UNIVERSIDADE FEDERAL DO CEARÁ

CENTRO DE TECNOLOGIA

DEPARTAMENTO DE ENGENHARIA DE TELEINFORMÁTICA

APLICAÇÕES DA TECNOLOGIA DE IDENTIFICAÇÃO POR RÁDIO FREQÜÊNCIA - RFID

LUCAS CAVALCANTE DE ALMEIDA

Fortaleza - Ceará

2011

LUCAS CAVALCANTE DE ALMEIDA

APLICAÇÕES DA TECNOLOGIA DE IDENTIFICAÇÃO POR RÁDIO FREQÜÊNCIA - RFID

Trabalho Final de Curso submetido à Coordenação do Curso de Engenharia de Teleinformática, como requisito parcial para a obtenção do título de Engenheiro de Teleinformática

Orientador: Prof. Elvio César Giraudo

Fortaleza - Ceará

2011

LUCAS CAVALCANTE DE ALMEIDA

APLICAÇÕES DA TECNOLOGIA DE IDENTIFICAÇÃO POR RÁDIO FREQÜÊNCIA - RFID

Este Trabalho Final de Curso foi julgado adequado para obtenção do título de **Bacharel em Engenharia de Teleinformática** da Universidade Federal do Ceará.

Fortaleza, 16 de junho de 2011

_____

Prof. Hilma Helena Macedo de Vascocelos, Dr.
Coordenador do Curso

Banca Examinadora:

_____

Prof. Elvio César Giraudo, Dr.
Orientador

_____

Prof. Sérgio Antenor de Carvalho, Dr.
Examinador – UFC

_____

Prof. George André Pereira Thé, Dr.
Examinador - UFC

Meus anos de faculdade e todo árduo trabalho eu dedico especialmente aos meus pais Carlos Flaubert Patrício de Almeida e Luzimar Cavalcante de Almeida, que sempre me apoiaram direta ou indiretamente para minha formação, acreditando no meu potencial de vencer desafios.

AGRADECIMENTOS

Primeiramente a Deus, por todo alento, ânimo e perseverança que me cedeu durante toda a minha vida.

Ao meu pai e minha mãe, por terem investido com todo carinho em minha formação, sem medir esforços. Ao meu irmão Rafael, por me servir como exemplo de empenho, perseverança e criatividade. Aos meus grandes amigos Bruno, Igor, Rafael, e Leonardo, pelo companheirismo e incentivo. A todos que estudaram comigo, em especial àqueles que ajudaram a tornar o curso mais divertido e enriquecedor: David, Rodolfo, Henrique, Marco Antônio, Caio e Raymundo.

Ao meu orientador Elvio, pela confiança depositada, e por me apresentar ao ramo muito importante da profissão. Enfim, dedico a realização deste sonho à minha família e a todos que torceram ou contribuíram de alguma forma para que eu chegasse até aqui.

RESUMO

A introdução desta tecnologia surgiu por volta da década de 40, mas seu advento se deu por volta dos anos noventa, pois surgiu como solução para automação na captura de dados, consciente dessas novas tecnologias, as empresas tenderam a suportar seus modelos de negócios de forma automatizada. Uma das tecnologias que mais tem impulsionado esta automação é o **RFID**(*Radio Frequency Identifier*), que permite acesso em tempo real sobre a informação da localização de bens e equipamentos, mas introduzir a tecnologia de Identificação por Rádio Frequência em diversos setores de negócios requer não apenas um profundo entendimento de seus processos, mas também da introdução de inovações. O presente trabalho tem como objetivo mostrar o panorama geral da tecnologia **RFID** e, de forma mais focada, analisar a implantação de sistemas **RFID**, algumas de suas aplicações e analisar as sua vantagens e desvantagens da sua utilização nos dias de hoje. O objetivo desta monografia é estudar as necessidades, pré-requisitos e melhores práticas para possibilitar o retorno sobre um investimento de um projeto **RFID**. Com o resultado da análise de algumas de suas aplicações é formado um procedimento de boas práticas que visa diminuir os problemas de implantação e aumentar as possibilidades de sucesso para este tipo de solução.

Palavras-chaves: Automação; tecnologia **RFID**; aplicações; investimento; problemas implantação.

ABSTRACT

The introduction of this technology emerged in the decade of 40, but their emergence occurred around the late nineties, it has emerged as the solution for automated data capture, aware of these new technologies, companies tended to support their business models in order automated. One technology that has driven more automation that is **RFID** (*Radio Frequency Identifier*), which allows real time access to information about the location of property and equipment, but to introduce the technology of Radio Frequency Identification in various business sectors requires not only a deep understanding of their processes, but also the introduction of innovations. This paper aims to show the overview of **RFID** technology and, more focused, examine the deployment of **RFID** systems, some of its applications and analyze their advantages and disadvantages of its use today. The purpose of this monograph is to study the needs, prerequisites and best practices to enable the return on an investment of an RFID project. With the result of analysis of some of its application procedures consists of best practices aimed at reducing the problems of deployment and increase the chances of success for this type of solution.

Keywords: Automation, **RFID** technology, applications, investment, deployment problems.

LISTA DE FIGURAS

LISTA DE TABELAS

LISTA DE ABREVIATURAS E SIGLAS

ANATEL – Agência Nacional de Telecomunicações

API – Application Programming Interface

Auto ID – Automatic Identification

ASK – Amplitude Shift Keying

BPS – Bits por Segundo

CRC – Cyclic Redundancy Check

DoD – United States Department of Defense

EAS – Electronic Article Surveillance

EPC – Electronic Product Code

FDX – Full Duplex

FSK – Frequency Shift Keying

GSM – Global System for Mobile

HDX – Half Duplex

HF – High Frequency

HP – Hewlett Packard

IBM – International Business Machines

ISM – Industry, Scientific and Medical Radio Bands

ISO – International Organization for Standardization

ITF – Interrogator Talks First

LF – Low Frequency

MIT – Massachusetts Institute of Technology

PDA – Personal Digital Assistant

PSK – Phase Shift Keying

RAM – Random Access Memory

RF – Radio Frequency

RFID – Radio Frequency Identification

ROM – Read Only Memory

SAW – Surface Acoustic Wave

UHF – Ultra High Frequency

USB – Universal Serial Bus

WORM – Write Once Read Many

SUMÁRIO

CAPÍTULO 1 – INTRODUÇÃO

1.1 MOTIVAÇÃO E ENQUADRAMENTO

Com o grande aumento do interesse mundial sobre a tecnologia de **RFID**, é necessário estudar como estas aplicações estão sendo desenvolvidas e quais são os desafios que devem ser vencidos para implantações de sucesso com esta tecnologia. Sob esse cenário, o setor aonde mais se espera pelo amadurecimento desta tecnologia é sem dúvida no setor de logística, no qual os ganhos com as implantações desta tecnologia vão muito além da substituição da tecnologia de automação de captura de dados tendo como principal objetivo aumentar a integração de toda a cadeia logística, de forma a fornecer ferramentas que possibilitem total rastreabilidade e controle dos processos que circulam na cadeia[10].

Com esta visão, vários projetos estão sendo desenvolvido nos últimos anos, com o intuito de promover a tecnologia e fazer medições dos ganhos que podem ser obtidos na cadeia logística com a inclusão do **RFID** para estas operações.

1.2 OBJETIVOS

Este presente trabalho irá estudar a tecnologia de **RFID** mostrando o desenvolvimento desta até os dias atuais, focando principalmente nas aplicações logísticas. Além de buscar identificar os fatores que estão por trás da adoção desta tecnologia e buscar parâmetros que evidenciem a real vantagem da implantação desta tecnologia.

1.3 JUSTIFICATIVA

A justificativa de tanta importância em torno da identificação por frequência de rádio deve-se a possibilidade de reconhecimento de produtos com potenciais ganhos de eficiência. O mercado global de **RFID** atualmente está concentrado em aplicações mais maduras, em quatro áreas básicas: controle de acesso, identificação de animais, indústria automotiva e cobrança automática de pedágios. Mas esse panorama deve mudar isso porque outras aplicações estão crescendo rapidamente. As principais estão na área de segurança, com os passaportes, documentos de identidades eletrônicos, gerenciamento da cadeia de fornecedores

e pagamentos com cartões sem contato[10]. Mesmo com a trajetória de **RFID** sendo visível, a velocidade de sua adoção é incerta, pois existe o custo do chip de identificação de radiofreqüência, o custo das leitoras de etiquetas e uma infraestrutura extremamente complexa necessária para coletar, examinar e mover o vasto volume de dados que as etiquetas de identificação por radiofreqüência geram.

CAPÍTULO 2 – O ESTADO DA ARTE

2.1 O SISTEMA DE COMUNICAÇÃO SEM FIO IDEAL

Há diversas tecnologias competindo entre si no mercado de dispositivos de comunicação sem fio. Com o crescimento desse mercado o número de opções tecnológicas para se embarcar em um dispositivo só tende a aumentar. Para avaliar quais são os parâmetros fortes e fracos das opções de comunicação que constituem o estado da arte, é necessário primeiro estabelecer os parâmetros de comparação[5].

Para descobrir que parâmetros são esses, basta propor como seria uma tecnologia de comunicação sem fio de curto alcance ideal. Tal tecnologia teria as seguintes características, todas simultaneamente:

1. Alta vazão de dados;
2. Imunidade à interferência de fontes externas e internas;
3. Boa convivência com outras tecnologias de comunicação;
4. Facilidade de uso;
5. Projeto simples;
6. Tamanho e peso reduzidos;
7. Baixo custo de fabricação;
8. Baixo consumo energético;
9. Aproveitamento da infraestrutura presente;
10. Segurança dos dados transmitidos;
11. Uso mundial sem restrições;

2.2 REPRESENTATIVIDADE DOS PARÂMETROS

Esta seção descreve o que cada um dos parâmetros apresentados significa, e o papel que cada representa em um contexto de mercado.

2.2.1 Alta vazão de dados

Medida em bits por segundo (bps), a vazão de dados, ou taxa de transmissão, é provavelmente a mais importante característica de um sistema de comunicação, pois ela limita fortemente o número de aplicações de uma tecnologia, em qualquer cenário. Quanto maior a taxa de transmissão, menor será o tempo em que o usuário ou outro sistema dependente terá de esperar para transmitir seus dados; assim como menor será o tempo em que os transceptores permanecerão ligados consumindo energia.

2.2.2 Imunidade à interferência

Em um ambiente repleto de dispositivos de comunicação sem fio, o sinal transmitido entre dois dispositivos em particular corre grande risco de sofrer interferências externas. A interferência pode corromper a transmissão, terminando por causar mau funcionamento da aplicação; seja pela perda de dados no caminho, seja pelo recebimento de dados incorretos.

A interferência ocorre por uma simples razão: o espectro eletromagnético utilizável é limitado. Como há muitas tecnologias competindo pela utilização desse, é vital regulamentar seu uso, determinando quem pode usar cada faixa de frequências. São as agências nacionais de telecomunicações que fazem essa regulamentação (no Brasil é a ANATEL).

Dependendo da intensidade do uso da faixa do espectro eletromagnético, ou seja, da banda de rádio frequência utilizada pela tecnologia, a performance de uma aplicação pode se tornar bastante degradada, a ponto de se tornar inviável.

Além de interferências externas, existem as internas, causadas pelo próprio equipamento. Estas também são prejudiciais e devem ser levadas em consideração numa análise.

Posto isso, é fundamental que a tecnologia seja suficiente capaz de lidar com esse problema, o qual só tende a aumentar devido ao crescente mercado de dispositivos sem fio.

2.2.3 Boa convivência com outras tecnologias

Dispositivos sem fio devem saber “se comportar” de forma a não prejudicar os que já se encontram em atividade, compartilhando o mesmo meio de transmissão. Caso isso aconteça, fatalmente um deles terá de ser desligado.

2.2.4 Uso mundial sem restrições

Se a tecnologia for inofensiva a outras em seu contexto de operação, será bem provável que não precise de uma concessão de espectro.

2.2.5 Facilidade de uso

No século 21 não há mais espaço para dispositivos bons, suficientes para seus propósitos, mas complicados de usar. Em se tratando de tecnologias de comunicação sem fio, a usabilidade é um diferencial quando se tem como consumidor alvo o usuário comum. Quanto menos tiver de pensar, lembrar que a tecnologia existe, tão melhor será.

2.2.6 Aproveitamento da infraestrutura presente

A facilidade de uso está fortemente relacionada com a compatibilidade que o dispositivo ou aplicação em particular tem com os outros dispositivos que já existem. A interação entre os dispositivos deve ser suave, invisível, intuitiva. Para se conseguir tal virtude, a tecnologia deve se adaptar às tecnologias mais comuns.

2.2.7 Projeto simples

Um projeto simples, seja no embasamento teórico de uma tecnologia, seja na sai implementação de hardware, influenciará positivamente na sua adoção por parte dos fabricantes de equipamentos. Quanto mais simples for um projeto, menos problemas surgirão, e mais fácil será a instalação e manutenção.

2.2.8 Tamanho e peso reduzidos

Quanto menor for a implementação do sistema, mais fácil será embarcá-lo em um dispositivo. A exigência de tamanho reduzido se faz pelo pouco espaço disponível nos equipamentos e por restrições de peso. O tamanho reduzido dos componentes eletrônicos anda de mãos dadas com o baixo consumo energético, isso porque as dimensões e o peso de um equipamento portátil sem fio são limitados pelo tamanho da bateria que este utiliza.

2.2.9. Baixo consumo energético

Equipamentos muito econômicos tendem a ter pequenas baterias. Um baixo consumo de energia também traz economia para o usuário final. Tecnologias de comunicação sem fio devem se preocupar com a eficiência energética se quiserem ser adotadas em dispositivos portáteis. Uma menor temperatura de operação traz menores preocupações com a dissipação do calor gerado, sem mencionar que diminui seu peso.

2.2.10 Baixo Custo

De nada adianta todas as virtudes de uma tecnologia se seu custo for proibitivo. O custo de embarque de uma tecnologia depende de diversos fatores, incluindo alguns já citados, como: número e diversidades de componentes, infraestrutura fabril necessária para a montagem, tamanho, peso, eficiência energética, adoção no mercado, licenciamento, etc.

2.2.11 Segurança dos dados transmitidos

Os maiores inconvenientes dos enlaces de comunicação sem fio são: a insegurança que trazem em termos de privacidade dos dados enviados, e a incerteza da autenticidade dos dados

recebidos. Enlaces sem fio são muito mais fáceis de serem interceptados do que os cabeados. Desta forma, deve-se levar em consideração quais mecanismos de segurança de informação são implementados por uma tecnologia de comunicação sem fio, antes de aplicá-la.

Um fator positivo inerente à comunicação sem fio de campo próximo é a menor chance de interceptação dos dados, uma vez que o ambiente, ou seja, o espaço para o qual o sinal se propaga, é menor, portanto, mais controlável.

2.3 DEFININDO O RFID

RFID é uma sigla para *Radio Frequency Identification*, ou seja, Identificação por Radiofreqüência.

Basicamente, o **RFID** é uma tecnologia que utiliza uma comunicação por radiofreqüência, sem fios, para transmitir dados de um dispositivo móvel, com uma simples etiqueta (que aqui serão chamadas simplesmente de *tag*), para um leitor.

As etiquetas **RFID** são hardwares que possuem uma antena e um chip envoltos por algum material, como vidro ou plástico, os quais respondem a sinais remotos de um leitor geralmente conectado a um computador.

Um sistema **RFID** é normalmente composto por dois componentes: as etiquetas, também chamadas de *transponders*, e um leitor[17].

Podem ser divididos em duas categorias: Sistemas Ativos e Sistemas Passivos. Estes, juntamente com os componentes, serão discutidos posteriormente.

A utilização desta tecnologia é muito vasta, podendo ser amplamente estudada e implantada em diferentes setores, de Biblioteconomia a Veterinária; em um contêiner ou numa lata de refrigerantes. Tudo sendo monitorado por leitores e checado via rede, como por exemplo, através da Internet.

De maneira resumida, é um sistema que transmite dados de um objeto qualquer, através de um meio não guiado, usando ondas de rádio. O gráfico a seguir mostra os resultados de um estudo feito pela Venture Development Corporation, referente à distribuição e utilização desta tecnologia nos mais variados setores, para o ano de 2008[10].

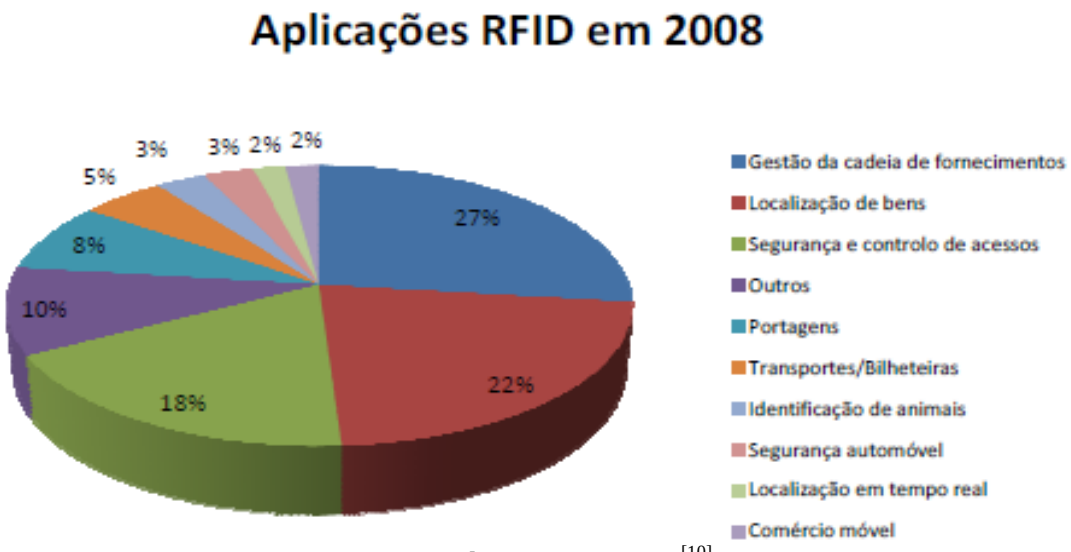


Figura 1 – Aplicações em RFID[10]

2.4 HISTÓRIA DO RFID

O **RFID**, como várias invenções que hoje são comuns, nasceu para fins militares[13].

Se hoje há tanta sofisticação na comunicação por radiofreqüência, boa parte do avanço é devido a *Sir* Robert Alexander Watson-Watt, físico escocês responsável por um grande aprimoramento, em 1935, dos sistemas de detecção e telemetria por rádio, mais conhecido como RADAR. Este sistema baseia-se na reflexão de ondas eletromagnéticas de objetos distantes que permitem sua localização.

O sistema RADAR foi usado pelos britânicos durante a Segunda Guerra Mundial, pois previam com antecedência os ataques alemães e possuíam a capacidade de saber, com precisões importantes dados, como a distância e velocidade dos bombardeiros inimigos. Este fato diminuiu muito o número de baixas civis, já que dava tempo para alarmar a população a fim de que se protegesse.

As potências do eixo, na mesma época, desenvolviam um projeto parecido, porém seu uso era para aumentar a precisão dos tiros.

A história do **RFID** começa, realmente, em 1973, quando Mario W. Cardullo requisitou a primeira patente americana para um sistema ativo de **RFID** com memória regravável. No mesmo ano, Charles Walton, um empreendedor da Califórnia, recebeu a patente para um sistema passivo, o qual era usado para destravar portas sem ajuda de chaves.

O governo americano também trabalhava no desenvolvimento de sistemas de **RFID** e construiu um sistema de rastreamento de material radioativo para o *Energy Department* e outro rastreamento de gado para o *Agricultural Department*.

Até o dado momento, as *tags* usadas eram de baixa frequência, 125 kHz, até que as empresas que comercializam estes sistemas mudaram para os de alta frequência, 13.56 MHz, a qual era irregular. Hoje, estes sistemas são usados em diversas aplicações, como nos controles de acesso e sistemas de pagamento.

No começo dos anos 80, a IBM patenteou os sistemas de Frequência Ultra Alta (UHF), *Ultra High Frequency*, possibilitando que o **RFID** fizesse leituras a distâncias superiores a dez metros. Hoje, em consequência de problemas financeiros na década de 1990, a IBM não é mais detentora da patente, que foi vendida para a Intermec, uma empresa provedora de códigos de barra. O grande crescimento do **RFID** UHF foi em 1999, quando o Uniform Code Council, EA Internatinal, Procter & Gamble e Gillete fundaram o Auto-ID Center, no MIT, Massachusetts Institute of Techonology, berço de vários outros avanços tecnológicos.

A pesquisa do Auto-ID Center era mudar a essência do **RFID** de um pequeno banco de dados móvel para um número de série, o que baixaria drasticamente os custos e transformaria o **RFID** em uma tecnologia de rede, ligando objetos à Internet através de *tags*.

Entre 1999 a 2003, o Auto-ID Center cresceu e ganhou apoio de mais de 100 companhias, além do Departamento de Defesa dos Estados Unidos. Nesta mesma época, foram abertos em vários outros países, desenvolvendo dois protocolos de interferência aérea (Classe 1 e Classe 0), o EPC (*Eletronic Product Code)*, o qual designa o esquema e a arquitetura de rede para a associação do **RFID** na Internet. Em 2004, a EPC ratificou uma segunda geração de padrões, melhorando o caminho para amplas adoções[15].

2.5 PRINCIPAIS COMPONENTES DE UM SISTEMA RFID

Um sistema **RFID** é tipicamente composto pelos seguintes componentes; conforme se representa na figura 2.

- *Tag* **RFID;**
- *Reader* RFID que incorpora também uma antena e um transmissor;
- Sistema de recolha de dados.

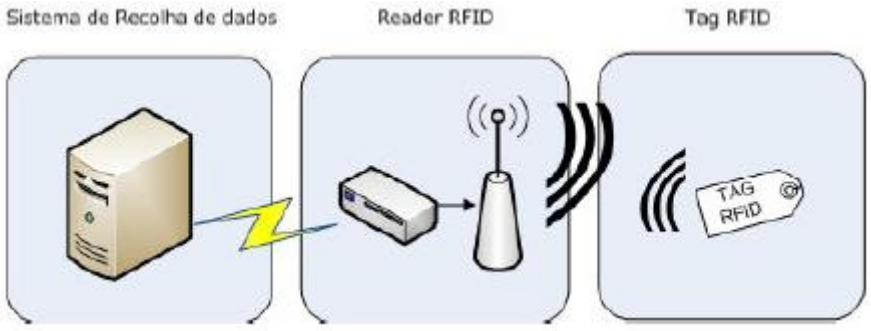


Figura 2 – Componentes RFID[10]

O princípio de funcionamento deste sistema consiste no envio de uma onda de rádio gerada pelo *reader* (atua como um transmissor), que pode ser recebida por uma tag. Por sua vez, a tag vai refletir alguma energia recebida de volta para o *reader*, duma forma que depende da ID da tag. Ao mesmo tempo em que esta reflexão acontece o *reader* está também a funcionar como um receptor rádio, de forma a poder detectar e decifrar o sinal recebido para poder identificar a tag. De seguida o *reader* vai enviar essa informação para um sistema de recolha de dados, através de qualquer ligação de dados (dependente da interface de comunicação do *reader*), que vai processar esta informação[10].

Na figura seguinte encontra-se apresentada uma arquitetura de referência para um sistema **RFID**.

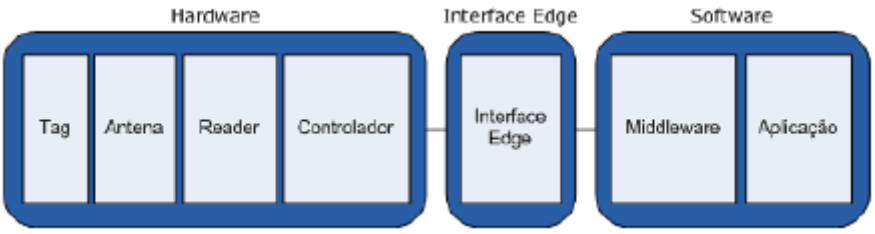


Figura 3 – Arquitetura do sistema RFID[10]

Esta arquitetura pode ser dividida em três blocos distintos, hardware, interface EDGE e software. No bloco de hardware, tal como o nome indica, é onde se encontram todos os dispositivos físicos, tais como a tag, o *reader* e a respectiva antena.

O controlador é usualmente chamado de *firmware*, e costuma estar integrado no *reader*. A função do controlador é a de permitir que um agente externo controle o comportamento do *reader*.

A interface EDGE é responsável pela integração do bloco de hardware com o bloco de software. A sua principal função é a de obter informação do *reader* e transferi-la para uma camada superior de software, que a saiba processar. Tal como em qualquer arquitetura estruturada por camadas, a utilização desta interface permite a existência de uma camada de abstração que possibilita a aplicação desenvolvida não esteja dependente da configuração do hardware, permitindo uma futura adição de hardware sem que seja necessária a modificação da aplicação.

O chamado bloco de software geralmente encontra-se no sistema de recolha de dados e é onde reside a inteligência desta arquitetura. É composto por uma camada de *middleware* que neste caso vai ser a camada responsável pela comunicação entre a interface EDGE e as futuras aplicações que irão necessitar da informação que esta interface irá recolher.

Vale ressaltar que esta é apenas uma arquitetura de referência, e não existe a obrigatoriedade da utilização de todos os componentes. Nestas circunstâncias, é possível construir uma aplicação que comunicasse diretamente com a camada de hardware sem a existência da interface EDGE ou *middleware*, mas pelo que é de boa prática é sempre bom incluir todos estes componentes quando se pensa numa arquitetura de um sistema **RFID**[2,10].

2.5.1 Tags

Sua função é transmitir e responder comandos que chegam por radiofreqüência. O *Transpoder*, RF *tag* ou simplesmente *tag*, é a etiqueta **RFID** em si. Sua estrutura básica é bem simples: um chip capaz de armazenar informações e uma resistência fazendo o papel de antena, envoltos por algum material com plástico ou silicone, em um determinado formato (chaveiro, etiqueta, cartões, entre outros). O propósito de uma *tag* **RFID** é a de, fisicamente, anexar dados sobre um objeto[10]. A Figura a seguir apresenta esta *tag*.

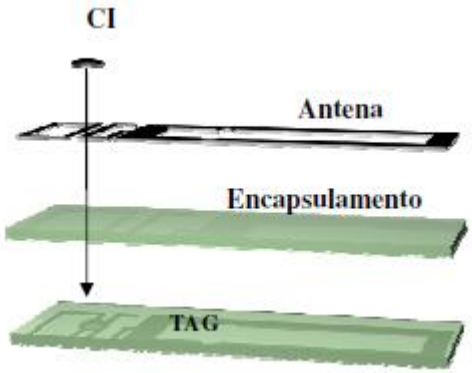


Figura 4 - Estrutura da TAG[10]

Primeiramente, as *tags* podem ser divididas em três grandes grupos: passivos, ativos e via dupla.

2.5.1.1 Tags Passivas

As *tags* **RFID** passivas são as mais comuns por serem mais simples, baratas e terem maior usabilidade. Os *transponders* passivos são identificados por não possuírem um transmissor. Sendo assim, eles apenas refletem de volta o sinal emitido pelo leitor. Na maioria dos casos, as *tags* passivas não possuem baterias, o que as tornam mais baratas e com uma maior vida útil. Elas obtêm sua energia utilizando o campo eletromagnético emitido do leitor. Muitas soluções atualmente em funcionamento empregam a tecnologia de etiquetas passivas, tais como o rastreamento de animais, automação industrial, vigilância eletrônica de produtos e controle de acesso.

2.5.1.2 Tags Ativas

As RF *tags* ativas são caracterizadas por terem um transmissor interno, funcionando sempre com o auxílio de baterias; os *transponders* ativos são capazes de emitir sinal, mesmo que a comunicação ainda seja feita pelo leitor, alimentando o microchip ou outros sensores. Em virtude das etiquetas ativas possuírem sua própria fonte de energia, elas podem transmitir dados sem que um leitor forneça energia a elas. Devido à bateria, as etiquetas ativas possuem uma vida útil finita. Um dos usos mais comuns das etiquetas ativas é o rastreamento de objetos de alto valor de longo alcance, tais como etiquetagem e rastreamento de suprimentos

militares transportados no mundo inteiro. Todavia, as etiquetas ativas também são usadas das aplicações exigem uma comunicação mais robusta entre etiqueta e o leitor.

2.5.1.3 Tags semiativas ou semi-passivas

Este tipo de etiqueta absorve energia da bateria interna para "energizar" e operar o CI da etiqueta e operar tarefas simples. Entretanto, ela ainda utiliza o campo eletromagnético do leitor para "despertar" e absorver energia para transmitir de volta os dados armazenados nela para o leitor.

2.5.1.4 Tamanho da memória das etiquetas

As etiquetas mais comuns atualmente consistem de um Circuito Integrado (CI) com memória, essencialmente um chip de microprocessador. Outras etiquetas não possuem chips e nem CI's internamente. As etiquetas sem chips são mais eficientes nas aplicações onde tudo o que é preciso é uma gama de funções mais simples, embora elas ajudem a alcançar mais acurácia e melhor alcance de detecção, a um custo potencialmente menor do que suas concorrentes que usam CI. A memória das etiquetas é um elemento muito importante dos sistemas de **RFID** com CI. O planejamento e o uso correto da memória da etiqueta aumentam significativamente a funcionalidade de uma aplicação. Em determinadas aplicações de cadeia de abastecimento, tais como rastreamento de animais vivos, a memória da etiqueta pode ser usada inicialmente para armazenar um identificador exclusivo. Em seguida, em qualquer etapa da cadeia de abastecimento, as informações críticas podem ser atualizadas, armazenadas e lidas. Nesta aplicação, as informações podem conter o histórico de saúde, o número de bezerros produzidos, a data e o local da transferência de propriedade, peso na época de venda, etc[2].

ATRIBUTOS	CARACTERÍSTICAS
Modelo	• Com CI – Etiqueta mais comum. Possui circuito integrado com memória para realizar computações simples. • Sem chip – Baseia-se nas propriedades do material da etiqueta para a transmissão de dados. Consegue alcances maiores e melhor acurácia. Não possui poder ou capacidade computacional para armazenar dados novos ou adicionais.
Tipo	• Passiva – Não requer bateria para operar. Oferece menor alcance e menor acurácia. Baixo custo • Ativa – Requer bateria para operar o CI e para se comunicar com o leitor. Oferece maior acurácia e alcance. Mais cara • Semiativa – Requer bateria somente para operar o CI. Oferece melhor alcance e melhor acurácia do que as etiquetas passivas a um custo menor do que as etiquetas ativas.
Memória	• Somente Leitura – Os dados gravados apenas na hora da fabricação da etiqueta tornam a etiqueta à prova de adulteração(característica nativa das etiquetas sem chips). • Uma Gravação/Várias Leituras – A capacidade de gravar os dados apenas uma vez torna a etiqueta à prova de adulteração, mas oferece a flexibilidade de gravação dos dados depois da fabricação da etiqueta, o que pode reduzir significativamente os custos de produção. • Leitura/Gravação – A mais flexível. Vulnerável a adulteração e sobreposição de dados.

Tabela 1 – Atributos e características das etiquetas[2]

As configurações da memória da etiqueta podem variar bastante com base no custo e nos requisitos físicos. No caso da EAS (vigilância eletrônica de produtos), as etiquetas possuem essencialmente 1 bit de memória e são relativamente baratas se comparadas com as

etiquetas com mais memórias. Estas etiquetas não possuem identificadores exclusivos e são usadas apenas para sinalizar sua presença quando estão no campo de um leitor. Além das etiquetas de 1 bit, o espaço típico ocupado de uma memória pode variar de 16 bits a várias centenas de kbits para determinadas etiquetas ativas. A quantidade de memória presente em uma etiqueta é definida pelas exigências da aplicação e/ou por qualquer norma ou regulamento relevante.

2.5.2 Etiquetas sem Chips

A tecnologia de identificação sem chips, uma forma emergente de **RFID**, oferece o potencial de ajudar a proliferar o uso da tecnologia **RFID** em um número ainda maior de aplicações. Essencialmente passivas, as etiquetas sem chips não possuem capacidade de memória de suas similares com CI. Entretanto, elas podem melhorar o desempenho das aplicações de outras formas. Em termos simples, a maioria das tecnologias sem chips emprega a ideia de "codificação" dos padrões exclusivos na superfície de vários materiais refletivos. Estes padrões tornam-se os dados que serão refletidos de volta por ondas de rádio para os leitores customizados. As etiquetas sem chips requerem energia apenas para transmitir as ondas de rádio. Elas não possuem o chip que exigiria energia adicional como nas etiquetas com CI's. Embora a tecnologia básica nas etiquetas sem chips esteja muito além do escopo desta monografia, é importante notar as vantagens significativas que elas podem oferecer:

- Melhor acurácia ao ler etiquetas em líquidos ou metais;
- Tratamento mais eficiente das interferências de RF;
- Maiores alcances de leitura;
- Operação em temperaturas extremas;
- Capacidade de ser embutida de forma invisível em documento de papel;
- Menor preço por etiqueta.

Observe que estas características não são os atributos de todas as tecnologias sem chips, porém elas representam a gama de características que existem entre os diversos tipos de tecnologia sem chips.

As etiquetas sem chips foram introduzidas em etiquetas de produtos, documentos e embalagens. Os desenvolvedores das etiquetas sem chips comercializam suas tecnologias com indústrias médicas, farmacêuticas e de embalagem de consumo, além de agências e entidades envolvidas com propriedade intelectual, informações classificadas, valores mobiliários e papel moeda.

2.5.3 Etiquetas Sensoras

As etiquetas sensoras oferecem a capacidade de monitorar, medir e registrar diversas condições ambientais. O conceito é bastante simples. Um dispositivo sensor é acondicionado junto com a etiqueta para interagir e registrar qualquer condição que o sensor for destinado a monitorar. A tecnologia envolvida pode ser desafiadora se uma aplicação exigir etiquetas sensoras passivas. Isto significa primeiro que o sensor não possui energia enquanto a etiqueta não estiver no campo de alcance de um leitor e segundo que a energia é muito limitada mesmo quando houver um leitor no campo de alcance. Algumas das etiquetas sensoras existentes mais interessantes atualmente, ou em desenvolvimento, incluem as etiquetas que conseguem detectar, registrar e transmitir as variações de pressão do ar, de temperatura, de volume de líquidos, ou a presença de agentes químicos ou bacterianos.

2.5.4 Leitor

Um leitor, em um sistema de **RFID** tem como medição de desempenho o fato de comunicar-se com as *tags* (etiquetas) através da antena e repassar a informação para o software. Um software que tem a função de ler e escrever dados a partir de um dispositivo sem fio necessita de um leitor como interface, pois do ponto de vista da aplicação, o acesso aos dispositivos móveis tem que ser o mais transparente possível. O funcionamento de um Leitor é descrito em resumo na Figura 5.

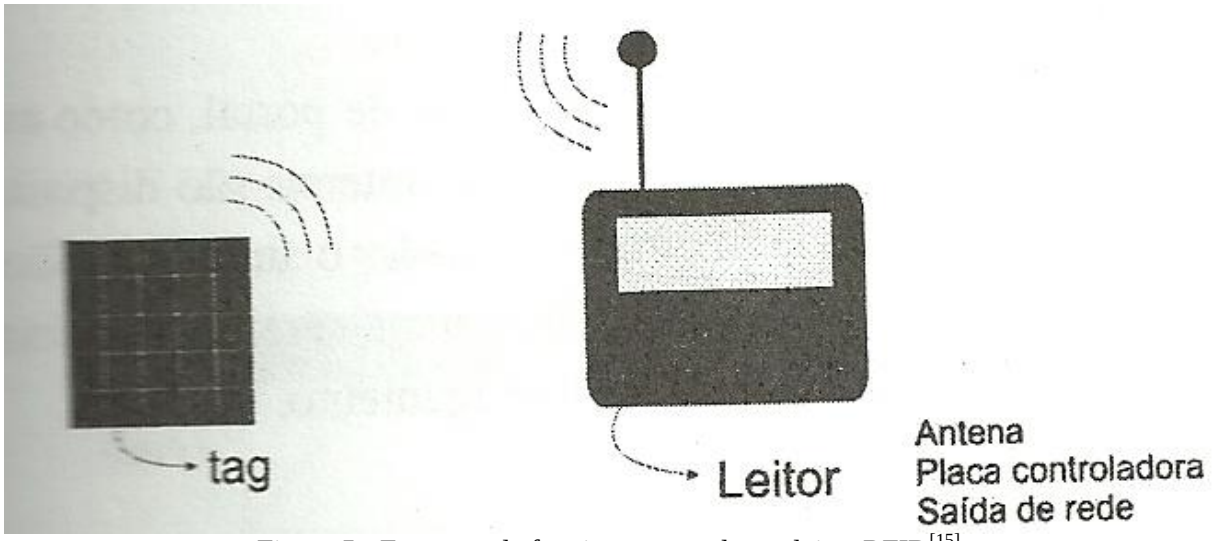


Figura 5 - Esquema de funcionamento de um leitor RFID[15]

Todos os leitores, independente da capacidade, funcionalidade ou tipo, têm como dispositivo de entrada uma antena. É através dela que o leitor obtém informações da *tag*, constituindo-se na interface entre os sinais de rádio recebidos e o Controlador da Leitora. Geralmente, as leitoras possuem apenas uma ou duas antenas as quais são conectadas; em alguns casos são antenas internas e, em outros, uma leitora pode controlar ao mesmo tempo várias antenas distantes entre si. Outra maneira de ligar as antenas é configurando-as para que uma apenas receba o sinal e outra o transmita. Outro componente físico é o Controlador, que é o dispositivo responsável por controlar o leitor. Ele pode variar em complexidade, sendo desde um pequeno leitor embarcado em um PDA (computador de tamanho reduzido dotado de grande capacidade computacional) ou celular até um microcomputador com sistema servidor e várias funcionalidades. Por fim, a interface de rede necessária para fazer com que as informações saiam da leitora, pode ser uma simples porta Ethernet, USB, Serial ou outra.

O layout de um leitor é essencial para saber qual tipo de sistema **RFID** será usado; eles são adequados conforme a necessidade de uso, variando em forma, tamanho e manuseio.

Talvez a mais conhecida seja em forma de portal. Neste tipo de disposição, as antenas são dispostas de maneira a reconhecer quando um *transponder* o atravessa. São usados em sistemas de EAS (Vigilância Eletrônica de Produtos) e quando os itens a serem inspecionados chegam ou vão através de docas de carregamento.

Figura 6 - Portal de sistema de segurança anti-roubo, EAS[1]

2.5.4.1 Energizando a Etiqueta

No caso das etiquetas passivas e semiativas, o leitor fornece a energia necessária para ativar ou energizar a etiqueta no campo eletromagnético dele. O alcance deste campo geralmente é determinado pelo tamanho da antena dos dois lados e pela potência do leitor. O tamanho da antena geralmente é definido pelos requisitos da aplicação. Todavia, a potência do leitor (através da antena), que define a intensidade e o alcance do campo eletromagnético produzido, geralmente é limitada por regulamentos.

2.5.4.2 Dados Lidos nas Etiquetas

A tarefa mais comum que um leitor desempenha é, naturalmente, a leitura dos dados armazenados na etiqueta. Este processo requer um algoritmo de software sofisticado para garantir confiabilidade, segurança e velocidade. Discutiremos mais adiante o software necessário para garantir estes objetivos.

2.5.4.3 Gravando Dados na Etiqueta

Para os sistemas de **RFID** com capacidade de gravação, um leitor pode realizar uma função dupla também gravando dados em uma etiqueta.

- As etiquetas podem ser produzidas em massa sem dados em suas memórias. Um leitor pode ser usado para inicializar a memória de uma etiqueta com base nos requisitos da aplicação. Por exemplo, um número de identificação exclusiva pode ser codificado na etiqueta pelo fabricante de um determinado produto imediatamente antes que a etiqueta seja aplicada à embalagem do produto.

- Com uma etiqueta de leitura/gravação, os dados podem ser alterados adicionados ou até mesmo eliminados a qualquer momento durante o seu ciclo de vida.

2.5.5 Antenas

As antenas são condutores da comunicação de dados entre a etiqueta e o leitor. O estilo da antena e o posicionamento representam um fator significativo na determinação da área de cobertura, alcance e acurácia da comunicação. Por exemplo, a chamada antena de leitura linear oferece um alcance maior do que a antena de leitura circular. Ao mesmo tempo, uma antena linear apresentará resultados de leitura menos acurados em aplicações onde a orientação da antena de uma etiqueta, com relação à antena do leitor, variar aleatoriamente. Isto faz com que a antena linear se torne mais adequada em aplicações onde a orientação de um item adequado seja sempre a mesma, como em uma linha de montagem automatizada.

A antena da etiqueta normalmente é montada na mesma superfície do CI e acondicionada como unidade única[2].

2.5.6 Componentes Lógicos

Os componentes lógicos são sistemas de softwares que fazem todo o controle de um sistema **RFID**. Vão desde a camada de comunicação de um leitor com uma antena, até o software instalado em um terminal que recebe estas informações.

A API (*Application Programming Interface* ou Interface de Programação de Aplicativos) é o primeiro dos componentes lógicos de um sistema **RFID**. A função da API é criar um conjunto de rotinas e padrões para estender as funcionalidades de um sistema, permitindo agregar valor e recursos ao sistema com a finalidade de ter o desempenho designado no início do projeto. A API é o que permite que outras aplicações comuniquem-se com o leitor; tem como principal função transformar informações vindas do *middleware* para as etiquetas (*tags*) e vice-versa. É na API em que são requisitados inventários, monitorada as atividades ou configurados ajustes no leitor.

Deve-se, também, controlar a comunicação no subsistema de comunicações. Este é responsável por selecionar o protocolo de comunicação com o *middleware*, como *Ethernet*, *Bluetooth*, serial ou algum outro tipo proprietário.

Com as informações adquiridas, um evento ocorre quando o leitor detecta uma *tag* no campo de sua antena e tem atrelado a essa observação uma ação requerida. Isto é a função do gerenciador de eventos. Cabe ao Gerenciador de Eventos definir o evento, filtrar esses eventos e, então, decidir qual seu destino, como ser enviado para um relatório ou uma aplicação externa.

O *middleware* é o software mediador. O *middleware* é o software responsável por pegar informações vindas do leitor ou do gerenciador de eventos e transferi-las para um sistema gerenciador de produtos ou um software de controle de estoques ou vendas por exemplo[2,15].

2.5.7 Definindo a Frequência de Operação

Um dos aspectos mais importantes da conexão entre uma etiqueta e um leitor é a frequência em que ele opera. A frequência de operação pode variar com base na aplicação, nas normas e nos regulamentos. Em geral, a frequência define a taxa de transferência de dados entre a etiqueta e o leitor. Quanto menor a frequência, mais lenta a taxa de transferência. Todavia, a velocidade não é o único aspecto a ser analisado no planejamento de uma solução de **RFID**. As condições ambientais podem desempenhar um papel significativo na determinação da frequência de operação ideal para uma aplicação em particular. Por exemplo, o substrato em que as etiquetas são afixadas (tal como latas de refrigerantes) e a presença de outros dispositivos geradores de onda de rádio podem gerar interferências nas faixas de UHF e de micro-ondas respectivamente[2].

Os sistemas de RFID estão delimitados na sua grande maioria a três faixas de frequências:

- LF (Low Frequency) – Faixa de operação de 125 kHz até 134 kHz. São denominados sistemas baixa frequência;
- HF (High Frequency) – Faixa de operação de 13,56 MHz. São denominados sistemas de alta frequência;

- UHF (Ultra Frequency) – Faixa de operação de 860 MHz até 960 MHz. São denominados sistemas de UHF.

Para que um sistema seja classificado como uns sistemas RFID LF ele deve operar na faixa de frequência de 125 kHz até 134 kHz. Nesta faixa de frequência encontramos os sistemas de RFID mais antigos e estáveis do mercado sendo que as principais características dos sistemas que operam nesta faixa de frequência são:

- Baixa taxa de transferência de dados (leva até 100 ms para a leitura de um *tag* de 16 caracteres);
- Leitura de apenas um *tag* por vez;
- Só existe com sistema de alimentação passivo;
- Pequenas distâncias de leitura (máximo de 30 cm);
- Não sofre absorção pelos líquidos;
- Baixo desempenho próximo a metais;
- Leitores de baixo custo e *tags* de alto custo;
- *Tags* de tamanho elevado;
- Aplicações: Identificação de gado, controle de acesso, identificação de atletas.

Para que um sistema seja classificado como um sistema RFID HF ele deve operar na faixa de frequência de 13,56 MHz. Os sistemas de HF são sistemas já estáveis que estão no mercado a mais de vinte anos. A faixa de frequência de 13,56 MHz é conhecida como banda ISM (Industrial, Scientific, Medical) sendo que é uma faixa de frequência que não necessita de licença para operar[9]. As principais características dos sistemas que operam nesta faixa de frequência são:

- Boa taxa de transferência de dados (leva até 20 ms para a leitura de um *tag* de 16 caracteres);
- Leitura de múltiplos *tags* por vez (40 *tags* por segundo);
- Só existe com sistema de alimentação passivo;

- Médias distâncias de leitura (máximo de 1 metro);
- Não sofre absorção pelos líquidos;
- Baixo desempenho próximo a metais;
- Leitores de alto custo e *tags* com custo médio;
- *Tags* de várias dimensões;
- *Tags* com várias funcionalidades de memória (password, criptografia);
- Possui padrões estabelecidos como o ISO 15636 e EPC;
- Aplicações: Controle de acesso, identificação de itens, chaves de ignição de veículos, controle de alimentos e identificação de pacientes.

Para que um sistema seja classificado como um sistema RFID UHF ele deve opera na faixa de frequência de 860 até 960 MHz. São os sistemas de RFID UHF que estão gerando a maior expectativa e motivação para as implantações de RFID. Esta faixa de frequência também é também é classificada como banda ISM. Além disso, as características eletromagnéticas desta faixa de frequência contribuem para a implantação de RFID para toda a cadeia logística e outras aplicações. As principais características destes sistemas são:

- Distância de leitura de até 10 metros (para *tags* passivos) e 100 metros (para *tags* ativos);
- Protocolo de anti-colisão, até 1000 *tags*/segundo;
- Absorção da energia pelos líquidos;
- Acoplamento Reflexivo;
- Alta taxa de transferência de dados;
- Bom desempenho perto do metal;
- *Tags* de menor tamanho;
- Utilizado para: Controle da cadeia logística, controle de falsificação;
- Identificação de veículos, Identificação de ferramentas, Padrão mundial EPC[6].

CAPÍTULO 3 – PADRÕES E ÓRGÃOS REGULAMENTADORES

3.1 PAPEL DOS PADRÕES NO AVANÇO E NA ADOÇÃO DA TECNOLOGIA

A criação e a adoção dos padrões oficiais poderão acelerar potencialmente a adoção da nova tecnologia. Os padrões prometem interoperabilidade, atraindo mais fornecedores a apresentarem soluções que melhorem os serviços e diminuam os custos. Com o cumprimento dos padrões, os desenvolvedores e fornecedores da tecnologia evitam o risco de modificações caras que podem resultar de implementações customizadas ou proprietárias, ou do não cumprimento dos regulamentos. Os padrões proporcionam aos consumidores a confiança de que os produtos funcionaram em conjunto, de que eles terão mais escolhas e de que eles não ficarão sujeitos a fornecedores exclusivos. Isto tem sido verdade em um mercado tecnológico após outro.

Os padrões ajudam a atender os consumidores de várias formas. Eles garantem que produtos diferentes não interfiram nas funções de cada um, independente de qual fabricante os tenha produzido. Por exemplo, um telefone celular opera em uma frequência específica. Estas frequências são diferentes das usadas para transmissão de sinais de TV. Como resultado, um telefone celular e uma TV não interferem entre si mesmo quando estão operando próximos um do outro.

Os padrões também permitem interoperabilidade entre as aplicações ou dispositivos. Quando um consumidor compra um telefone celular de acordo com o padrão GSM, ele vem equipado com um cartão SIMcard miniatura. Este cartão armazena todos os dados do telefone, tais como número do telefone e a agenda de telefones. Se o consumidor decidir trocar de telefone mais tarde, tudo o que ele tem a fazer é inserir o cartão SIMcard antigo no novo telefone. O seu número de telefone antigo irá chamar o novo telefone e a sua agenda de telefones estará disponível no novo telefone. O cartão SIMcard padronizado garante uma interoperabilidade perfeita de um equipamento para o outro. Portanto, quando os padrões de ponta a ponta da cadeia de abastecimento não existem, conforme foi o caso da **RFID**, a tecnologia pode ser adequada apenas para determinados nichos de mercados. Entretanto, com a criação da EPC (*Eletronic Product Code)* Global, os padrões de **RFID** de ponta a ponta tornaram-se possíveis[2].

3.2 OS PADRÕES E O RFID

Antes da criação dos padrões para as etiquetas e leitoras, as empresas criaram essencialmente sistemas de **RFID** proprietários, de modo que os leitores de um fornecedor geralmente liam apenas as etiquetas do mesmo fornecedor. As primeiras aplicações de **RFID**, tais como as de cobrança eletrônica de pedágio e rastreamento de animais vivos, foram baseadas nestes sistemas proprietários. Esta falta de interoperabilidade limitou os incentivos para que as empresas implementassem as soluções de **RFID** mais amplamente e para que os desenvolvedores criassem uma tecnologia de **RFID** inovadora.

Essa situação começou a mudar no final dos anos 1990, com a criação do Auto-ID Center. Ele iniciou a criação de um padrão para facilitar a interoperabilidade em larga escala entre os sistemas de **RFID** de múltiplos fornecedores.

A EPC Global é uma organização global mantida por indústrias e que trabalha na regulamentação do EPC, *Eletronic Product Code*, ou seja, o Código Eletrônico de Produtos. O EPC, segundo o site da EAN Brasil, entidade vinculada à EPC Global, define uma nova arquitetura que utiliza recursos oferecidos pelas tecnologias de radiofreqüência e serve como referência para o desenvolvimento de novas aplicações. Tem como premissa fazer uso completo das mais recentes infraestruturas como é a Internet, significando uma mudança de conceito na identificação e, principalmente, no intercâmbio de informações. O EPC agiliza os processos e permite dar maior visibilidade aos produtos por meio da disponibilização de informações superior ao que se alcança hoje com as tecnologias disponíveis. É o rastreamento total, não somente de um processo ou de uma empresa, mas de cada produto individual aberto para toda a cadeia de suprimentos. A EPC Global é uma organização sem fins lucrativos que tem como intuito controlar, desenvolver e promover padrões baseados nas especificações do sistema EPC[2].

O sistema EPC tem uma estrutura lógica bem básica. Um produto contendo o seu EPC, que é um número único que obedece a determinadas regras, é lido pelo leitor e, então, passado ao software (*middleware*), que irá administrar informações como fabricante, data de fabricação, data de entrega, etc. a estrutura do formato básico de um número EPC segue as regras descritas na Figura 7.

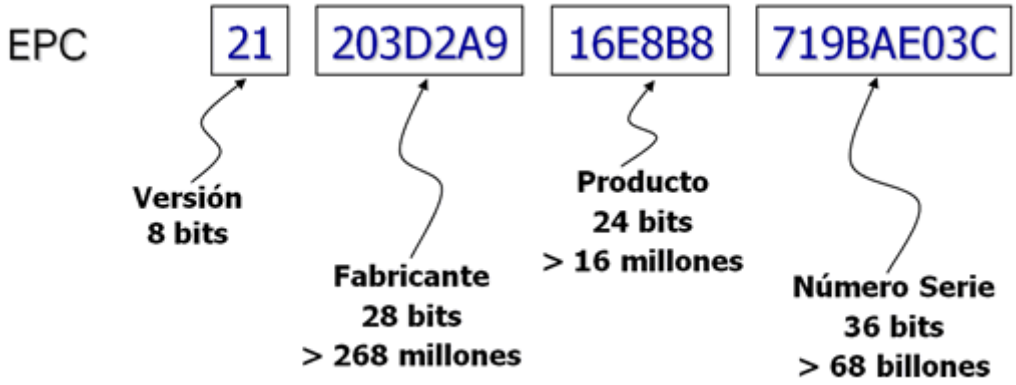


Figura 7 - Formato número EPC[4]

Todos os produtos que contenham um EPC têm o seu logotipo, identificando que aquele produto contém tal sistema, conforme mostra a Figura 8.

Figura 8 - Logomarca da EPC[4]

Os benefícios para estas especificações é a capacidade de identificar e rastrear exclusivamente cada objeto. Sem isto, o rastreamento e as medidas anti-falsificações não seriam possíveis. Vários outros problemas também podem ocorrer sem estas especificações. Por exemplo, os dados da etiqueta não seriam entendidos ou trabalhados por outras aplicações, diminuindo sua utilidade, ou as aplicações existentes teriam que se regravadas para lerem os dados da etiqueta, exigindo um gasto significativo para as empresas.

3.3 CLASSES DO PADRÃO EPC

Quanto às especificações, os sistemas **RFID** são descritos pela EPC Global em duas Classes: 0 e 1. Cada uma delas possui especificações e peculiaridades distintas. Vale lembrar que, nenhuma documentação regulamentar sobre sistemas **RFID** foi completamente fechada; todos ainda podem sofrer algum tipo de alteração por estarem em constante atualização.

As *tags* de classe 0 (zero) funcionam na frequência de 900 MHz e são mais comumente usadas no gerenciamento de cadeias de suprimento, como terminais de caixa de

supermercado e armazéns. Estes tipos de *tags* são programadas nas fábricas e são do tipo passivas (não contém uma fonte própria de energia). Os fatores de desempenho para estas etiquetas são:

- Regulamentações de Compatibilidade Eletromagnética – o principal impacto é na escolha de um algoritmo anti-colisão viável a ser empregado em UHF;
- Regulamentações para exposição humana a campos eletromagnéticos;
- Tamanha da antena da *tag* – é preciso um ajuste para que pequenas *tags* tenham uma melhor eficiência, ou seja, minimizar a força e maximizar a desempenho (*backscatter*);
- Parâmetros de Comunicação para a interface aérea (*air interface*) – comunicação compacta e com um nível apropriado de segurança para a leitura do EPC;
- Algoritmo anti-colisão para a leitura de múltiplas *tags* – o número de *tags* que podem ser lidas em um mesmo segundo é de grande importância.

Para o design destas *tags* temos os seguintes parâmetros:

- O design deve permitir a produção de *tags* a um custo muito baixo;
- A operação do sistema deve permitir uma alta entrada de *tags* por segundo;
- O design deve permitir um bom alcance para funcionamento da *tag*;
- O design deve ter uma tolerância de sistemas de leitura de *tags* similares nas redondezas.

Quanto ao algoritmo anti-colisão, é usado geralmente uma árvore binária, esta é escaneada por um método chamado "*reader talks first"* (leitor fala primeiro). Este protocolo vê a disputa entre as *tags*, por isto é livre de colisões, negociando os dados das várias *tags.*

As características da solução são: satisfazer os objetivos de designs descritos, serem compatíveis com a grande variedade de *tags* EPC e futuras versões, permitirem uma grande quantidade de operações com a *tag* e não diminuir a velocidade com o aumento do número de das mesmas, permitir a destruição das *tags*, ser fabricada com baixo custo e ser adaptável às atuais regulamentações americanas e europeias.

Quanto à classe 1 (um), o primeiro tipo a ser descrito é o de 13.56 MHz ISM Band. A Classe 1 tem o princípio de comunicar um identificador único e outras informações requeridas para obter um identificador único durante o processo de comunicação. As etiquetas de Classe 1 podem ser WORM (Uma leitura/Várias Gravações) ou de Leitura/Gravação, ou seja, é permitida a gravação de novas informações nas *tags* a qualquer momento de sua vida útil através de um leitor autorizado. Estas etiquetas são muito úteis para guardar os dados dinâmicos relacionados ao item, tais como procedência e modificações do item devido à montagem[9]. Pelo fato dos padrões ISO no **RFID** também usarem esta faixa de frequência, provavelmente muitas aplicações atuais de **RFID** nesta faixa de frequência serão encontradas. Esta especificação pode oferecer um caminho para garantir a interoperabilidade entre algumas das infraestruturas necessárias para estas aplicações. Os fatores de desempenho para estas etiquetas são:

- Natureza do gerador do campo de interrogação – geralmente a etiqueta funcionará no campo mais próximo, mas em alguns casos, estará em um campo mais distante;
- Regulamentações para exposição humana a campos eletromagnéticos;
- Tamanha da antena da *tag* – é preciso um ajuste para que as pequenas *tags* tenham melhor eficiência e que o mínimo de força seja requerido para o funcionamento da *tag*;
- Confiabilidade da leitura, gravação e destruição da *tag*;
- Algoritmo anti-colisão para a leitura de múltiplas *tags* – o número de *tags* que podem ser lidas em um mesmo segundo é o grande impacto. São usados algoritmos de escaneamento de árvores binárias.

Em relação ao design destas *tags* temos:

- Permitir produção a custo muito baixo;
- As especificações devem ser aplicadas a todas as variedades de etiquetas EPC de Alta-Frequência;
- Operação do sistema deve permitir uma alta entrada de *tags* por segundo;
- Bom alcance de operação, este depende do tamanho da antena;

- O design deve ter uma tolerância de sistemas de leitura de *tags* similares nas redondezas;

- Não permitir interferência entre etiquetas desenhadas para este padrão e etiquetas desenhadas para os padrões ISO de alta frequência.

Ainda, na Classe 1, o segundo tipo é o de 860-930 MHz. A Classe 1, como descrito anteriormente, tem como princípio o fato de comunicar um identificador único e outras informações requeridas durante o processo de comunicação. Porém, este sistema não se utiliza da Banda ISM, mas de uma faixa de frequência entre 860 MHz e 930MHz. Uma *tag* da Classe 1 contém um identificador único, corretor e identificador de erros e uma pequena senha. O identificador único é um número EPC válido; o corretor e detector de erros é o CRC (*Cyclic Redundancy Check*).

O último tipo de *tag* da Classe 1 são as da Classe 1 Gen2. Como já vimos, o padrão Classe 0 tinha a melhor performance de leitura só que não permitia gravação. Já a Classe 1 permitia gravação dos dados, mas tinha um desempenho inferior a Classe 0. Além destas limitações as necessidades da cadeia logística eram:

- Para alguns casos leitura superior a 10 metros;

- Baixa interferência entre leitores;

- Maior densidade de *tags* (mais de 1500 *tags* por segundo);

- Padrão único para o mundo todo;

- Capacidade de escrita e leitura quantas vezes fosse necessário.

Com esses dados foi criado o padrão que hoje domina todo o mercado de **RFID**, o EPC Classe 1 Gen2 ou simplesmente GEN2. As principais características deste padrão são:

- Distância de leitura de até 10 metros;

- Operação em ambientes com vários leitores próximos;

- Densidade de *tags* de até 1600 *tags* por segundo

- Padrão mundial e compatível com todos os fabricantes;

- Leitura e gravação;
- Capacidade de memória da *tag* de até 400 bits.

Desde a finalização do padrão em setembro de 2005 todos os esforços e investimentos das empresas de tecnologia estão focados no padrão GEN2. Todos os projetos já implantados com Classe 1 e Classe 0 deverão ser substituídos gradativamente por equipamentos GEN2. A EPC Global também determina quer os sistemas da Classe 1 Geração 2, trabalhem a uma faixa de frequência de 860 MHz a 960 MHz; estes são do tipo passivo (trabalham por *backscatter*) e são do tipo ITF (*Interrogator-talks-first*, interrogador fala primeiro). Para esta faixa de frequência adotada, a mesma inclui as frequências de UHF dos leitores usados tanto na América do Norte como na Europa. Para as empresas globais, os benefícios são óbvios. Os produtos etiquetados com as etiquetas da Geração 2 podem ser embarcados para o mundo inteiro e lidos pela infraestrutura dos leitores de UHF local, eliminando a necessidade de aplicação de diversos tipos de etiquetas nos produtos dependendo de seus destinos[15]. Para um projeto **RFID** os leitores e *tags* devem obedecer algumas regras, vejamos:

Os leitores devem:

- Conhecer os requisitos do protocolo;
- Implementar os comandos principais definidos no protocolo;
- Modular (transmitir) e demodular (receber) um conjunto suficiente de sinais elétricos definidos na camada de sinalização do protocolo conforme as *tags* e todas as regulamentações de sinais de rádio locais.

Os leitores podem:

- Implementar qualquer subconjunto de comandos opcionais definidos no protocolo;
- Implementar todos os comandos próprios, desde que estejam de acordo com o protocolo.

Os leitores não devem:

- Implementar comandos que entrem em conflito com o protocolo;
- Requerer, usando comandos próprios, as exigências do protocolo.

Quanto às *tags*, elas devem:

- Conhecer os requisitos do protocolo;
- Implementar os comandos principais definidos no protocolo;
- Modular um sinal refletido (*backscatter*) somente se receber um comando de requisição do interrogador;
- Estar em conformidade com todas as regulamentações de rádio locais.

As *tags* podem:

- Implementar quaisquer subconjuntos de comandos opcionais definidos no protocolo;
- Implementar quaisquer comandos próprios, desde que estejam de acordo com o protocolo.

As *tags* não podem:

- Implementar comandos que entrem em conflito com o protocolo;
- Requerer, usando comandos próprios, as exigências do protocolo;
- Modular um sinal refletido (*backscatter*) sem este ser sido comandado (requerido).

A Figura 9 mostra a distribuição do mercado global, de 2000 a 2005, para *transponders* na várias faixas de frequências, em milhões de unidades.

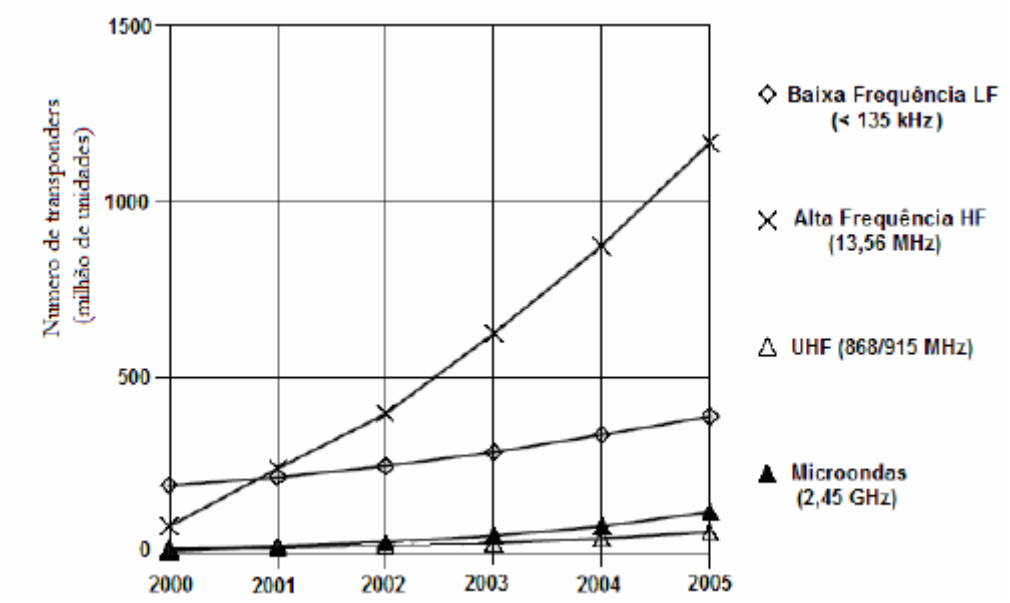


Figura 9 – Distribuição do mercado de transponders por faixas de frequências[8]

Vale ressaltar que devido à substituição de projetos já implantados com Classe 1 e Classe 0 para o padrão GEN2 a partir de 2006, que trabalha na faixa de frequência de 860 MHz a 960 MHz, o mercado para o *transponders* que operam nesta banda de frequência tiveram um aumento acentuado para os anos posteriores.

3.4 FREQÜÊNCIA APROPRIADA PARA SISTEMAS DE RFID POR ACOPLAMENTO INDUTIVO

As características das faixas de frequências disponíveis devem ser levadas em consideração na escolha da frequência adequada para se utilizar em um sistema **RFID** por acoplamento indutivo, iremos falar sobre esse mecanismo no próximo capítulo, pois são importantes na decisão de alguns parâmetros do sistema, como por exemplo, as dimensões da antena.

A Figura 10 descreve a transição entre o campo próximo e campo distante para a frequência de 13,56 MHz. Percebe-se que a atenuação na intensidade de campo magnético é de 60 dB/década em campo próximo e de 20 dB/década depois da transição para campo distante, que ocorre a uma distância de $\lambda/2\pi$ da antena transmissora. Este comportamento exerce uma forte influência na definição de sistemas **RFID**[14].

Para frequências menores que 135 kHz, as relações são mais favoráveis, devido estar na região de campo próximo, permitindo um acoplamento magnético, o que é necessário para etiquetas de baixa frequência, que será explicado mais adiante. Há um aumento da intensidade de campo H em torno de 60 dB/década, à medida que se aproxima do dispositivo de leitura.

A Figura 11 mostra a relação entre o alcance do *transponder* em função da frequência para uma intensidade de campo H = 105 dB μA/m. O alcance máximo ocorre na faixa de frequência em torno de 10 MHz, onde a eficiência na transmissão de potência é maior que para as frequências abaixo de 135 kHz ou acima de 40,68 MHz. Entretanto, esse efeito é compensado pela alta intensidade de campo admissível (campo próximo) para frequências abaixo de 135 kHz. Consequentemente, na prática o alcance de sistema **RFID** é aproximadamente o mesmo para ambas as faixas de freqüências[8].

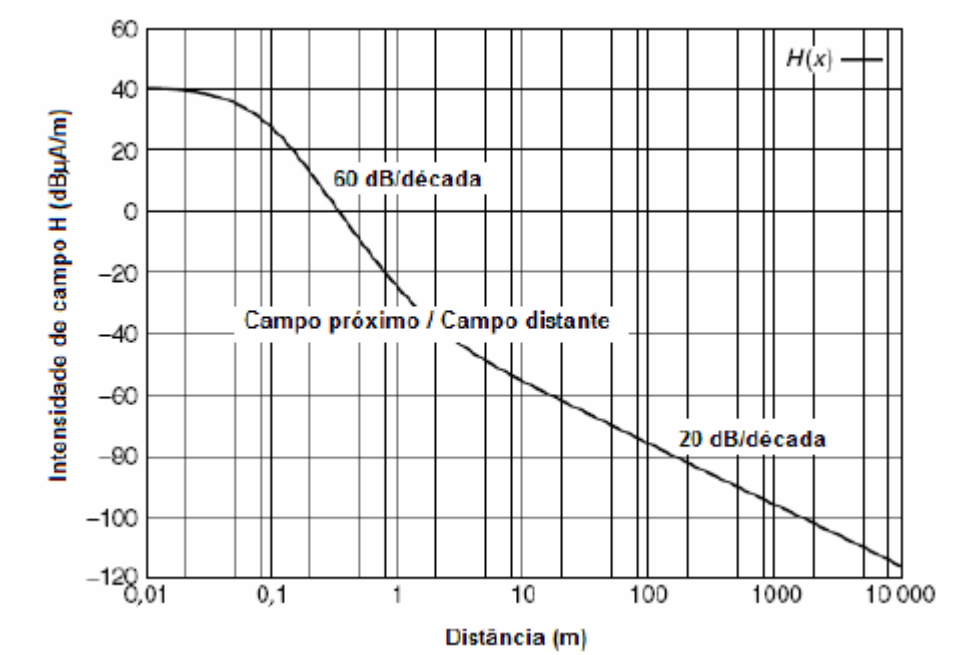


Figura 10 – Comportamento da Intensidade de Campo em Função da Distância Para a Freqüência de 13,56 MHz[8]

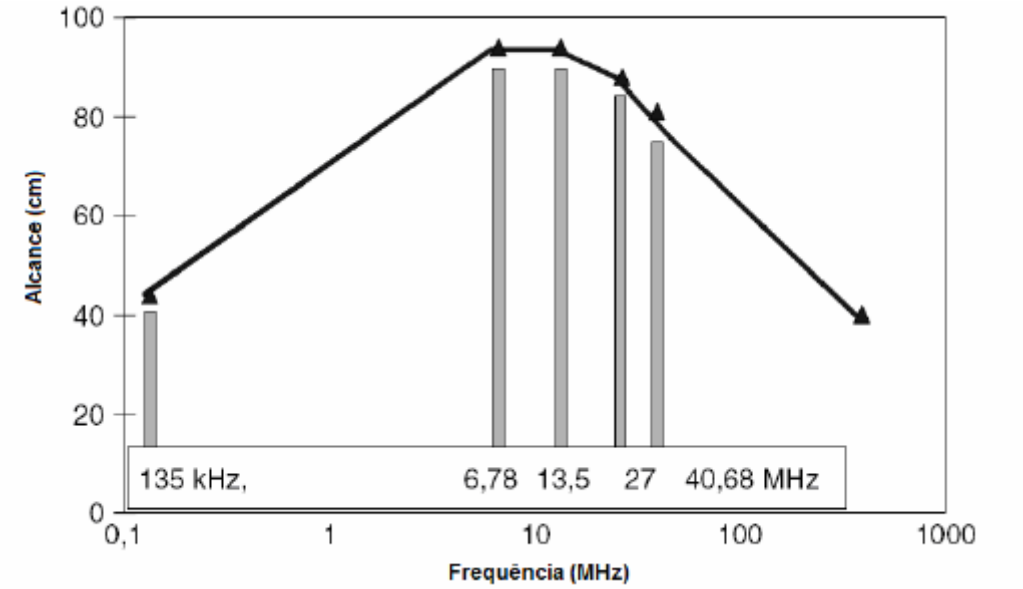


Figura 11 – Alcance do Transponder em Função da Freqüência de Operação, e Para H = 105 dBμA/m[8]

3.4.1 Dispositivos de Acoplamento Indutivo

Inclui os sistemas de **RFID** e os dispositivos de segurança utilizados em lojas de departamentos. Como exemplo, tem-se o mecanismo de segurança utilizado pela loja C&A, que possui antenas nas portas da loja e, em cada produto, é fixado uma *tag* do tipo 1-bit apenas para garantir que ninguém saia da loja com o produto sem antes passar pelo caixa.

3.5 PADRONIZAÇÃO ISO

A ISO, união internacional das instituições nacionais de padronizações, tem em seu comitê técnico a responsabilidade de desenvolver os padrões para os sistemas **RFID**. Nesta seção apresentados os padrões da ISO para sistemas de **RFID**. Vale lembrar que, assim como os padrões da EPC Global, tratados na seção anterior, os dos sistemas **RFID** sofrem constantes alterações.

A primeira padronização a ser abordada é a dos *Smart Cards*. Eles são cartões semelhantes aos cartões comuns: de crédito, bancários, de associados, de acesso e outros que fazem uso de uma faixa magnética. Os *Smarts Cards* possuem, em sua maioria, além da tarja magnética, um microprocessador e memória; da mesma forma, eles são encontrados nos chips

dos celulares GSM. *Smarts Cards* não possuem baterias, a energia é totalmente fornecida pelo leitor por acoplamento.

Existem três diferentes padrões para *Smarts Cards*: ISO 10536. Para cartões do tipo *Close Coupling* (acoplamento próximo), que operam a uma distância de 0 a 1 cm; ISSO 14443, para cartões do tipo *Proximity Coupling* (acoplamento de proximidade), para distâncias de 0 a 10 centímetros; e, por fim, ISSO 15693, para cartões *Vicinity Coupling* (acoplamento de vizinhança), que operam a distâncias de 0 a 1 metro.

Em segundo, as *tags* para ferramentas, seguem as especificações da ISSO 69873. Este padrão especifica as dimensões para as *tags* sem contato e seu espaço na montagem de ferramentas e cortadores; seus tamanhos e dimensões são necessários para o espaço de montagem.

O padrão que descreve os sistemas **RFID** para identificação de contêineres está descrito no ISSO 10374, que é um sistema automático de identificação específico baseado em *transponders* de micro-ondas. A faixa de frequência é de 580 a 950 MHz e 2400 a 2500 MHz.

No segmento de gerenciamento de itens, há um encontro da ISO com a EAN-UCC. Um grande número de novos padrões para gerenciamento de itens está em desenvolvimento. A iniciativa da Global é padronizar o **RFID**, pois milhões de companhias pelo mundo usam seus sistemas. Os padrões usados são o ISO 15961, ISO 15962, ISO 15963, ISO 18000 e o ISO 18001.

Para identificação animal, os padrões são o ISO 11784, ISO 11785 e ISO 14223. O padrão não descreve o design, por isto ele pode ser adaptado ao animal, em forma de coleiras, brinco ou vidro (injetável). O tamanho total é de 64 bits (8 bytes).

Por fim, os Sistemas Anti-Roubo (EAS Systems) não são padronizados pela ISO, mas pela VDI. O padrão está descrito no VDI 4470. Neste sistema, como já descrito, os usuários atravessam, com um produto etiquetado, um portal (*gate*) e este emite um alarme caso a *tag* não tenha sido desabilitada ou retirada do produto[15].

CAPÍTULO 4 – PRINCÍPIOS DE FUNCIONAMENTO

4.1 INTRODUÇÃO

Os sistemas **RFID** são classificados em duas principais categorias: 1-bit *transponder* e n-bit *transponder*. Os sistemas 1-bit funcionam, basicamente, por meio de fenômenos físicos e se subdividem em 5 categorias. Os sistemas n-bit são subdivididos conforme o mecanismo de transmissão de dados; neste tipo de sistema há, de fato, um fluxo de dados entre o *transponder* e o dispositivo de leitura. A Figura 12 apresenta a classificação dos diferentes tipos de **RFID**. Nesta figura, também estão indicadas as seções deste capítulo que tratam de cada um dos tipos de **RFID**.

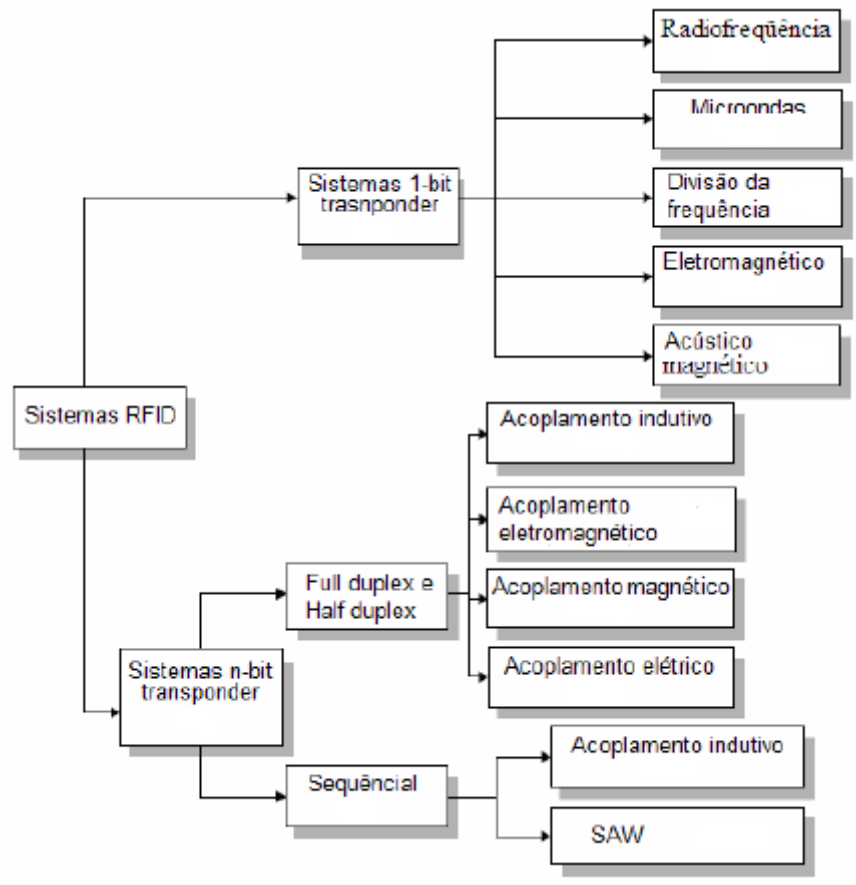


Figura 12 - Classificação dos sistemas RFID quanto ao princípio de funcionamento[8]

4.2 SISTEMAS 1-BIT TRANSPONDER

Os sistemas 1-bit *transponder* trabalham com apenas dois estados: ativado ou desativado. O estado ativado significa que a *tag* encontra-se na zona de leitura do receptor e, no estado desativado, não há presença da *tag* na zona de leitura. Todos os 5 tipos de sistemas de 1-bit seguem essa mesma ideia de identificação por estados[8,15].

4.2.1 Sistemas de 1-bit por Radiofreqüência

Esse mecanismo é baseado em circuitos ressonantes, contidos nos *transponders* passivos. O dispositivo de leitura gera um campo magnético alternado na faixa de radiofreqüência em torno de 8,2 MHz conforme a Figura 13. A região de atuação do campo é controlada por meio da potência fornecida à bobina do dispositivo de leitura. Se o *transponder* estiver na região de atuação do dispositivo de leitura, a energia proveniente do campo alternado gerado pelo dispositivo de leitura induz uma corrente no circuito LC do *transponder*. Se a frequência do dispositivo de leitura combinar com a frequência de ressonância do circuito LC contido no *transponder*, o sistema ressonante responde com uma pequena mudança na tensão entre os terminais da bobina (antena) do dispositivo de leitura (gerador).

A magnitude dessa queda de tensão depende da separação entre as bobinas do dispositivo de leitura e do *transponder*, e do fator de qualidade Q do circuito ressonante formado pelo sistema (gerador e *transponder*).

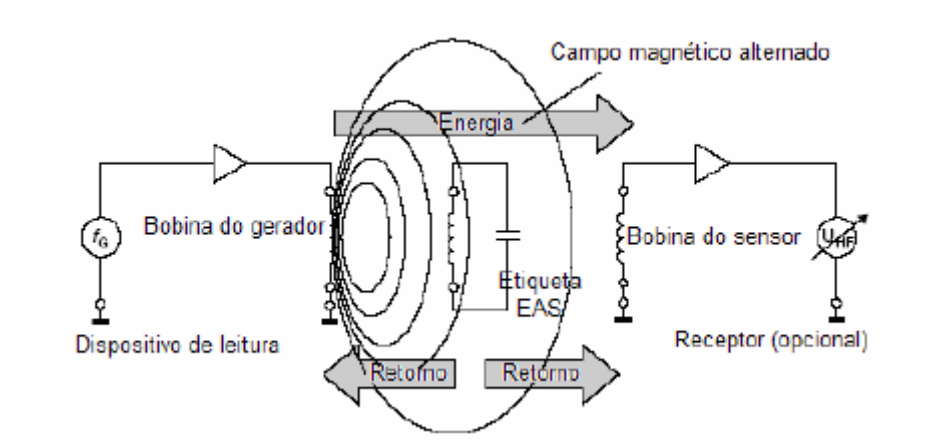


Figura 13 – Princípio de operação de um sistema 1-bit transponder por radiofreqüência[8]

Como as variações na tensão das bobinas do dispositivo de leitura ou do sensor são geralmente baixas e, portanto, difícil de serem detectadas, o sinal deve ser livre de interferência. Nesse caso, a frequência do campo gerado varia entre um valor mínimo e um valor máximo. O sistema começa a oscilar sempre que a frequência varrida pelo gerador corresponde a frequência de ressonância do *transponder*, produzindo uma queda de tensão nas bobinas do gerador e do sensor, se este for utilizado.

Tal queda de tensão é percebida e utilizada para sinalizar a presença do *transponder* na região de leitura. A Figura 14 mostra o comportamento da impedância nos terminais da bobina no dispositivo de leitura para esse tipo de sistema, onde a frequência do campo varia entre um valor mínimo e um valor máximo e, no momento em que as frequências se cruzam, ocorre uma variação na impedância da bobina do dispositivo de leitura e, consequentemente, uma queda na tensão entre os seus terminais.

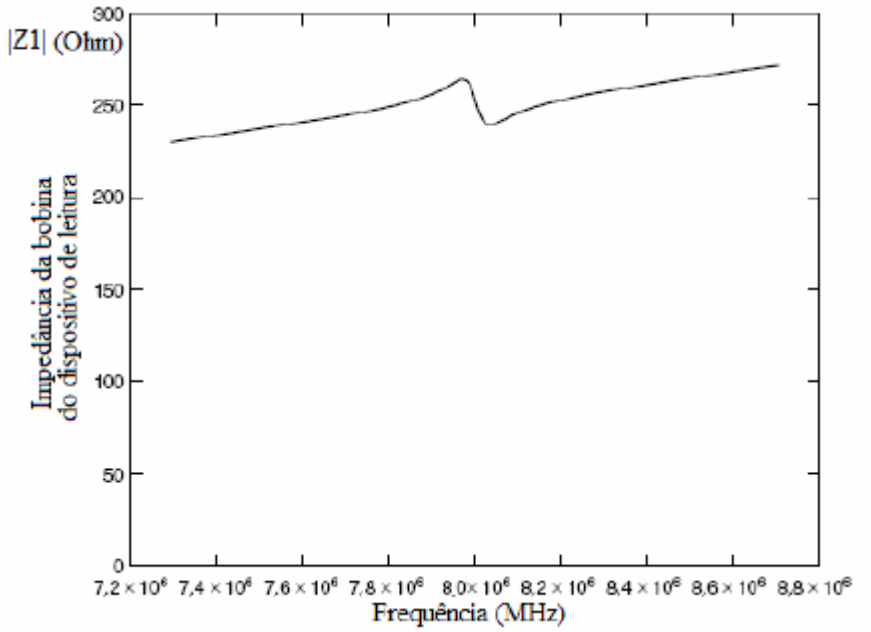


Figura 14 – Variação na impedância entre os terminais da bobina do dispositivo de leitura[8]

A impedância da bobina do dispositivo de leitura com a presença do *transponder* em uma área de atuação é dada pela equação 4.1 que é modelada a partir da Figura 15.

$$Z_1 = R_1 + j\omega L_1 + Z_T \qquad (4.1)$$

onde

$$Z_T = \frac{(\omega.k)^2.L_1.L_2}{R_2 + j\omega L_2 + \frac{R_L}{1+j\omega L_1 C_2}}$$

- Z_1é a impedância nos terminais da bobina do dispositivo de leitura;
- R_1é a resistência do enrolamento da bobina do dispositivo de leitura;
- R_2é a resistência do enrolamento da bobina do trasnsponder;
- L_1é a indutância da bobina do dispositivo de leitura;
- L_2é a indutância da bobina do *transponder*;
- C_2é a capacitância contida no circuito do *transponder*;
- *k* é o coeficiente de acoplamento;
- ωé a frequência angular gerada no dispositivo de leitura.

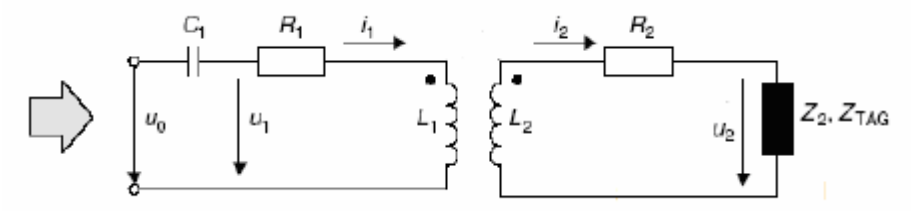


Figura 15 – Modelo do circuito elétrico para o sistema 1-bit transponder por radiofreqüência[]

Esse tipo de sistema é muito usado em lojas de departamentos como sistemas anti-furto. Os transponders podem ser destruídos por um campo magnético suficientemente intenso, de modo que a tensão induzida destrua o capacitor contido no *transponder*.

4.2.2 Sistema de 1-bit por Micro-ondas

Este também é um sistema utilizado em lojas de departamento, porém trabalha na faixa de micro-ondas explorando a geração de componentes harmônicas não-lineares. Neste tipo de sistema normalmente são utilizados diodos, devido à sua característica não-linear de

armazenar energia. O número e a intensidade das harmônicas dependem da característica do diodo capacitivo utilizado. O layout de um sistema 1-bit *transponder* por micro-ondas é muito simples: um diodo é conectado a uma antena dipolo projetada para a frequência da portadora, conforme a Figura 16. Em geral, a frequência da portadora para sistemas desse tipo é *fp* = 2,45 GHz e o comprimento do dipolo é 6 cm. Também são usadas as frequências de 5,6 GHz e 915 MHz (Europa) como portadoras[8].

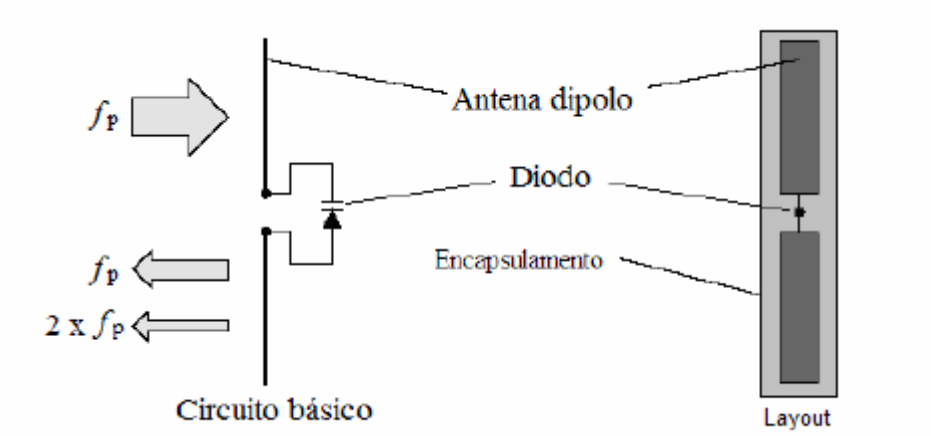


Figura 16 - Princípio de funcionamento de um sistema 1-bit transponder por microondas[8]

O funcionamento ocorre quando a *tag* está na zona de leitura e, devido ao campo elétrico alternado, flui uma corrente pelo dipolo até que o diodo que, por sua vez, gera e radia, em geral, os 2º e 3º harmônicos da frequência da onda portadora. O dispositivo de leitura é capaz de perceber a frequência dos harmônicos a que foi ajustada. A Figura 17 representa este sistema de identificação. Para garantir maior segurança e precisão ao sistema, faz-se uso da modulação em amplitude ou em frequência (ASK ou FSK) da onda portadora. Assim, as harmônicas terão a mesma modulação, permitindo que o sinal esteja livre de interferência do meio externo.

No exemplo da Figura 17, a onda portadora foi modulada em ASK com 1 kHz e a frequência da portadora é *fp* = 2,45 GHz. Portanto, o segundo harmônico é de 4,9 GHz e o terceiro de 7,35 GHz. Considerando que o dispositivo de leitura esteja ajustado para o segundo harmônico e que a *tag* esteja na zona de leitura, o alarme é ativado.

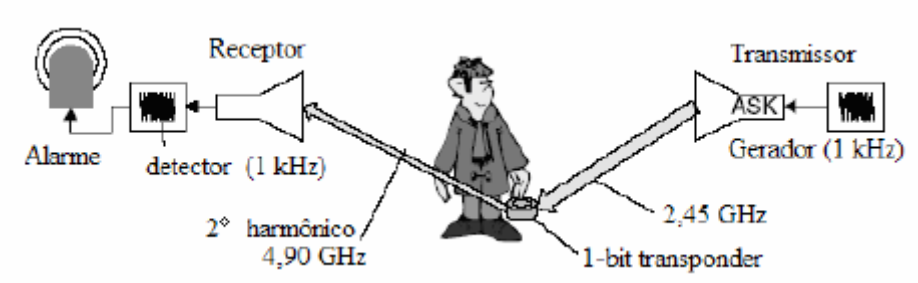


Figura 17 - Exemplo de um sistema de loja de departamentos utilizando 1-bit transponder por microondas[8]

4.2.3 Sistemas de 1-bit Transponder por Divisão da Frequência

Este tipo de sistema opera em uma grande faixa de frequência: de 100 Hz a 135,5 kHz. A *tag* é constituída por uma bobina, um circuito ressonante e um microchip que tem por função dividir por 2 a frequência da portadora e re-emitir o sinal para o dispositivo de leitura que fará a identificação e execução da aplicação. O processo é semelhante ao do sistema anterior, porém com uma redução da frequência da portadora pela metade. Também é usado modulação na amplitude ou na frequência (ASK ou FSK) a fim de melhorar o desempenho do sistema. A Figura 18 exemplifica este tipo de sistema.

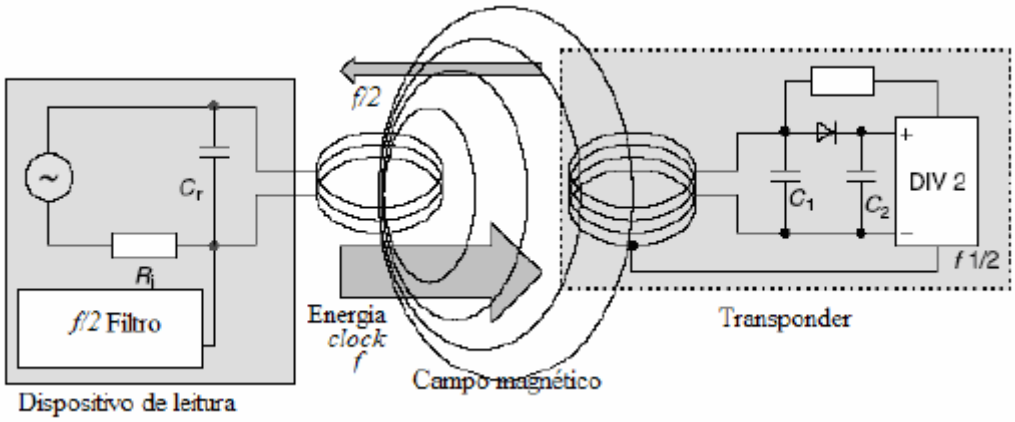


Figura 18 - Sistema de 1-bit transponder por divisão de freqüência[8]

4.2.4 Sistema 1-bit Transponder por Efeito Eletromagnético

Os *transponders* são constituídos por uma fita delgada de material magnético amorfo, possuindo uma curva de histerese. Este tipo de sistema utiliza campos magnéticos na faixa de frequência entre 10 Hz e 20 kHz. A saturação magnética desta fita ocorre quando a fita é submetida a um intenso campo magnético alternado. A característica não-linear entre o campo magnético H e a densidade de fluxo magnético B, próximo a saturação, mais a mudança

repentina da densidade de fluxo magnético B na vizinhança do campo H igual a zero, produz componentes harmônicas na frequência de operação do *transponder*.

O sistema por efeito eletromagnético pode ser melhorado sobrepondo-se seções adicionais de sinal com frequências mais elevadas sobre o sinal principal. Assim, o dispositivo de leitura reagirá com frequência harmônica básica e também com a soma ou diferença dos sinais extras, o que garante maior confiabilidade ao sistema. Devido à baixa frequência de operação, possuem a desvantagem de depender da posição do *transponder* presente na região de interrogação do dispositivo de leitura. As linhas de campo magnético do *transponder* devem estar verticalmente arranjadas através da fita do metal amorfo.

Este sistema é muito utilizado em loja de departamentos e bibliotecas devido ao baixo custo do dispositivo de leitura e do *transponder*. O *transponder* é muito pequeno e, portanto, pode ser escondido dentro da capa de um livro ou atrás da etiqueta de algum produto. Outro fator importante é que esse tipo de *transponder* pode ser ativado e desativado por inúmeras vezes através da magnetização e desmagnetização[15].

4.2.5 Sistema de 1-bit Transponder por Efeito Acústico-Magnético

Operando por efeito acústico-magnético, o sistema utiliza de duas fitas de material magnético amorfo, assemelhando-se muito ao sistema por efeito eletromagnético. Neste caso, porém, o efeito considerado é a vibração decorrente das variações inter-atômicas, ou seja, a distância entre os átomos varia com o campo magnético alternado aplicado na direção longitudinal. A amplitude da vibração é alta quando a frequência do campo magnético é igual à frequência de ressonância(acústica) da fita de metal. A Figura 19 mostra o funcionamento deste tipo de sistema. Quando a *tag* encontra-se na região de leitura do transmissor e do sensor, as fitas de metal começam a oscilar devido à influência do campo magnético. A oscilação na frequência de ressonância do material é facilmente percebida pelo dispositivo de leitura. A vantagem deste sistema em relação ao anterior é que a desmagnetização da fita só pode ser feita por um campo magnético intenso e com um decaimento lento na magnitude do campo magnético aplicado[8].

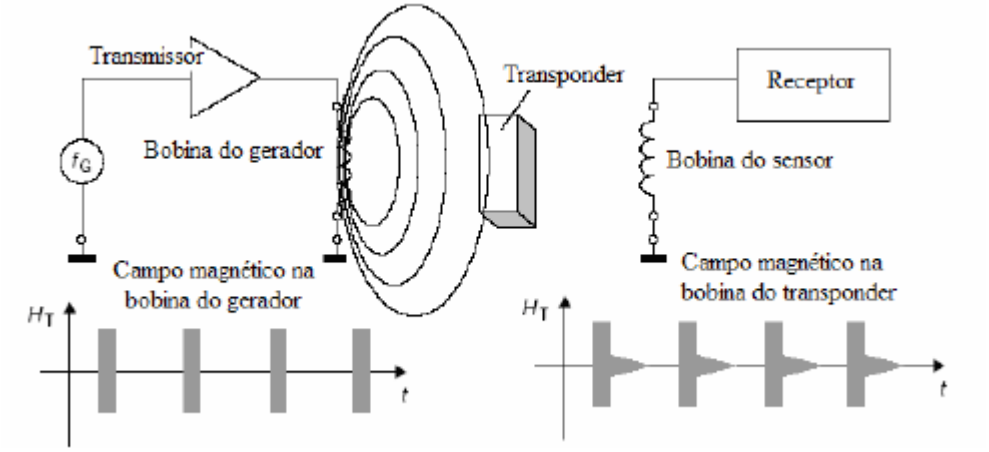


Figura 19 – Sistema 1-bit transponder por efeito acústico-magnético[]

4.3 COMPLEXIDADES DO SISTEMA

Nesta seção iremos tratar de sistemas mais complexos, que podem ser classificados como, *Low-end Systems, Mid-Range Systems e High-end Systems* que são três das denominações adotadas para classificar os sistemas de **RFID**.

Em uma das pontas, o *Low-end Systems* são os mais simples caracterizados pelo sistema; eles checam e monitoram se há presença de algum transponder na área de cobertura da antena, também chamada de área de interrogação. O tipo mais simples de um sistema *Low-end* é o sistema EAS. Também, neste tipo de classificação estão os *transponders* com microchip e memória de somente leitura, geralmente esta possui um único número de série imutável. Quando está na área de interrogação, a *tag* começa a espalhar o seu sinal por toda a mesma; esta ação é chamada de *broadcast*. Devido a essa característica, quando uma *tag* está dentro da área de cobertura da antena, outras *tags* não podem estar, pois haveria uma colisão e nenhum *transponder* poderia se comunicar com o leitor. Este é o motivo da necessidade de se colocar apenas uma *tag* por vez na sua área de interrogação quando usamos os *Low-end Systems.*

Apesar desta limitação, este tipo de sistema é excelente para várias aplicações, devido, justamente, a sua simplicidade; as *tags* podem ter tamanhos reduzidos, não há necessidade de baterias e memória e o consumo de energia é baixo, portanto, o preço pode ser drasticamente menor. Eles podem operar em todas as frequências e o alcance das *tags* pode ser bem mais amplo, graças ao baixo consumo do microchip. É usada onde a quantidade de dados requerida é baixa.

O tipo de sistema *Mid-range* é caracterizado por uma variedade de sistemas com memória que permite escrita, esta varia de alguns bytes a 100 Kbytes, com memórias EEPROM ou SRAM. Já neste tipo de sistema, os *transponders* conseguem processar algum tipo de informação, como um tratamento anti-colisão, ele pode possuir mais de um *transponder* na área de interrogação. Outra característica do *Mid-range System* é a capacidade de armazenamento de processos de criptografia, como uma autenticação entre o leitor e a *tag*, que pode operar em qualquer frequência disponível.

Por fim, o *High-end System* é o mais completo sistema **RFID** da cadeia, caracterizado por um microprocessador e um sistema operacional de *Smart Card (SmartCard OS)*. Devido ao uso deste microprocessador, é possível implementar algoritmos de autenticação e encriptação mais fortes. O topo desta cadeia é ocupado pelo *dual interface Smart Card*, no qual há um co-processador criptográfico. O tempo que se ganha no uso deste co-processador é enorme, o que torna os *Contactless Smart Cards* usáveis em aplicações que requerem altos níveis de segurança de transmissão de dados, como uma bolsa eletrônica ou sistemas de tickets para transporte público. Este tipo de sistema deve operar exclusivamente na frequência de 13.56 MHz.

Quanto à comunicação em si, é necessário lembrar que uma *tag* é atrelada ao leitor através de uma frequência de rádio, o que torna necessária sua classificação.

Na comunicação FDX (*Full Duplex*), a *tag* e o leitor podem falar ao mesmo tempo; os dados são transferidos do transponder para o leitor e o mesmo ocorre deste para aquele. Na comunicação HDX (*Half Duplex*), cada um tem a sua vez de “falar”: os dados transferidos do *transponder* para o leitor alternam com aqueles vindos do leitor para o *transponder*, semelhante à comunicação por *walk-talk*.

Em ambos os casos, o leitor provê energia suficiente durante toda a conversa, exceto no caso da comunicação sequencial (SEQ), na qual é exigido um capacitor, por exemplo; este deve armazenar a energia que será utilizada quando a transmissão do leitor cessa, pois a transmissão de dados da *tag* para ele ocorre em pausas, também chamadas pulsos[15].

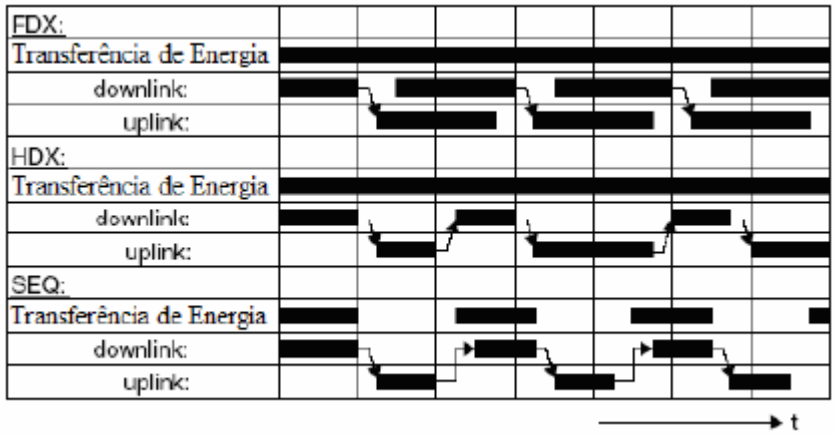


Figura 20 – Representação da transmissão full duplex, half duplex e seqüencial[8]

4.4 SISTEMAS N-BIT TRANSPONDER

Nos sistemas n-bit *transponder* há, de fato, uma comunicação e transmissão de dados entre os dispositivos de leitura e os respectivos *transponders*. Tais sistemas podem ser passivos ou ativos e a transmissão de dados entre eles pode ser do tipo *full duplex, half duplex* ou sequencial.

4.4.1 Sistema n-bit Transponder por Acoplamento Indutivo

Um *transponder* por acoplamento indutivo é constituído por um dispositivo eletrônico para armazenar os dados e uma bobina que funciona como antena. Em sua grande maioria, são elementos passivos que recebem a energia para seu funcionamento do dispositivo de leitura. A Figura 21 ilustra o princípio de funcionamento de um sistema **RFID** n-bit *transponder* por acoplamento indutivo. O dispositivo de leitura gera um campo eletromagnético nas frequências de 135 kHz ou 13,56 MHz, que penetra na área da bobina do *transponder* e induz uma tensão que é retificada e utilizada para alimentar o chip, que enviará de volta para o dispositivo de leitura o seu ID(código de identificação).

Na Figura 21, é visto que, paralelo à bobina do dispositivo de leitura e paralelo à bobina do *transponder*, têm-se capacitores cuja finalidade é formar um circuito ressonante ajustado na frequência de operação do dispositivo de leitura. Esse tipo de montagem pode ser comparado a um transformador. O acoplamento entre as duas bobinas do sistema é muito fraco e a eficiência na transmissão de potência entre as duas bobinas depende da frequência de operação, do número de enrolamentos, da área da seção transversal do *transponder*, do ângulo

entre as bobinas e da distância entre a bobina do *transponder* e a bobina do dispositivo de leitura. Seu funcionamento ocorre quando o *transponder* está na região de leitura (zona de interrogação) e sua frequência de ressonância corresponde à frequência do dispositivo de leitura.

Devido ao fraco acoplamento entre a bobina do dispositivo de leitura e a bobina do *transponder*, as flutuações na tensão da bobina do dispositivo de leitura, que representa o sinal útil, são de magnitudes menores que a tensão de saída do dispositivo de leitura, por exemplo, para sistemas de 13,56 MHz o sinal útil tem uma amplitude de tensão em torno de 10 mV. Para detectar estas pequenas flutuações, é necessário utilizar circuitos eletrônicos complexos e caros. A alternativa para controlar essa situação é utilizar a modulação de carga com sub-portadora. O processo é feito através da comutação da resistência de carga em frequência f_s = 212 kHz, o que gera duas linhas espectrais em $f_t \pm f_s$ em torno da frequência central de transmissão f_t = 13,56 MHz.

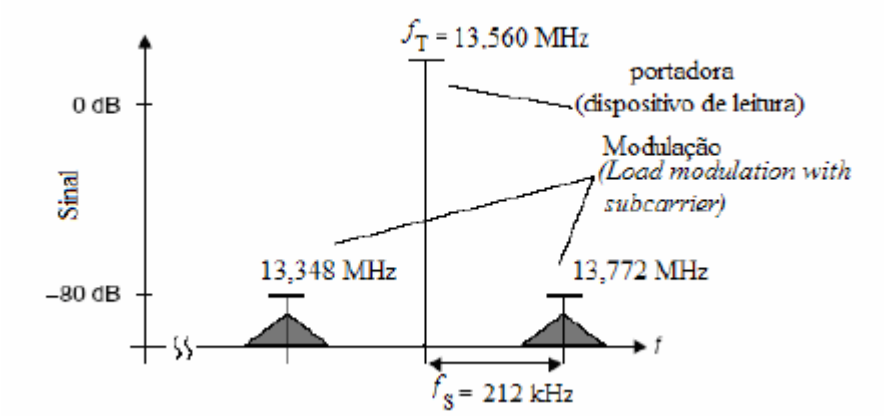


Figura 21 - Resultado da modulação de carga[8]

A modulação de dados é feita com modulação ASK, FSK ou PSK ou, ainda, modulando a sub-portadora no tempo através do fluxo de dados.

4.4.2 Sistema n-bit Transponder por Acoplamento Magnético

Os sistemas por acoplamento magnético (*Backscatter*) operam na faixa de UHF (868 MHz nos EUA e 915 MHz na Europa) e micro-ondas (2,5 GHz ou 5,8 GHz), possuem longo alcance e, por operarem em comprimentos de onda relativamente curtos, possibilitam o uso de antenas com pequenas dimensões e de boa eficiência.

A potência transferida para o *transponder* deve ser maior ou igual à perda no espaço livre mais a potência consumida pelo circuito eletrônico do *transponder*. A perda no espaço livre é dada por

$$P_{meio}(\text{dB}) = -147{,}6 + 20\log(\text{R}) + 20\log(f) - 10\log(G_T) - 10\log(G_R) \qquad (4.2)$$

em que R é a distância entre a antena do dispositivo de leitura e a antena (bobina) do *transponder*, G_T, o ganho da antena do transmissor, G_R, o ganho da antena do *transponder* (receptor) e *f*, a frequência de transmissão.

A tecnologia de semicondutores permite a fabricação dos circuitos integrados do *transponder* com consumo de potência em torno de 50 μW. Porém, para aplicações que exigem distâncias maiores que 15 m ou operam com circuitos integrados com alto consumo de energia, é necessário a utilização de um *transponder* ativo, ou seja, o uso de fonte de alimentação própria para suprir o consumo dos componentes e circuitos integrados que constituem o *transponder* a fim de realizar a comunicação entre os dispositivos. Neste caso, faz-se uso do modo *stand-by*, em que o *transponder* é ativado somente quando se encontra na região de interrogação. Então o processo de transmissão dos dados contidos no *transponder* para o dispositivo de leitura ocorre apenas em momentos discretos.

A transmissão de dados do *transponder* para o dispositivo de leitura ocorre por meio da modulação do sinal refletido pela seção de espalhamento. Da tecnologia do radar, sabe-se que as ondas eletromagnéticas são refletidas por objetos de dimensões maiores que a metade do comprimento de onda. Também, a eficiência com que um objeto reflete ondas eletromagnéticas é descrita pela seção transversal de espalhamento e dos objetos que estão em ressonância com a frente de onda que os atinge. Da potência P_1, que é emitida pela antena do dispositivo de leitura para o *transponder*, uma parcela é atenuada no espaço livre e a outra alcança a antena do *transponder*, Figura 22. A tensão no dipolo é retificada pelos diodos D_1 e D_2 e é utilizada para ativar ou desativar o modo *standy-by* do *transponder*. Essa tensão é usada também como uma fonte de alimentação para a transmissão em distâncias curtas.

A parcela da potência que é refletida pela antena, retorna com o valor P_2', que varia de acordo com as características da reflexão da antena do *transponder*, as quais são influenciadas pela variação da carga conectada à ela, e chega ao dispositivo de leitura um valor P_2. A fim de transmitir dados do *transponder* ao dispositivo de leitura, um resistor R_L, conectado paralelamente à antena, é ligado e desligado conforme os dados contidos na memória do

transponder. Portanto, a amplitude da onda refletida do *transponder* para o dispositivo de leitura é modulada por *backcatter modulation*.

Portanto, uma comunicação por *backscatter* é caracterizada, então, quando o sinal emitido pelo leitor volta refletido na mesma frequência, porém com caracterizações diferentes daquelas fisicamente alteradas através de um capacitor instalado no meio da antena, desta forma, a chegada de energia é alterada fazendo com que a amplitude da reflexão mude[15]. Devido ao leitor e ao *transponder* comunicarem-se na mesma frequência, eles precisam trabalhar cada um de uma vez, caracterizando assim uma comunicação HDX, pois o leitor continua a prover energia para a *tag*, mesmo quando está recebendo ou esperando uma resposta do *transponder*.

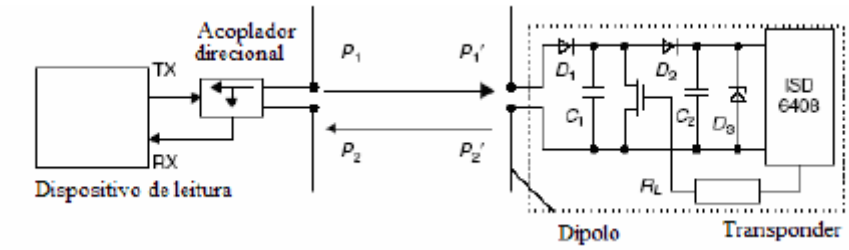


Figura 22 - Princípio de operação do sistema n-bit transponder por backscatter[8]

4.4.3 Sistema n-bit Transponder por Acoplamento Magnético (Sistemas de Proximidade)

Nos sistemas de proximidade, projetados para distâncias entre 0,1 cm e 1 cm, o *transponder* é inserido dentro do dispositivo de leitura. As aplicações que fazem uso deste tipo de sistema são conhecidas com *touch and go.*

A disposição funcional da bobina do *transponder* e da bobina do leitor corresponde àquela de um transformador, Figura 23, na qual o dispositivo de leitura é representado pelo enrolamento primário e o enrolamento do secundário representa a bobina do *transponder*. Ao se introduzir o *transponder* no dispositivo de leitura, a bobina do *transponder* é posicionada precisamente na abertura existente no núcleo em forma de U. uma corrente alternada de alta frequência no enrolamento do primário gera um campo magnético de alta frequência no núcleo e na abertura do arranjo em U. Quando o *transponder* está presente nesse espaço, conforme a Figura 23 mostra, a tensão que é induzida na bobina do *transponder* é retificada e utilizada como fonte para o funcionamento do *transponder*.

Devido à tensão induzida na bobina do *transponder* ser proporcional à frequência da corrente de excitação, a frequência selecionada para a transferência de potência deve ser tão elevada quanto possível. Na prática, as frequências de operação estão entre 1 MHz e 10 MHz, a fim de manter-se reduzidas as perdas no transformador. Para isso, é usado um material que seja apropriado para a frequência escolhida. Os sistemas com acoplamento de proximidade são muito utilizados para *transponders* constituídos com circuitos integrados contendo memória e microprocessador devido possuírem uma boa capacidade de fornecimento de potência sendo, assim, capazes de alimentar tais dispositivos eletrônicos, os quais consomem mais energia.

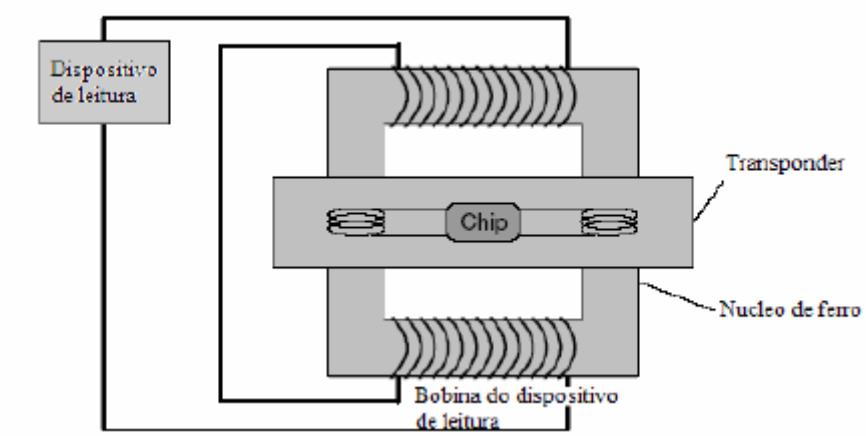


Figura 23 – Sistema n-bit transponder por acoplamento magnético[8]

A modulação de carga com sub-portadora também é usada para sistemas de proximidade por acoplamento magnético.

4.4.4 Sistema n-bit Transponder por Acoplamento Elétrico

Nos sistemas de acoplamento elétrico, o dispositivo de leitura gera um campo elétrico de alta frequência e a sua antena consiste em uma placa condutora, Figura 24. Quando uma tensão de alta frequência é aplicada ao eletrodo, um campo elétrico de alta frequência se forma entre o eletrodo e o potencial terra. As tensões requeridas para esse sistema variam entre algumas centenas de volts e alguns milhares de volts, as quais são geradas no dispositivo de leitura pela elevação da tensão em um circuito ressonante. A antena do *transponder* é composta de duas superfícies condutoras que se encontram em um mesmo plano. Se o *transponder* for colocado no campo elétrico do dispositivo de leitura, uma tensão elétrica é

induzida entre os dois eletrodos do *transponder*, suprindo a energia necessária para alimentação.

O circuito equivale da Figura 25 representa um sistema de acoplamento elétrico em seu modelo simplificado, funcionando como um divisor de tensão entre a capacitância do dispositivo de leitura e o *transponder* (capacitância C_{RT}) e a resistência de entrada do transponder (R_L) ou, ainda, com a capacitância entre o *transponder* e o potencial terra (C_{TGND}). As corrente que fluem nas superfícies do eletrodo do *transponder* são muito pequenas, consequentemente, nenhuma exigência particular é imposta para a condutividade do material do eletrodo. Porém, pode-se aumentar a distância de leitura do sistema variando-se a capacitância C_{TGND}.

Ao se colocar um *transponder* por acoplamento elétrico na zona de interrogação do dispositivo de leitura, a impedância de entrada R_L do *transponder* em conjunto com a capacitância C_{RT} atua como um circuito ressonante. O amortecimento do circuito ressonante pode ser comutado entre dois valores através do chaveamento do resistor de modulação R_{mod} contido no *transponder*. Por meio desse chaveamento, é gerada a modulação em amplitude da tensão presente na indutância L_1 e da capacitância C_1, conforme o circuito da Figura 25.

A modulação (chaveamento) deste resistor é feita de acordo com os dados que serão transmitidos para o dispositivo de leitura, sendo conhecida com modulação de carga.

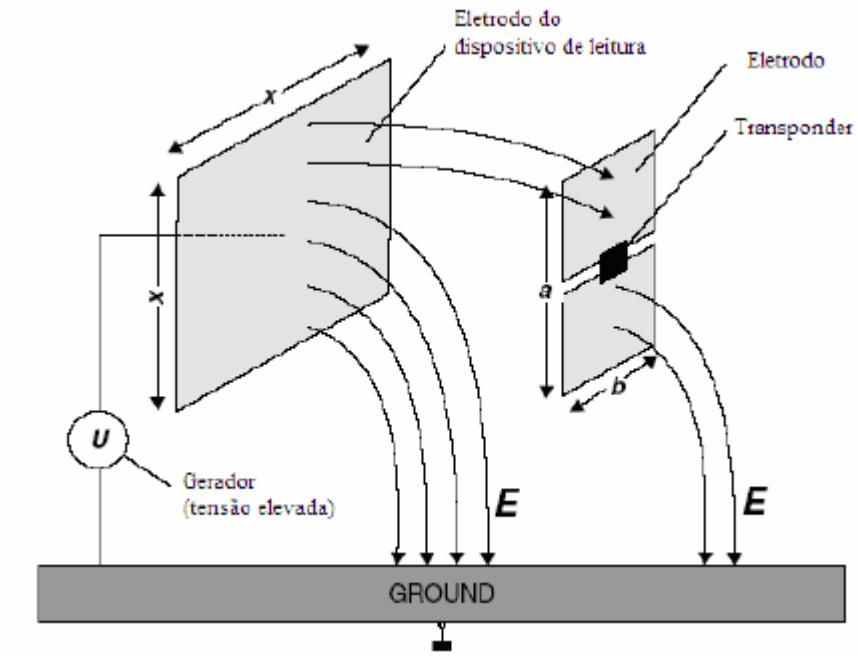


Figura 24 - Sistema n-bit transponder por acoplamento elétrico (campo eletromagnético transferindo dados e energia) [8]

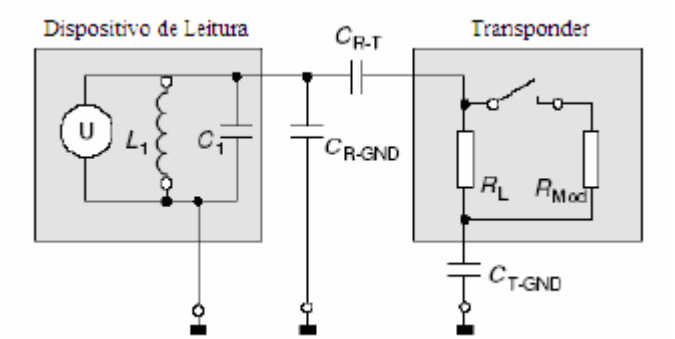


Figura 25 - Circuito equivalente do funcionamento do sistema (leitor + meio + transponder) para acoplamento elétrico[8]

4.5 SISTEMAS RFID SEQÜENCIAIS

Nos sistemas sequenciais, a transmissão de dados e de energia do dispositivo de leitura para o *transponder* ocorre de modo alternado. Um sistema sequencial é um sistema digital no qual a saída em determinado instante *t* depende do valor da entrada neste e em instante anteriores.

Os sistemas sequenciais são classificados em síncronos e assíncronos. Os sistemas síncronos são aqueles onde as transições ocorrem em instantes discretos definidos por um sinal de sincronização, conhecido como *clock*. Nos sistemas assíncronos, as transições podem ocorrer em qualquer instante, não existindo um sinal de referência.

4.5.1 Sistemas Seqüenciais por Acoplamento Indutivo

Os sistemas sequenciais por acoplamento indutivo operam com frequências abaixo de 135 kHz, com um acoplamento que é criado entre a bobina do leitor e a bobina do *transponder*, semelhante ao que ocorre no transformador. A tensão induzida gerada na bobina do *transponder* pelo efeito do campo magnético alternado do dispositivo de leitura é retificada e pode ser usada como uma fonte de alimentação. A fim de conseguir uma eficiência mais elevada na transferência de dados, a frequência do *transponder* deve ser igual ou muito próxima da frequência do dispositivo de leitura. Por essa razão, o *transponder* contém um capacitor *trimming* que serve para compensar as diferenças na tolerância dos componentes elétricos do sistema e na frequência de ressonância.

Ao contrário do que ocorre com os sistemas FDX e HDX, no sistema sequencial o transmissor do dispositivo de leitura e o *transponder* não operam de forma contínua. A energia transferida ao *transponder* pelo dispositivo de leitura é feita em períodos discretos. O funcionamento do sistema consiste em três operações: carga, leitura e descarga, de acordo com a Figura 26.

Durante a operação de carga, o dispositivo de leitura alimenta o capacitor do *transponder* o qual armazena essa energia a fim de utilizá-la posteriormente para a transmissão de dados, ou seja, na operação de leitura[15].

Na operação de leitura, o transmissor é desligado ficando apenas em *stand-by* para receber as informações que estão sendo enviadas pelo *transponder*. Após esse período de transmissão do *transponder*, ocorre o período de descarga, no qual é descarregado o resto da energia armazenada no capacitor. A capacitância mínima do capacitor de carga é calculada conhecendo-se a tensão e a potência mínima exigidas para operação do circuito integrado do *tansponder* por meio da equação

$$C = \frac{q}{V} = \frac{I.t}{V_{max} - V_{min}} \quad (4.3)$$

em que V_{max} e V_{min} são os valores limites para tensão de operação, I é a corrente de consumo do chip e t o tempo requerido para a transmissão dos dados do *transponder* para o dispositivo de leitura.

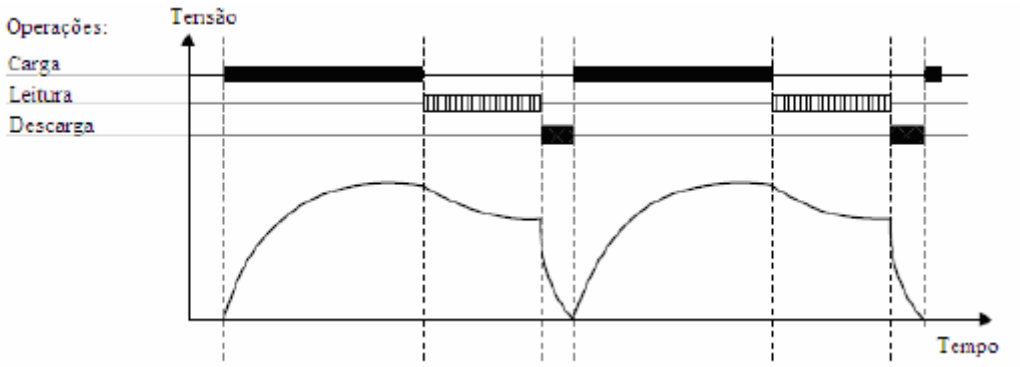


Figura 26 - Fases de operação do sistema seqüencial[8]

Em sistemas sequenciais, Figura 26 e Figura 27, um ciclo de leitura completo compreende duas fases: a fase de carregamento do capacitor e a fase de leitura dos dados. O final da operação de carregamento do capacitor é detectado pelo dispositivo *end of burst*

detector, que monitora a tensão na bobina do *transponder* e reconhece o momento em que o campo magnético do dispositivo de leitura é desligado. Ao final dessa fase, um circuito eletrônico oscilador contido no *transponder*, que utiliza circuito ressonante formado pela bobina do *transponder*, determina a sua ativação. O campo magnético alternado gerado pelo *transponder* é recebido pelo dispositivo de leitura e, embora seja fraco, a relação sinal ruído para o modo sequencial é melhorada em torno de 20 dB em comparação com a transmissão FDX e HDX.

A modulação do sinal de radiofreqüência gerado na ausência de uma fonte de alimentação é feita através da adição, paralelamente ao circuito ressonante, de um capacitor que é ativado no instante de tempo que ocorre o fluxo de dados. Ao fechar a chave do capacitor de modulação, ocorre um deslocamento na frequência, o que gera uma modulação FSK. Após o período de transmissão, é ativado o modo de descarga para efetuar a descarga completa do capacitor.

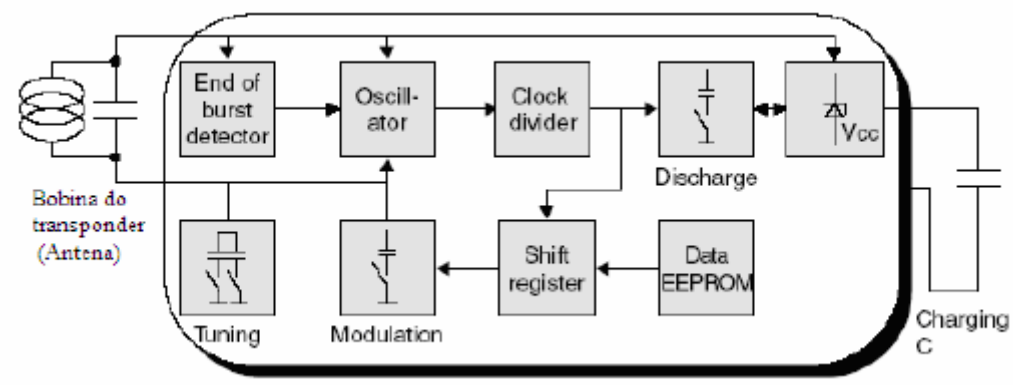


Figura 27 - Diagrama de blocos do tansponder seqüencial[8]

4.5.2 Sistema Sequencial SAW (*surface acoustic wave*)

Este tipo de sistema é baseado em ondas acústicas de superfície, ou seja, no efeito pizoelétrico e na dispersão superficial elástica da onda acústica para baixas velocidades. Se um cristal iônico for deformado elasticamente em determinado sentido, as cargas de superfície aparecerão, o que gera tensões no cristal. Porém, a aplicação de uma carga na superfície do cristal conduz a uma deformação elástica na grade do cristal. Os dispositivos SAW geralmente fazem uso de frequências na faixa de micro-ondas (2,45 GHz), onde transdutores eletroacústicos e refletores podem ser criados utilizando uma estrutura plana de eletrodos em um substrato pizoelétrico. Normalmente é utilizado um substrato de lítio com um processo similar ao usado na microeletrônica para manufatura de circuitos integrados.

A Figura 28 e a Figura 29 ilustram o layout básico de um sistema SAW. O transdutor interdigital é posicionado na extremidade do substrato pizoelétrico e uma antena dipolo apropriada é conectada ao seu barramento. O transdutor interdigital é usado para converter sinais elétricos em ondas de superfície acústica e vice-versa.

Um pulso elétrico aplicado no barramento do transdutor causa uma deformação mecânica no substrato que, devido ao efeito pizoelétrico entre os eletrodos, gera dispersões em ambos os sentidos na forma de onda de superfície acústica (SAW). Da mesma forma, a onda de superfície acústica que entra no conversor cria um pulso elétrico no barramento do transdutor devido ao efeito pizoelétrico.

Eletrodos individuais são posicionados ao longo do comprimento do *transponder* SAW. Os eletrodos de borda servem para reflexão de uma parcela das ondas de superfície que entram no substrato. As barras que compõem o refletor normalmente são feitas de alumínio.

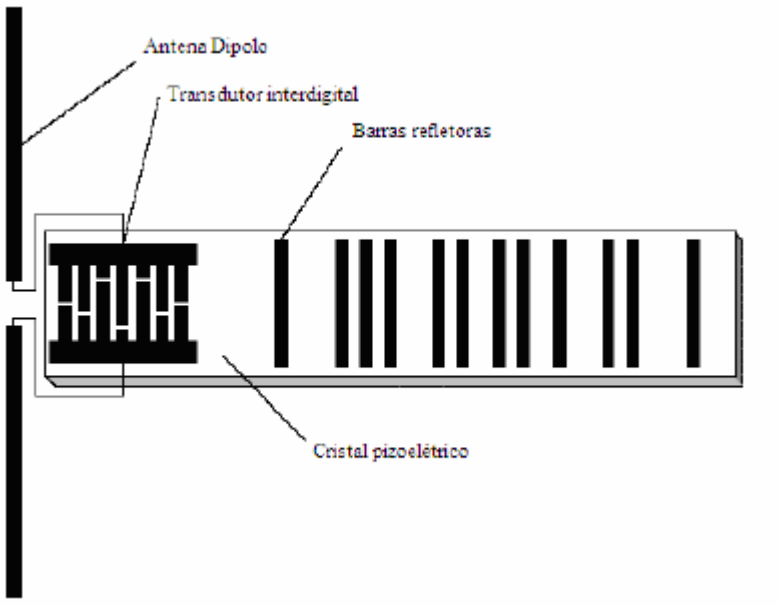


Figura 28 - Sistema seqüencial SAW[8]

O funcionamento do sistema ocorre da seguinte forma: um pulso de exploração de alta frequência gerado por um dispositivo de leitura é fornecido para a antena dipolo do *transponder*. No transdutor interdigital, o sinal elétrico é convertido em uma onda de superfície acústica, a qual percorre o substrato no sentido longitudinal. A frequência da onda de superfície corresponde à frequência da onda produzida pelo pulso de amostragem.

A frequência da portadora da sequência de pulsos refletidos corresponde à frequência da transmissão do pulso de amostragem. Parte da onda de superfície é refletida para fora de cada uma das tiras reflexivas e parte é absorvida na extremidade do substrato. A parcela das ondas que foram refletidas retorna para o transdutor interdigital, onde essas ondas serão convertidas em uma sequência de pulsos de alta frequência e, a seguir, emitidos pela antena dipolo para o dispositivo de leitura.

O número de pulsos recebidos corresponde ao número de tiras reflexivas existentes no substrato e o atraso entre os pulsos é proporcional à distância de separação entre as tiras reflexivas; ou seja, a informação é representada por uma sequência binária de dígitos semelhante ao código de barras, porém, sua leitura é feita por radiofreqüência ao invés de leitura óptica.

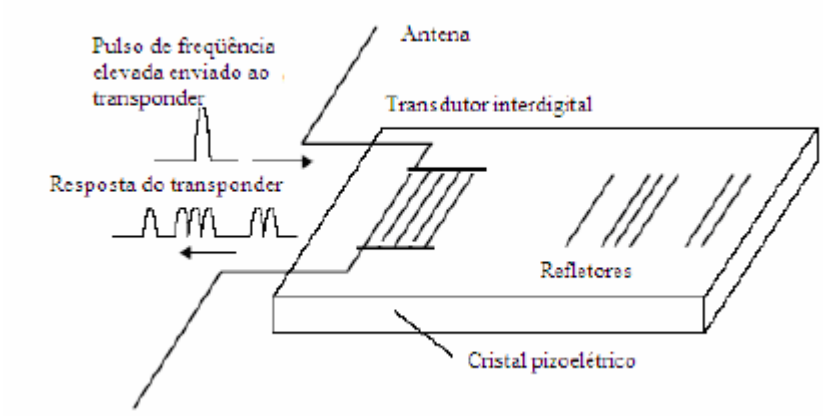


Figura 29 - Modelo do transponder SAW[8]

CAPÍTULO 5 – SEGURANÇA NOS SISTEMAS RFID

5.1 INTRODUÇÃO

Este capítulo destina-se a descrever a segurança dos sistemas de **RFID**. Serão discutidos, ente outras coisas, seus pontos fracos, o motivo de serem protegidos, quais tecnologias são utilizadas e como podem tornar esse sistema seguro.

RFID é um sistema computacional que utiliza hardwares (como *tags* e leitores), softwares (como o *midleware*) e um sistema de comunicação sem fio, via ondas de rádio, portanto, deve ter segurança a fim de proteger todos os elementos acima citados, bem como os dados que manipula.

Além de suas bases, o **RFID**, como qualquer outro sistema, deve se basear nos princípios de integridade, confidencialidade e disponibilidade.

Disponibilidade diz respeito ao sistema estar disponível no momento em que precisa ser acessado. Os sistemas **RFID** certamente têm vulnerabilidades que podem afetar a sua disponibilidade, por exemplo, alguém emitindo ondas de rádio entre leitores e as *tags*, fato que provoca uma falha de comunicação e faz com que este se torne indisponível.

A integridade tem o objetivo de garantir a exatidão e autenticidade da informação transmitida, impedindo sua alteração acidental ou maliciosa. Uma *tag* falsa poderia ser um exemplo de tentativa de quebra de integridade do sistema.

Confidencialidade são medidas tomadas para limitar o acesso às informações de pessoas não autorizadas. É aqui que se encaixa algo muito discutido, a privacidade dos consumidores. A principal preocupação em um sistema de **RFID**, no que tange a confidencialidade, é que deve haver o cuidado para que a informação não caia em mãos erradas.

A informação está cada vez mais móvel. Este aumento de mobilidade trouxe uma preocupação maior com a segurança, um maior desafio das empresas em relação com os consumidores de manter essas aplicações seguras.

Os sistemas de **RFID** expandem os limites de informação de uma corporação aos seus extremos, o que torna mais complexo manter dados sigilosos e seguros; uma grande quantidade de dados de uma empresa encontra-se disponível e exposta no ar.

Um sistema de **RFID** deve ser mais seguro do que os comuns; ele necessita de ter uma maior disponibilidade, por exemplo; em uma linha de produtos que contém código de barras e que são lidos para a entrada em uma empresa. Se algo ocorrer com o leitor de código de barras, o operador pode simplesmente digitar os códigos, logicamente com menor rapidez, mas o serviço continuaria. Agora, em um sistema **RFID**, no qual, por exemplo, há esteiras correndo em grande velocidade e lendo as *tags*, se o leitor para de funcionar, o impacto é muito maior do que na primeira situação.

Os sistemas de **RFID** estão sendo usados, cada vez mais, em aplicações que necessitam de alta segurança, como no controle de acesso ou em sistemas de pagamento e, portanto, o uso do **RFID** nesse tipo de aplicação deve passar por um processo de análise de riscos bem apurado. Existem dois tipos de tentativas de ataque: aquela em que o atacante tenta, apenas, ganhar acesso para ler as informações, sem modificá-las e, aquela em que ele modifica os dados na tentativa de obter privilégios que não possui.

Um sistema altamente seguro de **RFID** tem que estar protegido dos seguintes ataques:

- Leitura não autorizada de uma *tag* com o intuito de duplicar ou modificar os dados nela contida;
- A inserção de uma *tag* que não pertence ao sistema dentro da área de um leitor com o intuito de ganhar acesso indevido a um local ou receber serviços sem pagamento;
- Espionagem em uma comunicação de rádio usando repetição dos dados para imitar uma *tag* genuína do sistema.

A segurança de um sistema **RFID** está focada em se proteger de ladrões, espiões ou qualquer outra entidade não autorizada. A segurança de um sistema **RFID** deve ser condizente com a aplicação que será usada e as considerações como criptografia, procedimentos e manuseamento devem ser levados em conta. A implementação de um potente sistema de segurança e criptografia em um sistema de identificação de peças dentro de um processo de automação industrial seria oneroso, enquanto que, deixar de fora este tipo de procedimento em um sistema de pagamentos seria irresponsável.

Nas próximas seções, apontamos as áreas vulneráveis de segurança, avaliamos os riscos para as empresas e consumidores e descrevemos uma série de soluções possíveis[15].

5.2 ÁREAS DE VULNERABILIDADE DA SEGURANÇA NOS COMPONENTES DE RFID

Em um sistema de **RFID**, os dados são vulneráveis ao acesso não autorizado enquanto são armazenados na *tag*, no leitor ou no Computador Central, ou quando eles são transmitidos de um destes componentes para outro. Classificamos as áreas de vulnerabilidade da segurança em 4 categorias e descrevemos cada uma separadamente a seguir.

5.2.1 Vulnerabilidade no Acesso aos Dados das Etiquetas

Mais precisamente chamada de Zona 1, compreende as próprias *tags* **RFID**. Uma *tag* geralmente contém um circuito integrado (CI), essencialmente um microchip com memória. Os dados da *tag* podem ser comprometidos de forma similar aos dados de um computador. Os dados da *tag* são vulneráveis quando uma parte não autorizada ou acessa um leitor autorizado ou configura um leitor para se comunicar com uma etiqueta específica. Neste cenário, o usuário não autorizado pode acessar os dados da *tag* como se ele estivesse realizando uma leitura autorizada. No caso das etiquetas graváveis os dados também podem ser modificados ou até excluídos por um usuário não autorizado. Existe também outra vulnerabilidade; é quando os dados da *tag* são guardados de forma não encriptada, isso pode acontecer porque encriptar dados aumenta os gastos com espaço e circuitos. As contramedidas a serem tomadas para diminuir as vulnerabilidades são; ter um controle físico de acesso apropriado, ou seja, implementar segurança nas mercadorias etiquetadas com **RFID**, separar o código EPC de informações restantes, que sejam sensíveis à empresa e consumidores e, por fim, somente usar *tags* que permitem reescrita onde há controle de acesso físico e encriptação.

5.2.2 Vulnerabilidade na Comunicação da Etiqueta com o Leitor

Ainda compreende a Zona 1, onde abrange os leitores, geralmente conectadas a uma rede local, através de redes comuns ou *wireless*. Os dados percorrem o ar através das ondas de

rádio e durante este intercâmbio, os dados são vulneráveis. Alguns métodos de exploração da vulnerabilidade desse intercâmbio sem fio incluem:

- Um leitor não autorizado sequestra os dados. Neste cenário, um leitor não autorizado simplesmente intercepta os dados transmitidos pela etiqueta;

- Um terceira congestiona ou sabota a comunicação de dados. Uma parte não autorizada pode utilizar diversos métodos de evitar comunicação entre a *tag* e o leitor. Uma forma comum, *spoofing* (*tag* falsa), cria interferências eletromagnéticas sobrecarregando o leitor com muitas respostas falsas da etiqueta que o leitor não consegue distinguir nenhuma das respostas legítimas dela. Este método também é chamado de ataque de negação de serviço. Isso ocorre devido a qualquer pessoa que esteja conectada a mesma rede que os leitores ou nas proximidades, com alguma ferramenta de *sniffer* (ferramenta que busca por dispositivos conectados à rede).

- Uma *tag* impostora envia dados. Uma *tag* impostora fornece informações não desejadas ou dados errados ao leitor enganando efetivamente o sistema de **RFID** recebendo, processando e atuando os dados inacurados da *tag*.

Para solucionar esses problemas citados é preciso encriptar a comunicação entre os leitores e as *tag*, implementar mecanismo de autenticação para as *tags*, necessidade de autenticação e autorização para acessar os serviços dos leitores.

5.2.3 Vulnerabilidades dos Dados Dentro do Leitor

Também chamado de Zona 2. Quando uma *tag* envia seus dados ao leitor, ele armazena as informações em sua memória e as utiliza para executar diversas funções antes de limpar estes dados e/ou enviá-los ao sistema do computador central. Durante estes processos, vulnerabilidades e problemas de segurança tradicionais existem. Atualmente, a maioria dos leitores do mercado são proprietários e não podem fornecer uma interface que permita aos usuários aprimorarem as características de segurança do leitor além das capacidades oferecidas pelo fornecedor. Esta limitação torna a seleção cuidadosa do leitor especialmente importante.

5.2.4 Vulnerabilidade dos Serviços e do Sistema do Computador Central

Também chamado de Zona 3 e Zona 4. Depois que os dados são passados de uma etiqueta, através de um leitor, para um computador central, eles ficam sujeitos às vulnerabilidades já existentes ao nível do computador central. Estas vulnerabilidades possuem algumas contramedidas dentre as quais podemos citar; o controle de acesso à rede, implementação de firewalls, detecção de intrusos, *sniffers* e do acesso físico.

5.3 AVALIAÇÃO DOS RISCOS DE SEGURANÇA NAS APLICAÇÕES DE RFID

Os riscos dos dados comprometidos durante uma violação de segurança variam dependendo do tipo de aplicação. Para os propósitos da discussão deste capítulo, classificamos as aplicações de **RFID** em duas, ao Consumidor e à Empresa e descrevemos os riscos de cada uma em detalhes.

5.3.1 Riscos de Aplicações ao Consumidor

As aplicações da **RFID** ao consumidor incluem aquelas que coletam ou gerenciam os dados sobre os consumidores, ou são “tocadas” pelos mesmos. As aplicações típicas desta categoria incluem o controle de acesso, cobrança eletrônica de pedágio e qualquer aplicação que envolva a etiquetagem de itens de uma loja do varejo. Com as aplicações ao consumidor, o risco das violações se segurança podem ser prejudiciais tanto para empresas que implementam o sistema como para os consumidores. Os danos ao consumidor geralmente são relacionados à violação ou invasão de privacidade, mas também podem incluir danos financeiros diretos ou indiretos.

Mesmos nos casos onde nenhum dado pessoal do consumidor é diretamente coletado ou mantido por um sistema **RFID**, se o consumidor manusear, segurar ou carregar um objeto com uma *tag* de **RFID**, existe potencial de se criar uma associação entre o consumidor e a *tag*. Essa associação carrega dados pessoais sobre o consumidor e pode causar riscos à privacidade. Por exemplo, *tags* de **RFID** usadas para controlar a entrada de um carro não contêm qualquer informação sobre o proprietário do veículo, porém ainda existe a ameaça de que o detentor da chave do carro com *tag* de **RFID** possa ser rastreado. Isto pode ocorrer

somente se for possível construir uma série de leitores sofisticados, estrategicamente posicionados para interrogar a chave com a *tag* de **RFID**.

5.3.2 Riscos das Aplicações à Empresa

As aplicações de **RFID** à empresa são internas à empresa ou a um conjunto de empresas. As aplicações típicas à empresa incluem qualquer aplicação de melhoria do processo de gerenciamento da cadeia de abastecimento (por exemplo, controle do inventário ou gerenciamento da logística). Outra aplicação é na área de automação industrial onde os sistemas de **RFID** são usados para rastrear os processos de manufatura. Aqui, o risco de violação de segurança geralmente é limitado apenas à empresa. Estas violações de segurança podem interromper os processos e as funções da empresa ou comprometer as informações confidenciais da corporação.

Por exemplo, os *hackers* podem interromper os processos da cadeia de abastecimento com **RFID** entre os parceiros comerciais através da sabotagem e montando ataques de negação de serviço. Os concorrentes também podem roubar os dados confidenciais do inventário ou obter acesso as práticas específicas de automação industrial. Em, outros casos, os *hackers* podem acessar e divulgar dados confidenciais de empresas similares. Isto também pode comprometer a vantagem competitiva de uma empresa. Nos caos onde diversas empresas usam em conjunto um sistema de **RFID**, por exemplo, para criar uma cadeia de abastecimento mais eficiente entre fornecedores e fabricantes, a violação da segurança dos dados das etiquetas provavelmente será prejudicial a todas as empresas envolvidas.

5.3.3 Soluções para a Segurança e Proteção dos Dados de **RFID**

Nesta seção discutimos algumas das soluções mais comuns para a segurança e proteção dos dados e da comunicação de **RFID** para enfrentar as vulnerabilidades associadas aos dados das *tags* e à interação entre *tags* e leitores. A Tabela 2 indica um resumo destas soluções[2].

SOLUÇÃO	Vulnerabilidade enfrentada	
	Acesso aos Dados da *tag*	**Comunicação entre *tag* e Leitor**
Protegendo as Instalações	X	
Usando *tags* de Apenas Leitura (“Read-Only”)	X	
Limitando o Alcance da Comunicação		X
Implementando um Protocolo Proprietário	X	X
Blindagem	X	X
Usando o Recurso de Comando de Eliminação	X	
Destruindo Fisicamente uma *tag*	X	
Autenticando e Criptografando	X	X
Bloqueio Seletivo	X	X

Tabela 2 – Soluções de segurança e proteção dos dados de RFID[2]

5.3.4 Protegendo as Instalações

O uso tradicional dos meios de proteção das instalações onde se encontram os objetos com *tags* de **RFID** (por exemplo, em um armazém) enfrenta algumas vulnerabilidades associadas ao acesso direto às etiquetas. Esta solução funciona bem se houver a garantia de que todas as *tags* estejam em determinados locais e que não saiam das quatro paredes da empresa. Muitas aplicações de **RFID**, entretanto, requerem objetos com *tags* de **RFID** a serem movimentados entre duas ou mais empresas e possivelmente até as mãos dos consumidores.

5.3.5 Usando *tags* de Apenas Leitura (“*Read-Only*”)

A fabricação de *tags* de apenas leitura é uma medida de segurança “incorporada no projeto” que protege os dados das *tags* contra alterações ou exclusões por um leitor não autorizado. Todavia, por si só, esta solução deixa os dados vulneráveis a leituras não autorizadas – especialmente se os objetos com *tags* de **RFID** forem facilmente acessíveis ou públicos.

5.3.6 Limitando o Alcance de Comunicação Entre *Tag* e Leitor

O uso de frequências de operação e/ou outros atributos físicos da *tag*. Leitor ou antena para limitar o alcance da comunicação entre uma *tag* e um leitor minimiza o grau de vulnerabilidade. Embora esta solução limite efetivamente o potencial de ameaça leitores não

autorizados ao acesso dos dados das *tags*, ele não garante comunicações seguras a todo o tempo porque ainda existe um grau de vulnerabilidade, embora de menor escala.

5.3.7 Implementando um Protocolo de Comunicação Proprietário

A estratégia de implementação de um protocolo proprietário é conveniente para aplicações onde a interoperabilidade e a troca de dados não é um requisito. Ela envolve a implementação de um protocolo de comunicação e um esquema de codificação/criptografia de dados que não é publicamente acessível. Dependendo da sofisticação do protocolo e do método de codificação básico, este método pode oferecer um bom nível de segurança. Todavia, com os benefícios resultantes da troca de dados de **RFID** e a adoção de padrões de **RFID** de amplo alcance, os protocolos proprietários nem sempre são práticos. Estes protocolos proprietários dificultam os dados de **RFID** e a interoperabilidade das aplicações, resultando em menos benefícios e preços potencialmente elevados.

5.3.8 Blindagem

Também conhecida como *Gaiola de Faraday*, esta técnica consiste no envolvimento dos objetos com *tags* de **RFID** em materiais tais como folha de metal que bloqueia a penetração ou propagação das ondas eletromagnéticas. Embora este método proteja eficientemente as etiquetas de **RFID**, quando elas são blindadas, os leitores de **RFID** não conseguem lê-las, anulando os benefícios da **RFID**. Para algumas aplicações de **RFID**, a blindagem temporária reduz o risco de acesso não autorizado.

5.3.9 Usando o Recurso de Comando de Eliminação

O comando de Eliminação é destinado a desabilitar uma *tag* equipada para aceitar este comando. Após receber o comando de Eliminação, a *tag* para de funcionar e não consegue receber ou transmitir os dados. Tanto a blindagem como o comando de Eliminação tornam a *tag* ilegível. Entretanto, a blindagem não é permanente porque ela pode ser removida e uma *tag* pode voltar a ser funcional. Por outro lado, o comando de Eliminação torna a *tag* permanentemente não-funcional.

Em um futuro próximo, imagine que uma caixa de leite está etiquetada com uma variedade de informações incluindo seu preço e data de validade. Imagine ainda que o refrigerador do futuro possua um leitor embutido para alertar o consumidor quando a data de validade do produto está próxima. Se a *tag* fosse eliminada no ponto de venda, o consumidor não conseguiria utilizar as conveniências de potencial da **RFID**, neste caso, alertando o consumidor para usar ou substituir a caixa de leite que está vencendo.

5.3.10 Destruindo Fisicamente uma *tag*

A destruição física de uma *tag* atinge os mesmos resultados e possui as mesmas vantagens e desvantagens do comando de Eliminação. Uma vantagem adicional desta solução, entretanto, é que você não precisa se preocupar se o comando de Eliminação funcionou realmente. Todavia, em algumas aplicações, nem sempre é fácil ou possível localizar e retirar uma *tag*, pois ela pode ser imperceptível, inacessível ou embutida.

5.3.11 Autenticando e Criptografando

Diversos esquemas de autenticação e/ou criptografia podem ser usados para garantir que apenas leitores autorizados possam acessar *tags* e seus dados. Um esquema de autenticação pode ser tão simples quanto “bloquear” os dados da *tag* até que um leitor autorizado forneça uma senha válida para desbloquear os dados. Esquemas mais sofisticados podem incluir autenticação e criptografia dos dados que oferecem mais níveis de proteção. Embora estes esquemas tenham suas próprias vulnerabilidades, o custo é o fator mais proibitivo na implementação de soluções sofisticadas de autenticação e criptografia nos sistemas de **RFID**. Se as exigências obrigarem *tags* de baixo custo para itens baratos, as *tags* provavelmente terão reduzido a programabilidade para autenticação e criptografia. Itens de alto valor tais como joias ou equipamentos militares podem merecer *tags* mais caras que consigam oferecer mais segurança.

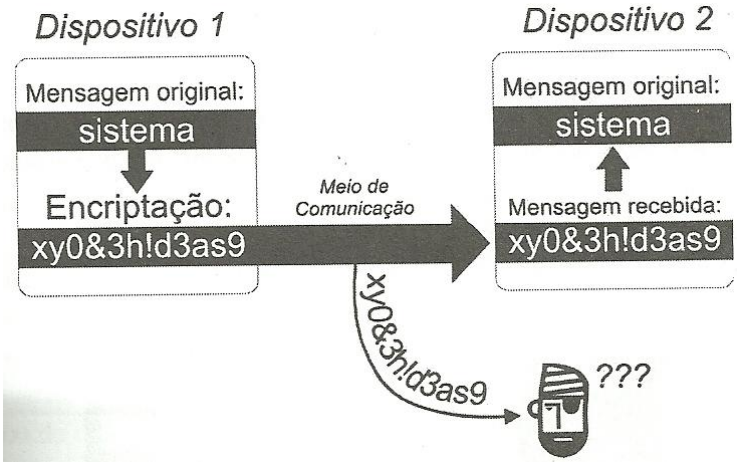


Figura 30 – Encriptar dados na transmissão pode ser efetivo em proteger contra espionagem[15]

5.3.12 Bloqueio Seletivo

Esta solução utiliza uma *tag* de **RFID** especial conhecida com *tag de bloqueio* para simular a presença de um número virtualmente infinito de um subconjunto de *tags*. Este método essencialmente impede que leitores não autorizados leiam um subconjunto de *tags*.

O bloqueio seletivo oferece uma solução versátil que minimiza algumas deficiências das técnicas anteriores e ao mesmo tempo evita o alto custo associado às soluções mais sofisticadas tais como autenticação e criptografia. A combinação de baixo custo e alta segurança faz do bloqueio seletivo uma solução apropriada para implementação de segurança em aplicações ao consumidor sensíveis à privacidade tais como etiquetagem ao nível de item em lojas do varejo. Neste caso, os consumidores podem usar as *tags* de bloqueio para evitar que todos os leitores das proximidades detectem e rastreiem as *tags* fixadas aos itens após a compra.

Pelo fato da técnica de bloqueio seletivo exigir *tags* graváveis, ela não pode ser implementada com sucesso em sistemas que usam *tags* de apenas leitura ou que não possuam chips. A técnica de bloqueio também pode ser usada de forma maldosa através da criação de *tags de bloqueio* que façam bloqueios totais ou "*spoofing*" (sabotagem) que possam afetar indiscriminadamente todos os leitores dentro de uma faixa e montar efetivamente um ataque de negação de serviço para interromper a função de todo os sistemas de **RFID**. Embora não haja atualmente soluções comerciais disponíveis que possam evitar ou contornar este problema, é possível construir inteligência de leitura que detecte os problemas de "*spoofing*" e alerte um atendente.

5.4 RECOMENDAÇÕES

Não existe solução única de segurança adequada área toda a classe de aplicação de **RFID**. Em alguns casos, um método combinado pode ser necessário. Para certas aplicações, as medidas são especificadas por organizações de padronização tais ISO ou EPCglobal e são automaticamente disponíveis por fornecedores que atendem a estes padrões. Por exemplo, a ISO 15693 – aplicado aos cartões de proximidade (cartões de identificação inteligente) – especifica as medidas de segurança relacionadas à autenticação dos dados das *tags* e é usado em aplicações de controle de acesso e pagamento sem contato[2].

Segurança, para a **RFID** é um tópico muito complicado, com obstáculos desafiadores a serem ultrapassados e soluções complexas a serem implementadas. Para implementar o esquema mais adequado para a segurança dos dados de **RFID** em sua aplicação, recomenda-se o seguinte:

- Avaliar as vantagens e desvantagens exclusivas de todas as soluções disponíveis no contexto do seu projeto de **RFID**;
- Analisar os custos de implementação de um esquema de solução de segurança em particular;
- Ponderar estes custos contra os riscos e custos de vulnerabilidade em seu projeto de **RFID**;
- Consultar um especialista no ramo de segurança em comunicações sem fio.

CAPÍTULO 6 – ESTUDO DE CASO

6.1 ESTUDO DE CASO: HP

Hewlett-Packard, conhecida como HP, é uma empresa situada em diversos lugares do mundo, responsável por uma clientela em mais de 178 países, com seus negócios girando em 43 moedas diferentes, em 15 línguas diferentes, com entregas diárias que geram milhões de dólares. Possuindo apenas cinco cadeias de suprimento, que alcançaram o mundo inteiro e sua operação de manufatura e distribuição terceirizada.

A empresa enfrentava alguns problemas como muitos produtos em série que incorporam dados essenciais para a realização dos serviços. Desta forma a empresa considera que a tecnologia **RFID** possibilita diversos meios de identificação único dos objetos a um custo baixo, consequentemente transformando sua cadeia de suprimento e reduzindo consideravelmente seus custos, juntamente com outras tecnologias de rastreamento de objetos, com uma infraestrutura inteligente, possibilitando um gerenciamento além da cadeia de suprimentos.

A empresa reforça o que foi abordado anteriormente: apesar da tecnologia de código de barras ter boa capacidade de identificação de itens há diversas limitações, em que a tecnologia **RFID** supera como na velocidade, processamento paralelo, simplicidade e a menor intervenção humana possível. Tais fatos e muitos outros levaram a empresa em 2002 a pesquisar como a tecnologia de rádio frequência poderia trazer resultados consistentes para a companhia e principalmente aos clientes e parceiros[7].

6.1.1 HP e **RFID**

O projeto começou em 2004, em São Paulo, testando etiquetagem de itens com a tecnologia **RFID**, já que a fábrica possuía uma cadeia de suprimentos completa, com manufatura, customização, distribuição e logística reversa diferente de outros lugares do mundo, em que esses processos são divididos: produz a impressora em um país e envia a outro para efetuar a customização.

Após o piloto bem sucedido, a empresa passou a etiquetar os chassis das impressoras, a fim de poder controlar as informações do início até o fim da cadeia e até os cartuchos de tintas passam a ser etiquetados.

A etiqueta de **RFID** é colocada no fundo do chassi da impressora, incorporando o número de série impresso e o part number. Atualmente é usada uma etiqueta **RFID** com um número padrão EPC e essa etiqueta possui uma memória extra, para gravar a informação do produto original durante o processo de manufatura, como o número de série HP, resultados do produto testado, firmware do produto, cartuchos "*install by date*" e destino do produto.

Com essa abordagem é permitido o acompanhamento da impressora através de toda a cadeia de suprimento, como se fosse um "DNA do produto", possuindo apenas uma etiqueta **RFID**.

Figura 31 - Implementação pioneira[7]

Etiqueta, antena e o *reader*, são apresentados na Figura 32.

Após o pálete ser embalado na linha de manufatura, o mesmo é transferido até um armazém passando por um portal, conforme a Figura 33.

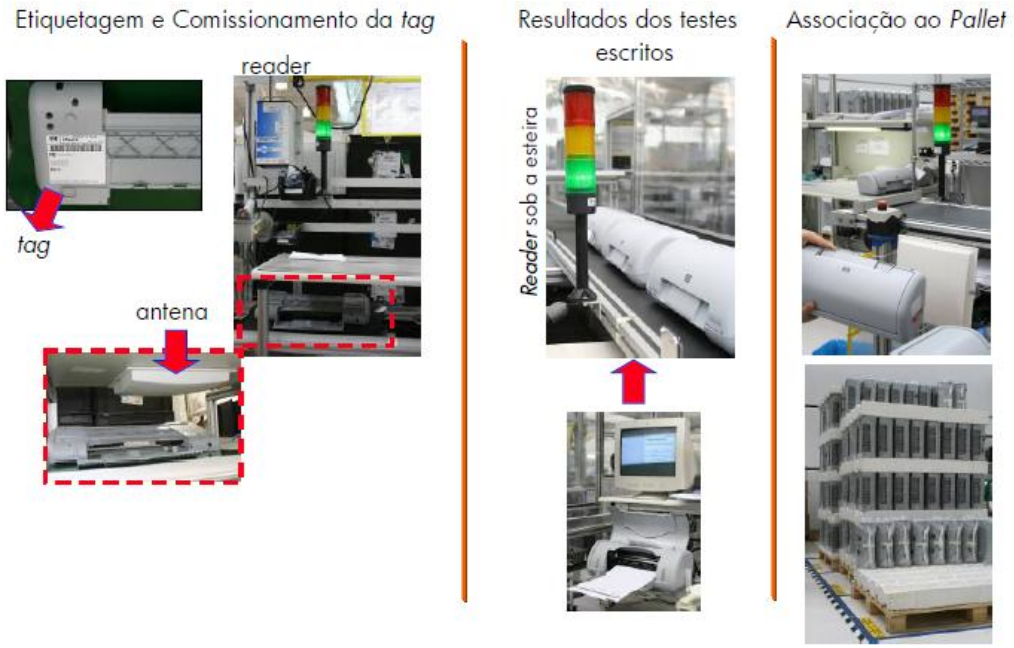


Figura 32 - Implementação na fábrica[7]

Figura 33 - Transação da manufatura ao armazém[7]

O **RFID** auxilia na identificação e detalhamento da investigação de processos específicos, com a possibilidade de verificar quais as linhas teve maior ou menor tempo de produção, bem como o controle online da produção pela HP, mantendo a qualidade dos produtos.

Com a aplicação desta tecnologia obteve-se uma análise de resultados que podemos destacar como positivos:

- Ajuda a diminuir os gargalos;
- Demanda melhoria no processo;
- Permite automação de processos;
- Rapidez na coleta de dados;
- Mais informações para os negócios.

Com lições aprendidas temos:

- Tecnologia ainda recente;
- Não se trata apenas de tecnologia: Revisão de processos;
- Interoperabilidade e falta de contato visual podem ser desafios;
- Preparado para a coleta de dados.

Na Figura 34 observa-se o impacto nas linhas de manufatura após a implementação do **RFID**.

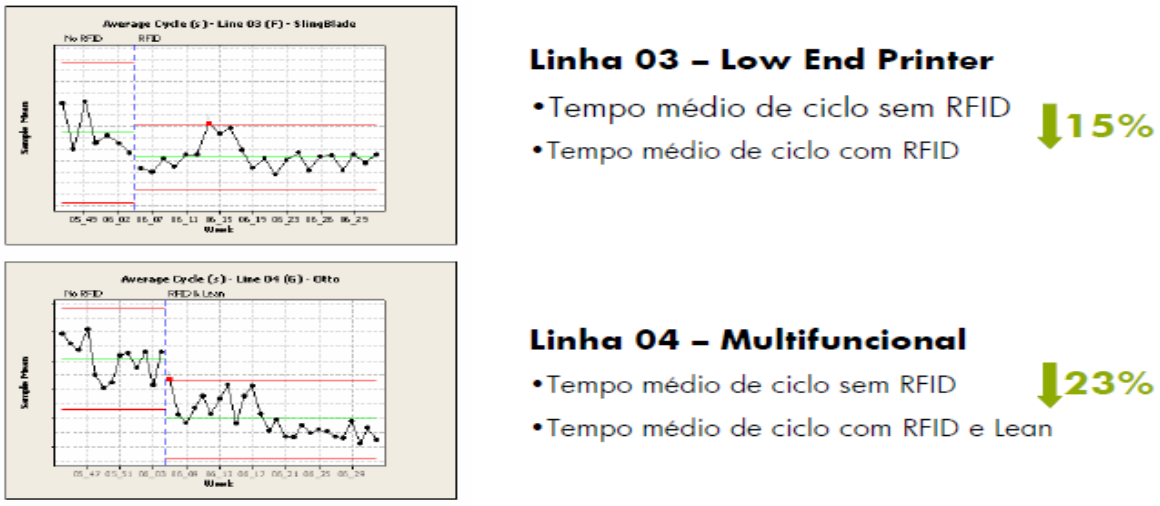


Figura 34 - Impacto nas linhas de manufatura[7]

A empresa HP disponibilizou um comparativo, podendo concluir mais uma vez o quão inferior a tecnologia de código de barras é em relação a tecnologia **RFID**:

Figura 35 - Código de barras versus RFID[7]

6.1.2 Mapeamento do Processo de Manufatura das Impressoras HP

As impressoras são produzidas no laboratório da Flextronics em Sorocaba, onde há onze linhas de manufatura para a produção de impressoras HP, cada uma seguindo um fluxo, e três portais que funcionam desde a produção até a expedição dos produtos, que passam por diversas integrações de RF. São produzidas 8.550 impressoras por dia e 170 mil por mês. As etiquetas e os *inlays* utilizados são importados e as antenas foram desenvolvidas pela Flextronics. Projetos de melhorias estão sempre em andamento, como por exemplo, a construção de um 4º portal para acompanhar a expedição das impressoras ou mudanças de processos e *layouts*.

6.1.3 Linhas de Manufatura

Cada linha de produção segue um fluxo dependendo do modelo da impressora. Em geral, os operadores iniciam a montagem da impressora com as matérias primas (placas, parafusos, etc.) e passa adiante o produto até chegar numa estação que é gerado o código EPC, a etiqueta é colocada por uma máquina em uma parte do produto, a impressora zebra imprime o código em cima da etiqueta e os dados são gravados na etiqueta, como fabricação, componentes, modelos e outros dados.

Após isso, o produto segue adiante passando por outros operadores que montam a impressora até chegar ao final da linha, que embalam o produto no isopor e a colocam em páletes. Os páletes são vedados por um plástico.

Esses produtos acabados recebem o nome de "*bulk*", pois são considerados subprodutos uma vez que não estão prontos para o cliente final e são movimentados até o armazém. Na entrada do armazém há o primeiro portal que lê todas as etiquetas contidas no pálete. Há três luzes: amarela (passar o pálete), verde (leitura correta) e vermelha (leitura incorreta). Quando houver algum problema, a luz vermelha acende e o monitor indica qual o problema encontrado.

Os páletes são armazenados e aguardam sua customização, que é feita quando ocorre uma ordem de produção.

6.1.4 Linhas de Customização

Quando há uma ordem de produção, os páletes são movimentados até a área de customização e passam pelo 2º portal que lê as informações contidas nas etiquetas.

Na linha de customização a impressora é customizada ao cliente: cartuchos de tintas, configuração de idioma, informativos, caixas, etc. na primeira estação de RF o número EPC do produto é trocado, pois ele passa de um subproduto para um produto pronto para entregar ao cliente e as novas informações são gravadas na mesma etiqueta colocada na linha de manufatura.

Na última etapa o sistema controla a quantidade de impressora por pálete, atualmente são 196 impressoras por pálete com taxa de leitura a 100% nos portais.

No final do processo a impressora pronta para o cliente é colocada sobre páletes e aguardam numa área chamada "pré-estocagem" até voltar ao armazém novamente, passando pelo 3º e último portal.

6.1.5 Problemas e Soluções

Alguns problemas foram enfrentados durante o projeto, sendo que a maioria era em relação à taxa de leitura e escrita de RF, pois havia diferentes postos **RFID** instalados e diversos produtos passando através do processo identificação. Problemas também surgiram quando o número de linhas e as taxas de leitura começaram a crescer.

Outro problema que virou um paradigma era a improvável leitura da etiqueta nos materiais que continham metal. Sendo assim, a empresa realizou diversos testes para que o metal contido nas impressoras não interferisse na rádio frequência. Esses testes implicam na identificação de uma etiqueta com alta capacidade de leitura, seu melhor posicionamento dentro do produto, quais os componentes podem ficar perto da etiqueta, com isso, o metal passou a não ser uma limitação para o projeto **RFID**.

Para evitar qualquer tipo de limitação, mais do que pesquisas e estudos sobre a tecnologia, a empresa realizava testes práticos no chão de fábrica e no armazém, avaliando possíveis implementações, os formatos de antena das etiquetas e capacidade de leitura dos equipamentos.

Todos os problemas foram resolvidos pela equipe técnica juntamente com o suporte do laboratório de **RFID** da HP no Brasil[12].

Um problema frequente era a interferência de sinal que incorria na leitura de itens indesejados. Para solução desse problema, foram realizados testes e captura das frequências de ruídos produzidos no laboratório HP, incluindo testes sobre: configuração de setup do leitor, posicionamento da etiqueta no produto, posicionamento do produto dentro da caixa, seleção de etiqueta e antena, para que fosse obtida a melhor combinação possível da antena, do leitor e a configuração da estação **RFID**.

Diversos processos foram modificados e ajustados, por exemplo, em diferentes estações na linha de produção a informação de teste era escrita na etiqueta e após alguns pilotos essa operação foi consolidada em apenas uma estação, simplificando a operação e acelerando o processo. Um *middleware* flexível é essencial para se adaptar às mudanças ao decorrer do projeto.

Com o crescimento das linhas e taxas de leituras, foram revisados todos os pontos críticos da arquitetura do sistema, para serem capazes de trabalhar com mais de 40.000 leituras e escritas diárias.

6.1.6 Benefícios do Projeto

A implantação da tecnologia **RFID** foi muito benéfica para a empresa HP e trouxe como resultado, por exemplo, redução das horas de trabalho, aumento de eficiência e menor tempo de produção. Esses benefícios podem ser quantificados ao medir o progresso em tempo economizado (nas operações) pelo sucesso no rastreamento de produtos, que trará como resultado a diminuição das horas de trabalho, preservando e aproveitando os recursos da empresa.

O tempo de ciclo de produção nas linhas de manufatura e customização foi medido antes e depois da tecnologia implantada, resultando na diminuição do tempo de ciclo da produção.

Com a possibilidade de rastreamento de seus produtos, a empresa obteve melhor visão sobre a eficiência de sua cadeia de suprimento, estando pronta para entregar seus produtos aos clientes. Essa percepção foi resultado de relatórios gerados com base nos dados obtidos pela **RFID**.

A HP estima que poderá reduzir o estoque das impressoras em cerca de 20% e com os produtos etiquetados do início ao fim do processo de montagem, a empresa possui dados que acusam quando uma etapa está demorando mais do que devia, podendo obter resultados na hora sobre o tempo e a quantidade de produtos que sofrem algum impacto durante o processo. Com isso a empresa pode solucionar seus problemas, checando o equipamento na linha de produção e a qualidade das peças que estão sendo utilizadas, analisando o processo de montagem e certos fatores a fim de sanar qualquer problema acusado.

Pelo fato de os cartuchos de tinta possuir data de validade, o "*install by date*" não deixa a mercadoria vencer no estoque, informando sua data limite. A empresa aponta que os tempos de embarque dos produtos foram diminuídos em 12% e os tempos de inventário em 17%[7,12].

6.2 ESTUDO DE CASO: PEDÁGIO SEM PARAR / VIA FÁCIL

Para este estudo de caso serão salientadas as questões da importância da visão sistêmica da coleta e tratamento da informação por meio do uso da tecnologia de **RFID** no que diz respeito à agilidade e maior eficiência na tomada de decisão.

Figura 36 - Processo de pagamento convencional do pedágio[16]

6.2.1 Análise da Problemática

A situação problema a ser analisada neste estudo de caso busca evidenciar a falta de agilidade no fluxo de cobrança dos tributos decorrentes da utilização de vias com pedágio e estacionamentos de estabelecimentos particulares que cobram pela estadia dos veículos em sues domínios. Assim, dependendo da intensificação da quantidade de veículos que trafegam pela localidade e a própria deficiência do fluxo de transação financeira no sistema; observa-se o impacto direto na situação caótica do trânsito.

Esse panorama se deve ao fato de que, cada veículo antes de cruzar a cancela da praça de pedágio deve efetuar o pagamento em espécie da tarifa de pedágio, assim, muitas vezes esse processo acaba perdendo desempenho no fluxo transacional para que o próximo veículo da fila alcance o caixa e promova o mesmo procedimento.

Da mesma forma nos estacionamentos em que se promove o formato de cobrança da taxa de estacionamento onde o cliente recebe um tíquete ou cartão de estacionamento na entrada e ao sair do local precisa validá-lo em guichês, o que novamente pode ocasionar filas e perda de eficiência no processo.

Nesses dois cenários abordados imperam a ineficiência dos sistemas em detrimento as filas e a necessidade de parar o veículo diante a cancela de barramento, para só após

confirmação do fluxo de pagamento, disponibilizar a liberação do veículo, o que acaba resultando em desperdício de tempo decorrente da imobilização do veículo mediante a transposição do ponto de bloqueio.

De acordo com o DETRAN-SP (2010), São Paulo, a maior cidade brasileira, tem 25% da frota nacional, que hoje representa perto de sete milhões de veículos. Em números comparativos, temos o valor de 1,62 habitantes por veículo.

Nos últimos 40 anos tem surgido sempre o questionamento sobre o possível futuro colapso ou travamento total do trânsito.

Figura 37 - Trânsito em praça de pedágio[16]

O foco do estudo não é na questão caótica do trânsito enquanto, é apontar as facilidades provenientes da aplicação da tecnologia de **RFID** para controle e automatização de processos outrora executados manualmente[3].

6.2.2 Análise da Proposta

O estudo visa apresentar a proposta do uso do serviço Sem Parar/Via Fácil e sua viabilidade por meio da cobrança de pedágio de forma automatizada, ou seja, sem que haja necessidade da figura do motorista do veículo estabelecendo o ela da transação financeira em espécie com o caixa do estabelecimento. Assim, a taxa é automaticamente debitada de uma conta pré-cadastrada, promovendo maior fluidez no trânsito, ao passo que incrementa a comodidade ao cliente usuário do serviço.

Neste contexto o estudo de caso proposto pretende analisar a utilização da tecnologia **RFID** na gestão da coleta e tratamento da informação gerencial na questão do tráfego de veículos nas praças de pedágios e estacionamentos que empregam a tecnologia do Sem Parar/Via Fácil.

6.2.3 Tecnologia

A tecnologia utilizada pelo Sem Parar/Via Fácil foi desenvolvida especialmente para trazer mais conforto e praticidade à suas viagens. A Figura 38 a seguir indica o dispositivo utilizado pela empresa.

Figura 38 - Tag usada pelo Sem Parar/Via Fácil[16]

Utilizada em países da Europa, Ásia e Américas, essa solução funciona de forma bastante simples: assim que você se aproxima do pedágio ou saída do estacionamento, uma antena detecta automaticamente a presença do seu veículo e libera a sua passagem, sem que seja necessário sequer parar o carro. Como as cancelas no Brasil são mecânicas, o carro pode passar numa velocidade de até 40 km por hora. Na Europa, no Canadá e no Chile já existem pedágios, sem cancela que permitem rodar a até 160 quilômetros por hora com esse sistema. A frequência utilizada é a de 5,8 GHz – a mesma das transmissões de rádio FM[3,16].

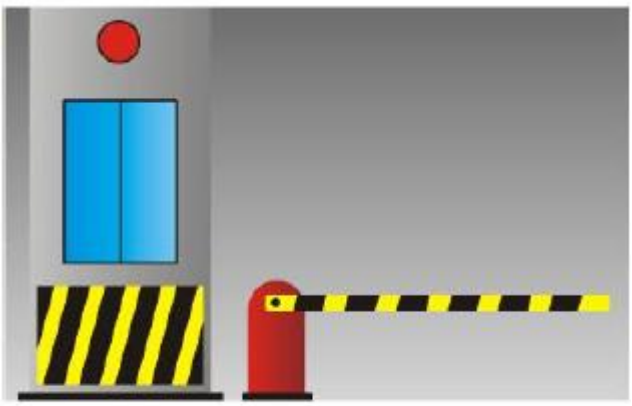
6.2.4 Princípio de Funcionamento do Sem Parar/Via Fácil

O sistema funciona por meio de um dispositivo eletrônico (*tag*) colado no lado interno do para-brisa. Por meio da tecnologia de rádio frequência, o sistema identifica o veículo que tem a *tag*, abre a cancela automaticamente e envia a informação aos computadores do Sem

Parar/Via Fácil, que faz a cobrança posteriormente. A Figura 39 a seguir indica o passo a passo do funcionamento do sistema.

Você passa com o seu veículo na pista devidamente sinalizada com o Via Fácil.

Você passa com o seu veículo na pista devidamente sinalizada com o Via Fácil.



A identificação do TAG é feita automaticamente pelo pedágio ou estacionamento.

Figura 39 - Sequência de funcionamento do sistema Sem Parar/Via Fácil[16]

A Figura 40 a seguir indica sob uma visão sistêmica a interação entre os componentes do **RFID** e a sua interação para o tratamento do fluxo de dados coleto no processo.

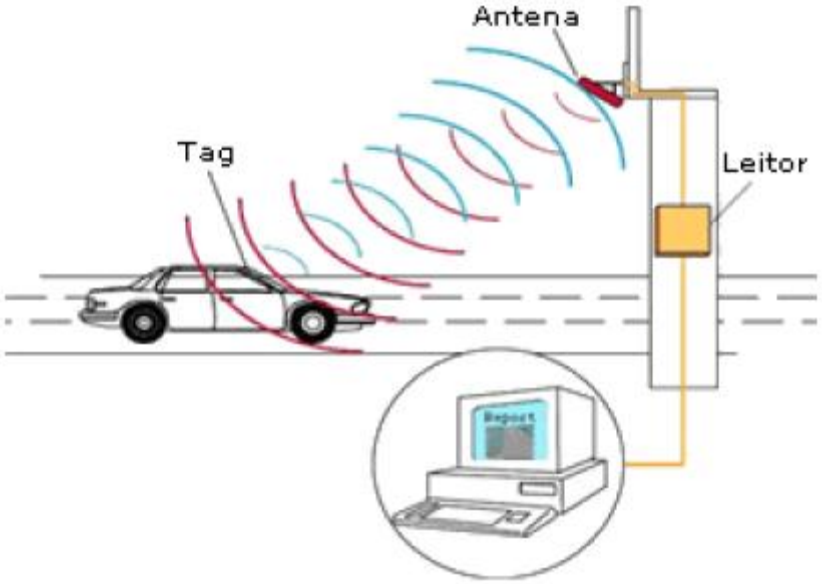


Figura 40 - Partes do sistema RFID[16]

Quando o veículo com a *tag* instalada se aproxima da cabine do Sem Parar/Via Fácil, a antena lê a identificação armazenada no chip da etiqueta e consulta o banco de dados antes de liberar sua passagem. Depois, envia a informação para o sistema da concessionária da rodovia ou do estacionamento, que junta as transações em lotes e as envia para a STP. Após emitir o extrato para o cliente, a empresa remete a ordem de cobrança para o banco. No caso de inadimplência do usuário, a STP atualiza automaticamente os bancos de dados de todas as concessionárias, bloqueando a passagem do veículo. Isso exige a troca constante de informações entre o sistema da STP e os utilizados pelas diferentes empresas e instituições financeiras com as quais opera[3].

6.2.5 Vantagens do Sistema

A seguir serão listadas algumas vantagens da utilização deste sistema:

- Rapidez – não é necessário mais guardar o tíquete de estacionamentos ou parar no meio do caminho para pagar pedágios;
- Sem fila do Caixa – nos estacionamentos credenciados, não se pega fila para validar o tíquete;
- Comodidade – não será preciso mais se preocupar com dinheiro ou mesmo em parar em uma cancela de pedágio;

- Facilidade – todas as tarifas são pagas uma única vez por mês, na data de vencimento escolhida pelo usuário, com débito em conta corrente ou no cartão de crédito de sua preferência;
- Tempo extra – o usuário tem até 30 dias para pagar suas despesas de pedágio e estacionamento;
- Economia – o veículo do usuário gasta menos combustível;
- Conforto – o usuário tem vários serviços à sua disposição, sem sair do computador, acessando o serviço “Minha Conta”[16].

CAPÍTULO 7 – CONCLUSÕES

O objetivo deste trabalho foi realizar uma análise sistêmica da tecnologia de identificação por radiofreqüência, ou **RFID**, com pouca ênfase aos aspectos técnicos e mais voltada para o funcionamento geral desta, bem como à caracterização de tudo o que compõe o sistema. Tal meta foi atingida com êxito, tendo em vista que foram detalhados, ao longo deste, cada componente, seus diversos tipos e suas respectivas funções dentro do sistema.

O estudo de caso foi muito importante para elucidar a aplicabilidade do **RFID**. Muitos desafios enfrentados na implantação do projeto **RFID** possibilitaram diversos estudos e avanços na área **RFID** e impulsionaram diversas outras empresas a estudar a adotar a nova tecnologia, sendo que o preço da tecnologia **RFID** ainda é um fator limitador para muitas empresas.

Em busca do aumento de eficiência na organização, controle e distribuição de produtos e mercadorias, uma tecnologia como o **RFID** se bem aplicada pode economizar tempo e mão de obra, prover mais agilidade, confiabilidade e rapidez atualizando banco de dados, rastreando mercadorias e minimizando a necessidade de intervenção humana no sistema.

Foi apresentada também a história do **RFID**, que não é uma tecnologia nova, e como funciona esse sistema. Suas frequências e padrões foram tratados destacando as duas principais padronizadoras do **RFID**: a ISO e a EPC Global. A segurança e os pilares da Segurança da Informação foram tratados, inclusive explicitando métodos e perigos na proteção do **RFID**.

Vale ressaltar que, apesar de toda a explanação sobre o **RFID**, ela é uma tecnologia em pleno desenvolvimento e vários padrões ainda não foram desenvolvidos. Os custos andam em declínio, já que, cada vez mais, grandes varejistas, fabricantes e empresas de tecnologia estão implementando **RFID** em suas linhas de produção, armazéns e prateleiras.

O **RFID** mostra-se uma tecnologia cada vez mais usada, agregando valor a produtos, solidificando processos e se tornando cada vez mais presente na vida das pessoas.

Portanto, tendo em vista o crescimento exponencial das necessidades de utilização do **RFID** em uma economia cada vez mais globalizada, iniciativas da UFC em pesquisa e desenvolvimento relacionadas a essa tecnologia seriam extremamente importantes.

As vantagens virão com certeza, mas para isso é necessário que o assunto seja abordado criteriosamente em todas as suas vertentes, assim poderá vislumbrar um cenário onde toda a cadeia produtiva e comercial esteja sintonizada na mesma frequência.

REFERÊNCIAS BIBLIOGRÁFICAS

[1] BERNARDO, Gonçalves Cláudio. A tecnologia RFID e os benefícios da etiqueta inteligente para os negócios. Disponível em: <http://www.unibero.edu.br/download/revistaeletronica/Set04_Artigos/A%20Tecnologia%20RFID%20-%20BSI.pdf>. Acesso em: 13 de abril de 2011.

[2] BHUPTANI, Manish.; MORADPOUR, Shahram. RFID: implementando o sistema de identificação por radiofreqüência, São Paulo, 2005.

[3] CARVALHO, Thiago Marques. Análise gerencial do fluxo da informação nos processos sistêmicos com o advento e adoção da tecnologia de RFID, São Paulo, 2009. Trabalho de Conclusão de Curso – Faculdade de Tecnologia da Zona Leste.

[4] EUROPEAN ARTICLE NUMBER. Disponível em: <http://www.epcglobalinc.org>. Acesso em: 02 de abril de 2011.

[5] FERRAZ**,** Onildo Luciano. Comunicação NFC (*Near Field Communication*) entre Dispositivos Ativos**,** Recife, 2010. Trabalho de Graduação em Engenharia da Computação – Universidade Federal de Pernambuco, UFPE.

[6] LIMA, Levi Ferreira Junior. A tecnologia de RFID no padrão EPC e o estudo soluções para a implantação desta tecnologia em empilhadeiras, São Paulo, 2006. Monografia programa de pós-graduação MBIS – Pontifícia Universidade Católica de São Paulo.

[7] MALTA, Camila Rodrigues. RFID: Aplicações e novas tecnologias, São Paulo, 2009. Trabalho de Conclusão de Curso – Faculdade de Tecnologia da Zona Leste.

[8] OLIVEIRA, Alessandro de Souza.; PEREIRA, Milene Franco. Estudo da tecnologia de identificação por radiofreqüência – RFID, Brasília, 2006. Projeto de Graduação – Universidade de Brasília, UnB.

[9] PASSARETTI, Caio Santi. RFID – Identificação por radiofreqüência movendo-se para o futuro, Brasília, 2008. Projeto de Graduação – Universidade de Brasília, UnB.

[10] PEDRO, Luís Manuel Dias. Plataforma de comunicações sem fios para ZIGBEE e RFID, Lisboa, 2008. Dissertação para obtenção de grau mestre – Instituto Superior Técnico – Universidade Técnica de Lisboa.

[11] RFID – Etiquetas com eletrônica de ponta, Saber Eletrônica Nº 401, Junho de 2006.

[12] RFID JOURNAL. HP implanta tecnologia RFID em toda a cadeia de suprimentos. Disponível em: < http://www.rfidjournal.com/article/view/8448/1>. Acesso em: 20 de maio de 2011.

[13] RFID JOURNAL. *The history of RFID technology*. Disponível em: <www.rfidjournal.com/article/articleview/1338/1/120/>. Acesso em: 06 de abril de 2011.

[14] RFID para UHF, Elektor Nº 88, Janeiro de 2009.

[15] SANTINI, Arthur Gambin. RFID: Conceitos, Aplicabilidades e Impactos, Rio de Janeiro, 2008.

[16] VIA FÁCIL. Sem Parar – Via Fácil. Disponível em: <http://www.viafacil.com.br/sp/>. Acesso em: 20 de maio de 2011.

[17] WIKIPEDIA. RFID. Disponível em: <pt.wikipedia.org/wiki/RFID>. Acesso em: 25 de março de 2011.

[18] WIRELESS BRASIL. Identificação por radiofreqüência. Disponível em: < http://www.wirelessbrasil.org/wirelessbr/colaboradores/sandra_santana/rfid_11.html>. Acesso em: 25 de março de 2011.