gen2*[2]

2.4 Importância da padronização para o desenvolvimento da tecnologia

A padronização de produtos é muito importante para o desenvolvimento de uma tecnologia. Através dela, todos os vendedores seguirão o mesmo padrão para fabricar equipamentos, o que traz uma padronização técnica, que permite a interoperabilidade dos equipamentos. Isso beneficia os consumidores e ajuda os vendedores a desenvolver uma competição mais sadia. Outro importante ponto a ser tocado é que devido aos órgãos padronizadores não estarem seguindo os interesses de determinada empresa, a padronização, geralmente, define uma plataforma mais eficiente para que as indústrias do mercado possam operar e avançar [2].

A criação de padrões também leva aos consumidores uma maior confiabilidade em uma determinada tecnologia, bem como, geralmente, reduz os custos da mesma e facilita a implementação.

2.5 Vantagens e Desvantagens

Regulamentações e padronizações dos sistemas de RFID têm influenciado diretamente no mercado, em várias áreas, incluindo em operações comerciais e na infra-estrutura de TI. Essa influência traz consigo as vantagens e as desvantagens, apesar das primeiras serem, normalmente, muito maiores do que segundas.

Uma das principais vantagens das regulamentações e das padronizações do RFID é que, por exemplo, as regulamentações estabelecem limites com relação à radiação eletromagnética emitida, fazendo, assim, com que diminua o risco de problemas causados pelo excesso de radiação, visto que os limites têm de ser atendidos. As regulamentações

também estruturam o mercado para que haja uma competição sadia, já que evitam a concorrência desleal, onde as empresas colocam vantagens em seus produtos que acarretam, por exemplo, em danos aos usuários (como é o caso de uma exposição à altas taxas de radiação eletromagnética). Assim, as regulamentações fazem com que as empresas produzam produtos diferenciados através de preços mais vantajosos, ou melhores características, ou, ainda, a prestação de serviços aos consumidores. Também pode se observar do ponto de vista de que as regulamentações possibilitam avanços na tecnologia, devido, principalmente, à maior facilidade à entrada de novas empresas no segmento, promovendo, da mesma forma, o empreendedorismo, que pode levar ao desenvolvimento de novidades no setor direta, ou indiretamente. As padronizações do RFID são muito vantajosas, pois, considerando-se que todos os dispositivos serão produzidos seguindo os mesmos padrões, eles se tornarão interoperáveis entre si, o que trará benefícios aos consumidores e, também, aos vendedores. Outra vantagem é que eles tendem a reduzir o custo das aplicações e facilitar a implementação, bem como tendem a desenvolver nos consumidores uma maior confiança na tecnologia.

Uma das desvantagens das regulamentações e das padronizações do RFID está relacionada com a diminuição do alcance de leitura das tags, devido à imposição de limites de potência emitida. Essa desvantagem afeta principalmente as aplicações com *tags* passivas, tendo em vista que essas necessitam da energia provinda do leitor para energizar seu circuito. Logo, se a potência emitida pelo leitor é limitada em um valor mais baixo, o alcance da leitura de tal *tag* será diminuída. As regulamentações também influenciam negativamente no que diz respeito às freqüências de operação, já que, devido à diferença entre as regiões do planeta, um determinado equipamento RFID que funciona em uma dada região, pode não funcionar em outra.

3 TECNOLOGIA *RFID* X *BarCode (Código de Barras)*

Um código de barras é um esquema no qual símbolos impressos representam informações. Tais símbolos geralmente são compostos de barras verticais, espaços, retângulos e pontos. Um método que codifica caracteres alfanuméricos usando esses símbolos é chamado de simbologia. Duas simbologias podem usar os mesmos ou diferentes símbolos para codificar um mesmo caractere. Em torno de 270 simbologias diferentes foram inventadas para suportar requisitos específicos e, aproximadamente, 50 são amplamente utilizadas hoje. As simbologias são classificadas em: linear, bi-dimensional e tri-dimensional.

A simbologia linear consiste em linhas verticais, com diferentes larguras e com espaços em branco separando duas linhas adjacentes. O número máximo de caracteres que pode ser codificado com uma simbologia linear é 50.

A simbologia bi-dimensional tem a maior capacidade de armazenamento de dados. O número máximo de caracteres que podem ser codificados com a simbologia de código de barras bi-dimensional é 3750.

Uma simbologia tri-dimensional é um código de barras em alto-relevo impresso em uma superfície. Um código de barras tridimensional não depende, assim, do contraste entre as linhas do código de barras e seus espaços para que a leitura seja efetuada. Este tipo de

código de barras pode ser sujeito a condições adversas do ambiente, enquanto um papel com um código de barras impresso, em situações ambientais semelhantes, pode ser facilmente destruído.

Leitores

O princípio de funcionamento de um leitor de código de barras, também chamados *scanner*, é através de um feixe de luz, conforme a figura 50. A direção do escaneamento é irrelevante, entretanto, durante a leitura, o feixe de luz não pode se mover para fora da região onde está o código de barras. Logo, geralmente, quanto maior o comprimento do código de barras, menor tem de ser a distância do leitor para que o escaneamento seja efetuado corretamente. Durante o processo de leitura o *scanner* mede a intensidade da luz refletida pelas regiões pretas e brancas, no caso de barras verticais. As barras pretas absorvem a luz, enquanto que as brancas, ou os espaços, refletem a luz. Um dispositivo eletrônico chamado fotodiodo, ou fotocélula, traduz esse padrão luminoso em uma corrente elétrica, ou em um sinal analógico. Circuitos elétricos, então, decodificam essa corrente em dados digitais (caracteres ASCII), dados esses que foram originalmente codificados pelo código de barras.[2] A seguir, figura 49, um ilustração do funcionamento do *BarCode*

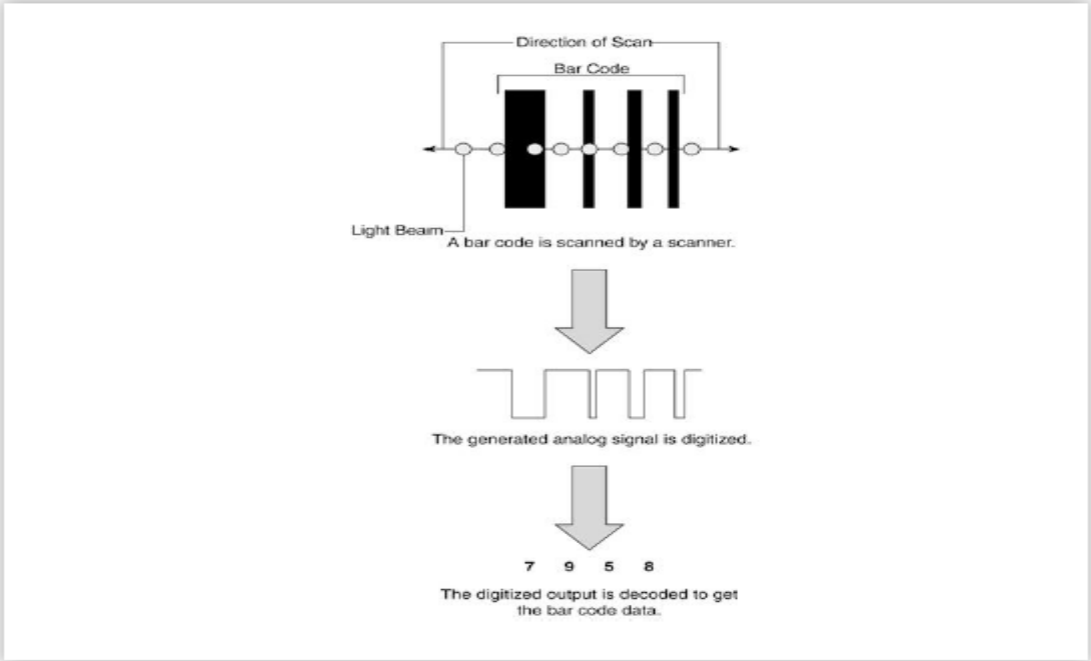

Figura 49 - Funcionamento de um leitor de código de barras [2]

Alguns dos tipos de leitores são as canetas, os à *laser*, os CCD (Charged Coupled Device) e as câmeras.

O leitor tipo caneta, mostrado na figura 50, é o mais barato e o mais leve, devido à não-existência de partes móveis (o usuário efetua a leitura manualmente). Por sua pequena área de leitura, o código de barras necessita estar em contato com o leitor durante todo o processo de escaneamento. Outra desvantagem desse tipo de leitor é mostrada quando um

código de barras é colocado em um objeto rugoso. Devido à necessidade do total contato entre o leitor e o código, se a superfície não é suficientemente plana o leitor pode não capturar os dados corretamente. [2] A seguir, figura 50, a imagem de um leitor do tipo caneta.

Figura 50- Leitor de código de barras, tipo caneta [2]

O leitor à *laser*, mostrado na figura 52, é o mais utilizado. Um *laser* localizado dentro do leitor automaticamente escaneia o código de barras. Uma das vantagens desse tipo de leitor é a sua capacidade de ler um código de barras mesmo se ele não estiver em uma superfície lisa. Ele consegue isso porque é possível focar seu feixe de luz em um ponto muito pequeno. Com isso, geralmente, apenas um escaneamento é necessário para ler um código de barras. Portanto, esse tipo de leitor pode ler códigos de barra a uma alta taxa, mesmo que o código esteja com uma má qualidade. Esse leitor é freqüentemente utilizado em indústrias, onde um objeto que possua um código de barras se move a uma velocidade constante. A distância máxima de leitura para um leitor à *laser* é em torno de 9 m. [2] A seguir, figura 51, imagem de um leitor à *laser*.

Figura 51 - Leitor de código de barras, à *laser* [2]

O leitor CCD, mostrado na figura 52, pode ler um código de barras sem ter contato com o produto, mas a uma distância próxima. Seu princípio de funcionamento é baseado em uma matriz de centenas de pequenos sensores de luz que está localizada na frente do leitor. Quando a imagem do código de barras é projetada nestes sensores, eles geram um padrão de voltagem. Esse padrão é idêntico ao padrão gerado pelo leitor à *laser*. Alguns desses sistemas utilizam fontes adicionais de luz, como um flash, para aumentar a distância focal. A máxima distância de leitura para esse tipo de leitor, e essa é sua principal desvantagem, é algo em torno de 15 cm, devido ao seu limitado campo de visão. O número de sensores luminosos no leitor é que determina o contraste mínimo necessário para que a leitura seja efetuada. [2]

Figura 52 - Leitor de código de barras, CCD [2]

Os leitores do tipo câmera, como o mostrado na figura 53, são os resultados dos últimos avanços na tecnologia do código de barras. Uma pequena câmera dentro do leitor captura a imagem do código de barras. Essa imagem é, então, processada usando tecnologia de processamento de imagens digital para determinar o conteúdo do código de barras. Uma desvantagem desse tipo de leitor é que ele é muito sensível quanto à qualidade do código de barras. Ou seja, um contraste insuficiente entre os símbolos brancos e pretos ou um espaço vazio podem comprometer a leitura. O leitor tipo câmera vêm se tornando cada vez mais barato, menor e mais veloz. Com isso, um grande número de usuários está substituindo seus scanners à laser pelos do tipo câmera. [2]

Figura 53 - Leitor de código de barras, tipo câmera. [2]

Simbologias de *BarCode* Lineares

- ***UPC (Uniform Product Code)***

O UPC , *Uniform Product Code*, é uma simbologia de código de barras dirigido pelo UCC, *Uniform Code Council*. Os dois maiores tipos de UPC são o UPC-A e o UPC-E.

O UPC-A consiste de 12 dígitos, dos quais o último é utilizado com um dígito de checagem; o primeiro representa o tipo do produto; os próximos cinco dígitos, o código do fabricante; e os cinco dígitos subseqüentes identificam o produto atual. Essa simbologia é a que é amplamente utilizada nas redes de varejo.

O UPC-E, mostrado na figura 55, consiste de sete dígitos, dos quais um é usado como dígito de checagem. Essa simbologia também é chamada de UPC com zeros suprimidos, porque ele pode comprimir um código UPC-A em um código de seis dígitos, suprimindo os zeros para o código do fabricante e controlando os zeros do produto atual. O sétimo dígito é usado como um dígito de checagem para os primeiros seis. Sendo assim, o UPC-E sempre pode ser convertido de volta a um UPC-A. Essa simbologia é utilizada em pequenos varejistas.

Tanto o UPC-A, quanto o UPC-E podem ser acrescidos de um código de dois ou cinco dígitos, conforme as figuras 54 e 55. Normalmente as publicações ou os periódicos contém esse acréscimo. A seguir, figuras 56, exemplo de código de barras UPC-E +5.

Figura 54- Exemplo de código de barras UPC-E [2]

Figura 55 - Exemplo de código de barras UPC-A +2 [2]

Figura 56 - Exemplo de código de barras UPC-E +5 [2]

- ***EAN (European Article Numbering)***

O EAN, *European Article Numbering*, é a versão européia do UPC. Os dois principais tipos do EAN são o EAN-13, mostrado na figura 57, e o EAN-8, mostrado na figura 58.

Figura 57 - Exemplo de código de barras EAN-13. [2]

A seguir, figura 61, exemplo de código de barras EAN-8.

Figura 58 - Exemplo de código de barras EAN-8 [2]

O EAN-13 é a simbologia européia equivalente ao UPC-A. Comparado ao UPC-A, um símbolo EAN-13 contém um dígito adicional, que, juntamente com o vigésimo dígito, representa o código do país. Essa simbologia é muito utilizada nas publicações, para representar os números ISBN dos livros. Um código ISBN é um código de barras EAN-13 com os três primeiros dígitos sendo 978 e os demais nove dígitos representando os primeiros nove dígitos do número ISBN. [2]

O EAN-8 consiste de oito dígitos, dos quais os dois primeiros são utilizados para o código do país. Os próximos cinco dígitos são usados para dados e o último, como dígito de checagem.

Da mesma forma que no UPC, o código EAN também pode ser acrescido de mais dois ou cinco dígitos, tanto no EAN-13, como no EAN-8. Quem utiliza esse acréscimo são, assim como no UPC, os periódicos e as publicações. Nos códigos ISBN, esses números suplementares começam com 5, sendo que os quatro dígitos restantes são utilizados para codificar o preço do livro.

Também há outras simbologias, como a simbologia linear Code 128, que utiliza letras e números, mostrado na figura 59, e as bi-dimensionais PDF417, que consiste de pequenos códigos de barra sobrepostos podendo representar até 2525 caracteres, mostrado na figura 60, Aztec Code, que é formado por vários blocos e pode representar até 3750 caracteres, como mostrado na figura 61, e DataMatrix, que pode codificar até 3116 caracteres, mostrado na figura 62.

Figura 59 - Exemplo de código de barras *Code 128* [2]

Figura 60 - Exemplo de código de barras *PDF417* [2]

Figura 61 - Exemplo de código de barras *Aztec Code* [2]

Figura 62 - Exemplo de código de barras *DataMatrix* [2]

Cada uma das soluções, tanto RFID, quanto *BarCode*, tem seus prós e contras. As vantagens que o *BarCode* tem sobre os sistemas de RFID são:

- **Baixo custo:** O custo de implementação de uma solução de *BarCode* é, geralmente, muito menor do que o de uma solução equivalente utilizando RFID;

- **Precisão:** Em alguns casos, a precisão da leitura em uma solução de *BarCode* é a mesma, se não maior, do que em uma equivalente de *RFID*. Os sistemas de código de barras possuem precisões de leitura em torno de 95%, enquanto que no *RFID* chega-se a 80%;

- **Independe do material:** Um sistema de código de barras pode ser utilizado com sucesso em qualquer tipo de material, ao contrário do RFID, que tem problemas com a leitura em materiais metálicos ou em embalagens que contenham líquidos;

- **Maturidade:** A tecnologia de *BarCode* existe há mais de 30 anos, sendo, provavelmente, a tecnologia mais amplamente empregada no mundo. Durante esse tempo, mais de 50 padrões foram desenvolvidos, dentre esses, alguns que tem aceitação mundial;

Já as vantagens do *RFID* com relação ao *BarCode* são:

- **Dinamismo:** Os dados de um tag *RFID* podem ser reescritos em torno de 10.000 vezes (assumindo um tag RW). Já os dados em um código de barras são inalteráveis; cada vez que se fizer necessário alterar algum dado, um novo código de barras precisará ser gerado;

- **Linha de visada:** Normalmente um leitor *RFID* não precisa de uma linha de visada para ler os dados contidos em um *tag*. Já os leitores de código de barras sempre precisam de uma linha de visada para efetuar a leitura corretamente;

- **Alcance de leitura:** Uma *tag RFID* pode ter uma distância de leitura muito maior do que a de um *BarCode*. Dependendo de alguns fatores, esse alcalce vai de alguns centímetros a centenas de metros;

- **Capacidade de armazenamento:** Um *tag RFID* pode armazenar muito mais informações do que um código de barras;

- **Múltiplas leituras:** Um leitor de *RFID* pode ler um número muito grande de *tags* de uma só vez. Um leitor de código de barras, entretanto, lê um código por vez;

- **Durabilidade:** Um *tag RFID*, geralmente, é robusta, resistindo à condições adversas do ambiente. Já o código de barras é facilmente danificado, por exemplo, por sujeira;

- **Duplicidade:** Um *tag RFID* é muito mais difícil de ser duplicado, quando comparada a códigos de barras;

Também existem as desvantagens que são comuns aos dois sistemas. Duas das principais são:

- **Presença de obstáculos:** Conforme dito anteriormente, um leitor de código de barras precisa de uma linha de visada para efetuar a leitura corretamente. Portanto, se houver qualquer tipo de obstáculo entre o leitor e o código de barras, a leitura não é feita. No caso do *RFID*, dependendo da freqüência utilizada e alguns outros fatores, como a potência transmitida, um leitor pode não estar apto a ler uma *tag*, caso haja, entre o leitor e a *tag*, materiais *RF-opaque*, como o metal, ou *RF-absorbent*, como a água;

- **Presença de umidade:** Para os leitores de código de barras, a presença de partículas de água no ambiente podem provocar a distorção da luz necessária para efetuar a leitura, através da refração. Para o caso dos leitores de *RFID* operando em UHF ou em Microondas, as partículas de água podem absover a energia RF, resultando em energia insuficiente para atingir os tags para que a transferência de dados seja efetuada.

4 UNIVERSO DE APLICAÇÃO DA TECNOLOGIA RFID(ASPECTOS ATUAIS)

4.1 USO DA TECNOLOGIA RFID NO TRANSPORTE URBANO.

O transporte urbano é um dos setores onde existe grande aplicabilidade dos sistemas de RFID, particularmente de *contactless smart cards*. Muitas empresas de transporte ainda operam com altos custos operacionais. Devido à redução dos recursos financeiros, há a necessidade de adotar soluções que reduzam tais custos. O uso dos *contactless smart cards* como sistema de passe eletrônico, também chamado de bilhetagem eletrônica, contribui muito para essa situação, além de contribuir com o conforto e a agilidade do sistema de transporte.

Esse tipo de aplicação se baseia, sinteticamente, na substituição dos bilhetes de papel por um *contactless smart card* e na instalação de um leitor no ônibus, metrô ou trem. Esse *smart card* porta informações do usuário, como informações pessoais, e armazena os créditos que são convertidos em passagens. Um problema crítico nos sistemas de bilhetagem eletrônica é o tempo tomado para aquisição dos créditos ou para a verificação do cartão, principalmente quando se trata da bilhetagem em ônibus e trens, onde a checagem do cartão e a passagem só podem ser efetuadas dentro do veículo. Apesar disso, as soluções utilizando

RFID, como as com *contactless smart card* levam ampla vantagem quando comparadas a outros sistemas. A tabela 4.1 mostra os tempos de processamento, aproximados, para diferentes tecnologias. [2]

Tecnologia	***Tempo de processamento (s)***
RFID (*Contactless Smart Card*)	1.7
Verificação visual pelo cobrador	2
Smart Cards com contato	3.5
Dinheiro	>6

Tabela 16 - Tempos de processamento para diferentes tecnologias [2]

O funcionamento do sistema de transporte urbano é descrito pela figura 63, a seguir:

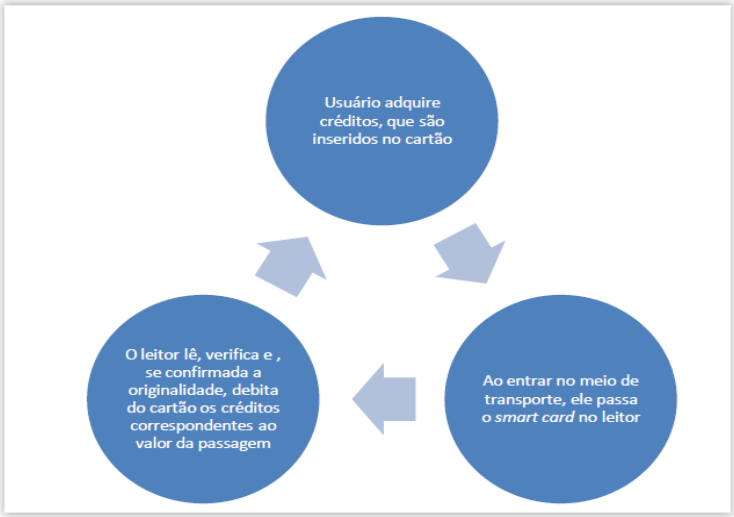

Figura 63 - Funcionamento do sistema de transporte urbano [2]

Alguns pontos importantes a se destacar nesta solução são a segurança da informação contida no cartão, que está criptografada através de algoritmos como o 3DES, AES e RSA, a portabilidade do cartão, visto que seu tamanho é semelhante ao de um cartão de crédito, a dificuldade de se falsificar um *smart card* e a resistência tanto do leitor, quanto do cartão, já que este último é projetado para uma vida útil de mais de 10 anos, resistindo à umidade, ao frio, à areia e à sujeira.

Sendo assim, há poucas desvantagens ao se implantar um sistema de bilhetagem eletrônica. O principal é o custo da solução, que é elevado quando comparado com o tradicional sistema de bilhetes. Porém, esse custo é rapidamente recuperado quando da instalação do sistema, pois haverá uma significativa redução dos custos operacionais.

São muitas as vantagens da bilhetagem eletrônica através de *smart cards*:

- **Para os passageiros:** Não há mais a necessidade de portar dinheiro; os *smart cards* podem ser recarregados com grandes quantias; os cartões continuam válidos quando da mudança das passagens; o passageiro não precisa saber a tarifa exata, nem portar diversos tipos de bilhete para utilizar transportes com tarifas diferentes, pois o sistema deduz do cartão a quantia correta.

- **Para os motoristas:** Quando da cobrança direta ao motorista, o sistema eletrônico evita o desvio da atenção do mesmo, para efetuar a venda da passagem; não há mais o porte de dinheiro no interior do veículo, evitando a ação de ladrões; não há mais a necessidade de efetuar o cálculo do balanço diário: o sistema faz isso automaticamente.

- **Para as empresas de transporte:** Redução dos custos de operação e manutenção de equipamentos de venda de bilhetes, como os existentes no exterior; maior facilidade para alterar o valor das tarifas, pois não precisa imprimir novos bilhetes; redução da dos roubos nos veículos, visto que não haverá mais o porte de dinheiro no interior dos mesmos; e a eliminação da falsificação dos bilhetes.

- **Para o governo:** Redução da necessidade de subsídios para o setor, devido à redução de custos.

Sistemas de tarifas

Normalmente o sistema de transporte de uma cidade é dividido em várias zonas e baseado em diferentes meios de transporte, como ônibus, trens, metrôs, etc. Isso dificulta muito para os passageiros, visto que precisam portar diferentes bilhetes, cada um custando um determinado valor e para um determinado itinerário ou meio de transporte. Os sistemas de bilhetagem eletrônica facilitam nesse ponto também, pois podem ser criadas diferentes formas de cobrança da tarifa, sendo que o usuário precisa portar apenas o seu *contactless smart card*. Quatro das principais formas de cobrança são:

- **Sistema de Tarifas 1:** Pagamento é efetuado no início da viagem. Uma quantia fixa é deduzida do *contactless smart card*, independentemente da distância percorrida. [2]

- **Sistema de Tarifas 2:** No começo da viagem, um *log* do momento do embarque é gravado no *contactless smart card*. Quando o usuário desembarca, a tarifa é automaticamente calculada e deduzida do cartão, de acordo com a distância viajada. Além disso, o cartão pode ser verificado a cada baldeação, para checar a existência de um *log* de embarque válido. Para coibir tentativas de manipulação, a inexistência de um *log* de saída pode ser penalizada pela dedução da tarifa máxima no começo da próxima viagem. [2]

- **Sistema de Tarifas 3:** Esse modelo é melhor aplicado à redes interligadas, nas quais a mesma rota pode ser viajada utilizando-se diferentes sistemas de transporte, à diferentes tarifas. Toda vez que o passageiro muda de veículo, uma quantia pré-determinada é deduzida do cartão; tarifas promocionais para viagens de longa distância e pessoas com tarifas especiais podem ser automaticamente descontadas do cartão. [2]

- **"*Best Price Calculation*":** Nesse sistema todas as viagens feitas são gravadas no cartão por um mês. Se um certo número de viagens for excedido, durante um dia ou um mês, então o cartão pode automaticamente utilizar uma tarifa bônus, durante um dia ou um mês. Isso dá ao consumidor máxima flexibilidade e as melhores tarifas possíveis. O cálculo do melhor preço aumenta o relacionamento com o consumidor e contribui muito para sua satisfação. [2]

A figura 64 abaixo mostra um exemplo de utilização que envolve duas viagens de ônibus e uma de metrô, com a demonstração dos locais onde são efetuadas leituras/escritas nos cartões – pode-se verificar que o número de passagens a serem cobradas depende do tipo de sistema de tarifas utilizado.

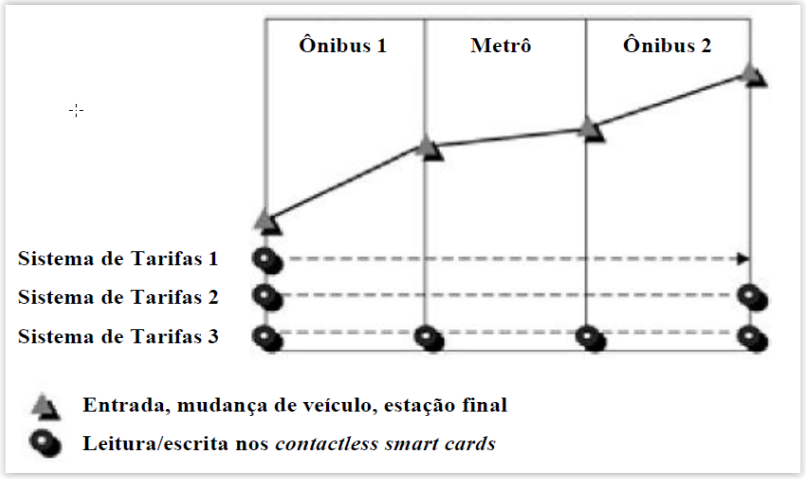

Figura 64 - Exemplo de utilização do sistema de transporte urbano [2]

Potencial de mercado

Estima-se que algo em torno de 50% do total de *contactless smart cards* vendidos no mundo são utilizados no setor do transporte público. As maiores áreas de utilização são, por exemplo, Seul, Hong Kong, Paris, Berlim e Londres [10]. No Brasil, São Paulo foi a cidade pioneira no sistema de bilhetagem eletrônica. A implantação do chamado "Bilhete Único" se deu em 2004. Hoje o **sistema** integra os serviços de ônibus, trens e metrôs que cortam a cidade e é a maior aplicação do gênero no Brasil, valendo-se de mais de 15.000 leitores e com mais de 10.700.000 *contactless smart cards* em circulação. Tal sistema tem integração temporal (2 horas), durante a qual o usuário pode utilizar quantas passagens forem necessárias, sendo que será debitada do seu cartão apenas uma. Em outros sistemas

implantados no Brasil já há a facilidade da aquisição dos créditos pela internet, além dos postos credenciados. [2]

4.2 USO DA TECNOLOGIA RFID NO CONTROLE DE ACESSO.

Sistemas de controle de acesso eletrônico, utilizando suportes de dados são usados para verificar automaticamente a autorização de acesso de indivíduos em edifícios, (comercial ou evento) instalações ou individuais. Ao projetar tais sistemas é preciso primeiro diferenciar entre dois fundamentalmente diferente sistemas com propriedades correspondentes: sistemas *on-line* e *off-line*.

4.2.1 Sistemas *on-line.*

Sistemas *on-line* tendem a ser usados quando a autorização de acesso de um grande número de pessoas deve ser verificada em apenas algumas entradas. Este é o caso, por exemplo, nas entradas principais para escritório edifícios e instalações comerciais. Neste tipo de sistema, a todos os terminais estão ligados a um centro computador por meio de uma rede. O computador central é executada um banco de dados em que cada um dos terminais é atribuído todos os suportes de dados autorizados para o acesso a esse terminal. Os dados de autorização gerado a partir da base de dados é carregado nos terminais (ou para uma unidade de comando da porta intermédiária) através da rede e é memorizado na unidade de uma tabela.

Mudanças na autorização de acesso de um indivíduo pode ser feita por uma única entrada no computador central do sistema de controle de acesso. O próprio suporte de dados não necessita de estar presente, desde unicamente uma entrada na base de dados central tem de ser editado. Isto é vantajoso, porque isso significa que áreas de segurança sensíveis podem ser protegidas contra o acesso não autorizado, mesmo no caso de um conjunto de dados da portadora sendo perdidos.

Os suportes de dados de um sistema *online* só tem que ser capaz de armazenar uma pequena quantidade de dados, por exemplo um número único de passe. O uso de *transponders* de *read-only*, também é possível.

4.2.2 Sistemas *off-line.*

Sistemas off-line tornaram-se prevalecentes, principalmente em situações em que muitos quartos individuais, a que apenas algumas pessoas têm acesso, devem estar equipados com um sistema de controle de acesso eletrônico. Cada terminal salva uma lista

de identificadores de chave (ex: 'general-chave-3', 'chão garçom-7', 'guest-room- 517 '), por que o acesso a este terminal deve ser autorizado. Não existe uma rede para outros terminais ou um computador central.

A seguir na figura 65 controle de acesso usando relógio com *transponder* integrado.

Figura 65 - Controle de acesso e tempo de manutenção são combinados em um único terminal. O relógio com um *transponder* integrado executa a função de um suporte de dados sem contato.

A seguir mais um exemplo de sistema *off-line*, figura 66.

Figura 66 - Do terminal off-line integrado em uma placa de porta. A trava é liberada, segurando o *transponder* autorizado em frente do mesmo. A porta pode então ser aberta pelo acionamento do punho.

Informação sobre os quartos para que o suporte de dados possa fornecer acesso é armazenado nos dados própria transportadora sob a forma de uma tabela de identificadores de chave (por exemplo, 'guest-room-517 "," sauna ","-sala de fitness'). O terminal compara

todos os identificadores de chave armazenados num suporte de dados com os armazenados na sua própria lista e permite o acesso assim que for encontrada uma correspondência. O transponder é programado em um centro de estação de programação, por exemplo na recepção de um hotel com a chegada do hóspede. Além para os quartos autorizados, o transponder também pode ser programado com o prazo de validade, de modo que as chaves de hotel, por exemplo, são automaticamente invalidadas na data da partida do hóspede.

Só no caso de um portador de dados serem perdidos faz os identificadores de chave precisar serem excluídos do terminal em questão, utilizando um dispositivo de programação adequado.

Sistemas *off-line* oferecem as seguintes vantagens sobre os sistemas convencionais de bloqueio com chave e cilindro:

- Especificação antecipada em um plano de bloqueio no sentido normal não é necessário. O sistema é inicialmente codificado para o uso como um 'local de construção. Quando o site for entregue, os terminais de porta são recodificados para utilização comercial por meio de uma interface de infravermelhos. As alterações subsequentes e expansões faz não levantar quaisquer problemas;
- A opção de programação de janelas tempo abre novas opções: trabalhadores temporários podem receber uma «chave de três meses", os suportes de dados de pessoal de limpeza podem ser dadas especificações de tempo precisos;
- A perda de uma chave não causa problemas. Os dados da chave perdida é excluído das estações de leitura, uma nova chave é programada, e os dados dessa chave é inserido nos terminais em questão.

4.2.3 – *Transponders*

Controle de acesso usando cartões de PVC tem sido usado por um longo tempo. Os cartões perfurados foram utilizados inicialmente, os quais foram substituídos por passes de infravermelhos (IR) de código de barras, passes de banda magnética, *Wiegand* passe (tiras de metal magnético), e finalmente cartões inteligentes dotados de um microchip. A principal desvantagem destes processos é o inconveniente do Processo de funcionamento devido ao fato de os cartões deverem ser sempre inserido num leitor, a correta maneira de usar. O controle de acesso que utiliza sistemas sem contato permite uma flexibilidade muito maior porque o transponder só necessita de passar a uma curta distância a partir da antena do leitor. Os passes podem ser feitos na forma de cartões inteligentes sem contato, chaveiros, e até mesmo relógios de pulso. [1]

A grande vantagem dos sistemas de controle de acesso sem contato é que o leitor é livre de manutenção e não é influenciado pela poeira, sujeira ou umidade. A antena pode ser montada por baixo da superfície de uma parede, onde é completamente invisível e protegida contra o vandalismo. Leitores mãos-livres também estão disponíveis para montagem em

catracas ou para aumentar a conveniência. Nesses projetos, os *transponders* não precisam mesmo de ser removidos do clipe de bolso ou jaqueta. [1]

A seguir, na figura 67, um exemplo de sistema *off-line* para proteção de um cofre de hotel.

Figura 67 - O cofre do hotel com um terminal *off-line* integrado só pode ser aberto por um portadora autorizado de dados. [1]

Aletas do gato operadas por um *transponder* na coleira do gato representam outra aplicação no campo de controle de acesso, assim como o uso de *transponders* somente leitura como sensores anti-roubo para a abertura ou fechamento de portas e janelas. [1]

4.3 USO DA TECNOLOGIA RFID NA IDENTIFICAÇÃO DE ANIMAIS;

4.3.1 CONSERVAÇÃO DE ESTOQUE

Sistemas de identificação eletrônica têm sido utilizados na manutenção de estoque por quase 20 anos e são agora o estado de arte na Europa. Além de aplicações internas para fornecimento automático e cálculo da produtividade, esses sistemas também podem ser usados na identificação interna da empresa, para o controle de epidemias e da garantia de qualidade, e para rastrear a origem dos animais. A transmissão de dados unificados necessária e os procedimentos de codificação são fornecidos pelas normas ISO 11784 e ISO 11785 de 1996. A frequência é especificada em 134,2 kHz, e o FDX ou o SEQ transponders podem ser usados. [1]

A seguir na figura 68 alguns exemplos de *transponders(tags)* usados na identificação de animais, comparação de tamanho de variações diferentes de transponders de identificação eletrônica dos animais.

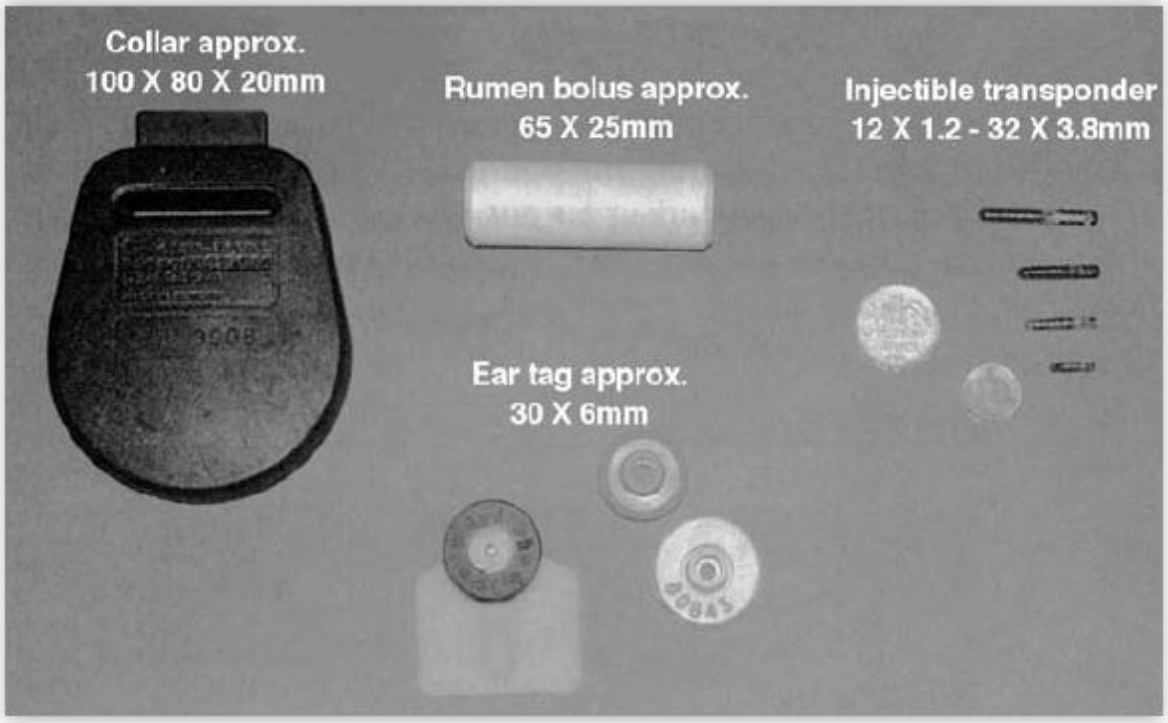

Figura 68 – Exemplos de *tags* usadas na identificação de animais: colar *transponder*, bolus ruminal, marcas auriculares com *transponder*, *transponder* injetável.

Existem quatro procedimentos básicos para fixar o transponder nos animais: transponders colarinho, transponders orelha tag, transponders injetáveis e o chamado bolus (Figura 69). A seção transversal de diferentes tipos de transponders são mostrados na Figura 70. [1]

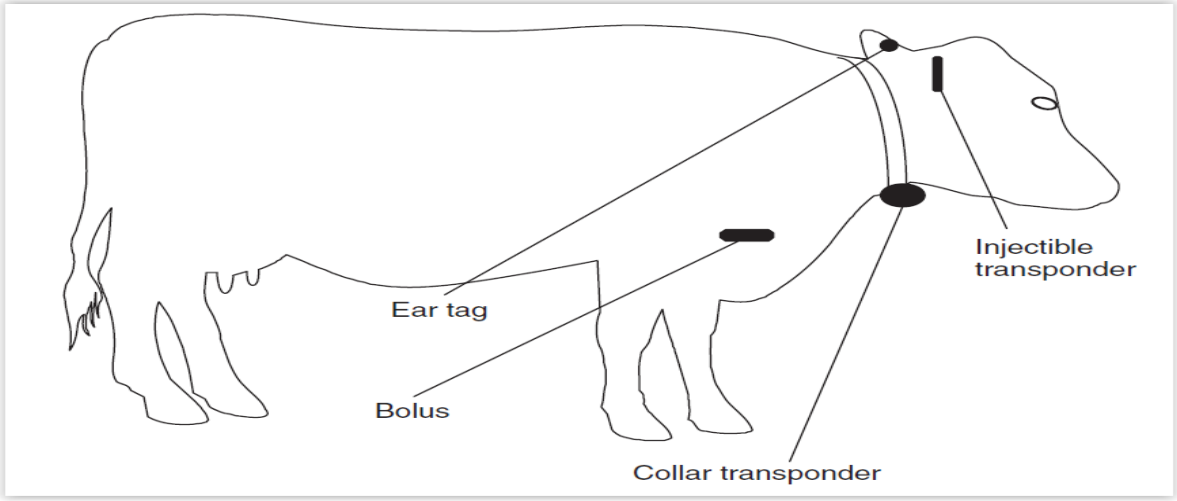

Figura 69 - As opções para a fixação do transponder em uma vaca. [1]

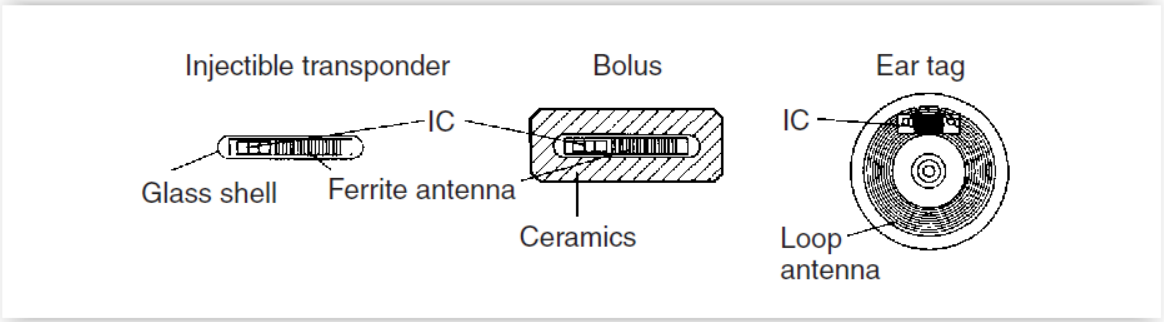

Figura 70 - As seções transversais de vários projetos de transponder para identificação de animais [1]

A seguir , figura 71, diferentes tamanhos de *transponder* injetáveis.

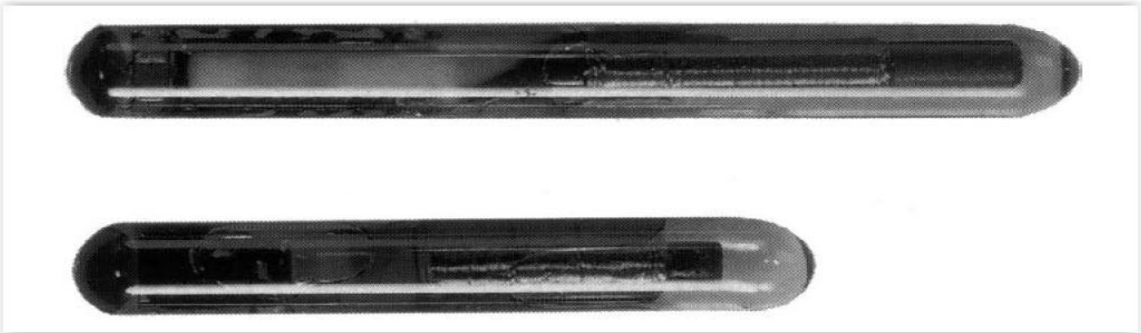

Figura 71 – A largura dos diferentes tipos dos *transponders* de vidro. [1]

Transponders colar pode ser facilmente transferido de um animal para outro. Isto permite a utilização deste sistema dentro de uma empresa. As aplicações possíveis são a alimentação automática em uma tenda de alimentação e medir a produção de leite. [1]

As marcas auriculares incorporam um *transponder RFID* que competem com as marcas auriculares de código de barras muito mais baratas. No entanto, este último não é adequado para automação total, em virtude de as etiquetas de código de barras de ouvido

terem que ser passadas a poucos centímetros de um leitor de mão para identificar o animal. Marcas auriculares *RFID*, por outro lado, pode ser lida a uma distância de até 1 m. [1]

Transponders injetáveis foram utilizados pela primeira vez a cerca de 10 anos atrás. Neste sistema, o *transponders* está colocado sob a pele do animal utilizando uma ferramenta especial. Uma ligação fixa é assim feita entre o corpo do animal e o *transponder*, o qual só pode ser removido por uma operação. Isso permite o uso de implantes em aplicações internas das empresas, tais como a verificação da origem e do controle de epidemias. [1]

O implante é na forma de um transponder de vidro de comprimento 10, 20 ou 30 milímetros (figura 71). O *transponder* é fornecido numa embalagem esterilizada ou com uma dose de desinfectante. As dimensões do *transponder* de vidro são incrivelmente pequenas, considerando que eles contêm o chip e uma bobina em torno de uma vareta de ferrite. Um formato típico é 23,1 × 3,85 milímetros. [1]

Vários instrumentos e agulhas de injecção estão disponíveis para executar a inserção:

Dispositivos de *'Single-shot'* usam agulhas ocas apertadas ('O' SHAPE), que são carregadas individualmente. Agulhas de uso único contendo transponders em um pacote estéril também estão disponíveis. As agulhas ocas são afiadas na ponta, de modo que a pele do animal é rasgada quando a agulha está sendo inserida. A parte superior sem corte da ponta da agulha pressiona a borda do corte da pele de um lado para que o ponto de inserção seja coberto de novo, quando a agulha tiver sendo removida, permitindo que a ferida cicatrize rapidamente. [1]

O dispositivo 'multi-shot' tem um compartimento para vários transponders, dispensando assim a necessidade de recarregar o dispositivo. Agulhas ocas abertas (em forma de U) são utilizadas, uma vez que estas são mais fáceis de limpar, desinfetar e verificar que as agulhas ocas fechadas podem ser usadas várias vezes. [1]

A seguir são mostradas duas figuras 72 e 73 que mostram um transponder sendo injetado em uma vaca e uma cabine de ordenha onde se calcula a produção de leite e se identifica automaticamente os animais respectivamente.

Figura 72- A injecção de um transponder sob a scutulum de uma vaca [1]

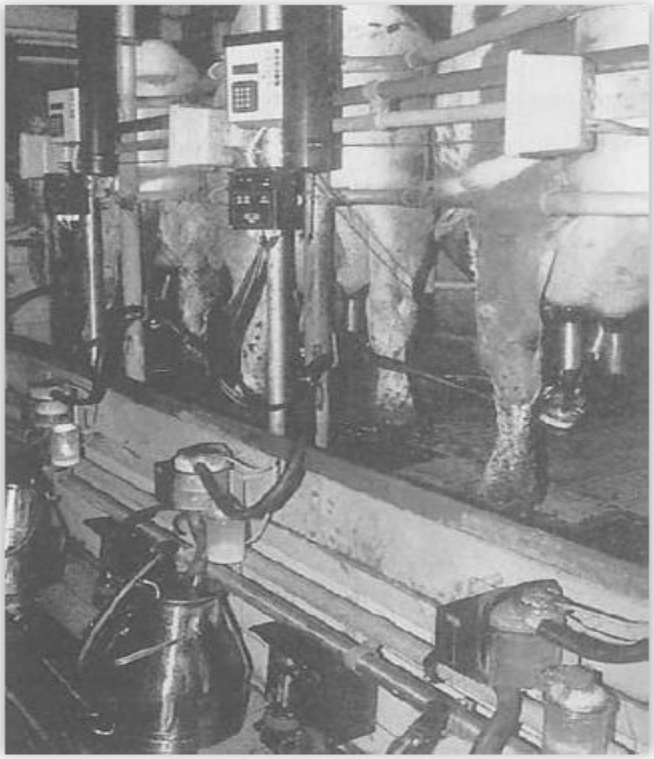

Figura 73 - Identificação automática e cálculo da produção de leite na cabine de ordenha. [1]

A injeção não fere o animal e pode ser realizada por leigos com pratica. Contudo, Deve ser dada atenção à higiene para assegurar que a ferida se cure com segurança.

Um transponder injectado representa um corpo estranho nos tecidos do animal. Isto pode levar a problemas na estabilidade de localização do transponder dentro do corpo do

animal, podendo, portanto, causar problemas quando a leitura do transpondedor. A partir de nossa experiência com ferimentos de guerra sabemos que estilhaços muitas vezes pode se mover vários decímetros através do corpo durante a vida de uma pessoa. Um transponder injetado também podem 'se mover ' em torno do ponto de inserção. Para resolver este problema, o Bayerischen Landesanstalt für Landtechnik em Weihenstephan, um ramo da Universidade Técnica de Munique, tem sido investigar vários locais de injecção desde 1989. Como resultado destes estudos, injecção sob a scutulum está atualmente favorecida através da utilização da orelha direita, com a injeção sendo dirigida para o osso ocipital. Segundo as conclusões do Landanstalt, esta posição é também apropriada para medir a temperatura do corpo do animal. [1]

O chamado bólus é um método muio útil para alojar o *transponder*. O bolus é um transponder montado em uma caixa cilíndrica resistente ao ácido, podendo ser feito de um material cerâmico. O bolus é depositado no rúmen, o omaso está presente em todos os ruminantes, através do esófago usando um sensor. Em circunstâncias normais, o bólus permanece no estômago durante todo tempo de vida do animal. Uma vantagem particular do presente método é a simples introdução do transponder no corpo do animal, e, em particular, o fato de que ela não causa qualquer prejuízo para o animal. A remoção do bolo no matadouro também é mais simples do que a localização e a remoção de um transponder injectado. [1]

É claro que o transponder injetado e o bolus são os únicos sistemas de identificação infalíveis. A seguir na figura 74 uma vaca recebendo a dosagem exata de ração depois de ter sido identifica pelo transponder em seu pescoço.

Figura 74 - Dosagem de alimento concentrado em um estande de alimentação automática para vacas leiteiras relacionada com a saída. Na ilustração a vaca é identificada pelo transponder no seu pescoço [1]

A seguir, na figuara 75, a imagem da inserção de um transponder do tipo bolus em uma vaca.

Figura 75 - A aplicação oral de um transponder do tipo bolus

4.4 IMOBILIZAÇÃO ELETRÔNICA DE VEÍCULOS

O forte aumento no roubo de veículo no início da década de 1990 - em especial na Alemanha - impulsionou a procura de sistemas anti-roubo eficazes. Dispositivos de controle remoto funciona com bateria com uma gama de 5-20m já tinha sido disponibilizado no mercado há anos. Estas são pequenas de infravermelhos ou RF transmissores operam na frequência UHF 433,92 MHz, que são principalmente utilizados para controlar a sistema de travamento central e um alarme integral. O imobilizador (electrónica) também pode ser acoplado a função de controle remoto. Neste tipo de dispositivo anti-roubo, no entanto, o bloqueio mecânico pode ainda ser utilizado para ter acesso ao veículo - no caso de o dispositivo de controlo remoto deixar de funcionar devido ao falhas da pilha no transmissor. Esta é a maior fraqueza deste tipo de sistema, como o sistema não pode verificar se a chave mecânica é genuína. Veículos garantidos desta maneira podem, portanto, ser aberto com uma ferramenta adequada (por exemplo picklock) e começou a ser abertos por uma pessoa não autorizada. [1]

Desde meados dos anos 1990, a tecnologia de *transponder* providenciou uma solução que pode ser usada para verificar a autenticidade, ou seja, a autenticidade, da chave. Esta solução tem-se revelado ideal para a realização da função de imobilização electrónico através da fechadura de ignição. Hoje, a tecnologia de *transponder* é geralmente combinado com um sistema de controle remoto como o acima mencionado: o controle remoto opera o sistema de trancamento e de alarme central do veículo, enquanto executa a tecnologia de *transponder* função de imobilização. A seguir, na figura 76, um exemplo de chave de ignição com *transponder* integrado.

Figura 76 - Chave de ignição com *transponder* integrado[1].

4.4.1 A FUNCIONALIDADE DE UM SISTEMA DE IMOBILIZAÇÃO

Em um sistema de imobilização eletrônica de uma chave de ignição mecânica é combinado com um *transponder*. O *transponder* em miniatura com uma antena de ferrite é incorporado diretamente na parte superior da chave (veja a Figura 76). [1]

A antena do leitor está integrada na fechadura de ignição, de tal maneira que, quando a chave de ignição é inserida, um (indutivo) acoplamento entre antena do leitor e a bobina do transponder é otimizado. O *transponder* é alimentado com energia proveniente do acoplamento indutivo e é, portanto, totalmente livre de manutenção. Imobilizadores eletrônicos tipicamente operam a uma freqüência de transmissão na faixa LF 100-135 kHz. A modulação ASK é o procedimento preferido para a modulação da transferência de dados para o transponder, uma vez que permite o leitor e o *transponder* poçam ser fabricados muito mais baratos. Modulação de carga é o único procedimento usado para a transmissão de dados a partir do *transponder* para o leitor. [1]

Quando a chave de ignição é girada na fechadura da ignição para ligar o veículo, o leitor é ativado e os dados são trocados com o *transponder* da chave de ignição. Três processos são empregados para verificar a autenticidade da chave. [1]

- **Verificação de um número de série individual.** Em quase todos os sistemas de *transponder* este possui um número de série simples indivídual (número exclusivo). Se o número normal de posições binárias é usado, significativamente mais diferentes códigos estão disponíveis do que o necessário para a produção de automóveis em todo o mundo (2^{32} = 4.3 bilhões ; 2^{48} = 2.8 $\times$ 10^{14}). Muitos sistemas simples (primeira geração de imobilização) leem o número de série do transponder e comparam este com um número de referência armazenado no leitor. Se os dois números são idênticos a eletrônica do motor é liberada. O problema aqui é o fato de o número de série do transponder não estar protegido contra a leitura não autorizada e, em teoria, este número de série pode ser lido por um atacante e copiado para um transponder especial com um número de série gravável. [1]

- **Procedimento *rolling code***. Cada vez que a chave for operada, um novo número é escrito no *transponder* com memória da chave. Este número é gerado por um gerador de números pseudo-aleatórios no leitor do veículo. É, portanto, impossível de duplicar o *transponder* se este sistema for utilizado. Se várias chaves são utilizadas com um veículo, em seguida, cada chave é executada através de sua própria pseudo-aleatório sequência**.** [1]

- **Procedimentos de criptografia (de autenticação) com chaves fixas**. A utilização de procedimentos criptográficos oferece uma segurança muito maior (segunda geração de imobilização). Na sequência de autenticação (resposta à provocação) o conhecimento de uma chave secreta (binária) é verificada, sem que esta chave seja transmitida. Em aplicações de veículos, no entanto, a autenticação unilateral do transponder da chave pelo leitor na fechadura de ignição é suficiente.

O leitor RFID agora se comunica com a eletrônica do motor do veículo, embora esta comunicação seja protegida por meio de processos de criptografia. O sistema eletrônico de controle de motores de funções da mais alta importância do veículo, em particular, o sistema de ignição e do sistema de combustível. Simplesmente curto-circuitar ou desconectar certos cabos e fios não é mais suficiente para contornar uma imobilização eletrônica do sistema. Mesmo a tentativa de enganar o sistema eletrônico do motor através da inserção de outra chave de ignição do mesmo tipo na fechadura de ignição está fadada ao fracasso por causa do procedimento de autenticação entre leitor e motores eletrônicos. Só chave do próprio veículo tem a chave correta (binário) para concluir com êxito a sequência de autenticação com a eletrônica do motor. [1]

A seguir uma antena do sistema de imobilização eletrônica integrado com a fechadura de ignição, figura 77.

Figura 77 - A antena do sistema de imobilização eletrônica está integrada diretamente à fechadura da ignição. [1]

A seguir um diagrama com partes do sistema de imobilização eletrônica de veículos, figura 78.

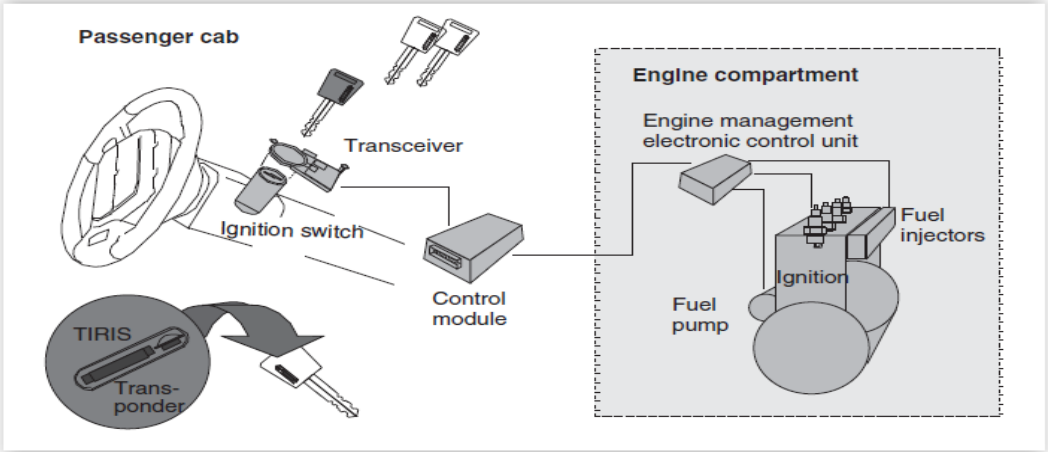

Figura 78 - Grupo funcional de um sistema de imobilização electrónico. O leitor RFID se autentica no que diz respeito ao sistema electrónico do motor para

evitar a manipulação do leitor. Controla os componentes eletrônicos do motor o ignição, combustível e motor de arranque e, portanto, pode bloquear todas as funções cruciais do veículo.

A instalação de tal imobilizador eletrônico para o sistema de gestão do motor só pode ser realizados na fábrica pelo fabricante do veículo, garantindo assim a melhor interação entre o sistema de controle do motor e dispositivo de segurança. Os dados de chave individual são programados na fábrica por fusíveis a laser programável no chip ou escrevendo em uma OTP-EEPROM. O fabricante veículo também é responsável pela implementação de medidas de segurança adequadas para impedir que os criminosos desde a aquisição de peças de reposição ilegalmente (Wolff, 1994). Com poucas exceções, sistemas eletrônicos de imobilização foram instalados em todos os carros novos como padrão desde o início de 1995.

4.4.2 BREVE HISTÓRIA DE SUCESSO

Em 1989 foram abertos muro de Berlim ea fronteira para a Europa Oriental, e os anos seguintes 1989 foram caracterizados por aumentos dramáticos nos roubos de veículos na Alemanha. A partir de 48 514 furtos em 1988, o número subiu para 144 057 roubos de apenas cinco anos depois, em 1993 - quase um triplo aumentar. Isso levou o Instituto Alemão de Fiscalização Federal de Seguros a declarar uma mudança para as Condições Gerais de Seguros para Automóvel Seguro (AKB) no início de 1993. [1]

De acordo com as antigas condições, os proprietários de veículos com seguro totalmente abrangente, poderiam ao abrigo de certas condições, reivindicar o preço total para um carro novo, se seu veículo fosse roubado, embora o valor de revenda do veículo roubado e, assim, o dano sofrido fosse significativamente inferior a este. O valor de um veículo depois de apenas alguns meses cai muito aquém do preço de um carro novo. [1]

Sob as novas condições, apenas o custo da substituição do veículo, ou seja, o seu valor real de mercado, é devolvido no caso de perda (acidente, roubo, etc). Além disso, se a perda é devido ao roubo de um excesso é deduzido do pagamento, que pode ser dispensado se o veículo estiver equipado com um aprovado dispositivo anti-roubo. O próprio interesse do proprietário do veículo em ter um eficaz dispositivo anti-roubo foi significativamente aumentando devido novas condições de seguros. [1]

A eficácia da imobilização eletrônica foi claramente demonstrada pela tendência de diminuição em roubos de veículos na Alemanha. Em 1994, já tinha havido uma ligeira queda de cerca de 2000 a 142 113, em comparação com a cifra recorde de 1993. Dois anos depois - 1996 - 110 764 roubos foram relatados. Isto representa uma diminuição de 22% em apenas 2 anos. [1]

Outro fator é que desde 1995 imobilizadores eletrônicos foram instalados em todos os carros novos – com algumas exceções - na fábrica como padrão. Se considerarmos

veículos garantidos desta maneira só, então podemos esperar que uma redução na taxa de roubo por um factor de 40.[1]

4.4.3 PREVISÕES

A próxima geração de imobilizadores também iram incorporar um acesso passivo, sistema de acesso garantido criptograficamente. Neste sistema, um leitor irá ser montada em cada uma das portas do veículo. Sistemas seqüenciais (TIRIS□) iram ser capazes de atingir uma alcance remoto, em que o *transponder* é alimentado por uma bateria, para que o sistema de travamento central do veículo possa ser operado a partir de uma distância maior. Isto é semelhante na sua função para a combinação de um imobilizador e fechamento central no controle remoto com um único *transponder*. [1]

A seguir a figura 82 com um esquema do sistema de imobilização eletrônica do veículo e fechamento remoto.

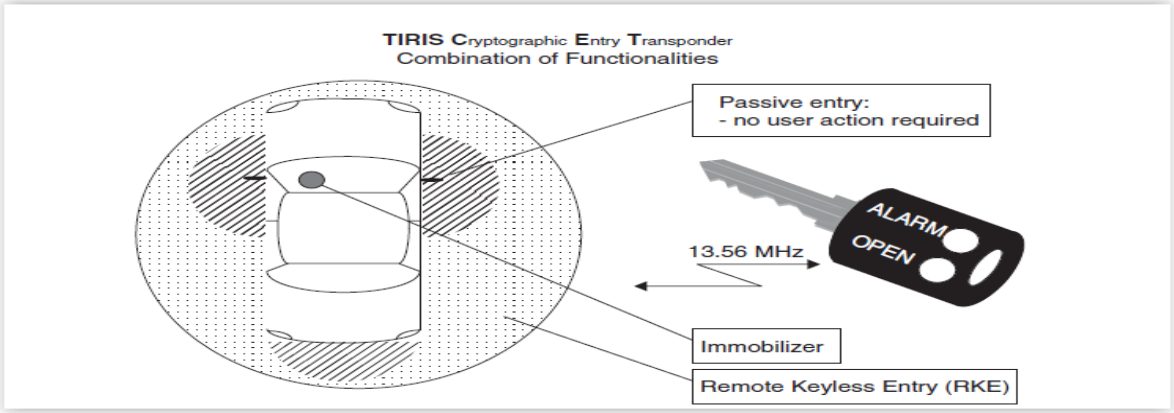

Figura 82- Imobilizador eletrônico e sistema de porta de bloqueio são integrados em um transponder na chave de ignição. Na fechadura de ignição e na proximidade das portas (entrada passiva), o transponder é alimentado com energia por acoplamento indutivo. A distâncias maiores (entrada de *keyless* remota) o transponder é alimentado com energia de uma bateria (células redondas na parte superior da chave) com o premir de um botão ("OPEN")[1]

4.5 USO DA TECNOLOGIA RFID EM PASSAPORTES ELETRÔNICOS.

Desde novembro de 2005, a Alemanha emitiu passaportes eletrônicos, o chamado *ePass*. Assim Alemanha é, juntamente com vários outros países, um dos precursores em relação à introdução da escalada europeia de passaportes eletrônicos com base na Diretiva

da UE 2252/2004 (Amtsblatt der Europäischen Union, 2004), que tem de ser implementado por todos os 24 estados membros da UE até agosto de 2006. Também fora da UE, vários países, como o Japão, Cingapura e os EUA, estão prestes a introduzir passaportes eletrônicos. Estes passaportes são marcados como passaportes eletrônicos com um *stilisied* chip  na capa exterior. [1]

O próprio *ePassport* consiste de um chip microprocessador sem contacto que - juntamente com a antena - é laminado para a página de dados do passaporte ou integrado na capa do passaporte (ver Figura 80). O objetivo do microchip sem contato é melhorar a segurança dos passaportes contra falsificação. Em 2002, ou seja, antes da introdução de passaportes eletrônicos, 290 passaportes forjados foram completamente detectados. O conteúdo de mais de 394 passaportes foi forjado. [1]

A primeira etapa do *ePassports* UE define que as lojas de chips *RFID* como dados relacionados com a pessoa: os nome, data de nascimento, gênero, bem como uma característica biométrica e uma fotografia do titular do passaporte.

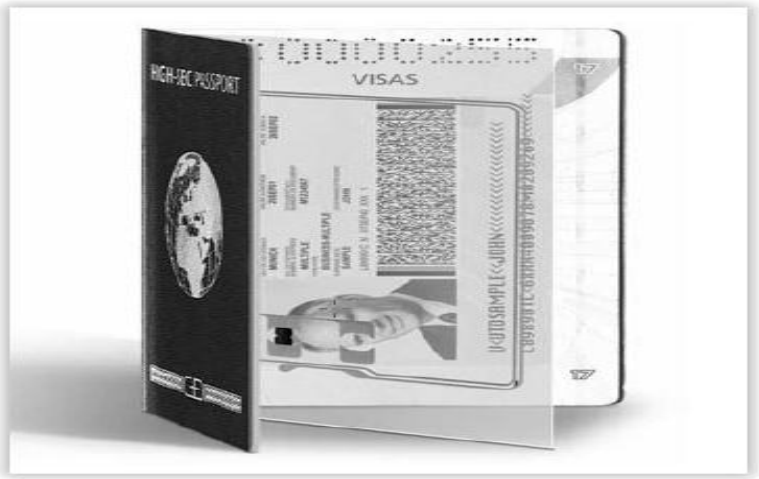

Figura 80 - Posição e design da antena RFID em passaportes eletrônicos. O circuito integrado do microprocessador pode ser reconhecido como um pequeno ponto preto sobre a fotografia do passaporte.[1]

A seguir, na figura 81, outra maneira de disposição dos chips e antenas *RFID* em um passaporte eletrônico.

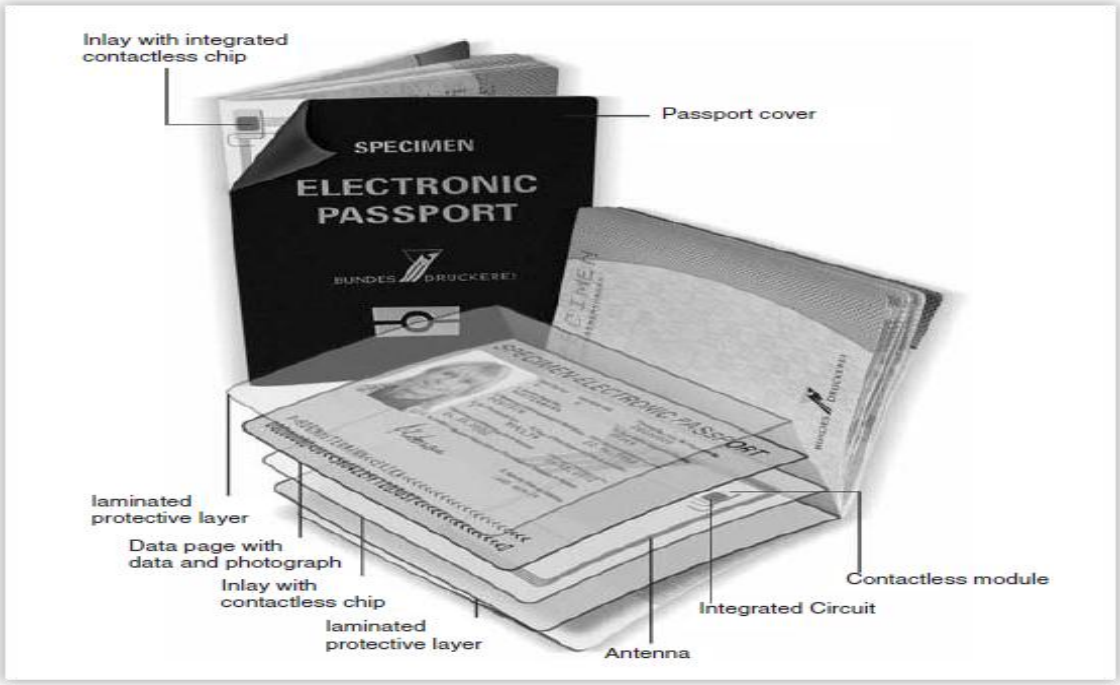

Figura 81 - O chip RFID pode ser integrado à página de dados ou à capa do passaporte. [1]

As especificações técnicas do passaporte biométrico segue as recomendações do Novo

Grupo de Trabalho Tecnologias (GTTN) da Organização da Aviação Civil Internacional (ICAO).

A Alemanha está representada no Conselho pelo Ministério Federal de Assuntos Internos (IMC) e tecnicamente apoiada pelo Escritório Federal de Polícia Criminal (BKA) e o Serviço Federal de Segurança da Informação (BSI, http .// www.bsi.bund.de). As especificações estão disponíveis ao público através do site da ICAO (http://icao.org/mrtd). Durante os controles nas fronteiras, os leitores e passaportes de diferentes países têm de ser compatíveis; caso contrário, não será possível alcançar a interoperabilidade internacional de leitura do *ePassport* no tráfego transfronteiriço internacional. Por esta razão, a ICAO inicialmente definiu critérios mínimos para passaportes biométricos. Internacionalmente, somente a fotografia do rosto é obrigatória como uma característica biométrica para todos os países. Desde 2008 *ePassports* da UE têm incluído as impressões digitais do titular do passaporte. [1]

Uma parte importante das especificações da ICAO são a interface sem contato ea organização de dados no chip RFID. A interface sem contato de *ePassports* está em conformidade com a norma ISO / IEC 14443. A gama de leitura nominal de um passaporte eletrônico é de 10 cm. A fim de alcançar curto momento de leitura de dados a transmissão entre *ePassport* e leitor deve apoiar, além da taxa de bits padrão de 106 kbit / s, também taxas de bits mais elevadas de até 848 kbit / s de acordo com a ISO / IEC 14443. Para os

passaportes eletrônicos emitidos na Alemanha, o número de série necessário para o algoritmo de anticolisão de acordo com a ISO / IEC 14443 é gerado de forma aleatória, de modo a impedir que o rastreamento de *ePassports*, possa ser possível com números de série fixos e óbvios.

A seguir a organização de dados em um chip de *ePassport*, figura 82.

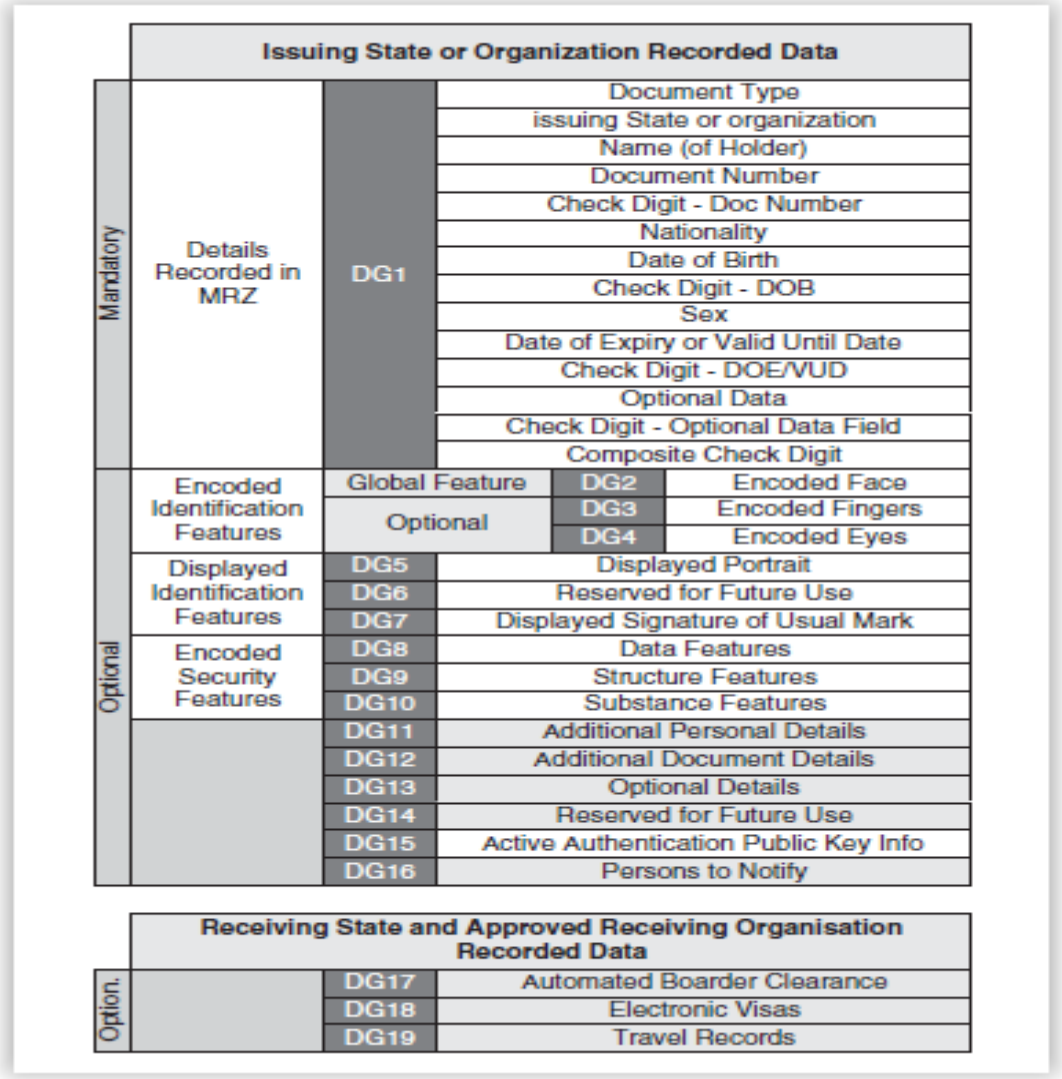

Figura 82 - A organização dos dados no chip sem contato de *ePassports*.[1]

Grupo de dados 1 (DG1) salva todos dados que está impresso na zona de leitura óptica (MRZ) de página de dados do passaporte. Grupo de dados 2 (DG2) armazena uma cópia digital da fotografia do passaporte em formato JPEG2000. As impressões digitais do titular do passaporte devem ser salvos no grupo de dados 3 (DG3), também como uma imagem. Os outros grupos de dados são opcionais e não estão atualmente a ser utilizado. [1]

A memória mínima de 32 kByte EEPROM é necessário que seja capaz de salvar todos os dados necessários no chip. EPassports alemães utilizam os seguintes dois microprocessadores sem contato: Infineon SLE 66CLX641P (64 kByte) e Philips inteligente MX P5CT072 (72 kByte) (CCC, 2005). [1]

A integridade e autenticidade dos dados armazenados no chip *RFID* é garantido por uma assinatura digital. Desta forma, é possível detectar dados falsos ou manipulados. Entidades autorizadas, por exemplo, empresas de impressão, que também produzem os documentos físicos usam um código secreto para a assinatura eletrônico dos documentos. Um código de público - que por sua vez tem de ser certificado pela certificação da assinatura do país, autoridade do país de emissão - é usada para verificar os documentos eletrônicos (BSI, 2005). [1]

Enquanto os *ePassport* estão fechados os dados no chip sem contato deve ser protegido contra acesso de leitura não autorizada. Se o *ePassport* é entregue a um funcionário de controle das fronteiras, que deveria ser possível lê-lo, no entanto. O chamado *ePass* deve igualar as características de passaportes atuais. Controle de acesso básico (BAC) tecnicamente implementa esse comportamento em posição para o leitor realmente ter acesso óptico às páginas de dados do passaporte. [1]

A seguir, na figura 83, um exemplo de acesso básico de *ePassport*.

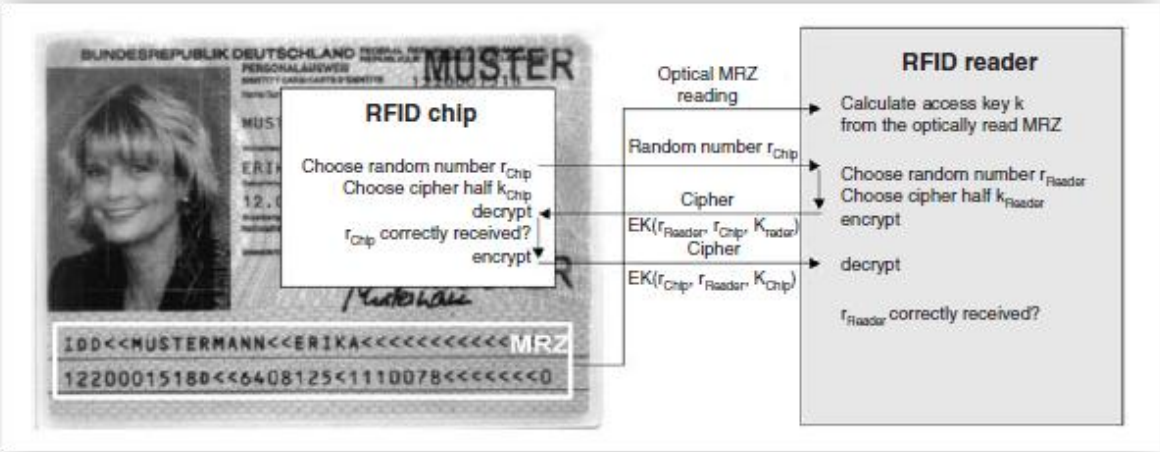

Figura 83 - Controle de acesso básico simula o comportamento de passaportes atuais. [1]

Se o passaporte eletrônico é colocado em um leitor, num primeiro momento, opticamente lê os dados da zona de leitura óptica (MRZ). Os campos MRZ, que são protegidos contra erros de leitura por um dígito de verificação, ou seja, o número do passaporte , data de nascimento do titular do passaporte ea data de expiração do passaporte, são utilizados para calcular código de acesso k (veja a Figura 81). Isto inicia o código de autenticação mútuo do leitor e do *ePassport*. A conclusão bem sucedida deste processo é um pré-requisito para a leitura dos grupos dados (BSI, 2005). [1]

4.6 USO DA TECNOLOGIA RFID EM EVENTOS DESPORTIVOS.

Em eventos esportivos de grande escala, tais como principais maratonas, os corredores que começam na parte de trás do campo estão sempre em desvantagem, porque os seus horários são calculados a partir do momento em que a corrida é iniciado. Para muitos corredores que levam vários minutos antes que eles realmente cruzem a linha de partida. Em muitos grandes eventos, com 10.000 participantes ou mais, pode ser 5 minutos antes dos últimos corredores ter cruzado a linha de partida. Sem tempo individual, os corredores nas fileiras traseiras estão, portanto, em grande desvantagem. [1]

Para corrigir esta injustiça, todos os corredores carregam um transponder com eles. O sistema baseia-se na idéia de que cada corredor coloca seus pés várias vezes no chão e, portanto, vem muito perto de uma antenas terrestres. Em eventos experimentais, verificou-se que usando um engenhoso arranjo de múltiplas antenas em uma matriz e um chip no sapato, mais de 1000 corredores podem ser registrados até oito vezes em um minuto com uma largura de início de apenas 4m. [1]

O transponder é baseado em um transponder de vidro operando na gama de frequência de 135 kHz, encaixado em um (ABS) injecção habitação moldado de forma especial (Figura 84). Para obter o transponder mais próximo possível do chão - e, assim, das antenas de medição do tempo do dispositivo - este está ligado ao sapata do corredor usando os cadarços. [1]

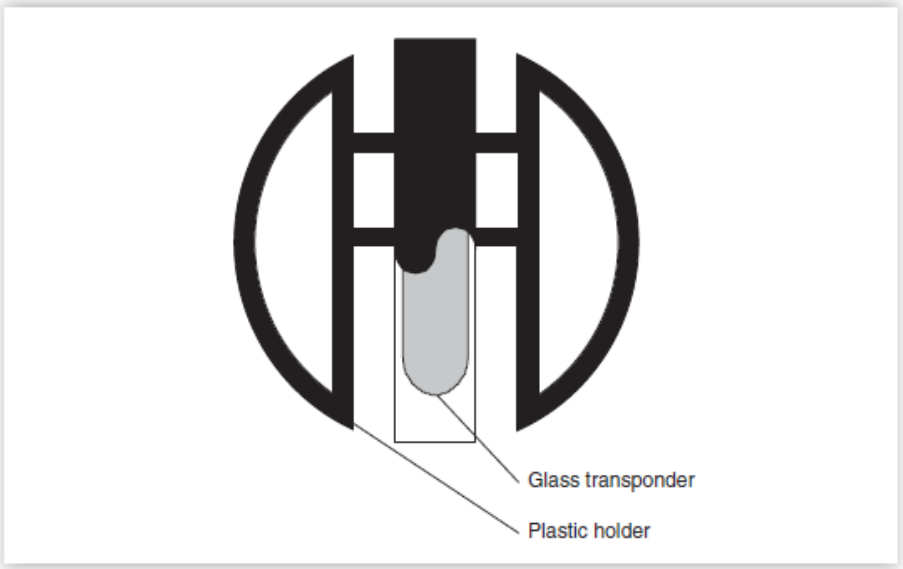

Figura 84 - O *transponder* é constituído por um *transponder* de vidro, o qual é injetado numa caixa(suporte) de plástico que é moldada de acordo com a sua função. O diagrama mostra a carcaça(suporte) de plástico parcialmente cortada.

As antenas do leitor são fundidas (presas) em tapetes finos e pode, assim, ser colocadas no solo e ainda ser protegidas contra todas as influências ambientais. As dimensões de um único tapete são 2,10 × 1,00 m. Em uma velocidade normal de corrida uma resolução de tempo líquido de ± 1 s é possível, derivada do tempo que o corredor mantém-se dentro do alcance de leitura do tapete. A precisão para ciclistas melhora a ± 0,2

s. A medida do tempo é imediatamente exibido em uma tela, de modo que o leitor pode ler o tempo intermediário atual ou última vez quando ele passou em uma estação de controle. [1]

O corredor pode fazer uma compra *one-off* do *transponder* por €20 e,em seguida, usá-lo onde quer que o sistema de cronometragem compatível seja utilizados. [1]

O desempenho do sistema de temporização baseado no *transponder* foi demonstrado nos seguintes eventos: *Rotterdam Marathon* (10.000 participantes), *Shell Hanseatic Marathon*, Hamburgo (11.500 participantes) e da Maratona de Berlim (13.500 participantes).

A seguir, na figura 85, um exemplo de transponder usado em eventos desportivos, o *ChampionChip transponder*.

Figura 85 - O *transponder ChampionChip* é preso ao sapato do corredor com o cadarço. [1]

A seguir, figura 86 e 87 um diagrama de uma estação de controle de cronometragem e uma imagem de local de controle de cronometragem com o tapete de leitura, respectivamente.

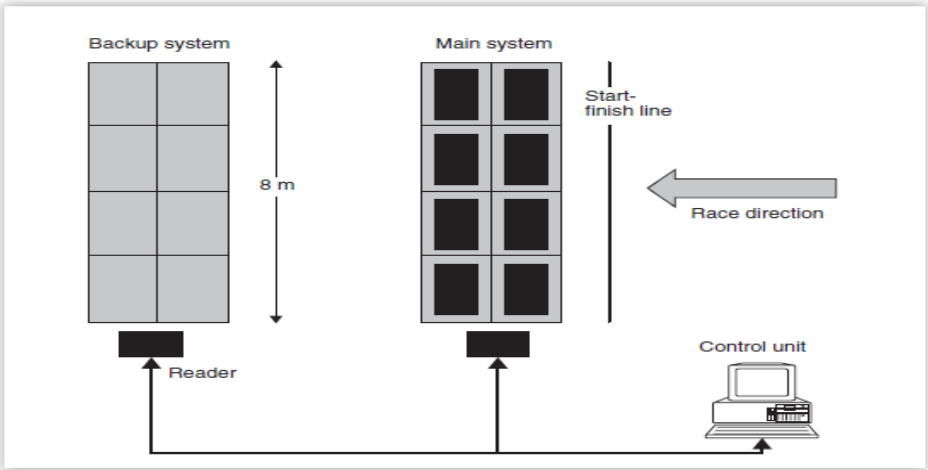

Figura 86 - A estação de controle consiste em um sistema principal e um sistema de reserva. O sistemas são constituídos por matrizes de antenas em tapetes. [1]

Figura 87 - Corredores passando pela estação de controle no final da maratona de Boston 101. Em primeiro plano podemos ver os tapetes contendo os leitores. O tempo pode ser exibida em uma tela imediatamente. [1]

5 ESTUDO DE CASO

5.1 A EXPERIÊNCIA DA REDE DE VAREJO, Grupo Pão de Açucar.

HISTÓRICO DA EMPRESA

Fundada em 1948 pelo Sr. Valentim dos Santos Diniz, a Companhia Brasileira de Distribuição(CBD) – Grupo Pão de Açúcar é a maior empresa de varejo do Brasil, com faturamento bruto de R$ 15,3 bilhões em 2004. A CBD opera hoje 560 lojas em 13 estados no país, no conceito multiformato, destaando-se: supermercados (Pão de Açúcar, Comprebem e Sendas), hipermercados (Extra) e lojas de eletroeletrônicos (Extra-Eletro), totalizando 1,2 milhão de metros quadrados em área de vendas. O grupo conta com quatorze centros de distribuição, localizados nas cidades de Brasília, Fortaleza, Curibiba, Rio de Juaneiro, Salvador e Recife (multicategoria) e São Paulo (especializados), totalizando uma área de armazenagem de mais de 350 mil metros quadrados, com 85% de índice de centralização. Um dos pilares que sustentam a razão de ser da CBD é o domínio da tecnologia: "Atenção a tudo que acontece no mundo avaliando sua utilidade e retorno para o nosso negócio, para extrair destas tecnologias disponíveis o máximo aproveitamento." Seguindo esta orientação, a CBD participa de fóruns internacionais sobre RFID desde o ano 2000. [3]

PILOTO

RFID e EPC são consideradas, hoje, tecnologias revolucionárias pela indústria e pelo varejo, e mudar completamente a forma como o mundo vende compra e transponta matérias-primas e produtos acabados na próxima década. Por isso, líderes mundiais do setor estão debruçados sobre suas aplicações e potencialidades. [3]

Descendente da tecnologia do *transponder* criado pelos ingleses para identificar aviões durante a 2ª Guerra Mundial, a F+RFID utiliza ondas de radio para passar informações de indetificação entre um produto etiquetado e um dispositivo de leitura. As indústrias as utilizam há anos para rastrear produtos de alto valor através nas linhas de montagem, mas os altos custos e as tecnologias proprietárias dificultaram a utilização em massa da aplicação. Agora, novas técnicas de produção, custos decrescentes das etiquetas e padrões abertos da indústria estão levando a identificação automática de objetos para um maior leque de utilizações. No topo da lista de aplicações priotárias está o imenso fluxo entre a cadeia de suprimento de produtos de bens de consumo e o verejo. Etiquetas RFID/EPC são formadas por microchips e antenas de rádio intergrados e aplicados a produtos e caixas. Numa implementação RFID/EPC, cada etiqueta (*tag*) armazena um único código eletrônico de produtos (EPC) de 96 bits que identifica o item por tipo e um número de série único. Múltiplas etiquetas podem ser lidas simultaneamente sem as restrições de visada dos sistemas de "scaneamento" de códigos de barras. Todo um contetor de carga, um palete, uma caixa ou uma embalagem de venda podem ser identificados em segundos por equipamentos de leitura automática. [3]

A seguir, na figura 88, a disposição do componentes da cadeia de suprimento.

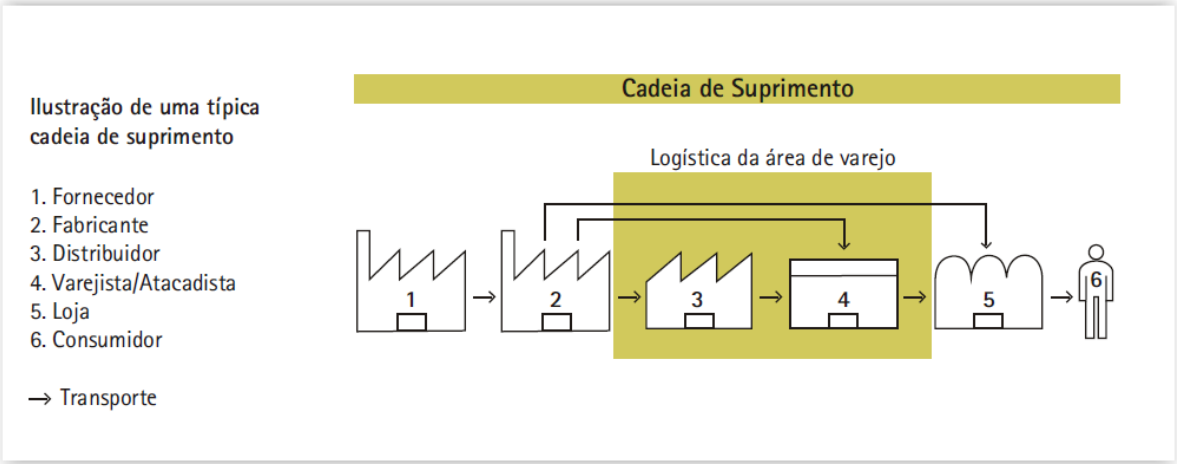

Figura 88 – Elementos que compõem a cadeia de suprimentos de uma rede de varejo. [3]

Estudos conduzidos nos EUA e Europa indicam que a adoção da solução RFID/EPC implica impactos diretos sobre a cadeia de suprimento, trazendo melhorias operacionais consideráveis, como mostra o quadro abaixo. [3]

A seguir, figura 89, um diagrama com as vantagens do uso da tecnologia RFID/EPC na cadeia de suprimentos.

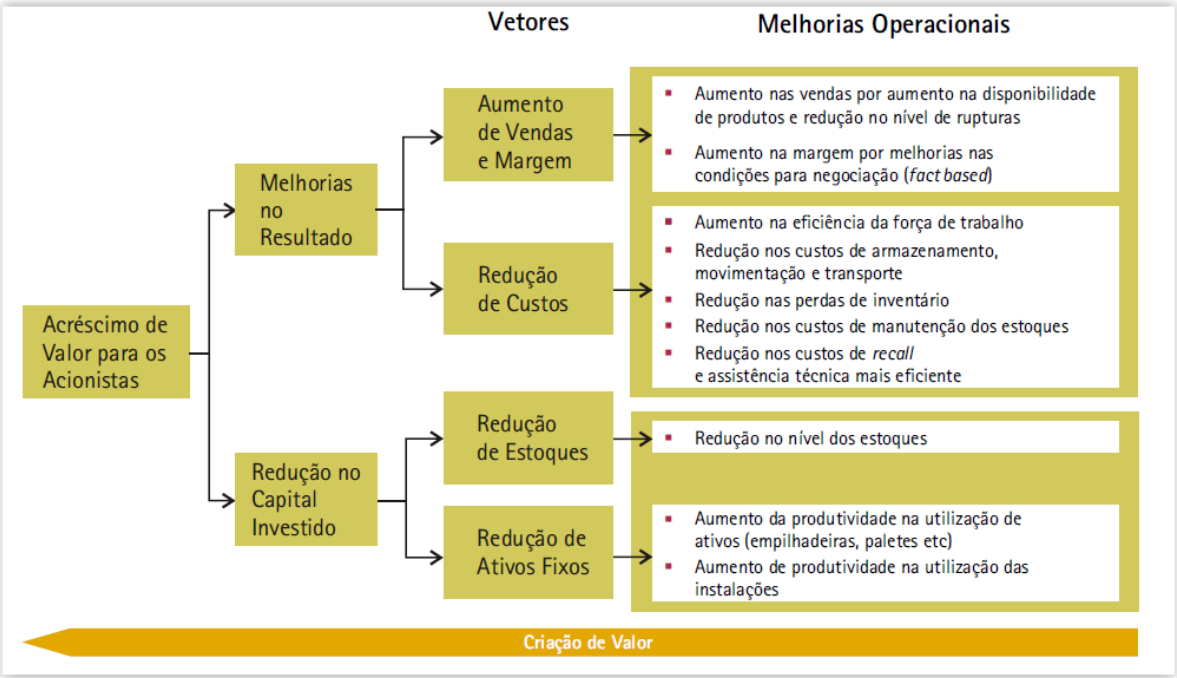

Figura 89 – Vantagens na aplicação da tecnologia RFID/EPC na cadeia de suprimentos. [3]

No entanto, essas melhorias indicadas serão capturadas dee forma e em graus diferentes de benefícios para cada fornecedor e varejista, ao longo da cadeia, como poderemos ver a seguir.

METODOLOGIA

O objetivo maior do estudo e do piloto era testar a aplicação da solução RFID/EPC no mercado brasileiro, desvendando as oportunidades mais relevantes, os desafios de implantação na cadeia como um todo e em categorias específicas, fazendo, ao mesmo tempo, um diagnóstico da base tecnológica dos atores da cadeia. A meta era, ao fim do projeto, relacionar custos e benecícios, além de traçar um mapa de aplicação da tecnologia no país. [3]

O piloto foi desenvolvido nas kinstalações industriais e centros de distrituição das empresas parceiras, instaladas na Via Anhanguera, em São Paulo, e compreendeu a circulação e o monitoramento de 1.000 paletes CHEP etiquetados. [3]

Em dois meses foi possível provar um pouco dessa nova tecnologia entre fábricas e centros de distrituição. [3]

A dinâmica adotada permitiu a utilização da solução RFID/EPC em escala, o que gerou experiências práticas de situações e conceitos nunca testados previamente no Brasil. Assim, foi possível monitorar o funcionamento da tecnologia nas condições brasileiras, avaliar os potenciais benefícios de sua aplicação, identificar pontos focais de evolução nos processos e em tecnologia da informação. [3]

FOCO DO PROJETO

O foco do projeto foi concentrado nos processos de recebimento e expedição de mercadorias, assim como na troca de informações entre os parceiros por meio da nova solução. Para que o processo se desse por inteiro, foi necessário sincronizar as informações dos produtos numa base de dados criada especificamente para o piloto e de acordo com os parâmetros da EPCglobal.[3]

DESCRIÇÃO DO PROJETO PILOTO

Os paletes CHEP foram etiquetados para a movimentação de produtos da Procter & Gamble e da Gillette até o centro de distribuição da CBD. [3]

Durante o processo, houve a continuidade da utilização do código de barras em conjunto com as etiquetas RFID/EPC. Não foram implementadas mudanças nos processos comerciais e logísticos vigentes nas quatro empresas participantes, assim como não foram feitas integrações com os sistemas operacionais de cada elo da cadeia de suprimento. [3]

Os centros de distribuição foram dotados de portais de *RFID*, que realizavam as leituras com base em aplicativos desenvolvidos pela Accenture em conjunto com os parceiros e também de acordo com os parâmetros da EPCglobal. [3]

A seguir, figura 90, o sistema *RFID* na cadeia de suprimento.

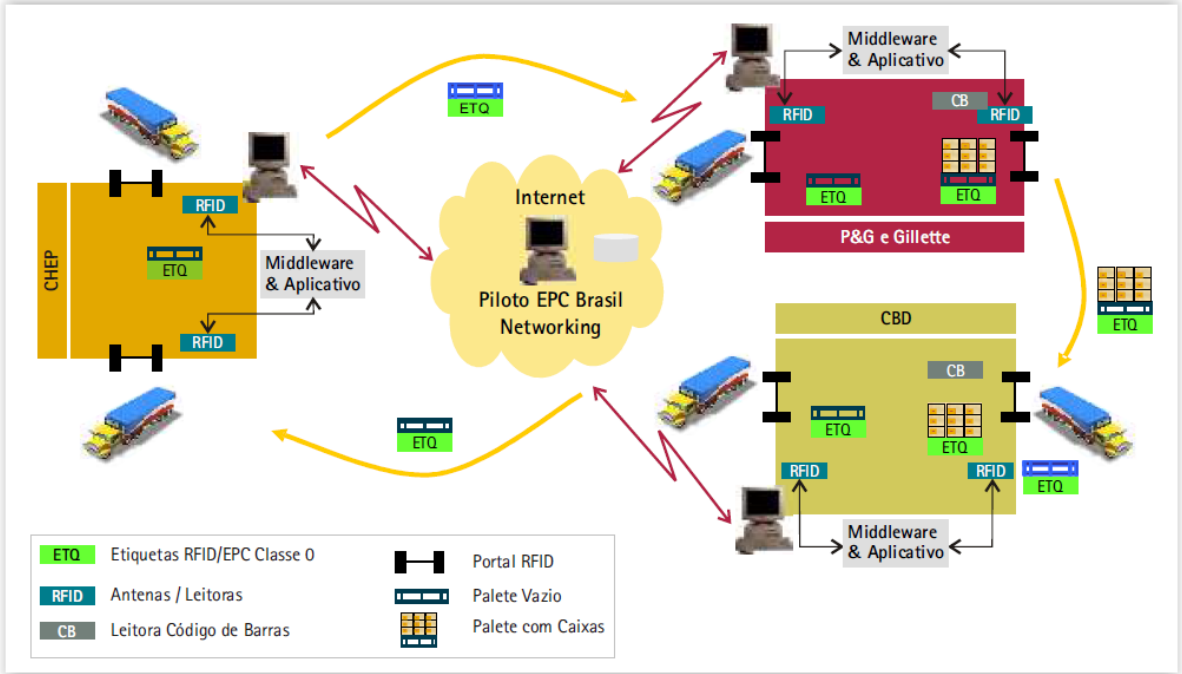

Figura 90 – Os diversos elementos do sistema RFID na cadeia de suprimento. [3]

Os paletes CHEP etiquetados circularam, de maneira controlada, dutante dois meses, entre os diversos centros de distribuição de acordo foram monitorados com índice de leitura de 97% pela rede de comunicação implantada, o que está alinhado com a média dos resultados de outros pilotos realizados nos Estados Unidos e Europa, uma vez que foram utilizados leitores e antenas de primeira geração. A infra-estrutura funcionaou de

maneira adequada, de acordo com a expextativa inicial, não excluídos, entretanto, os ajustes específicos para cada ambiente. [3]

O piloto também permitiu uma visão mais apurada dos benefícios provenientes dos ganhos no recebimento e na expedição dos paletes CHEP. Ficou claro que os novos processos e controles estabelecidos geraram melhor entendimento e percepção da maior produtividade e redução de perdas. [3]

RESULTADOS

Antes da análise propriamente dita dos resultados obtidos o piloto, convém ressalvar que o mercado brasileiro guarda especificidadades que geram impactos importantes no processo de adoção e utilização da solução RFID/EPC. São elas: [3]

- **Escala de operação**: Pode ser considerada baixa porque o número de caixas que circulam na operação é pequeno em relação à infra-estrutura demandada quando comparada â mesma relação em outros mercados. [3]

- **Valor unitário médio dos produtos**: Também pode ser considerado baixo.

- **Custo da tecnologia**: É alto, quando confrontado com as estimativas para outros países.

- **Custo da força de trabalho**: O custo da mão-de-obra é baixo em relação a outros custos. No entanto é importante estimar os custos da não conformidade, o que reduz esta vantagem, quando comparada a outros mercados.

- **Custo do capital**: É alto no Brasil, e tende a ser um fator inibidor, mas, por outro lado, pode contribuir quando é considerado o potencial de redução de estoques e, portanto, o nível de capital imobilizado.

As melhorias operacionais estimadas pelo grupo ainda assim, tomaram como ponto de partida a base de dados compilados a partir de pesquisas e de *business cases* desenvolvidos pelo *Auto-ID Center*, do *Massachussets Institute of Technology*. [3]

Aumento de vendas e margem

- Redução de 10% nos índices de ruptura nos centros de distribuição do varejo e do fabricante.

Redução de custos

- Aumento de 3% a 12% na produtividade da força de trabalho;
- Redução de 18% a 26% nas perdas de inventário;
- Redução de 10% no custo de manutenção de estoques;
- Redução de 2% a 5% nos retornos.

Redução de estoques

- Redução de 10% no nível dos estoques;
- Redução de 10% nos itens de baixo giro.

6 DESAFIOS AO USO DA TECNOLOGIA RFID.

A tecnologia de *RFID* está crescendo muito rapidamente. As iniciativas do *Wal-Mart* e do *DoD*, as quedas crescentes dos custos de implementação da tecnologia, o desenvolvimento de um padrão para o *RFID* e o alto retorno dos investimentos no setor são fatores que contribuem para essa evolução. Outra iniciativa que deve produzir um efeito de redução de custos ainda maior é a lei *US Health*, que exige que até 2010 todos os medicamentos que necessitam de receita nos Estados Unidos deverão conter uma *tag*, posto pelo fabricante do produto, a fim de conter o enorme crescimento da falsificação de remédios.

Apesar de tudo isso, há vários desafios a serem transpostos pela tecnologia de RFID para que se torne uma unanimidade entre os provedores de solução. Tais desafios se devem, principalmente, às práticas do mercado e ao fato de ser uma tecnologia nova.

Alguns desafios são:

- **Precisão:** A cada vez maior necessidade de confiabilidade e precisão das informações obtidas pelos sistemas de coleta de dados exige um constante aprimoramento dos mesmos. Este é um dos principais desafios para os fabricantes de leitores e *tags*, que precisam ser continuamente atualizados visando assegurar a precisão absoluta nos processos em que são aplicados tais componentes.

- **Integração das empresas:** Tendo em visa a não existência de uma padronização das informações e de normas comuns para o RFID, muitas empresas do setor encontram dificuldades na adaptação de seus sistemas às novas exigências tecnológicas.

- **Tags para cada tipo de material:** O desempenho de um sistema de *RFID* depende do tipo de objeto que está sendo monitorado, bem como do ambiente onde o sistema está sendo implantado. Dessa forma, objetos que contenham materiais como metais ou líquidos, que absorvem a energia RF emitida por um leitor comum, comprometem a aplicabilidade da solução de *RFID*. Para que haja tal implantação, se faz necessária a utilização de tags especiais para cada tipo de material. Isso representa um grande problema para a afirmação da tecnologia, visto que uma empresa que possui diversos tipos de produtos, e que deseje instalar um sistema de *RFID*, precisará adquirir e lidar com diversos tipos de *tags*, o que torna a solução muito complexa e, na maioria das vezes, cara.

- **Custo:** Este é a principal barreira da evolução da tecnologia de *RFID*, representando, assim, o maior desafio para a indústria do setor. O alto custo de uma solução de *RFID*, principalmente quando comparado a outros sistemas, como o Barcode, muitas vezes inviabiliza a implantação da mesma. Ou limita a aplicação do *RFID* no monitoramento e/ou rastreamento de produtos de alto valor, ou de conjuntos de produtos, como palets e fardos.

7 FUTURO DA TECNOLOGIA RFID.

7.1 A INTERNET DAS COISAS.

O conceito original para a Internet das Coisas foi introdizido pelo Massachusetts Institute of Technology (MIT) utilizando-se o código eletrônico de produto (*Electronic Product Code* – EPC) como forma de identificação de objeto. O conceito estabelecia que o número único especificado por EPC contido em um transportador de dados RFID de um objeto conectado poderia ser lido usando leitores ou interrogadores adequeados e, por meio de um *Object Naming Service* (ONS), direcionado como um ponteiro para informação armazenada em algum outro lugar (uma visão similar sem o uso ezplícito de RFID foi proposta anteriormente pelo projeto TRON no Japão nos anos de 1980). [4]

O mesmo princípio está relacionado ao uso de transportadores de dados em aplicações do tipo "placa de identificação", sendo que os dados ou a informação são armazenados localmente em vez de participar de uma estrutura de suporte a serviço prospecgtivamente global servindo a um número potencialmente grande de clientes do serviço. Em princípio, a informação armazenada, para uma função de suporte a serviço local ou mais abrangente, pode dizer respeito ao objeto em questão ou ser uma infomação relacionada ao manuseio ou processamento do objeto. Funções definidas localmente podem ser simplesmente usadas para ativar um atuador de algum tipo relacionado ao processo, como uma barreira operada eletricamente. [4]

A visão do projeto CASAGRAS a respeito da Internet das Coisas vai além da noção baseada em EPC. A visão CASAGRAS inclui uma ampla gama de tecnologias de 'borda' capazes de prover a interface com o mundo físico e também de acomodar sistemas de numeração diferentes do EPC. Isso é feito mantendo-se aderência ao conceito de IoT, que é mais formalmente baseado nos desenvolvimentos de computação e *networking* ubíquos e na noção de smart object'. Nesse contexto, smart objects são objetos que possuem dispositivos de sutporte embutidos, dixados ou que os acompanham, capazes de prover meios de identificação do objeto, comunicação e/ou processamento, sendo que o nível de complexidade depende da funcionalidade especificada. [4]

Na tentativa de identificar aplicações para a IoT, é primordial estabelecer a natureza do desenbolvimento e o que o distingue da funcionalidade da Internet existente (à qual ele será inevitavelmente integrado) e de outros desenvolvimentos de rede, tais como aqueles entre organizações comerciais que são da natureza de um grupo de susuários privado ou fecado (redes privativas). Com a IoT em sua fase nascente de desenvolvimento, só é possível chamar a atenção para a forma que as aplicações podem tomar e prover um *framework* precursor paraq aplicações e serviços que podem se basear em princípios, arquitetura e tecnologias que provavelmente terão impacto em seu desenvolvimento. [4]

Qualquer modelo para IoT deve claramente prover um elo entre o mundo físico e o mundo virtual, com o último sendo o mundo físico e o mundo virtual, com o último sedno significativamente influenciado pela Internet em si. [4]

A atenção para as 'coisas' aponta a necessidade de se definir uma metodologia de aplicação que possa auxiliar na construção de uma fundação melhor para o desenvolvimento

de aplicações e serviços dentro dos contextos doméstico, p[ublico, industrial e de negócios. A partir da caracterização de ‘coisa’ nos processos de negócios com respetio a dados/informe Uação, pessoas, lugares, ativos, mateiais e utilidades públicas, podem-se derivar princípios para se atingir uma funcionalidade aumentada em que os identificadores correspondentes são usados para ligar e melhorar processos. Esses princípios fornecem as chaves para o processamento de *background*, suportado por rede, da informação, que explora o conceito da IoT, ver figura 94. [4]

7.1.1 **Definição da Internet das Coisas**

Definções da Internet das Coisas apareceram em profusão, usualmente estruturadas para veicular alguma noção fantasiosa do que tal Internet pode oferecer. Como base para se considerar uma implementação realista de tal rede, é necessária uma proposição mais incisiva. Apesar do fato de o conceito Internet das Coisas estar evoluindo há praticamente uma década, ainda está sendo definido. [4]

O conceito da Internet das Coisas, conforme determinado pelo projeto CASAGRAS, é o seguinte:

> Uma infraestrutura de rede global, interligando objetos físicos e virtuais por meio da exploração de captura de dados e capacidades de comunicação. Essa infraestrutura inclui a Internet existente e em evolução, bem como os desenvolvimentos de rede. Ela oferecerá identificação de objeto específica, capacidade de sensoriamento e de conexão como base para o desenvolvimento de aplicações e serviços independentes cooperativos. Estes serão caracterizados por um elevado grau de captura autônoma de dados, transferência de enentos, conectividade e interoperabilidade de rede.[4]

O conceito IoT se baseou inicialmente em tecnologias habvilitadoras como a Identificação por Radiofrequência (RFID) ou redes sem fio de sensores e atuadores (*Wireless Sensor and Actuator Networks* – WSAN), mas atualmente cobre uma grande variedade de dispositivos com diferentes capacidades de computação e comunicação – genericamente designados por Networked Embedded Devices (NED). Tendo se originado de aplicações como o gerenciamento de cadeia de suprimentos e logística, a IoT agora visa obter múltiplos domínios, incluindo automação, energia, *e-health* etc. Ideais mais recentes levarama IoT venham a colaborar com outros conceitos emergentes como a inernet de Serviços (Internet of Services – IoS) e com blocos construtivos de outros esforços paralelos, como o da Internet da Energia (Internet of Energy – IoE) e com blocos construtivos de outros esforços paralelos, como o da Internet da Energia (Internet of Energy – IoE) que deverá revolucionar a infraestrutura de energia ou juntar a IoS e a IoT/RWI. É claro que a IoT terá um impacto umuito forte sobre a maneira de interação entre o mundo virtual e o físico, contribuindo de maneira geral para o esforço da Internet do Futuro. [4]

7.1.1.1 Qualificando a definição do projeto CASAGRAS

Em relação aos termos que contribuem para a definição, há os seguintes significados:

- "*Global network infrastricture*": descreve o que o próprio nome diz. É uma estrutura que de muitas maneiras é similar à da Internet em si. Ela permite que mensagens dos dispositivos que podem se comunicar sejam transmitidas a outos dispositivos que também podem se comunicar por meio de uma rede de conexões entre computadores, pacotes de dados incluindo a mensagem e sendo enviados através de dispositivos de roteamento ao desgtino fianal e na ordem correta. lA Internet das Coisas irá invariavelmente explorar essa infraestrutura da Internet, ao menos inicialmente, mas com os computadores terminais sendo de maneira crescente substituídos por uma funcionalidade computacional autônoma facilitada por smart devices ou embutidas em sisitamas baseados em computadores que evitam a necessidade de intervenção humana ainda que sejam para satisfazer certas necessidades humnas, sejam elas pessoais, corporativas ou outras. [4]

- "Physical object": refere-se a qualquer entidade ou coisa física tangível, seja animada ou inanimada, de complexidade em nível de item ou qualquer outro, que seja capaz de ser caracterizado de alguma forma para o proósito de identificação única. [4]

- "Virtual objects" são aqueles objetos representados no espaço de mídia e que podem exibir uma relação do tipo *proxy* com o objeto físico. Mais uma vez é reconhecida a necessidade de se atribuir uma identidade ao objeto e verificar se ele deve ser acomodado dentro da Internet das Coisas. [4]

- "Data capture" e "Autonomous data capture": referm-se aos processos de obternção de dados de uma fonte em particular e de introdução dos mesmos em sistemas de comunicação, computação ou qualquer outro de meanuseio de dados. De forma crescente, o processo de captura de dados explorará as vantagens dos sistemas automátivos de identificação e captura de dados (*Automatic Identification and Data Capture* – AIDC) com cada vez menos intervenção humana na implementação de aplicações e serviços dentro da Internet as Coisas. [4]

- "Specific object-identification": refer-se à maneira pela qual os objetos serão identificados, seja por meio de características naturais se for apropriado ou por códigos em transportadores de dados, tais como códigos de barra lineares, códigos de barra bidimensionais ou etiquetas de identificação por radiofrequência (RFID). [4]

- "Sensor" ou "Sensors": referem-se a uma categoria particular de dispositivos que podem sentir ou medir grandezas físicas, químicas ou biológicas definidas e gerar dados quantitativos associados. Isso contrasta com outras definições de sensor que são encontradas em relação à Internet das Coisas para as quais dispositivos como etiquetas RFID realizam o sensoriamento dos dados que adquirem. [4]

- "Connection capability" e "Connectivity": ambos referem-se à capacidade de se introduzir ou promover que possa transportá-lo ou manuseá-lo. Quanto maior for a

capacidade kou conectividade, mais efetivamente os dados podem ser ransferidos. Fatores e critérios de desempenho serão associados com tais capacidades. [4]

- "Event transfer": refere-se a uma transferência de funcionalidade embutida na mensagem entreque da fonte ao destino ou a qualquer outra situação ou atividade relacionada a uma aplicação ou serviço. [4]

- "Independente cooperative services and applications": refere-se a serviços e aplicações em que há um acordo por parte dos participantes para se usar uma infaraestrutura particular (embora limitada por detalhes contratuais) para desenvolver suas respectivas aplicações e serviços, mas são livres para determinar na natureza daqueles serviços e aplicações (dentro dos limites contratuais da infraestrutura) e como gerenciá-los. [4]

O último aspecto introduz mais uma, e potencialmente muito significativa, dimensão à TIC de objetos conectados e ao impacto prático que ela pode ter sobre os negócios e a vida em geral. Definindo-se uma estrutura de suporte adequada e de acesso comum, de comunicações e servidores para aplicações baseadas em objetos, podem-se prover facilidades para o desenvolvimento independente desses serviços cooperativos, análogas à – e potencialmente expansiva – World Wide Web (WWW). Explorando o potencial das novas estruturas de domínio, tal como a World Object Web (WOW), o framework de serviço e aplicação associada podem ser consideravelmente incrementados e expandidos. O mesmo tipo de abordagem também pode ser usado para acomodar em uma estutura integrada de internet conceitos emergentes de Internet de serviços, pessoas e mídia. [4]

7.1.2 Modelos para uma Internet das Coisas

O modelo mais básico para uma Internet das Coisas possui transportadores de dados que são essencialmente etiquetas RFID passivas levando identificafores únicos, com cada etiqueta tendo a capacidade de interrogação/resposta por meio de um calnal sem fio. Não existe nenhuma capacidade intrinseca de processamento dentro das etiquetas e nenhuma possibilidade de comunicação entre as etiquetas. [4]

Aplicações que utilizam esses transportadores de dados confiam no identificador como a maneira de localizar informação armazenada remotamente a respeito do item ao qual está presa. As etiquetas são interrogadas usando-se leitor, interrogador ou dispositivos *gateway* que podem se comunicar sem fio com as etiquetas e ainda se comunicar com um sistema de gerenciamento de informação para o suporte da aplicação. [4]

Os leitores podem ser dispositivos fixos ou móveis. O enlace de comunicação entre o dispositivo leitor e o hospedeiro pode ser com ou sem fio, dependendo do tipo de dispositivo, necessitando de interface e protocolos de comunicação apropriados. Os leitores podem executar funções particulares de processamento, possuir facilidades adicionais para se comunicar com outros dispositivos leitores e estar ligados em rede. [4]

Também deve ser reconhecido que dispositivos RFID ativos podem realizar tanto a função de uma etiqueta respondedora e, em outra cirtcunstâncias, aquela de um leitor para obter/agregar dados de outros dispositivos RFID dentro de seu alcance, como formar redes

locais *ad hoc*. Tais capacidades apropriadamente distribuídas podem melhorar substancialmente a conversão em realidade da IoT. [4]

Sistemas hospedeiros tratam as necessidades das aplicações, explorando os esquemas de numeração de itens para facilitar as funções de suporte específicas de item e paera obter e comunicar respostas apropriadas, incluindo aquelas que resultam em atuação física. Os sistemas hospedeiros podem estar conectados, via canais de comunicação com ou sem fio, e em rede. Essa capacidade adicional de comunicação e networking pode incluir a Internet e a *World Wide Web*, dependendo dos requisitos das aplicações. Para se conseguir esse grau de comunicação, é necessária a padronização apropriada da numeração, da estrutura de dados, dos protocolos de interface e comunicação em um nível global se o objetivo for obter uma Internet das Coisas verdadeiramente global. [4]

7.1.2.1 O Modelo inclusivo da internet das Coisas proposto pelo CASAGRAS.

Apesar de ter-se sugerido que modelos kpara a Internet das Coisas são simplesmente baseados em RFID e outras tecnologias de borda baseadas em rádio, um modelo mais inclusivo é necessário para acomodar o potencial de interface com o mundo físico e as inevitáveis excentricidades de conectividade que podem surgir na conversão em realidade de sistemas práticos e escaláveis. Enquanto o modelo inclusivo é mais exigente, tanto em aparência quanto em realização, ele também é uma visão que pode ser desenvolvida em etapas e suportada po padrões. [4]

As considerações de *framework* podem ser agrupadas naquelas que se relacionam com as várias camadas que distinguem os objetos do mundo real e a integração com a Internet em evolução. [4]

As camadas compreendem:

- Camadas físicas – nas quais os objetos físicos ou coisas são identificados e tornam-se componentes funcionais da Internet das Coisas por meio de tecnologias de transportadores de dados para objetos conectados, incluindo RFID. Os objetos assim identificados podem também ser agrupados ou colocados em rede para atender necessidades de uma aplicação em particular. Dispositivos com funcionalidade adicional, na forma de capacidade de sensoriamento, localização, posicionamento global e comunicação local, podem ser usados para se consetuir estruturas em rede bem como operação com dispositivo único. Capacidade de processamento é vista como uma característica importante e difenrenciada dos dispositivos que constituem os nós dentro da IoT. Com os desenvolvimentos em poder de processamento e redução de custo e tamanho, espera-se que uma porcentagem crescente de aplicações baseadas em objetos explore nós de processamento embutidos ou atados. O alcance e a flexibilidade desses dispositivos e redes terão uma influência importante no alcance das aplicações. [4]

O relatório da Comissão Europeia (2006), *From RFID to the internet of Things – Pervasive networked systems* identifica os seguintes dispositivos de comunicação com suporte à rede: [4]

1. Dispositivos puramente passivos (RFID) que produzem uma saída de dados fixa quando interrogados.
2. Dispositivos com capacidade de processamento moderada para formatar mensagens de transporte, podendo modificar o conteúdo com respeito ao tempo e ao espaço.
3. Dispositivos sensores que são capazes de gerar e comunicar informação a respeito do ambiente ou o status do item quando interrogados.
4. Dispositivos com capacidade de processamento aumentada, que facilita as decisões a serem comunicadas entre dispositivos sem intervenção humana, introduzindo um grau de inteligência nos sistemas ligados em rede. [4]

Essas categorias de tecnologia claramente têm implicações com relação à interface da zona física e com os requisitos para se formar rede. Elas também têm ramificações com respeito a outras partes da cadeia de transferência e processamento de dados, e com as necessidades de estruturação dos dados. As comunidades de desenvolvimento dos padrões ISO/IEC têm desenvolvido padrões internacionais para satisfazer essas necessidades. [4]

Apesar de não se afirmar exelicitamente, as tecnologias (1- 4) são essencialmente estruturas com base em RF, mesmo que não sejam em sua totalidade dispositivos RFID. [4]

Podem-se identificar camadas que dizem respeito a tecnologias AIDC (Automatic Identification and Data Capture) distintas que oferecem diferentes níveis de funcionalidade. Elas naturalmente incluem a RFID como uma camada, mas outras camadas podem estender a faixa global das tecnologias AIDC, incluindo códigos de barra lineares , códigos bidimensionais, dispositivos para gravação ótica de dados, dispositivos de memória de contato e uma gama de tecnologias de identificação de características naturais, incluindo identificação biométrica e pessoal. Também são relevantes para prover a interface com o físico as tecnologias de comunicação baseadas em transmissão de rádio, algumas das quais são conectadas aos objetos (incluindo WiFi, BluetoothZibbee e comunicação de campo próximo [*Near Field Communication* – NFC]) e outras que propiciam a comunicação em áreas muito mais amplas (GPRS, 3G). Redes banda larga e móveis e o desevolvimento de serviços associados aumentam as possib ilidades de implementação das camadas de borda para a Internet das Coisas. [4]

Sobre essa base podem ser identificadas camadas para diferentes dispositivos de captura de dados. Acomodá-las dentro de uma arquitetura para a IoT idealmente requer o desenvolvimento de um protocolo utilitário universal para captura de dados (*Universal Data Capture Appliance Protocol* – UDCAP), do tipo *plug-and-play*. Além disso, definindo-se as camadas dessa maneira cria-se uma base para se migrar para uma acomodação completamente inclusiva das tecnologias de borda em um determinado intervalo de tempo. [4]

- Camada do leitor-*gateway* – provendo efetivamente as interfaces entre dispositivos conectados a objetos e entre o leitor e os sistemas de gerenciamento de informação. Tecnologias de comunicação fixa, banda larga e móvel propiciarão a conectividade exigida pela Internet das Coisas. A colocação em rede de leitores e dispositivos gateway também pode, a camada de ser vista como uma característica importante da infra-estrutura nessa camada que muito contribui para a Internet das Coisas. A interface com dispositivos de atuação e controle nas aplicações do mundo real também é uma característica importante dessa camada. [4]

- Camada de gerenciamento da informação e aplicação – realizando a interface com a camada do leitor-*gateway* gerenciamento da informação provê a plataforma funcional para suportar aplicações e serviços. A colocação em rede e a possibilidade de prover capacidade inteligente (de acordo com os desenvolvimentos do estado da arte) constituem características adicionais importantes na implementação da Internet das Coisas. [4]

- Camada de comunicações em área mais ampla e Internet – provê a interfacecom outras estruturas e redes, incluindo a Internet.

Embora as interfaces sejam necessárias entre cada camada, a interface pode também permitir que não se utilize uma dada camada, acrescentando flexibilidade e opções para aplicações e serviços de objetos conectados. Estruturas bseadas em rede, bem como aquelas que requerem o suporte de gateway, também incrementam a flexibilidade. Além disso, os desenvolvimentos em computação ubíqua e *networking*, com capacidade integral de comunicação, proveem a fundação tecnológica chave para a infraestrutura da Internet das Coisas e sua integração com a Internet existente e em evolução. [4]

7.1.2.2 Migração para um modelo inclusivo para a Internet das Coisas

As complexidades envolvidas para tornar real um modelo completamente inclusivo para a internet das Coisas são certamente intimidadoras e ampliadas pela necessidade da cooperação internacional. No entanto, boas perspectivas podem ser percebidas para uma migração progressiva e sistemátiva paral, ou ao menos na direção de, uma estrutura completamente inclusiva para a IoT baseada em um *roadmap* estratégico para desenvolvimento. [4]

Esse *roadmap* estratégico, suportado internacionalmente, tomaria como princípio geral a abordagem em camadas apresetada no modelo inclusivo do CASAGRAS, começando com um *framework* minimalista genérico e acrescentando a esse *framewok* as camadas das tecnologias de borda de suporte, apoiada por um UDCAP apropriadao, um sistema de suporte à codificação baseado em resolvedores, uma rede orientada a serviços e estruturas de suporte a interfaces. [4]

O *roadmap* permitirá ainda a intergração e o suporte a sistemas de identificação legados, serviços de descoberta para desenvolvimentos independentes em relação aos propostos por meio do EPCglobal, consideração e acomodação apropriada de fatores socioeconômicos, tais como privacidade e segurança, e desenvolvimento de tecnologias aplicáveis. [4]

7.1.3 IoT e aplicações e serviços de Internet

Ao se considerar aplicações e serviços no âmbito da Internet das Coisas, é importante distinguir soluções que nitidamente dependem de uma funcionalidade do tipo Internet como distintqas de soluções localizadas que exploram capacidadesconvencionais de controle e processamento. Dada a natureza do espaço de objetos e a difusão evolucionária da capacidade de kprocessamento embutida para o mundo físico, podem ser indentificadas

oportunidades para aplicações que se estendem dos serviços ao nível pessoal, através dos níveis doméstico, corporativo, público e de cidade, regional, ambiental até serviços e acplicaçãoes nacionais, continentais e internacionais. [4]

Considerando-se a integração com a Internet existente e futura, vários tipos de aplicações podem ser vistas, as quais exploram as interfaces de comunicação entre objetos e seres humanos, bem como as comunicações de objeto a objeto. As várias categorias de aplicação ou serviço podem ser assim descritas: [4]

1. Objeto-para–Internet-para-humano (por ex., serviço iniciado por objeto que resulta em um e-mail para um humano que deve responder); [4]

2. Humano-para-Internet-para-objeto (por ex., um humano comunica via Internet para ativar um dispositivo de controle em sua casa); [4]

3. Objeto-para –Internet-para-objeto (por ex., serviço de controle ativado por um objeto via Internet que resulta na ativação de um objeto ou sistemas, em um evento de controle ou atualização de informação, possivelmente com uma interface humana para permitir o monitoramento de eventos); [4]

4. Objeto-para –infra-estrutura IoT dedicada - para –objeto (por ex., similar a três, mas explorando uma infraestrutura dedicada e características de domínio para suportar uma nova gama de aplicações e serviços orientados a objetos, possivelmente com interfaces humanas apropriadas a funções interativas). [4]

Há muitas redes: nas casas, nos e entre negócios, dentro de ambientes contruídos em instalações públicas e privadas, ambientais, nacionais e internacionais, à disposição de serviços colaborativos internacionais relacionados à movimentação de mercadorias, pessoas e informação. O conjunto é virtualmente ilimitado. No entanto, deve haver uma justificativa para interligar redes para distinguir uma IoT de redes isoladas. [4]

8 CONCLUSÃO

Este trabalho focou sua atenção nos aspectos técnicos da crescente tecnologia RFID, evitando um trabalho meramente expositivo com muitos já foram feitos, buscando uma analise dos aspectos técnicos permitindo um início de preparação para trabalhar com esta tecnologia por parte de seus leitores.

Além desse objetivo foi possível demonstrar que como já aconteceu com outras novas tecnologias que mudam a forma de se relacionar com o meio e principalmente entre as pessoas, como por exemplo o que proporcionol o avanço da internet hoje existente, a tecnológica RFID mostra podemos estar diante do advento de um revolução no modo das pessoas lidarem umas com as outras e no modo de as pessoas lidarem com os objetos e no modo de as pessoas lidarem com outros seres vivos enfim no modo com que as pessoas vão lidar com o mundo a sua volta. Essas mudanças irão se refletir principalmente no ambiente domestico com casas inteligentes e nas empresas com controle do processo produtivo e controle de acesso de funcionários. Assim estamos diante de uma tecnologia com imenso potencial de desenvolvimento da nossa chamada vida moderna.

Referências Bibliograficas:

1) FINKENZELLER, Klaus. RFID Handbook: ***Fundamentals and Applications in Contactless Smart Cards and Identification***, 3ª ed. John Wiley & Sons Inc., 2003.

2) PASSARETTI, Caio Santi. TCC – ***RFID identificação de radiofrequência movendo-se para o futuro***, Unb-FT – Departamento de Engenharia Elétrica – 2008.

3) Mário Duarte e Mitsuru Sakaguchi. Piloto RFID/EPC Brasil: **A Cadeia de Suprimento do Futuro**, em agosto de 2005.

4. RAMPIM, Renata. Implementando ***RFID na cadeia de negócios tecnologia a serviço da Excelência*** ediPUCRS 2ª EDIÇÃO, 2011.

5. GLOVER, Bill. BHATT, Himansu. ***RFID essencials***, O'Reilly, 2006.

6. AUTO-ID Labs of MIT – Massachusetts Institute of Technology. http://autoidlabs.mit.edu. Acesso em … de outubro de 2015.

7. RANKL,Wolfgang. EFFING, Wolfgang. ***Smart Card Handbook***, 3ª ed. John Wiley & Sons Inc., 2003.

8 Akaa Agbaeze Eteng, Sharul Kamal Abdul Rahim, and Chee Yen Leow. ***Wireless Nonradiative Energy Transfer*****,** em junho de 2015.