Faculdade de Engenharia da Universidade do Porto

# RFID Versus Código de Barras

# da

# Produção à Grande Distribuição

Jorge Rei

VERSÃO PROVISÓRIA

Dissertação realizada no âmbito do
Mestrado Integrado em Engenharia Electrotécnica e de Computadores
Major Telecomunicações

Orientador : Prof. Dr. João Barros (FEUP)
Co-orientador: Dr. Tiago Vinhoza (Instituto de Telecomunicações)

<Junho 2010>

# Resumo

As tecnologias de identificação automática são uma realidade omnipresente no mundo em que vivemos.

De entre as tecnologias de identificação automática, o código de barras é a mais usada em todo o mundo e a sua utilização não levanta qualquer polémica.

O sistema de identificação por radiofrequência aspira a substituir a tecnologia de código de barras, acrescentando novas funcionalidades e facilidades, mas a sua aceitação não é pacífica, já que pode ter subjacente uma invasão da privacidade.

Neste trabalho pretende-se analisar os requisitos de implementação da tecnologia RFID numa empresa do sector agro-industrial, os ganhos esperados internamente e na melhoria do relacionamento com todos os intervenientes na cadeia de valor, desde a produção até à grande distribuição.

Serão também analisados os problemas de segurança e privacidade levantados pela introdução desta tecnologia.

# Abstract

The automatic identification technologies are a pervasive reality in the world we live.

Among the technologies of automatic identification, bar code is the most used around the world and their use does not raise any controversy.

The system of radio frequency identification aims to replace the bar code technology, adding new features and facilities, but its acceptance is not peaceful, because it may have an underlying invasion of privacy.

This paper aims to assess the requirements for implementation of RFID technology in the agro-industrial sector, the internal benefits and improving the relationship with all stake-holders in the value chain, from production to supermarkets.

Will also be examined security and privacy issues inherent to this technology.

# Agradecimentos

Ao Prof. Dr. João Barros que acolheu a ideia deste trabalho e indicou o Dr. Tiago Vinhoza para o orientar.

Ao Dr. Tiago Vinhoza que aceitou orientar este trabalho.

Ao Eng. Silvério Neves pelos preços que me forneceu.

Ao meu filho pelo desafio.

A todos eles expresso a minha gratidão.

Com os meus melhores cumprimentos

Jorge Rei

# Índice

# Lista de figuras

# Lista de tabelas

# Abreviaturas e Símbolos

| | |
|---|---|
| AI | Application Identifier |
| AIDC | Automatic Identification and Data Capture |
| API | Application Programming Interface |
| BI | Bilhete de Identidade |
| BRIDGE | Building Radiofrequency Identification Solutions for the Global Environment |
| CASPIAN | Consumers Against Supermarket Privacy Invasion and Numbering |
| DoD | Department of Defense, dos Estados Unidos da América |
| DNS | Domain Name System |
| DoS | Denial of Service |
| DRM | Dense Reader Mode |
| EAN | European Articl Number |
| EDI | Electronic Data Interchange |
| EIRP | Equivalent Isotropically Radiated Power |
| EMEA | Europe, Middle East and Africa |
| EPC | Electronic Product Code |
| ERP | Effective Radiated Power |
| ERP | Enterprise Resource Planning |
| ETSI | European Telecommunication Standards Institute |
| EUA | Estados Unidos da América |
| FCC | Federal Communications Commission |
| GDSN | Global Data Syncronization Network |
| GIAI | Global Individual Asset Identifier |
| GLN | Global Location Number |
| GRAI | Global Returnable Asset Identifier |
| GTIN | Global Trade Identifier Number |
| GPS | Global Positioning System |
| HF | High frequency |
| IEC | International Electrotechenical Commission |
| IFF | Identification Friend or Foe |
| ISBN | International Standard Book Number |
| ISM | Industrial, Scientific and Medical |

| | |
|---|---|
| ISO | International Organization for Standardization |
| ITF | Interrogator Talks First |
| ITU | International Telecommunication Union |
| LBT | Listen Before Talk |
| LF | Low frequency |
| MIB | Management Information Base |
| MIT | Massachusetts Institute of Technology |
| OCR | Optical character recognition |
| ONS | Object Name Service |
| PME | Pequena e Média Empresa |
| RFC | Request for Comments |
| RFID | Radio Frequency Identification |
| RTLS | Real Time Location System |
| SNMP | Simple Network Management Protocol |
| SSCC | Serial Shipping Container Code |
| TTF | Tag Talks First |
| UCC | Uniform Commercial Code |
| EU | União Europeia |
| UHF | Ultra High Frequency |
| UID | Unique Identification |
| UPC | Universal Post Code |
| UPCC | Uniform Product Code Council |
| WMS | Warehouse Management System |

Lista de símbolos

| | |
|---|---|
| λ | Comprimento de onda |
| c | Velocidade da luz no vácuo |
| f | Frequência da onda |

# Capítulo 1

# Introdução

## 1.1 - Motivação

Ao longo dos últimos anos as empresas das áreas de produção, distribuições e comercialização de bebidas e produtos alimentares, têm implementado várias soluções baseadas em código de barras. A introdução desta tecnologia provocou ganhos de produtividade apreciáveis e que podiam ser facilmente mensuráveis como por exemplo: diminuição de tempos de digitação, eliminação dos erros de digitação e a eliminação dos efeitos nefastos que esses erros introduziam nas operações efectuadas a jusante, entre outros.

O mercado é uma entidade dinâmica, em constante evolução, e os desafios que hoje são colocados na forma de informar, nas relações de interdependência entre todos os intervenientes da cadeia de valor, na diminuição dos tempos de resposta admissíveis às solicitações dos intervenientes no processo, no atendimento cada vez mais personalizado e na tendência global para uma gestão de stocks *just in time* exigem novas respostas.

As perdas que as organizações assumem, que são comprovadas por vários estudos e imputadas a uma deficiente gestão de stocks são, cada vez mais, uma área prioritária para a gestão, razão pela qual, qualquer solução que minimize essas perdas e que apresente um retorno de investimento garantido são normalmente adoptadas.

As soluções baseadas em código de barras não permitem a implementação de soluções de *track and trace* em tempo real, uma interactividade on-line entre os intervenientes na cadeia de abastecimento nem a alteração da informação contida no código de barras, além de outras limitações.

A resposta a muitas das limitações apresentadas pelo código de barras é dada por uma tecnologia relativamente recente e que cada vez ganha mais adeptos a nível global. Essa tecnologia é denominada RFID (Radio Frequency Identification), cujas principais características, potencialidades, limitações e implementação serão abordadas neste trabalho, porque acredi-

ta-se que a sua utilização abre uma nova visão sobre a forma de encarar a sociedade em que vivemos e que será uma das componentes fundamentais de uma nova visão das tecnologias da informação e comunicação que é designada por *'Internet of Things'*

## 1.2 - Objectivos

Um dos objectivos deste trabalho é analisar as possibilidades da tecnologia de RFID (Radio Frequency Identification) substituir ou complementar a curto prazo, 3 a 5 anos, muitas das implementações baseadas no código de barras actualmente usado na troca de informações entre as empresas do sector agro-industrial, as empresas transportadoras, as plataformas logísticas e a grande distribuição. Também analisamos os impactos ao nível da segurança e privacidade resultantes da adopção da tecnologia RFID e apresentamos um modelo que pretende minimizar as ineficiências e limitações intrínsecas, ao modelo actual baseado em código de barras. Finalmente analisamos os custos e impactos resultantes da adopção da tecnologia RFID por uma empresa do sector agro-alimentar.

## 1.3 - Enquadramento

Neste trabalho pretendemos integrar os conhecimentos obtidos nas áreas de formação académica específicas de PGRE (Planeamento e Gestão de Redes), SSRE (Segurança em Sistemas e Redes), Telecomunicações e a minha actividade profissional.

O Planeamento e Gestão de Redes será usado, na avaliação de toda a infra-estrutura da rede que será necessário projectar, alterar ou implementar, para que uma solução baseada em RFID possa ser introduzida minimizando os impactos negativos na organização bem como no dimensionamento dos meios necessários para garantir uma elevada qualidade dos serviços oferecidos a nível de transporte dos dados envolvidos.

Uma especificação de requisitos da empresa deve ser efectuada e o processo de implementação da infra-estrutura projectada deve ser testada de forma a garantir que as soluções adoptadas cumprem os requisitos especificados.

A Segurança em Sistemas e Redes será utilizada para avaliar a segurança do sistema quanto a potenciais ataques, selecção das metodologias a sugerir/implementar que garantam uma efectiva confidencialidade e integridade dos dados, bem como das medidas tendentes a evitar a contrafacção ou detecção de artigos contrafeitos.

As Telecomunicações, são a base de toda a infra-estrutura a ser usada para aquisição e transmissão de dados. Uma análise individual terá que ser efectuada em cada organização em que se pretenda implementar uma solução com tecnologia RFID. Um estudo aprofundado deve ser efectuado para, escolher o tipo, quantidade e localização dos leitores e respectivas antenas, controladores e tipo de tags a usar de forma a garantir uma efectiva cobertura de toda a área abrangida.

A actividade profissional, porque o objectivo é, implementar efectivamente os conhecimentos obtidos com este trabalho. Se este objectivo for alcançado, será mais um passo, na direcção de uma efectiva interligação, entre um estudo académico e o mercado de trabalho, que é tantas vezes discutida e nem sempre pelas melhores razões.

## 1.4 - Organização

Este trabalho está dividido em nove capítulos de acordo com os vários temas abordados, de uma forma sequencial, até ao objectivo final.

O capítulo 1 serve de introdução ao trabalho a desenvolver.

O capítulo 2 aborda a tecnologia de código de barras e apresenta as suas principais vantagens, limitações e vulnerabilidades.

O capítulo 3 aborda a tecnologia de RFID e seus componentes fundamentais.

O capítulo 4 aborda as tags de RFID, suas classificações, características e alimentação.

O capítulo 5 aborda a rede EPCglobal, sua estrutura, componentes e identificadores.

O capítulo 6 aborda os problemas de privacidade e segurança levantados pela tecnologia de RFID.

O capítulo 7 aborda os pontos principais a ter em conta na implementação de uma infraestrutura de RFID numa organização.

O capítulo 8 apresenta um modelo de possível solução para a gestão de stocks de produtos acabados de uma empresa do sector agro-industrial e respectiva estimativa de custos.

O capítulo 9 apresenta algumas conclusões que se podem tirar desta dissertação e o trabalho futuro que pretendo efectuar.

# Capítulo 2

# Código de Barras

O código de barras é uma representação gráfica de dados que podem ser numéricos ou alfanuméricos, dependendo do tipo de código de barras utilizado.

## 2.1 Sistemas de Identificação Automática

**AIDC (Automatic Identification and Data Capture)** - Este conceito engloba um conjunto de métodos para identificar 'objectos', recolher informação acerca deles e fornecer essa informação a sistemas de tratamento de dados de forma automática.

Este conceito engloba, além do código de barras, outras tecnologias como:

- Biometria;
- OCR – Optical Character Recognition;
- Smart Cards e Contact Less Smart Cards;
- RFID - Radio Frequency IDentification.

**Biometria** - As características biométricas individuais são utilizadas para identificar um indivíduo e conceder/retirar permissões. As aplicações mais conhecidas desta tecnologia são o relógio de ponto, controlo de acessos e a activação de serviços, funcionando a característica biométrica seleccionada como *password*. As características biométricas individuais mais usadas são a impressão digital, a voz e a íris.

**OCR** - O reconhecimento óptico de caracteres permite, através da digitalização de um texto impresso, obter um ficheiro que é posteriormente tratado num editor de texto.

**Contactless Smart Cards** - São normalmente cartões de plástico que incorporam um microprocessador e memória, que permitem implementar mecanismos de segurança para proteger a informação que contêm ou disponibilizam e permitir o acesso às funcionalidades que implementam, após validação. Embora as tecnologias de Smart Cards e RFID tenham muito

em comum são normal distingui-las com base no tipo de informação que contêm, nível de segurança que implementam, distância de leitura e áreas de aplicação.

**RFID** – A identificação por rádio frequência é uma tecnologia AIDC sem fios, que usa sinais de rádio para remotamente identificar um 'objecto', armazenar ou recuperar informação acerca dele, guardada num dispositivo chamado tag, que está colocado no 'objecto'.

As tecnologias de AIDC encontram-se hoje largamente implementadas em variadas áreas de actividade, entre as quais se destacam: pontos de venda, gestão de stocks, rastreabilidade, logística, distribuição, anti-roubo, controlo de acessos, pagamento de transportes, identificação animal, documentos de identificação, controlo de bagagens, track and trace de objectos, etc.

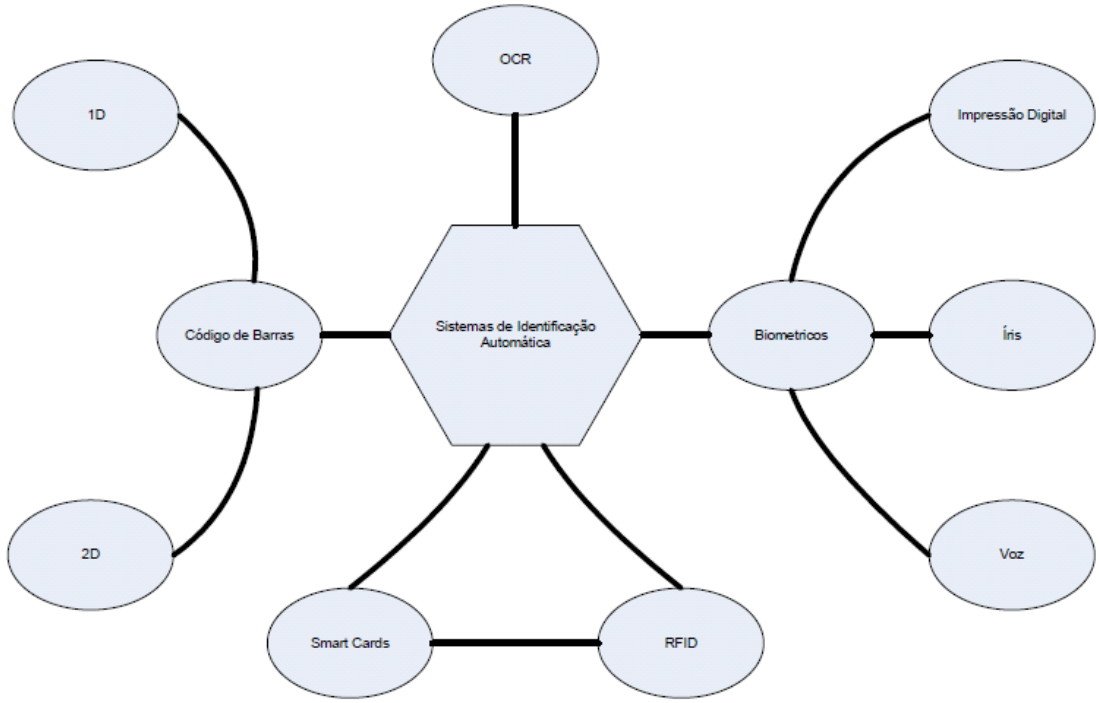


**Figura 2.1** – Sistemas de Identificação Automática

## 2.2 – História do Código de barras

O código de barras e respectivo leitor são uma patente atribuída em 1952 aos norte-americanos Joseph Woodland e Bernard Silver que apresentaram uma matriz de identificação baseada em círculos concêntricos. Posteriormente, Joseph Woodland inspirou-se no código Morse que usa pontos e traços e prolongando-os na vertical criou o primeiro código de barras linear. [1]

A 26 de Junho de 1974, um pacote de pastilhas elásticas foi o primeiro produto identificado no *check-out* de uma loja usando o código UPC dando-se, assim, início à aplicação comercial de uma tecnologia que é hoje uma realidade omnipresente no nosso dia-a-dia. [1]

O código de barras é a tecnologia de identificação automática mais usada em todo o mundo e a sua presença pode ser encontrada nas mais diversas áreas de actividade.

Actualmente são usadas duas simbologias de códigos de barras:

- Simbologia linear ou 1D que usa barras verticais de diferentes larguras separadas por espaços em branco e cuja representação GS1 será abordada em maior profundidade;
- Simbologia bidimensional ou 2D que usa além de barras, pontos, quadrados e outros símbolos e cujas representações mais conhecidas são PDF417 (Portable Data Format) e DataMatrix.

**Figura 2.2** – Exemplos de PDF417

Esta tecnologia deve grande parte da sua aceitação global ao facto de, na sua génese, se encontrarem associações que se preocuparam com a implementação de standards que pudessem ser usados globalmente e orientados a sectores de actividade. Entre as entidades que mais contribuíram encontram-se a UPCC (Uniform Product Code Council) responsável pelo código UPC (Universal Post Code) e que daria origem à UCC (Uniform Code Council), a AIM (Association for Automatic Identification and Mobility) e a EAN (European Article Numbering).

Em 2005 a fusão entre a UCC e a EAN deu origem a uma nova entidade, a GS1, que gere o uso global dos sistemas baseados em código de barras.

'*O Sistema GS1 é um conjunto de Normas integradas abertas e globais, reconhecidas internacionalmente, para a gestão eficiente das cadeias de valor multi-sectoriais, baseada numa identificação única e inequívoca de produtos, unidades de expedição, activos, localizações e serviços, que agiliza todos os processos comerciais, incluindo o comércio electrónico e a rastreabilidade.*' [02]

Fazem parte da GS1 as seguintes entidades:

- GS1 BarCodes – Normas globais para identificação automática;
- GS1 eCom – Normas globais para mensagens electrónicas comerciais;
- GS1 GDSN – Ambiente para sincronização global de dados;
- GS1 EPCglobal – Normas globais para identificação por rádio frequência.

Em Portugal a entidade que representava a European Article Numbering Association era a Codipor que, com a criação da GS1, passou a ser designada por GS1 Portugal CODIPOR.

A Codipor – Associassão Portugesa de Identificação e Codificação de Produtos foi fundada em 1985. É uma organização privada sem fins lucrativos formada por industriais, distribuidores e prestadores de serviços.


**Figura 2.3** – Áreas de implementação de normas GS1 [02]

A cada associada da GS1 é atribuído um código de entidade (Company Prefix) que a identifica, univocamente, em todo o mundo. Os três primeiros dígitos do código de entidade indicam o país de origem. Seguem-se quatro, cinco ou seis dígitos que identificam a empresa. A atribuição de quatro, cinco ou seis dígitos ao código da empresa depende do número de dígitos de que ela vai necessitar para a codificação dos itens que comercializa.

## 2.3 – Identificadores GS1 Código de Barras

Na base do sistema estão um conjunto de identificadores-chave e dados adicionais que permitem a interligação entre o código de barras e as bases de dados que contêm a informação complementar.

Os identificadores-chave ou dados primários são aqueles que identificam apenas o produto ou serviço e que são usados em transacções comerciais.

Os dados adicionais ou identificadores aplicacionais (AIs) são aqueles que intervêm nos processos de produção, armazenamento e distribuição de mercadorias.

Os identificadores-chave são únicos, multi-sectoriais e internacionais.

Identificadores-chave mais utilizados no código de barras:

- GTIN – Global Trade Item Number:
- GLN – Global Location Number;
- SSCC – Serial Shipping Container Code;
- GRAI – Global Returnable Asset Identifier;
- GIAI – Global Individual Asset Identifier.

### 2.3.1 - GTIN

O GTIN identifica um item (mercadoria ou serviço) acerca do qual é necessário obter informação adicional, armazenada na base de dados do sistema informático, para proceder à transacção pretendia.

O GTIN, tanto pode ser aplicado ao nível do item (GTIN-8 e GTIN-13), como ao nível da embalagem (GTIN-14).

| **GTIN – *Global Trade Item Number* (14 dígitos)** | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **Estrutura de Dados** | T1 | T2 | T3 | T4 | T5 | T6 | T7 | T8 | T9 | T10 | T11 | T12 | T13 | T14 |
| GTIN-14 | N1 | N2 | N3 | N4 | N5 | N6 | N7 | N8 | N9 | N10 | N11 | N12 | N13 | N14 |
| GTIN-13 | 0 | N1 | N2 | N3 | N4 | N5 | N6 | N7 | N8 | N9 | N10 | N11 | N12 | N13 |
| GTIN-8 | 0 | 0 | 0 | 0 | 0 | 0 | N1 | N2 | N3 | N4 | N5 | N6 | N7 | N8 |

**Figura 2.4** – Estrutura de dados GTIN [03]

Esta estrutura de dados serve de chave de acesso às bases de dados dos sistemas informáticos quando justificada à direita, num campo de 14 dígitos numéricos.

Ao contrário do GTIN-14 e do GTIN-13 que é da responsabilidade da organização que introduz as mercadorias ou serviços no mercado, o GTIN-8 é atribuído pela GS1 ou seu representante legal.

### 2.3.2 - GLN

O GLN é composto por 13 dígitos que identificam uma localização dentro de uma entidade associada da GS1, normalmente um armazém, e é atribuída pela GS1 ou pelo seu representante legal.

| GS1 Company Prefix > | | | | | < Location Reference | | | | | | | Check Digit |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| $N_1$ | $N_2$ | $N_3$ | $N_4$ | $N_5$ | $N_6$ | $N_7$ | $N_8$ | $N_9$ | $N_{10}$ | $N_{11}$ | $N_{12}$ | $N_{13}$ |

**Figura 2.5** – Estrutura de dados GLN [03]

### 2.3.3 – SSCC

Este identificador é composto por 18 dígitos e permite identificar univocamente uma unidade logística destinada ao transporte ou armazenamento e pode ser monoproduto ou multiproduto. As unidades logísticas mais usadas são a palete e o contentor.

| Extension Digit | GS1 Company Prefix > | | | | | | | < Serial Reference | | | | | | | | Check Digit |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| $N_1$ | $N_2$ | $N_3$ | $N_4$ | $N_5$ | $N_6$ | $N_7$ | $N_8$ | $N_9$ | $N_{10}$ | $N_{11}$ | $N_{12}$ | $N_{13}$ | $N_{14}$ | $N_{15}$ | $N_{16}$ | $N_{17}$ | $N_{18}$ |

**Figura 2.6** – Estrutura de dados SSCC [03]

### 2.3.4 – GRAI

Este identificador é composto por um máximo de 30 caracteres que se destinam a identificar os activos retornáveis de uma empresa. O termo, normalmente usado para o activo retornável, é tara retornável e refere-se a embalagens ou unidades usadas no transporte das mercadorias que são reutilizáveis e possuem valor comercial.

| | GS1 Company Prefix > | | | | | < Asset Reference | | | | | | Check Digit | Serial Number (optional) |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 0 | $N_1$ | $N_2$ | $N_3$ | $N_4$ | $N_5$ | $N_6$ | $N_7$ | $N_8$ | $N_9$ | $N_{10}$ | $N_{11}$ | $N_{12}$ | $N_{13}$ | $X_1$ variable $X_{16}$ |

**Figura 2.7** – Estrutura de dados GRAI [03]

### 2.3.5 - GIAI

Este identificador é composto por um máximo de 30 caracteres que se destinam a identificar um activo fixo de uma empresa. Um activo individual é um bem com carácter duradouro que deve ser identificado individualmente para controlo do imobilizado corpóreo.

| GS1 Company Prefix > | < Individual Asset Reference > |
|---|---|
| $N_1 \ldots N_i$ | $X_{i+1} \ldots X_j$ (j<=30) |

**Figura 2.8** – Estrutura de dados GIAI [03]

## 2.4 – Check Dígito

O check dígito ou dígito de controlo é um dígito calculado função dos dígitos anteriores e destina-se a detectar possíveis erros de codificação ou digitação.

Para calcular o check dígito de um número:

- Numerámos os dígitos desse número da direita para a esquerda;
- Atribuímos aos dígitos ímpares um peso 3;
- Atribuímos aos dígitos pares um peso 1;
- Calculámos o somatório das parcelas individuais pesadas;
- Subtraímos ao múltiplo de 10 maior ou igual ao somatório o valor do somatório;
- O resultado da subtracção é o check dígito.

| Dígitos | d12 | d11 | d10 | d9 | d8 | d7 | d6 | d5 | d4 | d3 | d2 | d1 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Número | 5 | 6 | 0 | 1 | 3 | 1 | 2 | 0 | 2 | 4 | 7 | 2 |
| Peso | 1 | 3 | 1 | 3 | 1 | 3 | 1 | 3 | 1 | 3 | 1 | 3 |
| Peso x Dígito | 5 | 18 | 0 | 3 | 3 | 3 | 2 | 0 | 2 | 12 | 7 | 6 |
| Somatório **Σ**: | 5 + 18 + 0 +3 +3 +3 +2 + 0 +2 + 12 + 7 + 6 = **61** | | | | | | | | | | | |
| Subtrair ao múltiplo de 10 maior que o **Σ** o valor do **Σ** → **70 - 61 = 9** | | | | | | | | | | | | |
| O valor do check dígito do número **560131202472** é : **9** | | | | | | | | | | | | |

**Figura 2.9** – Cálculo do check dígito


**Figura 2.10** – Exemplo de Código EAN-13

Analisando o código EAN-13 apresentado podemos concluir que:

- O item foi produzido em Portugal - **560;**

- O Company Prefix atribuído pela GS1 Codipor é - **1312;**
- O código do item é - **02472;**
- O cheque dígito é **9.**

## 2.5 EAN-128 ou GS1-128

Os identificadores-chave são numéricos e necessitam, muitas vezes, de ser complementados com informações contidas noutros identificadores.

A concatenação entre identificadores é implementada no código GS1 – 128 com recurso ao uso de AIs (Aplication Identifeiers).

O GS1-128 deriva do Code 128 que é um código alfanumérico. Num código GS1-128 podemos ter várias linhas de códigos de barras que se complementam. Cada linha não deve ter mais que 48 caracteres e se o SSCC for usado num código GS1-128 deverá ser incorporado isoladamente na última linha dos códigos de barras.


**Figura 2.11** - Exemplo de Etiqueta Logística GS1-128

## 2.6- O Código de Barras na Cadeia de Abastecimento

Da cadeia de abastecimento fazem parte todas as entidades que, desde a produção até ao consumo, cooperam no processamento das mercadorias.

Os intervenientes na cadeia de abastecimento fazem um uso intensivo do código de barras e a codificação utilizada é normalmente a GS1-128. Esta codificação, através do uso de AIs, permite concatenar várias informações numa única etiqueta, com informações referentes ao conteúdo e à embalagem em que está colada.

Ao longo de uma linha de produção é possível observar a aplicação de vários tipos de códigos de barras:

- No item individual que vai ser vendido ao consumidor final é colocado normalmente um código de barras GS1-13 que irá ser lido no ponto de venda;
- Um conjunto de itens individuais é normalmente agrupado numa embalagem para facilitar o manuseamento e abastecimento dos retalhistas. Na embalagem é colocado, normalmente, um código de barras GS1-14 ou ITF-14, dependendo a escolha do código do material em que é feita a impressão e que vai ser lido no check-out do grossista quando ele a vende ao retalhista;
- No fim da linha de produção um conjunto de embalagens é normalmente agrupado dando origem a uma palete que recebe um código de barras GS1-128 com o SSCC da palete e outras informações. Este código de barras vai acompanhar e identificar univocamente a palete durante todo o seu tempo de vida permitindo, a todos os intervenientes nos processos por onde vai passando, uma forma simples, rápida e fiável de identificação, se ninguém falsificar ou destruir essa etiqueta.

Apesar de o SSCC identificar univocamente uma palete, não fornece qualquer informação acerca do seu conteúdo ou destino, o que é fundamental para os vários intervenientes na cadeia de abastecimento. Para fornecer essa informação adicional é usado o código de barras GS1–128 com recurso a AIs.

Existem mais de 100 AIs que podem ser incorporados numa etiqueta. Os AIs devem ser criteriosamente seleccionados para fornecer a informação necessária.

| IA's | DADOS | FORMATO |
|---|---|---|
| 00 | Número de Série Unidade Expedição | n2 + n18 |
| 01 | GTIN da Unidade Comercial | n2 + n14 |
| 02 | Identificação Unidades numa UE | n2 + n14 |
| 10 | Número do Lote | n2 + an..20 |
| 13 | Data de Embalamento | n2 + n6 |
| 15 | Data mínima de validade | n2 + n6 |
| 30 | Número de Itens Contidos UE Variável | n2 + n...8 |
| 37 | Quantidade Contida na UE | n2 + n...8 |
| 310(x) | Peso Líquido [(x) nº decimais] | n4 + n6 |
| 400 | Nº da Nota de Encomenda | n3 + an..30 |
| 422 | País de Origem do Produto | n3 + n3 |

**Figura 2.12** – Alguns dos AIs mais utilizados [02]

## 2.7 Vantagens do Código de Barras

A introdução desta tecnologia teve um impacto enorme nas mais diversas áreas de actividade, mas foi no ponto de venda que esse impacto foi mais sentido.

Esta tecnologia deve o seu enorme sucesso a:

- Existência de standards aceites a nível mundial;
- Tecnologia perfeitamente estabilizada;
- Simplicidade da infra-estrutura necessária: leitor, impressora, computador e respectivo software;
- Baixo custo de implementação e manutenção;
- A sua implementação não tem qualquer impacto negativo no normal funcionamento da empresa;
- Não exige qualquer formação adicional dos operadores;
- Evita erros de digitação;
- Ganhos de produtividade imediatos e facilmente mensuráveis;
- Fiabilidade do sistema;
- Alternativa simples em caso de avaria em muitas situações;
- Imune ao material em que é colocada;
- Imune a interferência electromagnética;
- Isenta de legislação restritiva aplicada pelos diversos países;
- Tecnologia de criação de etiquetas de código de barras simples e barata;
- Isenta de contestação.

## 2.8 Vulnerabilidades e Limitações

Esta tecnologia, apesar das suas enormes vantagens, tem algumas vulnerabilidades/limitações que condicionam a sua utilização:

- Facilmente falsificável, pois não possui qualquer mecanismo de segurança;
- A generalidade das etiquetas de código de barras são impressas sobre papel ou cartão que são materiais de suporte frágil, o que faz com que as etiquetas se tornem inúteis por deterioração do material em que são impressas;
- Facilmente sujeitas a actos de vandalismo, já que estão normalmente acessíveis e são fáceis de inutilizar, basta usar uma esferográfica, marcador, navalha, etc;
- Sensível à cor do fundo sobre que é impressa;
- Sensível ao material sobre que é impressa;
- A informação contida numa etiqueta de código de barras é estática e a forma de a actualizar é colar uma nova etiqueta. A quantidade de etiquetas que se colam numa embalagem é uma fonte potencial de erros e perda de tempo para escolher a etiqueta correcta;

- Quantidade de informação que transportam é muito limitada na simbologia 1D;
- Não identifica univocamente um item na simbologia 1D que é a usada na esmagadora maioria das situações;
- *Tracking* manual;
- Para que um código de barras possa ser lido tem que estar em linha de vista com o leitor;
- A distância entre o leitor e o código de barras a ser lido é muito pequena (< 1 m);
- Os leitores sem fios proporcionam uma melhor mobilidade ao operador, mas quando englobados num processo on-line o seu raio de acção varia normalmente entre os três e os cinco metros de distância à base, têm custos muito mais elevados que os leitores com fios e estão sujeitos a interferências;
- A luminosidade ambiente pode afectar a capacidade de leitura;
- Em tapetes transportadores é necessário manter o sincronismo entre o tempo de disparo do feixe de leitura, o tempo em que o feixe de leitura se mantém activo e a velocidade do tapete para que a leitura seja efectuada;
- Um leitor só pode ler um código de barras de cada vez;
- O tempo de accionamento entre leituras consecutivas pode introduzir atrasos numa linha de transporte;
- Os códigos de barras são muitas vezes impressos na linha de produção, não existindo normalmente qualquer sistema de confirmação da validade do código impresso, razão pela qual qualquer erro de impressão só é detectado *a posteriori* com todas as consequências resultantes da existência de um código inválido em todos os processos a jusante;
- A afinação das impressoras é normalmente um factor crítico numa linha de produção dada a elevada carga de trabalho a que estão sujeitas e ao ambiente em que operam;
- A leitura é normalmente efectuada manualmente estando portanto dependente do operador.

# Capítulo 3

# RFID – Radio Frequency Identification

RFID - Radio Frequency Identification, é uma tecnologia AIDC sem fios, que usa sinais de rádio, para remotamente identificar um 'objecto', armazenar e recuperar informação acerca dele, guardada num dispositivo chamado tag que está colocada no 'objecto'.

Esta tecnologia tem subjacente um novo conceito de individualização na identificação dos objectos e mesmo dos seus constituintes.

## 3.1 A História

A tecnologia RFID tem a sua origem na II Guerra Mundial. Ingleses, Alemães e Japoneses utilizavam os seus radares para saberem, com antecedência, que aviões se aproximavam, mas não identificavam se eram amigos ou inimigos.

Os alemães descobriram que se o piloto, na rota de aproximação, girasse o seu avião, o sinal de retorno era alterado. Este simples procedimento avisava os controladores de que se tratava de um avião alemão. Este é considerado o primeiro sistema passivo de RFID. [04]

Sob o comando de Sir Robert Watson-Watt, que é considerado o inventor do radar, os ingleses desenvolveram um dispositivo que era colocado nos seus aviões. A esse dispositivo deram o nome de IFF – Identification Friend or Foe. Este dispositivo era um transponder que respondia aos sinais enviados pela estação de rastreio. Se o avião respondia era considerado amigo se não respondia era considerado inimigo. [04]

A história da RFID começa verdadeiramente em 1973, quando o americano Mario W. Cadullo consegue a patente de um dispositivo activo de RFID, com memória regravável. No seu pedido de patente, além da descrição técnica englobava, também, áreas de aplicação do seu invento e uma delas é muito semelhante à nossa actual via verde. [05]

## 3.2 O Mercado de RFID

Segundo o relatório, RFID Forcasts, Players & Opportunities 2009-2019, elaborado pela IDTechEx, apresentam-se alguns valores e previsões que dão uma dimensão do valor e dinamismo do mercado mundial de RFID.

| TOTAL MARKET ($BN) | 2009 | 2010 | 2011 | 2012 | 2013 | 2014 | 2015 | 2016 | 2017 | 2018 | 2019 |
|---|---|---|---|---|---|---|---|---|---|---|---|
| Tags - passive | 2.18 | 2.49 | 2.88 | 3.31 | 3.90 | 4.81 | 5.98 | 6.72 | 7.83 | 9.27 | 10.81 |
| Tags - active/BAP | 0.21 | 0.22 | 0.28 | 0.37 | 0.57 | 0.75 | 0.99 | 1.16 | 1.26 | 1.43 | 1.57 |
| Interrogators (incl. cellphones) | 1.20 | 1.22 | 1.69 | 2.25 | 3.20 | 4.08 | 5.09 | 5.12 | 5.35 | 5.47 | 5.71 |
| Networking, Software, Services | 1.97 | 2.28 | 2.68 | 3.38 | 5.17 | 6.85 | 8.38 | 8.97 | 9.03 | 9.33 | 9.50 |
| **Total value $ bn** | **5.56** | **6.21** | **7.53** | **9.32** | **12.84** | **16.49** | **20.44** | **21.97** | **23.47** | **25.49** | **27.59** |

**Tabela 3.1** – Valor do mercado de RFID [06]

| | 2009 | 2010 | 2011 | 2012 | 2013 | 2014 | 2015 | 2016 | 2017 | 2018 | 2019 |
|---|---|---|---|---|---|---|---|---|---|---|---|
| Drugs | 15 | 20 | 30 | 130 | 450 | 1,000 | 1,800 | 2,600 | 4,000 | 5,800 | 7,300 |
| Other Healthcare | 16 | 20 | 45 | 164 | 385 | 469 | 572 | 687 | 785 | 960 | 1,150 |
| Retail apparel | 200 | 300 | 450 | 883 | 1,417 | 4,406 | 7,505 | 10,411 | 12,610 | 15,890 | 18,500 |
| Consumer goods | 10 | 25 | 75 | 220 | 650 | 4,700 | 31,200 | 61,400 | 158,000 | 320,000 | 550,000 |
| Tires | 0 | 0 | 1 | 1 | 1 | 3 | 5 | 8 | 10 | 15 | 20 |
| Postal | 10 | 50 | 100 | 350 | 700 | 1,100 | 2,000 | 5,000 | 15,000 | 30,000 | 60,000 |
| Books | 100 | 130 | 200 | 400 | 800 | 1,600 | 2,400 | 3,000 | 4,000 | 5,000 | 6,000 |
| Manufacturing parts, tools | 90 | 140 | 280 | 500 | 1,000 | 1,750 | 2,600 | 3,700 | 5,700 | 8,000 | 10,000 |
| Archiving (documents/samples) | 10 | 15 | 25 | 50 | 100 | 200 | 1,000 | 1,300 | 2,000 | 3,000 | 5,000 |
| Military | 80 | 160 | 360 | 670 | 1,350 | 2,310 | 3,000 | 4,000 | 5,400 | 6,900 | 8,400 |
| Retail CPG Pallet/case | 225 | 250 | 300 | 450 | 600 | 1,500 | 4,000 | 8,000 | 11,000 | 20,000 | 25,000 |
| Smart cards/payment key fobs | 550 | 594 | 714 | 850 | 920 | 1,036 | 1,167 | 1,281 | 1,436 | 1,860 | 2,110 |
| Smart tickets | 350 | 450 | 770 | 1,010 | 1,200 | 1,300 | 1,400 | 1,900 | 2,600 | 4,100 | 6,000 |
| Air baggage | 65 | 70 | 80 | 100 | 150 | 260 | 450 | 1,000 | 1,300 | 1,400 | 1,500 |
| Conveyances/Rollcages/ULD/Totes | 39 | 75 | 130 | 500 | 900 | 1,300 | 1,500 | 1,650 | 1,850 | 2,200 | 3,000 |
| Animals | 105 | 220 | 335 | 450 | 500 | 600 | 800 | 1,000 | 1,260 | 2,200 | 3,000 |
| Vehicles | 5 | 6 | 9 | 10 | 12 | 18 | 20 | 23 | 26 | 29 | 35 |
| People (excluding other sectors) | 2 | 3 | 4 | 5 | 7 | 8 | 10 | 15 | 20 | 30 | 40 |
| Passport page/secure documents | 75 | 95 | 110 | 120 | 130 | 150 | 180 | 220 | 300 | 400 | 500 |
| Other tag applications | 350 | 500 | 600 | 700 | 800 | 900 | 1,000 | 1,100 | 1,200 | 1,400 | 2,000 |
| **Total (million)** | **2297.2** | **3123.3** | **4617.5** | **7562.6** | **12071.7** | **24610** | **62609** | **108295** | **228497** | **429184** | **709555** |
| **Total (billion)** | **2.30** | **3.12** | **4.62** | **7.56** | **12.07** | **24.61** | **62.61** | **108.30** | **228.50** | **429.18** | **709.56** |

**Tabela 3.2** – Número (em milhões) de tags passivas por área de actividade [06]

| | 2009 | 2010 | 2011 | 2012 | 2013 | 2014 | 2015 | 2016 | 2017 | 2018 | 2019 |
|---|---|---|---|---|---|---|---|---|---|---|---|
| Drugs | 3.0 | 3.3 | 4.2 | 12.5 | 33.8 | 65.0 | 100.8 | 143.0 | 204.0 | 237.8 | 240.9 |
| Other Healthcare | 7.7 | 9.4 | 20.3 | 70.5 | 154.0 | 164.2 | 160.2 | 151.1 | 157.0 | 144.0 | 138.0 |
| Retail apparel | 24.0 | 33.0 | 36.0 | 57.4 | 113.4 | 286.4 | 412.8 | 520.6 | 390.9 | 238.4 | 148.0 |
| Consumer goods | 1.2 | 2.8 | 6.8 | 11.0 | 29.3 | 131.6 | 592.8 | 736.8 | 1106.0 | 1280.0 | 1925.0 |
| Tires | 0.4 | 0.5 | 0.9 | 1.0 | 1.5 | 4.2 | 6.5 | 9.6 | 11.0 | 15.0 | 18.0 |
| Postal | 2.5 | 7.5 | 10.0 | 28.0 | 49.0 | 60.5 | 94.0 | 185.0 | 300.0 | 450.0 | 600.0 |
| Books | 22.0 | 18.2 | 20.0 | 36.0 | 64.0 | 112.0 | 120.0 | 120.0 | 140.0 | 125.0 | 90.0 |
| Manufacturing parts, tools | 32.4 | 35.0 | 56.0 | 90.0 | 160.0 | 262.5 | 364.0 | 481.0 | 684.0 | 880.0 | 1000.0 |
| Archiving (documents/samples) | 2.6 | 3.0 | 3.8 | 5.5 | 6.0 | 10.0 | 40.0 | 19.5 | 16.0 | 15.0 | 24.0 |
| Military | 32.0 | 32.0 | 68.4 | 93.8 | 162.0 | 184.8 | 210.0 | 240.0 | 270.0 | 345.0 | 420.0 |
| Retail CPG Pallet/case | 18.0 | 17.5 | 18.0 | 24.8 | 30.0 | 75.0 | 200.0 | 400.0 | 550.0 | 1000.0 | 1250.0 |
| Smart cards/payment key fobs | 1265.0 | 1378.1 | 1492.3 | 1615.0 | 1711.2 | 1916.6 | 2077.3 | 1947.1 | 2082.2 | 2027.4 | 2131.1 |
| Smart tickets | 42.0 | 31.5 | 42.4 | 50.5 | 48.0 | 49.4 | 50.4 | 57.0 | 52.0 | 61.5 | 42.0 |
| Air baggage | 12.4 | 12.6 | 13.6 | 15.0 | 16.5 | 20.8 | 31.5 | 60.0 | 65.0 | 70.0 | 75.0 |
| Conveyances/Rollcages/ULD/Totes | 18.7 | 28.5 | 39.0 | 125.0 | 198.0 | 260.0 | 270.0 | 264.0 | 277.5 | 264.0 | 300.0 |
| Animals | 102.9 | 209.0 | 301.5 | 382.5 | 400.0 | 456.0 | 584.0 | 710.0 | 819.0 | 1320.0 | 1500.0 |
| Vehicles | 10.0 | 12.0 | 16.2 | 16.0 | 18.0 | 23.4 | 24.0 | 25.3 | 26.0 | 24.7 | 24.5 |
| People (excluding other sectors) | 2.8 | 3.9 | 5.0 | 6.0 | 7.4 | 8.0 | 8.0 | 8.3 | 8.0 | 9.0 | 8.0 |
| Passport page/secure documents | 281.3 | 351.5 | 396.0 | 408.0 | 416.0 | 450.0 | 486.0 | 506.0 | 540.0 | 620.0 | 700.0 |
| Other tag applications | 297.5 | 300.0 | 330.0 | 266.0 | 280.0 | 270.0 | 150.0 | 132.0 | 132.0 | 140.0 | 180.0 |
| **Total (million)** | 2178 | 2489 | 2880 | 3314 | 3898 | 4810 | 5982 | 6716 | 7831 | 9267 | 10815 |
| **Total (billion)** | 2.18 | 2.49 | 2.88 | 3.31 | 3.90 | 4.81 | 5.98 | 6.72 | 7.83 | 9.27 | 10.81 |

**Tabela 3.3** – Valor (em milhões de US $) de tags passivas por área de actividade [06]

**RFID Tag Revenues by market 2008**

| Tag Value ($million) | 2008 | Highlights |
|---|---|---|
| Airline and Airports | 25.9 | Excludes passports, cards |
| Animals and Farming | 90.0 | Animals |
| Books, Libraries, Archiving | 27.4 | Retail books, documents |
| Financial, Security, Safety | 1126.4 | Access control, passports |
| Healthcare and Pharmaceutical | 37.7 | Drugs, people, assets |
| Land and Sea Logistics, Postal | 38.9 | Conveyances, vehicles, postal |
| Manufacturing | 24.0 | Assets, tools etc |
| Military | 86.5 | Pallets, assets, items etc |
| Passenger Transport, Automotive | 650.7 | Card,ticket, clicker,tire |
| Retail, Consumer Goods | 86.5 | Pallet, case,apparel,cpg |
| Other | 162.6 | Research, education etc |
| **Total Tag Value ($million)** | **2357** | |
| **Total Tag Value ($billion)** | **2.36** | |

Source IDTechEx

**Tabela 3.3** – Valor das Tags em 2008 por ramo de actividade [06]

Consciente da importância deste sector, a UE lançou o projecto BRIDGE, (Building Radio-frequency Identification Solutions for the Global Environment), que teve início em Julho de 2006, com uma duração de três anos, envolveu 30 parceiros, teve um investimento de 13 milhões de euros e um co-financiamento comunitário de 7,5 milhões de euros. [07]

| $ BILLION | 2009 | 2014 | 2019 |
|---|---|---|---|
| North America | 1.45 | 5.47 | 7.88 |
| East Asia | 2.8 | 6.01 | 11.02 |
| Europe | 1.01 | 4.05 | 6.68 |
| Other | 0.3 | 0.96 | 2.01 |
| **Total** | **5.56** | **16.49** | **27.59** |

Tabela 3.4 – Valor do mercado de RFID por região [06]

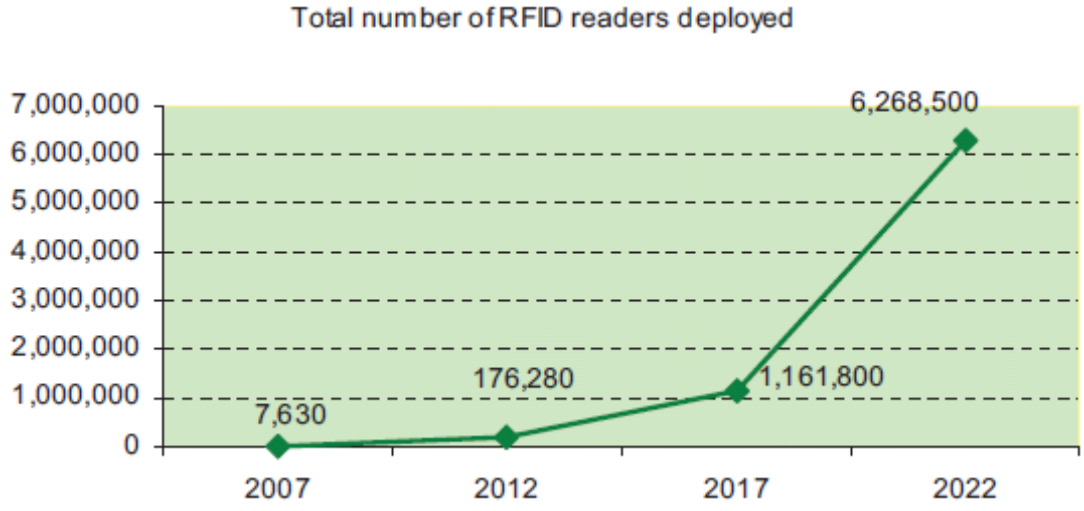


**Figura 3.1** - Número de Leitores RFID Comercializados e Previsões [08]

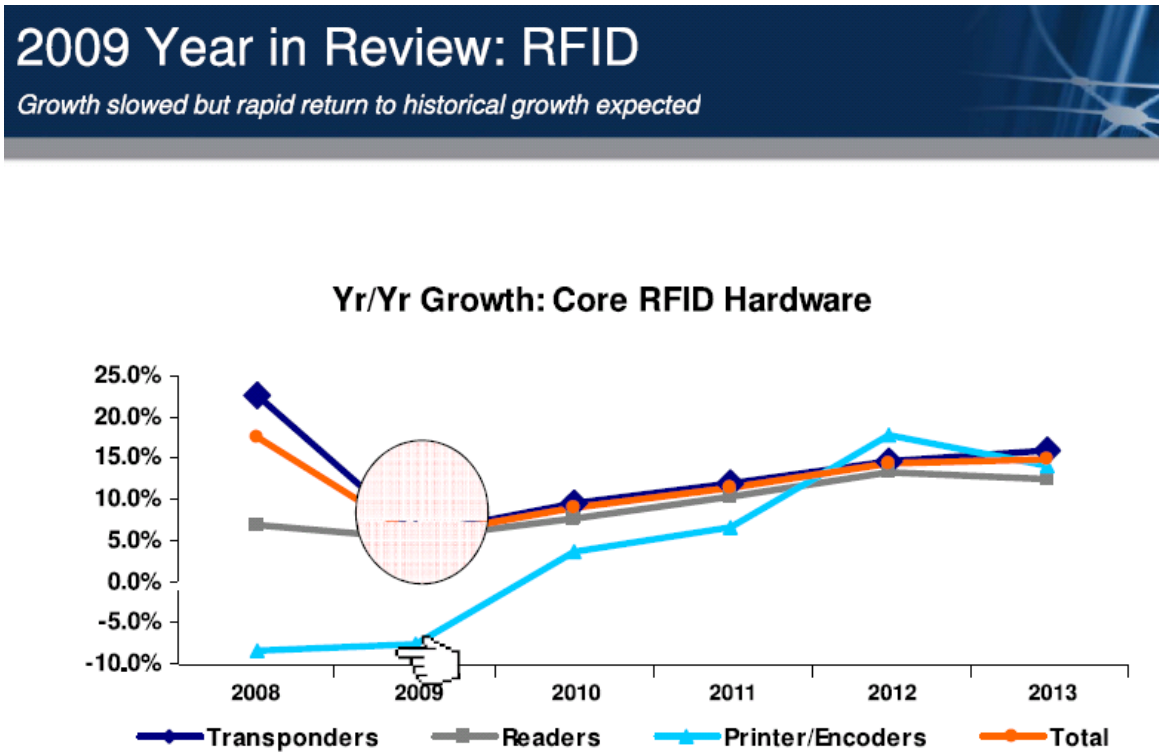


**Figura 3.2** – Perspectivas de evolução do mercado de RFID – Hardware [09]

Estas tabelas e gráficos indiciam, sem qualquer dúvida, que existe uma tendência de aceitação desta tecnologia pelo mercado, em que um crescimento anual superior a 20% é esperado para os próximos 10 anos pela generalidade dos analistas. Quanto à realidade nacional não foi possível encontrar valores fiáveis.

A análise das vendas de Printer/Encoders indica que as smart labels vão ser uma opção muito importante no tipo de tag a adoptar e uma análise dos sectores que estão predispostos a aderir a esta tecnologia fornecem indicações muito importantes sobre as áreas de maior crescimento da tecnologia RFID.

A complementaridade que as empresas pretendem adoptar entre as tecnologias de código de barras e RFID é um indicador muito importante das incertezas que hoje são apresentadas e da penetração esperada para esta tecnologia.

## 3.3 Principais Áreas de Aplicação

A chegada da tecnologia de RFID ao grande público é relativamente recente, mas ela está hoje presente em muitas áreas de actividade com uma quota de mercado que não cessa de crescer.

Apesar das enormes potencialidades desta tecnologia, a principal razão da sua adopção não deriva de uma atitude voluntária da generalidade das empresas, mas da decisão de

alguns grandes *players* do mercado que a impuseram aos seus fornecedores, como é demonstrado pelo gráfico da figura 3.3. Estão, neste caso, empresas/organizações que pelo peso específico que possuem no mercado têm um grande poder de arrasto. De entre essas empresas/organizações destacam-se:

- Wal-Mart - O anúncio foi efectuado em 2005 pelo grupo norte-americano, um dos maiores retalhistas mundiais, que deu instruções aos seus fornecedores para que usassem tags de RFID em todas as paletes, caixas e outras embalagens usadas para fornecer as respectivas mercadorias. Esta é uma fase intermédia já que o objectivo final é a identificação dos artigos no ponto de venda;
- DoD - Uma grande contribuição para a credibilidade, visibilidade e potencialidades da tecnologia RFID foi a sua adopção pelo DoD. Desde 1994 e, na sequência da Operação Tempestade no Deserto, as forças armadas dos EUA têm em funcionamento uma das maiores redes de RFID a nível mundial. O sistema RFID In-Transit Visibility (RF-ITV) proporciona um acesso imediato a informações sobre toda a sua cadeia logística, tanto de equipamentos como de abastecimentos, melhorando desta forma a segurança e a capacidade de resposta. Desde Janeiro de 2005, todos os fornecimentos entregues nos dois grandes centros logísticos, San Joaquin, California e Susquehanna, Pennsylvania, das forças armadas dos EUA, têm que ser identificados através de uma tag RFID. [10]

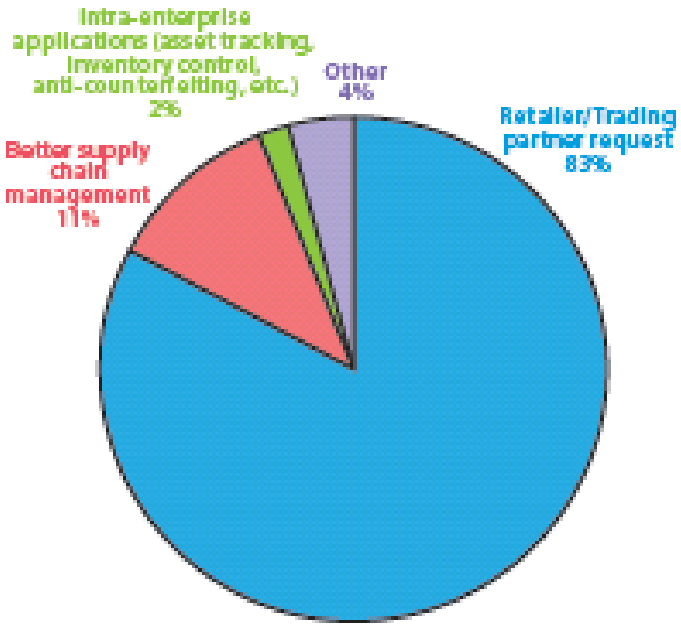


**Figura - 3.3** – Principais razões para adopção da tecnologia RFID em 2009 nos EUA [11]

Apresentamos agora algumas empresas de diferentes áreas de actividade que adoptaram soluções de RFID;

- **Aeronáutica – Airbus**: começou por usar a tecnologia para identificar ferramentas na linha de montagem e, muito recentemente, expandiu-a ao histórico das peças sujeitas a manutenção [12];
- **Vestuário – Rica Lewis**: usa uma smart label em todas as jeans que introduz no mercado para evitar a contrafacção, gerir os stocks nas lojas, obter dados sobre as vendas e poder programar a produção [13];
- **Automóvel – Iveco**: usa a tecnologia RFID para gerir e autenticar as peças sobressalentes que introduz no mercado destinadas à manutenção dos camiões que fabrica [14];
- **Química** – BASF: usa a tecnologia para localizar e controlar as condições de transporte de produtos químicos perigosos [15];
- **Alimentar** – Lavaza: usa smart labels em todas as paletes de café que introduz no mercado. A tag é usada, essencialmente, para controlo interno de stocks e a mesma informação é também fornecida em código de barras de forma a estar disponível em qualquer dos formatos a todos os intervenientes na cadeia de abastecimento [16];
- **Saúde - Mississípi Blood Service**: no banco de sangue e seus derivados do estado do Mississípi é colocada uma tag em todas as embalagens de sangue que são recolhidas dos dadores com a informação necessária para controlar os seus stocks e poder satisfazer os pedidos de mais de cinquenta hospitais de que é responsável pelo abastecimento de sangue e seus derivados e evitar erros no manuseamento [17];
- **Farmacêutica – Pfizer**: usa uma tag conjuntamente com e-pedigree para combater a contrafacção do seu produto Viagra e controlar toda a cadeia de abastecimento [18];
- **Produção – Michelin**: usa, desde 2005, uma tag embebida em muitos dos pneus que fabrica. Esta tag, além de conter toda a informação técnica sobre o pneu, pode ser actualizada nas oficinas permitindo, assim, saber a matrícula e outros dados da viatura em que foi montado e fornecer ao fabricante dados importantes sobre a vida do pneu e controlar a reciclagem do mesmo [19];
- **Desporto** – Nas grandes maratonas a nível mundial é normal que os atletas sejam controlados através de uma tag que é colocada no dorsal ou na sapatilha. A tag serve para controlar o percurso do atleta, tempos parciais e tempo final [20];
- **Agro-Pecuária** – na indústria agro-pecuária várias espécies são controladas através de uma tag RFID que regista um conjunto de dados sobre o animal e vai sendo actualizada sempre que o animal muda de proprietário, é vacinado ou sujeito a outros tratamentos veterinários. A tag acompanha o animal ao longo do seu ciclo de vida até ao abate, sendo a sua identidade confirmada em todos os con-

trolos a que é sujeito. Idêntico procedimento é adoptado em relação a animais domésticos como cães e gatos permitido a tag além do controlo sanitário identificar o seu proprietário em caso de extravio;

- **Mobiliário** – A empresa portuguesa Vicaima usa uma tag UHF EPC Class 1 Gen 2 para controlar o processo de fabrico e o stock das portas que produz. [20]


**Figura 3.4** – Jeans Rica Lewis com smart label [15]

As exigências actuais do mercado implicam que todos os intervenientes num processo tenham acesso on-line à informação necessária às respectivas actividades que são complementares podendo, deste modo, intervir sobre o processo ou activar planos alternativos caso se verifique qualquer anomalia no planeamento estabelecido.

O modelo de gestão de stocks adoptado por muitas empresas implica que um atraso não previsto em qualquer ponto da cadeia de abastecimento possa ter consequências graves para todos os intervenientes no processo, podendo mesmo levar à suspensão da laboração de algumas unidades. Esta situação mostra o valor cada vez maior que a informação tem para a sociedade em que vivemos e a necessidade de implementar mecanismos tendentes a minimizar os impactos negativos de situações imprevistas. A implementação de procedimentos de *track and trace* é já uma prática corrente em muitas empresas da cadeia de abastecimento.

## 3.4 Standards RFID

Devido à sua relativa juventude, à forma como foi introduzida no mercado e às características intrínsecas à própria tecnologia, a quantidade de standards existentes e a legislação

de cada país, geram muita confusão na adopção desta tecnologia. Podemos dividir os protocolos em três layers [21]:

- Data Link Layer – Descrevem os mecanismos de anti-colisão, inicialização, conteúdo e endereçamento das tags;
- Physical Layer – Descrevem as comunicações entre as tags e os leitores de RFID;
- Application Layer – Descrevem como os standards são aplicados nas tags que são introduzidas no mercado e as respectivas conformidades.

### 3.4.1 Air Interface Protocol – ISO/IEC 18000 [22]

A família de standards ISO/IEC 18000 define os parâmetros das comunicações leitor → tag e tag → leitor que são aplicados a cada frequência para a identificação de itens:

- ISO/IEC 18000-1 – Define genericamente a arquitectura, conceitos e parâmetros necessários para a troca de dados via interface aéreo;
- ISO/IEC 18000–2 - Define o interface aéreo para dispositivos de RFID que funcionam abaixo dos 135 KHz e pode ter dois tipos de funcionamento. No tipo A as comunicações entre leitor e tag são full duplex e funcionam a 125 KHz. No tipo B as comunicações são half duplex e podem funcionar a 125 ou 135 KHz;
- ISO/IEC 18000–3 – Define o interface aéreo para a frequência de 13,56 MHz e descreve dois modos de funcionamento que não interferem nem são intermutáveis. No modo 1 existe a possibilidade de bloquear permanentemente a memória da tag sem que o comando de lock seja protegido por *password*. No modo 2 a execução do comando lock é protegida por *password*;
- ISO/IEC 18000–4 – Define o interface aéreo para a frequências de 2,45 GHz e descreve dois modos de funcionamento. O modo 1 descreve o funcionamento ITF (Interrogator Talks First) para tags passivas. O modo 2 descreve o funcionamento TTF (Tag Talks First) para tags activas;
- ISO/IEC 18000–5 – Este standard definia o interface aéreo para a frequência de 5,8 GHz mas foi descontinuado;
- ISO/IEC 18000–6 – Define o interface aéreo usado na banda UHF entre os 860 e os 960 MHz. Descreve três modos de funcionamento e respectivos procedimentos anti-colisão usados para a singularização das tags. O modo C é a aprovação pelo ISO da especificação EPCglobal Gen 2 e descreve o algoritmo Probabilistic Slotted Aloha para singularização das tags. O modo A descreve o algoritmo Framed Slotted ALOHA para singularização das tags. O modo B descreve o algoritmo Deterministic Binary Tree para singularização das tags;
- ISO/IEC 18000-7 – Este interface descreve o interface aéreo para a frequência de 433 MHz.

### 3.4.2 Outros standars RFID [22]

Além da família de standards ISSO/IEC 18000 outros standards são aplicados em RFID:

- ISO 14443 – Proximity cards que usam a frequência de 13,56 MHz e têm um alcance muito pequeno (alguns cm) e são usados pelo sistema financeiro para os seus cartões;
- ISO 15693 – Contact less cards ou Vicinity cards que usam a frequência de 13,56 MHz e têm um alcance inferior a um metro;
- ISO 11748/11785 usados para identificação animal;
- ISO 18185 descreve as características das tags que servem de selo para controlo e localização electrónica dos contentores usados na cadeia de abastecimento. Qualquer violação do selo deve ser guardada e transmitida;
- ISO/IEC 18046 descreve o desempenho que os leitores e tags devem apresentar e os testes a efectuar para medir esse desempenho;
- ISO/IEC 18047 descreve a conformidade para uma frequência específica;
- ISO/IEC 24769 e 24770 descrevem os testes de conformidade para dispositivos RTLS;
- ISO 28560 define as especificações de um sistema de RFID para o sector livreiro;
- ISO/IEC 15961 descreve os comandos, respostas e dados da aplicação usados no processo de comunicação entre leitor e tag;
- ISO/IEC 15962 descreve o processo de codificação e descodificação dos dados gravados na tag.

Da enumeração de alguns dos standards existentes para RFID conclui-se que existe um grande dinamismo, mas a proliferação de standards sectoriais e posturas nacionais são um entrave a uma verdadeira aceitação global desta tecnologia.

## 3.5 Componentes de um Sistema de RFID

Os principais componentes de um sistema RFID são: tags RFID, leitores RFID, antenas e Enterprise Subsystem, que estão representados na Figura 3.5.

**Tag RFID (Transponder)** – Dispositivo de identificação constituído por um chip e uma antena que é aplicado num 'objecto' e usa um sinal de rádio frequência (RF) para comunicar.

**Leitor RFID (transceiver)** – Dispositivo utilizado para comunicar com a tag, fornecer informação à tag, recuperar a informação armazenada na tag e estabelecer comunicações com o middleware do enterprise subsystem.

**Enterprise Subsystem** – Interliga os diversos componentes do sistema de gestão da informação da empresa, recebe a informação que vai ser processada e disponibilizada aos respectivos processos/utilizadores.

**O Middleware** é responsável pelo interface entre o sistema específico de RFID composto por, leitores, tags e respectiva infra-estrutura de comunicações e o sistema de gestão da empresa. É ele que incorpora o software que permite o registo das comunicações entre tag e leitor, solicita as informações necessárias à base de dados e fornece essas informações ao leitor para que ele possa dialogar com a tag, recebe as informações do leitor que deve guardar e actualiza as bases de dados mantendo o sincronismo entre todos os intervenientes no processo.

**O Analytic Systems** é responsável pela salvaguarda da informação que lhe é fornecida pelo Midlware, processar essa informação e disponibilizá-la aos diversos utilizadores que dela necessitam. É também o responsável por fornecer ao middleware a informação necessária à comunicação entre leitor e tag.

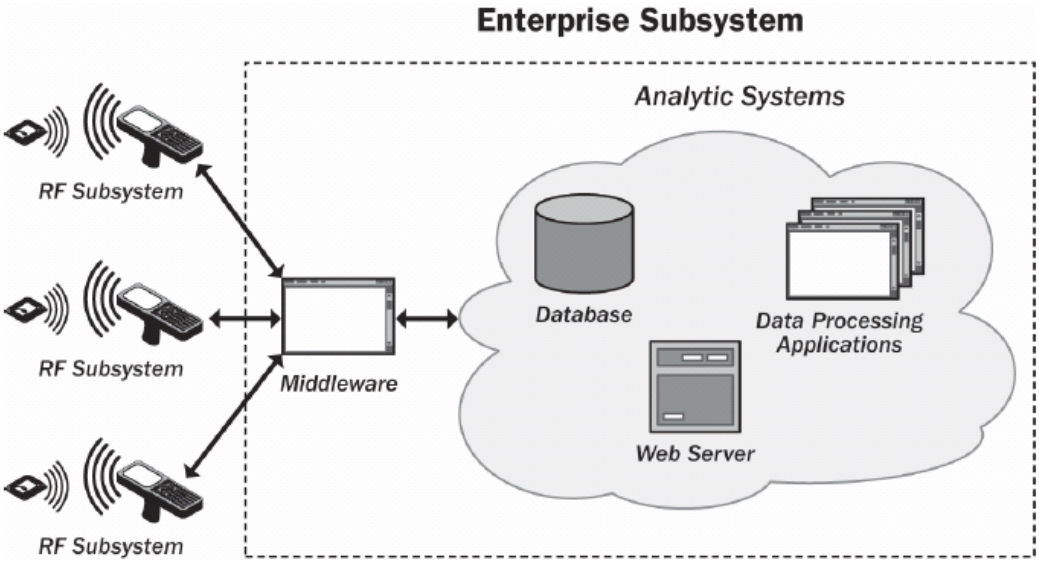


**Figura 3.5** - Componentes de um sistema de RFID **[22]**

## 3.6 Leitores de RFID

Os leitores de RFID servem para obter a informação contida na tag ou alterar essa informação. A informação obtida da tag é enviada ao middleware para ser processada. A informação recebida do middleware serve para terminar/continuar o processo de inquérito à tag ou gravar informação na tag.

Para que o leitor e a tag possam comunicar devem suportar o mesmo protocolo de comunicações.

Existem três tipos de leitores quanto à mobilidade:

- Fixos – Normalmente montados nos cais de carga/descarga, pórticos e outras estruturas fixas;
- Móveis – Normalmente montados em equipamentos usados no transporte das mercadorias como porta-paletes e empilhadores;
- Handheld – Utilizados pelos operadores que fazem a leitura de tags e se deslocam de uma forma mais ou menos aleatória ou são utilizados em situações de falha dos outros leitores.

De entre as características que um leitor deve possuir destacam-se:

- Uso de vários métodos de modulação tanto na emissão como na recepção sem qualquer alteração ao hardware;
- Possibilidade de alterar/actualizar as funcionalidades do leitor por actualização do respectivo software;
- Possibilidade de seleccionar a frequência e modo de funcionamento mais adequados às condições de trabalho;
- Capacidade de detectar e evitar interferências provocadas por leitores ou outros equipamentos de comunicações a operar no mesmo meio ambiente;
- Flexibilidade na selecção e gestão da frequência de funcionamento;
- Em situações de colisão com outros leitores deve diminuir de uma forma automática a sua potência de emissão de um determinado factor para evitar a ocorrência de colisões.

No processo de diálogo entre leitores e tags três situações problemáticas podem ocorrer:

- Interferência entre leitores impedindo que uma tag seja identificada;
- A resposta simultânea de várias tags a um leitor impedindo a identificação da tag;
- A identificação simultânea de uma tag por vários leitores.

### 3.6.1 Interferência entre Leitores

A existência de vários leitores no mesmo ambiente e a capacidade de mobilidade de alguns tipos de leitores podem provocar interferência entre os leitores de uma rede, pelo que é necessário coordenar as respectivas comunicações de forma a evitar interferências mútuas.

Existem diversos procedimentos para tentar resolver este problema e a maior parte é implementada por software, o que permite o uso de diversos standards no mesmo equipamento, interoperabilidade e facilidade de actualização.

A generalidade das soluções baseiam-se em mecanismos standard de multiplexagem e os fabricantes de leitores implementam as soluções que consideram mais vantajosas.

As soluções mais utilizadas são:

- FDMA – Frequency Division Multiple Access – A largura de banda é dividida em vários canais e o leitor altera de canal em intervalos de tempo fixos;

- TDMA – Time Divison Multiple Access – Um espaço temporal é dividido em vários intervalos e cada leitor usa um desses intervalos para transmitir;
- CSMA – Carrier Sense Multiple Access – O canal é escutado antes da transmissão. Se o canal estiver livre é efectuada a transmissão, se o canal estiver ocupado será novamente escutado após um certo intervalo de tempo.

Os leitores, num determinado espaço, por exemplo um armazém, podem estar interligados através de um controlador central, geridos em conjunto e executar os mesmos comandos simultaneamente. Podem, assim, ser postos em escuta e terminar o estado de escuta ao mesmo tempo. A gestão centralizada permite também atribuir dinamicamente canais aos leitores optimizando, desta forma, o uso da banda de frequências disponível e minimizando as colisões.

O raio de acção normal de um leitor é de cerca de 10 m, no entanto, a generalidade das aplicações não necessitam desta distância de leitura. Um cais de carga/descarga tem normalmente 3 m de largura pelo que se diminuirmos a potência de emissão diminuímos o seu raio de acção e as probabilidades de interferências entre os leitores diminuem.

### 3.6.2 Singularização das Tags

No raio de acção de um leitor podem coexistir várias tags e, quando um leitor efectua um inventário, se várias tags respondem ao leitor ocorrem colisões. Os leitores implementam algoritmos para individualizar as tags e alguns standards indicam mesmo o protocolo anti-colisão a adoptar. Existem dois protocolos em que se baseiam a generalidade das implementações: Aloha e Árvore Binária.

#### 3.6.2.1 Baseados em Aloha [24]

O protocolo Aloha foi desenvolvido na década de 70, na Universidade do Havai, para redes rádio e tem como princípio a transmissão da informação por uma estação sempre que tem algo para enviar. Sempre que é detectada uma colisão, a estação retransmite a informação após esperar durante um período de tempo aleatório.

Devido ao elevado número de colisões registadas na rede foram aparecendo outros protocolos baseados no Aloha, com o objectivo de aumentar a sua eficiência:

- Slotted Aloha;
- Framed Slotted Aloha;
- Dynamic Framed Slotted Aloha;
- Enhanced Dynamic Framed Sloted Aloha.

No protocolo Framed Slotted Aloha o tempo é dividido em frames e cada frame em slots. No início de cada frame o leitor pede a identificação das tags e indica o número de slots disponíveis para resposta das tags. Cada tag selecciona aleatoriamente um slot e responde nesse

slot. Se mais que uma tag responde no mesmo slot ocorre uma colisão e as tags não podem ser identificadas e têm que seleccionar um novo slot no frame seguinte e voltar a responder. Nos slots em que responde apenas uma tag essa tag é identificada. As tags já identificadas não respondem nas frames seguintes. O processo repete-se até que todas as tags sejam identificadas.

O desconhecimento da população de tags a identificar e a morosidade do processo representam uma grande limitação à performance deste protocolo, pelo que várias alterações têm sido introduzidas para aumentar a velocidade de leitura, já que na presença de um grande número de tags algumas podem não ser identificadas e esta situação pode ter consequências graves.

Há leitores que permitem parametrizar o número de slots a usar, número máximo, mínimo e médio de tags no raio de acção do leitor e outros parâmetros de forma a optimizar o ciclo de identificação das tags permitindo, assim, que a velocidade de identificação aumente e que um maior número de tags possam ser identificadas.

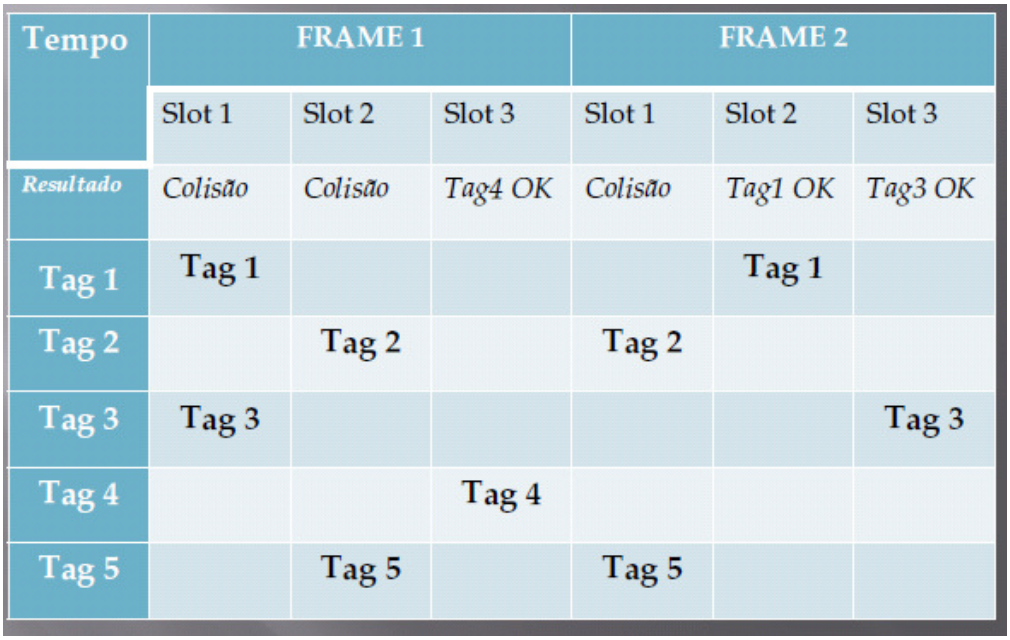


**Figura 3.6** - Framed Slotted Aloha [25]

### 3.6.2.2 Baseados em Árvore Binária [24]

Nos protocolos baseados neste algoritmo o leitor interroga iterativamente um subgrupo de tags que possuem uma determinada característica até que todas as tags sejam identificadas.

**Binary Tree Algorithm** – O leitor escolhe o valor inicial '0' ou '1' e envia o prefixo seleccionado às tags. Só as tags cuja identificação possui um prefixo igual ao prefixo enviado pelo leitor respondem enviando para o leitor o bit seguinte da sua identificação.

Se ocorrer uma colisão, um novo prefixo é construído por adição de '0' ou '1' ao prefixo anterior e reenviado às tags. Se não ocorrer colisão o bit enviado pelas tags é adicionado ao prefixo e reenviado às tags. Se não existir resposta o ramo é ignorado.

O processo repete-se até que todos os ramos sejam pesquisados e as respectivas tags identificadas. A unicidade das tags permite a sua identificação.

**Query Tree Algorithm** – Neste algoritmo, como resposta ao envio de um prefixo de tamanho K pelo leitor, as tags respondem com os elementos da sua identificação a partir do elemento K+1 até ao fim. Se ocorrer uma colisão um novo prefixo é criado adicionando '0' ou '1' ao prefixo actual e retransmitido para as tags. Se não existir colisão a identificação da tag é obtida pela concatenação do prefixo com o bloco enviado pela tag.

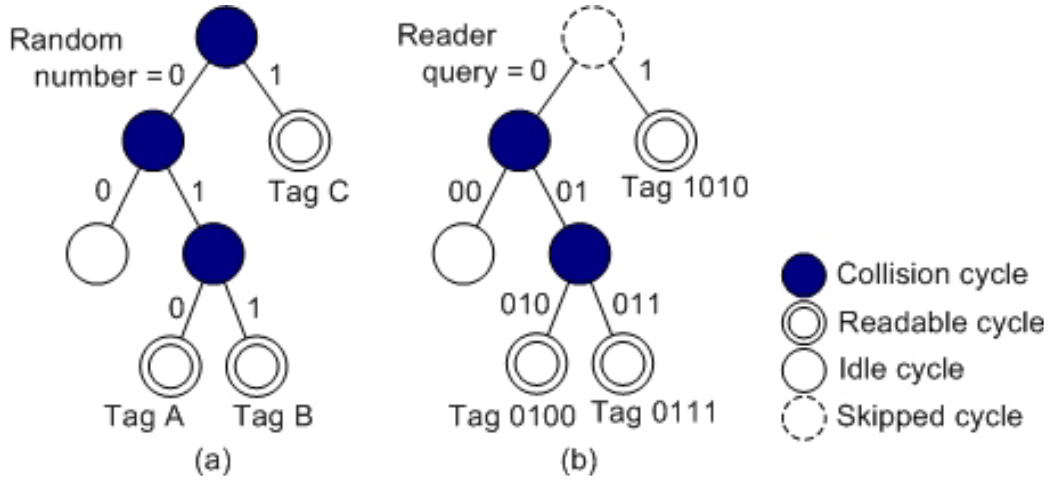


**Figura 3.7** – Identificação de tags. (a) Binary Tree. (b) Query Tree [26]

### 3.6.3 Identificação Simultânea de uma Tag por Vários Leitores

A ocorrência desta situação é facilmente resolúvel através do software do middleware, do controlador ou na actualização da base de dados analisando a sequência lógica das operações e a data/hora das ocorrências. Este procedimento de filtragem/validação de ocorrências deve ser sempre usado para detectar possíveis duplicações.

## 3.7 Middleware

O middleware é um elemento chave de qualquer implementação de RFID e de entre as características que deve possuir destacamos:

- **Filtragem e agregação de dados** – Uma das características comuns a todas as aplicações que usam informação capturada automaticamente é a necessidade de receberem os dados resultantes dos eventos devidamente filtrados e agregados. Cada aplicação apresenta as suas especificidades próprias quanto ao conjunto de dados a processar pelo que só os dados necessários lhe devem ser passados;

- **Distribuição de dados** – Os dados capturados pelos leitores, sensores e outros intervenientes no processo interessam normalmente a mais que uma aplicação, quer internamente à organização, quer aos seus parceiros comerciais. Esta informação deve ser enviada aos respectivos interessados no formato apropriado e dentro do intervalo de tempo útil. Existem aplicações que têm necessidade da informação on-line e outras cuja necessidade pode ser diferida. Com esta diferenciação podemos diminuir a carga dos sistemas;
- **Leitura e gravação** – A existência de tags que possuem memória adicional implica que o middleware deve disponibilizar os procedimentos para leitura e gravação na memória adicional das tags;
- **Gestão dos leitores e impressoras/codificadoras** – O elevado número de leitores e impressoras/codificadoras e os diferentes tipos, modelos e respectivos fabricantes, que existem em muitas organizações, implica a sua integração na infra-estrutura e a necessidade da implementação de processos de gestão de incidentes, instalação, configuração, actualização e controlo;
- **Segurança** – As tags são uma fonte de informação pelo que essa porta de entrada deve ser devidamente protegida e a informação por elas fornecida devidamente filtrada para evitar possíveis ataques ao sistema;
- **Performance e Escalabilidade** – Estas características do middleware devem ser também analisadas tendo em conta as necessidades actuais da organização, as necessidades previsíveis a curto e médio prazo e as evoluções esperadas para a tecnologia.

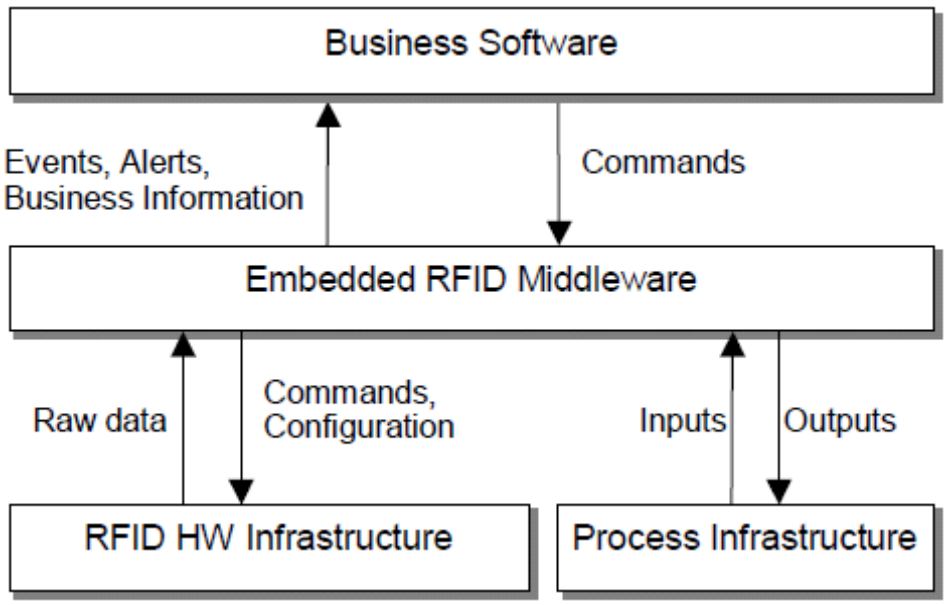


**Figura 3.8** – Principais componentes de software num sistema de RFID [27]

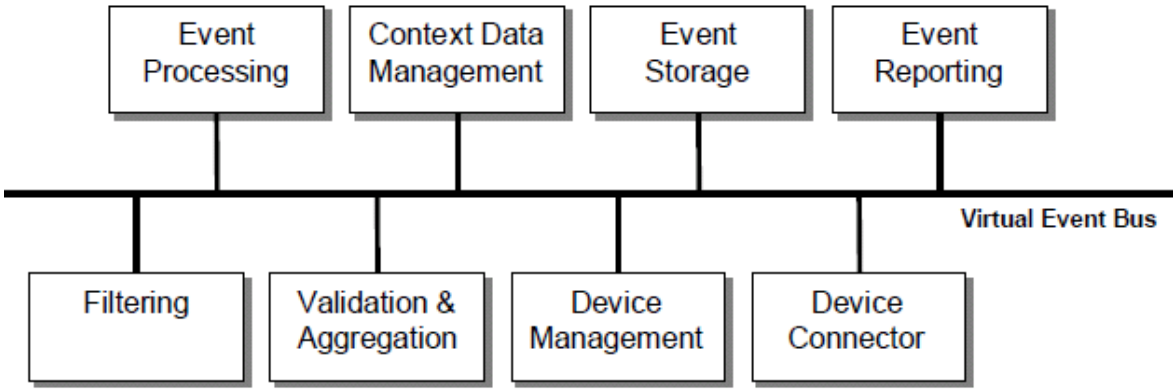


**Figura 3.9** – Funções do Middleware [27]

# Capítulo 4

# Tags RFID

**Tag RFID (Transponder)** – Dispositivo constituído por um chip e uma antena que é aplicado a um 'objecto', usa um sinal de rádio frequência (RF) para comunicar e permite identificar univocamente o 'objecto' em que está aplicada.

As capacidades de memória e computacional que uma tag possui são muito variadas e estão dependentes do tipo e modelo da tag.

## 4.1 Classificação das Tags função do tipo de Alimentação

As tags são normalmente divididas em quatro tipos função da fonte de alimentação que usam: passivas, activas, semi-activas e semi-passivas. **[22]**

**Tags Passivas** – Não possuem fonte de alimentação própria. Obtêm a energia que necessitam para o seu funcionamento do sinal emitido pelo leitor. São as mais baratas e as mais usadas, possuem um tempo de vida muito grande, mas memória e capacidade computacional muito limitadas.

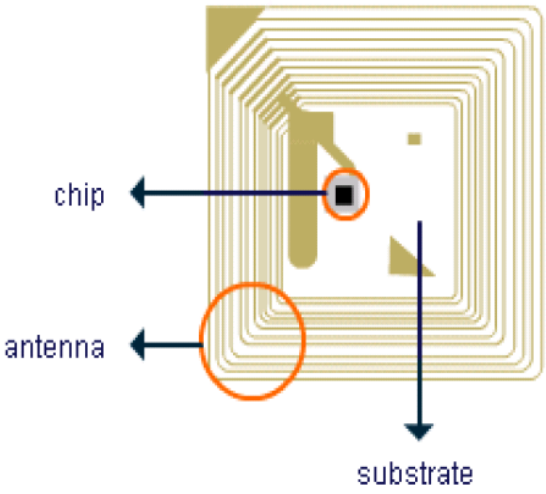


**Figura 4.1** - Componentes de uma Tag Passiva [28]

**Tags Activas** – Possuem uma fonte interna de alimentação (bateria) que alimenta as comunicações com o leitor, os circuitos integrados que a compõem e possibilita um aumento da distância de leitura. Podem iniciar uma sessão de comunicação com o leitor de RFID ou com outras tags formando desta forma uma rede. São as mais caras e apresentam um tempo de vida limitado imposto pela duração da bateria (cerca de 3 anos). A existência de uma fonte de alimentação própria permite alimentar circuitos mais complexos e dotar as tags activas de capacidades de memória e computacional que não podem ser implementadas numa tag passiva. Estas tags podem incorporar sensores que registam a evolução de determinadas variáveis e são utilizadas para conhecer a evolução de variáveis como temperatura, pressão ou humidade a que o 'objecto' em que estão aplicadas está sujeito. Este tipo de tag é muito utilizada em contentores e quando interligada a um sistema de GPS (Global Position System) permite um efectivo acompanhamento das mercadorias em trânsito (RTLS -Real Time Location System).

**Tags Semi-activas** – São tags activas que se encontram sem actividade até serem activadas pelo leitor. Uma vez activadas entram num modo de funcionamento idêntico ao das tags activas. Este modo de funcionamento tem a vantagem de prolongar o tempo de vida da bateria (cerca de 5 anos). Para serem activadas precisam de estar dentro do raio de acção do leitor e o atraso provocado pelo processo de activação pode fazer com que a tag não seja lida em processos em que a tag passa pelo leitor a uma velocidade elevada ou em que existe um número muito elevado de tags para serem lidas num curto espaço de tempo.

**Tags Semi-passivas** – São tags passivas que possuem uma fonte interna de alimentação (bateria) e podem possuir sensores. A comunicação com o leitor é idêntica ao das tags passivas. A fonte de alimentação permite alimentar circuitos mais complexos e com maiores funcionalidades e também alimentar os sensores que são utilizados para monitorizar a evolução de determinada variável numa mercadoria. A leitura do valor da variável deve ser feita a determinados intervalos para que o histórico da sua evolução possa ser efectuado e a existência de uma fonte de alimentação própria garante que a tag possa efectuar essas leituras independentemente da existência de um leitor para a alimentar. Este modo de funcionamento permite, também, aumentar o raio de acção já que toda a energia absorvida é destinada a alimentar apenas a comunicação com o leitor, sendo a parte electrónica alimentada pela bateria. O tempo de vida da bateria é superior a 5 anos.

## 4.2 Classificação EPCglobal das Tags

Neste tipo de classificação cada classe implementa todas as características da classe anterior e expande-as. Define também uma classe 5 de tags activas que não são verdadeiras

tags mas dispositivos que podem criar uma rede sem fios entre eles e comunicar com outros tipos de dispositivos.

**Tags Classe-1** – Tags de identificação.

São tags passivas do tipo WORM (Write-Once, Read-Many) com as seguintes características mínimas:

- Um identificador EPC (Electronic Product Code);
- Um identificador da Tag (TID);
- Uma função que permite colocar a tag permanentemente num estado em que não responde.

Podem possuir ainda as seguintes características opcionais:

- Uma função que altera o estado da tag entre activada e desactivada;
- Uma *password* de controlo de acesso;
- Memória do utilizador.

**Tags Classe-2** - Tags de elevada funcionalidade.

São tags passivas do tipo regravável que possuem, para além de todas as características definidas para a classe-1, as seguintes características adicionais:

- Identificador de tag adicional;
- Memória do utilizador adicional;
- Autenticação do controlo de acesso;
- Características adicionais a definir.

**Tags Classe-3** – Tags semi-passivas.

São tags passivas no seu modo de comunicação com os leitores, mas que possuem uma bateria que alimenta os circuitos electrónicos da tag e possíveis sensores nela incorporados. As tags da classe-3 precisam que o leitor inicie a comunicação e enviam informação para o leitor em modo backscatter.

**Tags Classe-4** – Tags activas.

São tags que possuem bateria e emissor próprios, o que lhes permite iniciar a comunicação com o leitor, com outras tags ou outros dispositivos. As comunicações das tags da Classe-4 não podem interferir com as comunicações das tags das classes 1, 2 e 3.

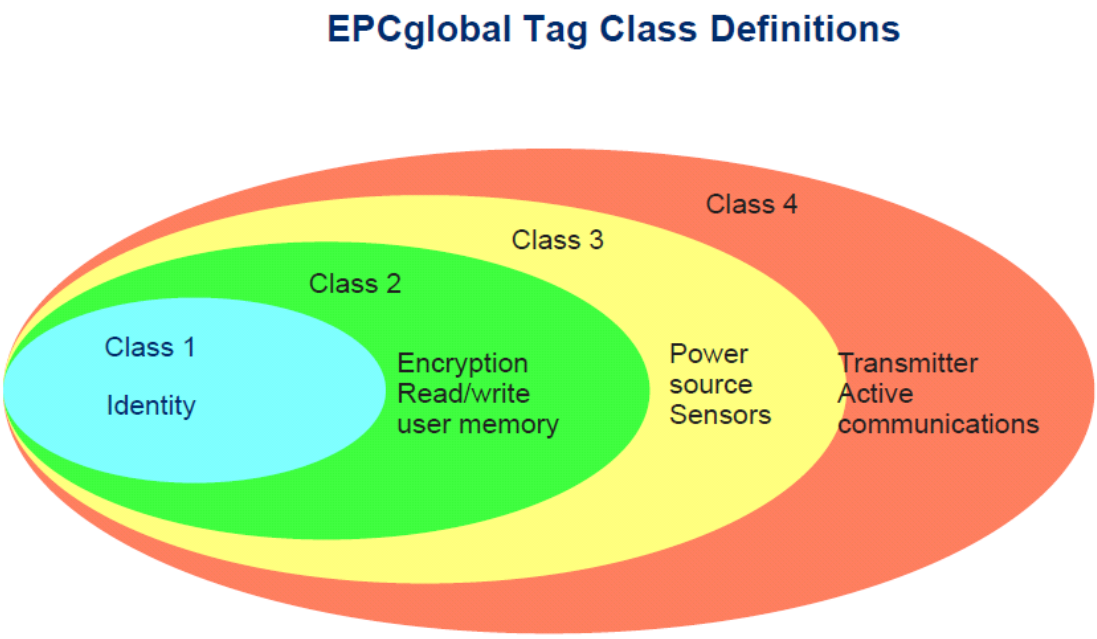


**Figura 4.2** – Classificação das tags segundo o standard EPCglobal [29]

## 4.3 Frequências de Funcionamento

Os sistemas de RFID funcionam em gamas de frequências não licenciadas, conhecidas como ISM, (Industrial, Scientific and Medical), mas as frequências atribuídas ao ISM variam de acordo com a legislação de cada país, que define as frequências e potências que podem ser utilizadas.

A frequência em que a tag recebe e envia informação tem influência em:

- **Performance** da tag relativamente à velocidade de transferência de dados e raio de operação. Geralmente, quando aumenta a frequência de funcionamento da tag aumenta a velocidade de transferência de dados, o que permite a leitura de um maior número de tags no mesmo intervalo de tempo. O aumento do raio de funcionamento é visto como uma vantagem para a generalidade das aplicações, mas levanta problemas de segurança e privacidade já que permite uma leitura rápida e a longa distância da informação contida na tag por um leitor não autorizado;
- **Penetração** – Geralmente, quanto maior é a frequência menor é a capacidade do sinal atravessar certos meios como água ou metal. Dependendo da aplicação desejada a frequência correcta deve ser seleccionada. Para identificação animal (objecto maioritariamente líquido) é usada a baixa frequência. A tabela 4.1 apresenta o impacto de vários materiais na propagação do sinal nas várias frequências de funcionamento das tags;

- **Interferência -** É uma das causas de erro na transmissão. Determinar as potenciais fontes de interferência deve ser objecto de um *site survey* para cada implementação de um projecto de RFID. A tabela 4.2 apresenta algumas das fontes de interferência mais comuns;
- **Portabilidade** – A legislação que regula o espectro electromagnético pode diferir entre países, já que nem todos os reguladores atribuem as mesmas frequências para os mesmos fins, o que levanta problemas de portabilidade. Quando uma tag tem que ser lida em várias regiões deve ser seleccionada uma frequência permitida em todas elas. Algumas tags podem responder a uma gama alargada de frequências o que lhes permite serem lidas em países com diferentes legislações. Estão, nesta situação, as tags que cumprem o standard EPCglobal Class1 Gen 2 e que operam na banda UHF desde 860 até 960 Mhz. Nos Estados Unidos da América a legislação permite o funcionamento entre 902 e 928 Mhz, enquanto na Europa a gama normal de funcionamento é de 865,6 a 867,6 Mhz. Alguns leitores permitem seleccionar a gama de funcionamento, mas a tag responde a qualquer uma delas, o que permite a compatibilidade entre as duas regiões. A tabela 4.3 apresenta um resumo das frequências usadas em RFID e respectivas características.

Tabela 4.1 – Impacto de alguns materiais na propagação do sinal de RF [22]

| Material | LF<br>30-300 kilohertz (kHz) | HF<br>3-30 MHz | UHF<br>300 MHz-1 GHz | Microwave<br>> 1 GHz |
|---|---|---|---|---|
| | 125 or 134 kHz (common US RFID usage) | 13.56 MHz[11] (Worldwide ISM band) | 433.5-434.5 915 MHz[12] (common US RFID usage) | 2.45 GHz[13] (Worldwide ISM band) |
| Clothing | Transparent | Transparent | Transparent | Transparent |
| Dry Wood | Transparent | Transparent | Transparent | Absorbent |
| Graphite | Transparent | Transparent | Opaque | Opaque |
| Metals | Transparent | Transparent | Opaque | Opaque |
| Motor Oil | Transparent | Transparent | Transparent | Transparent |
| Paper Products | Transparent | Transparent | Transparent | Transparent |
| Plastics | Transparent | Transparent | Transparent | Transparent |
| Water | Transparent | Transparent | Absorbent | Absorbent |
| Wet Wood | Transparent | Transparent | Absorbent | Absorbent |

Tabela 4.2 – Fontes frequentes de interferência [22]

| Frequency Range | RFID Applications | Possible Interference Sources in US |
|---|---|---|
| Less than 500 kHz | Access control, animal tagging, automobile immobilizers, EAS systems, inventory control, and track and traceability applications | Maritime radio and radio navigation applications |
| 1.95 MHz - 8.2 MHz | EAS systems | Aeronautical radio, amateur, land mobile, maritime mobile radios, and radio location applications |
| 13.553 - 13.567 MHz | Access control, item-level tagging, EAS systems, and smart card applications | ISM applications and private land mobile radio |
| 433.5 - 434.5 MHz | In-transit visibility and supply chain applications | Amateur radio and radio location applications |
| 902 - 928 MHz | Railcar, supply chain, and toll road applications | ISM applications including cordless phones and radio location |
| 2.40 - 2.50 GHz | Real-time location systems (RTLS), and supply chain applications | ISM applications including Bluetooth, cordless phones, and Wi-Fi as well as radio location, and satellite technologies |

Tabela 4.3 – Frequências usadas em RFID e respectivas características

| Banda | LF<br>Low Frequency | HF<br>High Frequency | UHF<br>Ultra High Frequency | Microondas |
|---|---|---|---|---|
| Frequência Usada em RFID | 125 ou 135 KHz | 13,56 MHz | 433 MHz<br>ou<br>860 a 960 MHz | 2,45 ou 5,8 GHz |
| Alcance Aproximado | Inferior a 0,5 metros | Até 1,5 metros | Até 100 metros | Até 30 metros |
| Velocidade de Transferência | Inferior a 1Kbit/s | Aproximadamente 25 Kbit/s | Aproximadamente 30 Kbit/s | Até 1 Mbit/s |
| Áreas de Aplicação | Animal ID<br>Controlo de Acesso<br>Imobilização de Veículos | Bagagem Aérea<br>Smart Cards<br>Livrarias<br>Bibliotecas<br>Controlo de Acesso<br>Item ID | Item ID<br>Logística<br>Supply Chain<br>Controlo de Armazéns | Identificação de Veículos em Movimento<br>Portagens Automáticas |

## 4.4 Origem da Energia das Tags

Uma tag necessita de energia para processar os comandos recebidos do leitor e para enviar a resposta ao leitor. Pode possuir a sua própria fonte de alimentação (tag activa) ou obter a energia de uma fonte externa (tag passiva).

As tags activas possuem uma fonte interna de alimentação, um emissor e um receptor independentes, o que lhes permite um funcionamento autónomo.

As tags passivas obtêm a energia de que necessitam do sinal que recebem do leitor e podem funcionar de duas formas: acoplamento indutivo e backscatter.

**Acoplamento Indutivo** – As tags passivas que funcionam nas bandas LF (Low Frequency) e HF (High Frequency) obtêm essa energia do sinal emitido pelo leitor através de um processo de indução magnética. O sistema indutivo é baseado num transformador do tipo acoplamento indutivo entre a bobina do leitor (primário) e a bobina da tag (secundário). Este acoplamento só se verifica se a distância entre as bobinas não exceder 0,16 λ.

Em RFID as frequências típicas nestas bandas são 125, 135 KHz (LF) e 13,56 MHz (HF). O comprimento de onda (λ) é dado pela fórmula $\lambda = {}^{c}/_{f}$. Para estas bandas de frequências os comprimentos de onda são de aproximadamente 2400 m e 22 m respectivamente. Como o comprimento de onda é várias vezes maior que a distância entre a antena do leitor e a tag, o campo electromagnético pode ser tratado como um campo magnético alternado. Se a tag está localizada dentro do campo magnético alternado gerado na antena do leitor uma parte deste campo magnético alcança a antena da tag e é gerada uma tensão por indução. Esta tensão é rectificada e vai servir de fonte de alimentação para os circuitos electrónicos da tag.[30]

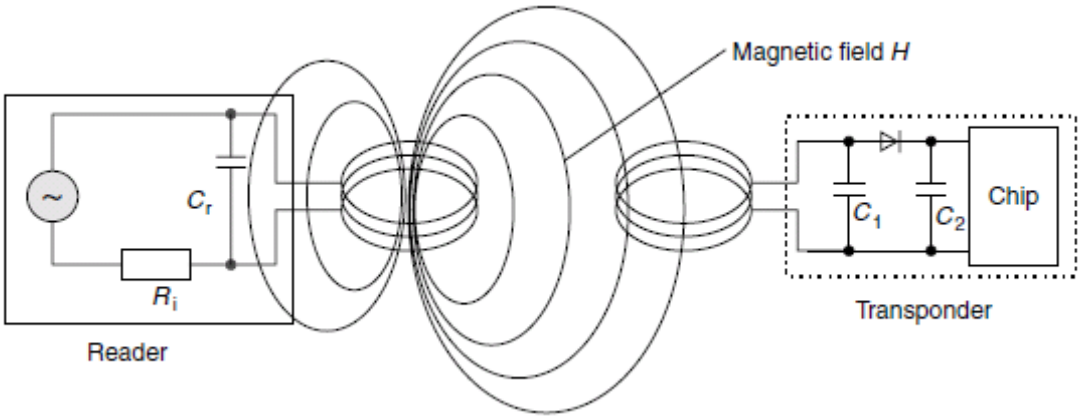


**Figura 4.3** – Acoplamento Indutivo [30]

**Backscatter** – As tags passivas que funcionam nas bandas UHF (Ultra High Frequency) 860 a 960 MHz e Microondas 2,45 e 5,8 GHz usam a capacidade de reflexão das ondas rádio por um corpo para comunicar com o leitor. A tag possui uma antena que é usada para obter energia do sinal emitido pelo leitor e para enviar informação ao leitor. A quantidade de energia que a tag recebe depende de muitos factores, mas a distância entre o leitor e a tag, a potência de emissão do leitor e eficiência da antena da tag são os principais. As impedâncias da antena e dos circuitos electrónicos da tag determinam a quantidade de energia que é transmitida da antena para a alimentação da tag. Quando as impedâncias são iguais é transferido o

máximo de energia possível. Isso acontece quando as partes imaginárias das respectivas impedâncias se anulam mutuamente. Quando a equivalência não é exacta, uma reactância está presente na impedância podendo ser indutiva ou capacitiva, o que faz com que a energia transferida seja menor provocando uma diminuição da distância de leitura da tag. A tag pode alterar esta equivalência adicionando ou removendo reactância normalmente com a inclusão de um condensador no circuito através de um interruptor. Quando o condensador é introduzido no circuito a equivalência não é exacta e a tag reflecte uma quantidade de energia. Quando o condensador é retirado do circuito a equivalência de impedâncias é exacta e uma outra quantidade de energia é reflectida. Usando esta diferença a tag pode modular a informação na onda reflectida e, desta forma, comunicar com o leitor.

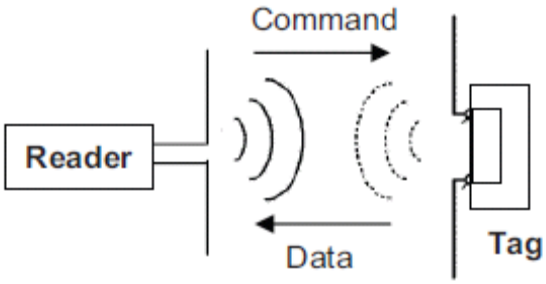


**Figura 4.4** – Backscatter [31]

## 4.5 Smart Labels

Smart labels são etiquetas que incorporam um RFID *inlay* (combinação de chip, antena e substrato), uma cobertura do inlay que vai ser impressa, uma base sobre a qual o inlay é aplicado e o material adesivo que cola o inlay tanto à cobertura como à base.

No processo de impressão/codificação são gravados no chip do inlay os dados desejados e impressos na cobertura o(s) código(s) de barras e restante informação. A cobertura e a base devem proteger devidamente o *inlay*.

O processo de codificação requer grande precisão pelo que a escolha da smart label a usar deve ter em conta as especificações da impressora/codificadora em que vai ser usada. Devido à complexidade do processo as impressoras de smart tags devem efectuar dois testes:

- Antes da gravação o inlay é testado para garantir que se encontra funcional e pode receber dados;
- Após a gravação é testada a informação contida no inlay para garantir que é legível e confirmar que a informação foi correctamente gravada.

O uso de smart labels apresenta grandes vantagens para a cadeia de abastecimento actualmente usada, já que permite a coexistência das duas tecnologias e uma migração tran-

quila entre as tecnologias de código de barras e de RFID. Esta solução que está a ser adoptada por muitas empresas permite implementar uma solução de RFID de uma forma gradual e perfeitamente controlada, sendo as novas funcionalidades implementadas e testadas sem afectar o normal funcionamento da organização. Qualquer erro detectado na implementação do sistema de RFID não afecta o normal funcionamento da empresa que é garantido pelo sistema de código de barras.

Esta solução tem como inconvenientes a duplicação de algumas tarefas, a coexistência de duas tecnologias que são concorrentes/complementares em muitas áreas, o que nem sempre é pacífico, e um aumento dos custos.

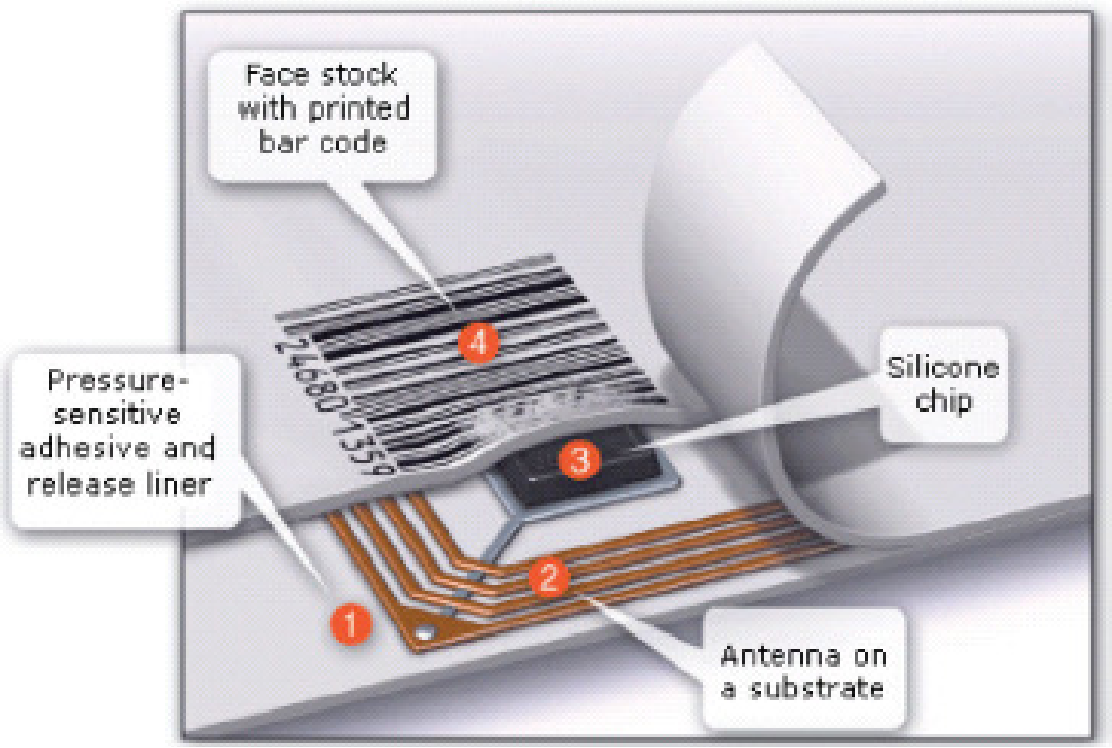


**Figura 4.5** – Constituição de uma Smart Label. [32]

# Capítulo 5

# EPCglobal Network

A EPCglobal é uma organização sem fins lucrativos responsável pelo desenvolvimento, promoção e controlo a nível mundial de normas para identificação por rádio frequência baseadas nas especificações EPC (Electronic Product Code).

## 5.1 EPCglobal a História [33]

Em 1999, um grupo de fabricantes e retalhistas de diversos sectores de actividade, aperceberam-se que a tecnologia de RFID poderia substituir o Código de Barras e começaram a trabalhar na criação de um standard para RFID, a que chamaram Electonic Product Code (EPC). Este grupo financiou as pesquisas que foram efectuadas no Auto-ID Center do Massachusets Institute of Technology (MIT) e nos seis centros de investigação que, posteriormente, se lhe juntaram e com o apoio das organizações de normalização UCC e EAN. O Auto-ID Center tinha um projecto para desenvolver a "Internet of Things" e a ele se associaram os laboratórios congéneres:

- Institute for Manufacturing, University of Cambridge, Reino Unido
- RFID Laboratory, University of Adelaide, Austrália
- St. Gallen University and Swiss Federal Institute of Technology, ETH Zurich, Suíça
- Keio University Shonan-Fujisawa Campus Murai Laboratory, Keio University, Japão
- Fudan Auto-ID Center, China

A EPCglobal é o resultado da associação entre a UCC e a EAN, em 2003, para comercializar e estabelecer standards baseados na propriedade intelectual desenvolvida pelo Auto-ID Center do MIT e pelos laboratórios associados.

Conjuntamente com fabricantes, distribuidores, fornecedores de tecnologia, empresas de logística, retalhistas e equipas de investigação estão a construir uma rede mundial para gerir, de forma segura, a informação relativa aos EPCs.

## 5.2 Desenvolvimento de Standards EPCglobal

A EPCglobal estabeleceu um procedimento para o desenvolvimento de standards (EPCglobal, 2007a). Este procedimento começa pelo levantamento dos requisitos do utilizador que dão origem a um conjunto de especificações tendentes a satisfazer os requisitos do utilizador. As especificações são implementadas num protótipo que é testado e vai evoluindo até ser aceite como standard pela respectiva comissão de avaliação (Board of Governors Technology Commities). A EPCglobal trabalha com distribuidores, fabricantes e integradores de hardware e software para criar e partilhar propriedade intelectual que é disponibilizada aos seus associados.

Os seus princípios orientadores são:

- Facilitar a troca de informação e de mercadorias entre parceiros comerciais;
- Promover a existência de um mercado efectivo para os componentes do sistema;
- Promover a inovação;
- Apoiar a adopção universal dos seus standards.

## 5.3 Standards EPCglobal [34]

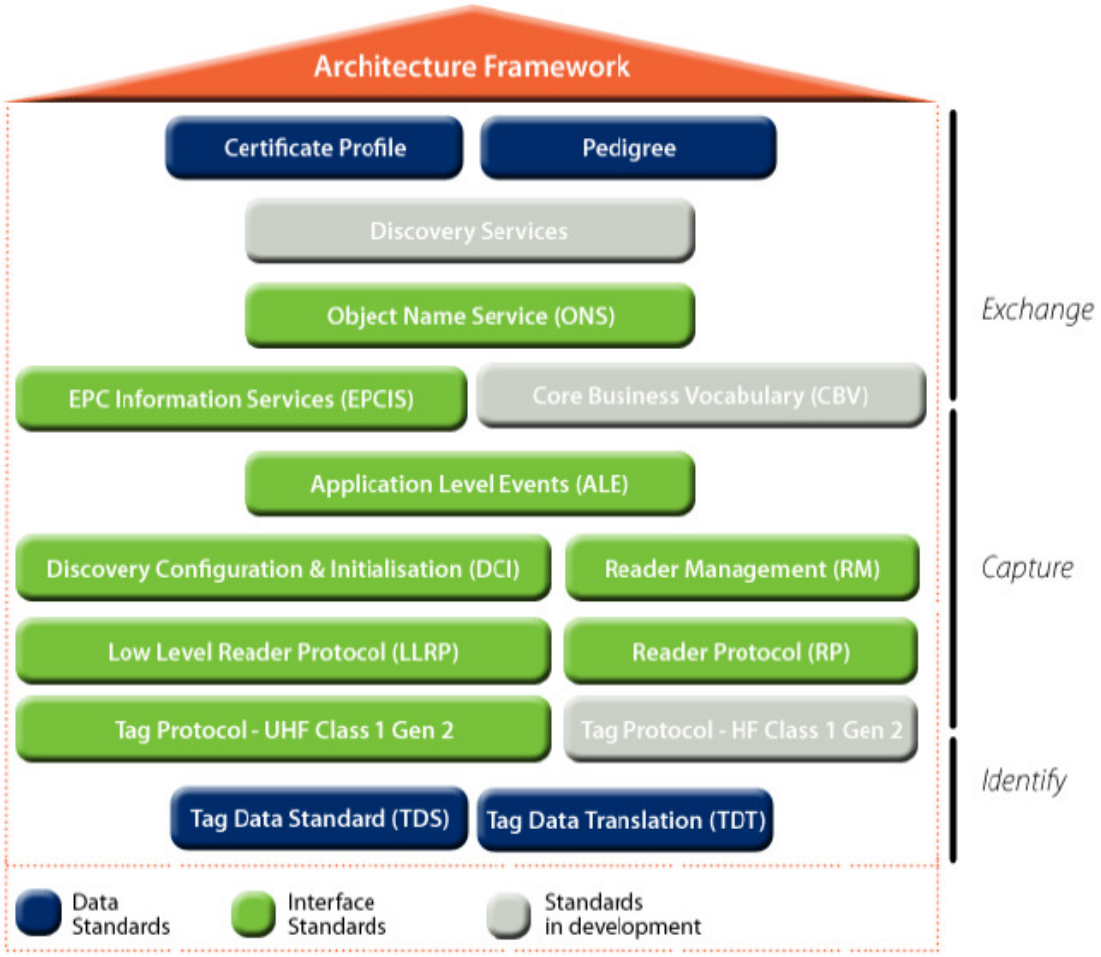


**Figura 5.1** – Standars EPCglobal [34]

**Architecture Framework -** Este documento (EPCglobal, 2005a) é uma colecção interligada de standards relativos ao hardware, software e interface de dados que, em conjunto com um grupo de serviços, têm como objectivo comum melhorar a cadeia de abastecimento através do uso do EPC.

Esta rede tem como objectivo disponibilizar a todos os intervenientes no processo a informação de que necessitam de uma forma fácil, atempada e segura.

Os principais objectivos deste Framework são:

- Enumerar os standards a nível de hardware, software e dados que fazem parte do EPCglobal Architecture Framework e mostrar o modo como estão interligados;
- Fornecer directrizes aos utilizadores e fornecedores de tecnologia que pretendem implementar os standards EPCglobal e usar os seus serviços;
- Explicar os princípios que presidiram ao desenvolvimento de cada standard;
- Definir os serviços fundamentais prestados pela EPCglobal e seus representantes.

A versão actual do EPCglobal Architecture Framework é a V 1.3, aprovada em 19 de Março de 2009.

**EPCglobal Certificate Profile Standard -** Este documento define um perfil de emissão e uso de certificados X.509 pelas entidades que usam a rede EPCglobal, com o objectivo de garantir uma grande interoperabilidade e rápida implementação, ao mesmo tempo que garante segurança na utilização. Os perfis definidos são baseados em dois standards que foram amplamente implementados e testados em diversos ambientes:

- RFC 3280 - Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile;
- RFC 3279 - *Algorithms and Identifiers for the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile*.

**Pedigree Standard** – Este documento define os procedimentos a adoptar na manutenção e troca dos documentos electrónicos usados pelos intervenientes na cadeia de abastecimento de produtos farmacêuticos, de forma a certificar a sua autenticidade.

**Discovery Services Standard (em desenvolvimento)** – Este documento pretende definir a forma de um interveniente no processo encontrar e obter a informação de que tem necessidade e a que está autorizado a aceder quando essa informação está na posse de uma entidade com a qual não tem qualquer relação anterior.

**Object Name Service (ONS) Standard** – Este documento especifica a forma como o DNS (Domain Name System) é usado para localizar informação acerca de um EPC específico. O ONS transforma o EPC num endereço internet permitindo, desta forma, acesso à informação pretendida.

**EPCIS (EPC Information Services)** – Este documento define a forma como diferentes aplicações partilham a informação acerca de um determinado EPC, tanto dentro de uma organização, como entre organizações. Esta partilha de informação é fundamental ao funcionamento da rede EPCglobal.

**CBV (Core Business Vocabulary – em desenvolvimento)** – Define a estrutura da linguagem e os valores usados conjuntamente com o EPCIS no tratamento de eventos, quer dentro de uma empresa, quer entre empresas. Esta uniformização no tratamento de eventos por todos os intervenientes no processo é fundamental para aumentar a compreensão dos dados referentes aos eventos registados pelo EPCIS.

**ALE (Application Level Events)** – Este standard especifica um interface através do qual as aplicações cliente podem obter ou gravar dados numa tag a partir de várias fontes. O conjunto de API's disponibilizadas pelo ALE permite aos programadores uma forma fácil de aceder aos leitores e às tags.

**Discovery, Configuration & Initialization for Reader Operitions** – Este standard especifica o interface entre o leitor de RFID e os controladores de acesso e a rede a que estão ligados. Define, também, os parâmetros de configuração e os valores de inicialização de cada leitor que lhe permitem comunicar com os outros elementos da rede. Para facilitar a execução destas tarefas pelo leitor, o controlador de acesso disponibiliza as seguintes funções:

- Forma de um leitor descobrir um ou vários controladores de acesso;
- Forma de um controlador descobrir um ou mais leitores;
- Forma de os leitores e controladores se identificarem mutuamente e de autenticação das respectivas identidades;
- Forma de configurar o leitor através do controlador e de actualizar o respectivo software e firmware.

**RM (Reader Management)** – Este standard descreve a forma como o leitor deve ser monitorizado e define o EPCglobal SNMP RFID MIB (Simple Network Management Protocol RFID Managment Information Base).

**LLRP (Low Level Reader Protocol)** – Este documento especifica o interface entre os leitores de RFID e os clientes. O protocolo do interface é denominado de baixo nível porque fornece controlo do tempo de operação do protocolo de RFID aéreo e acesso aos parâmetros de comando do protocolo aéreo.

Cliente – Qualquer entidade, hardware ou software, que comunica com o leitor.

**RP (Reader Protocol)** – Este standard especifica as interacções entre dispositivos de leitura/escrita de tags e aplicações.

**Tag Protocol UHF Class 1 Gen 2** – Este standard define os requisitos físicos e lógicos de um sistema de RFID, passive-backscatter, ITF (Interrogator Talks First) a funcionar na banda UHF entre os 860 e os 960 MHz. Do sistema fazem parte os leitores e as tags.

**Tag Protocol HF Class 1 Gen 2 (em desenvolvimento)** - Este documento pretende definir os requisitos físicos e lógicos de um sistema de RFID, passive-inductive coupling, ITF (Interrogator Talks First), a funcionar na banda HF a 13,56 MHz. Do sistema fazem parte os leitores e as tags.

**TDS (Tag Data Standard)** - Este documento define dados padronizados para as etiquetas EPC, incluindo o modo como eles devem ser inseridos na etiqueta e como devem ser codificados para utilização nos sistemas de informações da rede EPCglobal. Define, também, a forma como os identificadores GS1 (GTIN, GLN, SSCC, GRAI e GIAI) devem ser gravados numa tag EPC.

**TDT (Tag Data Translation)** – Este standard define o formato machine-redable dos dados da tag EPC permitindo a sua interpretação.

## 5.4 UHF Class 1 Generation 2

A especificação UHF Class 1 Gen 2 descreve, detalhadamente, as comunicações entre o leitor de RFID e a tag e contém as especificações sobre o interface aéreo. Estas especificações foram publicadas pela EPCglobal, em 2004, e adoptadas como ISO 18000-6C, em 2006.

As comunicações entre o leitor e a tag são baseadas no princípio ITF (Interrogator Talks First), em que o leitor envia comandos, conjuntamente com parâmetros, a um grupo de tags que estão no seu raio de acção com o objectivo de individualizar uma tag, obter a sua identificação e/ou outros dados gravados na sua memória, num ambiente em que coexistem várias tags.

A frequência de funcionamento do leitor de RFID pode ser qualquer uma entre 860 e 960 MHz, de acordo com a regulamentação específica de cada país, enquanto as tags funcionam normalmente em toda a banda de frequência respondendo à configuração local do leitor. Muitos fabricantes de tags lidam com este facto optimizando a antena da tag para uma frequência na zona central da banda (910 MHz), enquanto outros desenvolvem as antenas das tags para poderem funcionar em toda a gama de frequências, mas optimizadas para funcionar na Europa ou nos Estados Unidos da América.

A ITU (International Telecommunication Union) divide o mundo em três regiões:

- Região 1 (Europa, Médio Oriente e África) – Normalmente 865 a 868 MHz, 2 W ERP e Frequency Agile.
- Região 2 (América do Norte e do Sul) – Normalmente 902 a 928 Mhz, 4 W EIRP e Spread Spectrum Frequency Hopping;

- Região 3 (Extremo Oriente, Ásia e Austrália) – A maioria segue a Europa, outros os EUA.

Cada país gere as frequências a atribuir de acordo com as directrizes da ITU.

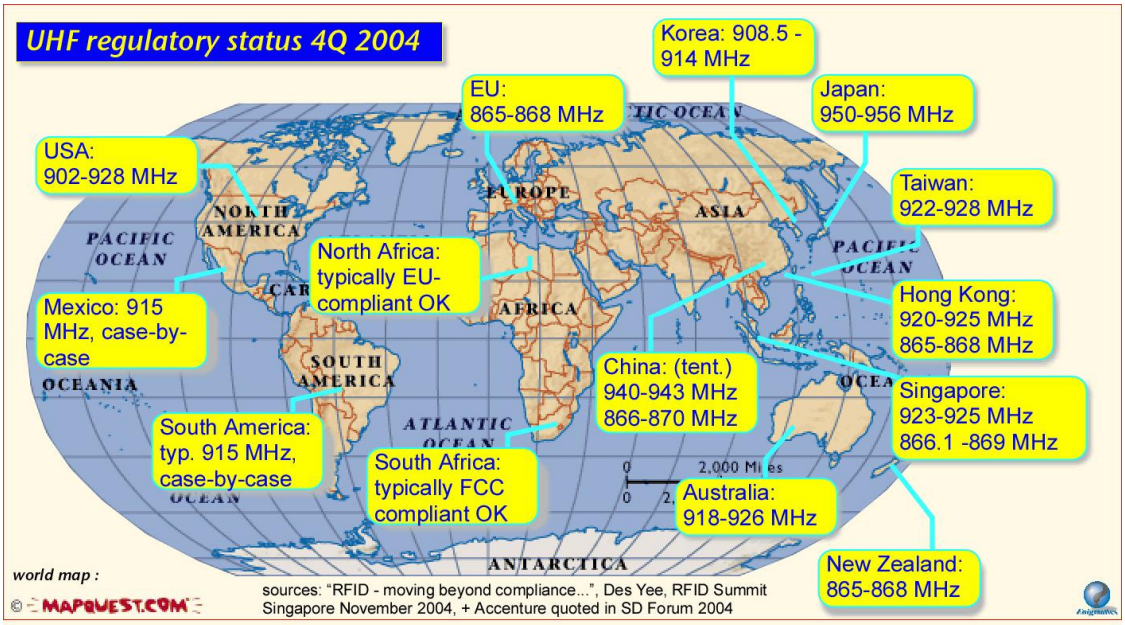


**Figura 5.2** – Frequências atribuídas por vários países na banda UHF

### 5.4.1 UHF Class 1 Generation 2 – Europa

A ETSI (European Telecommunications Standards Institute) EN 302 208 não só prescreve a banda de funcionamento e potência máxima, mas também a divisão da banda em canais, o método de transmissão do leitor e o tempo máximo de transmissão.

A largura de banda de 865 a 868 MHz está dividida em 15 canais de 200 KHz cada, com uma potência máxima de emissão de 2 W ERP (Effective Radiated Power) e em que os 3 canais mais baixos têm uma potência máxima de 100 mW, os dez canais seguintes (865,6 a 867,6 MHz) estão disponíveis para funcionar na potência máxima de 2 W e os dois canais superiores têm uma potência máxima de 500 mW. Como a potência de emissão está directamente ligada com a distância de leitura, muitos fabricantes optam por ter os leitores a funcionar apenas nos dez canais em que é autorizada a potência máxima evitando, assim, que tags que se encontram mais afastadas não sejam lidas.

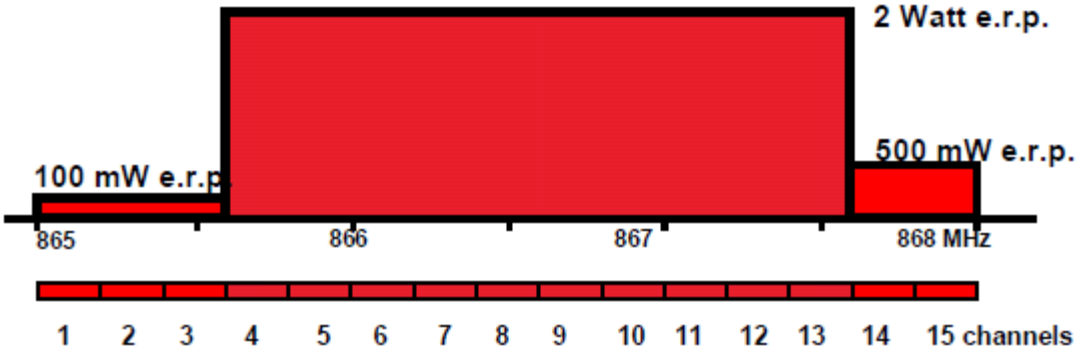


**Figura 5.3** – Canais e Respectivas Potências máximas de emissão [35]

Para evitar a colisão entre leitores os regulamentos do ETSI prescrevem o uso de uma 'frequency agile technique'. Esta técnica é usada para encontrar um canal livre de forma a minimizar a interferência com outros dispositivos no mesmo canal. O ETSI prescreve como 'agile technique' uma tecnologia conhecida por LBT (Listen Before Talk).

A tecnologia de Listen Before Talk (LBT) é também conhecida por Listen Before Transmit e é uma técnica usada para encontrar um canal livre antes de iniciar uma transmissão.

Quando o receptor do leitor detecta que um canal já está ocupado por um outro dispositivo o leitor muda automaticamente de canal e testa a sua disponibilidade antes de iniciar uma transmissão. Numa situação em que todos os canais estão ocupados por outros dispositivos o leitor fica inactivo até que o seu receptor detecte um canal livre. Quando detecta um canal livre fica à escuta durante 5 milissegundos para confirmar que o canal está livre antes de iniciar a transmissão. Num canal livre o leitor pode transmitir por um período máximo de quatro segundos. Após estes quatro segundos o leitor deve mudar para outro canal onde tem que escutar durante 5 milissegundos novamente ou, caso deseje continuar a comunicar no mesmo canal, tem que se manter inactivo durante 100 milissegundos.

### 5.4.2 UHF Class 1 Generation 2 – EUA

Analisando os regulamentos do ETSI e comparando-os com os da FCC (Federal Communications Commission) Part 15 usados nos EUA ficam evidentes as origens das diferenças de performance entre os sistemas de RFID usados nos dois continentes:

- Largura de Banda atribuída;
- Número de Canais;
- Largura de Banda por Canal;
- Método de Transmissão;
- Potência de emissão.

**Largura de Banda Atribuída** – Nos EUA uma parte maior do espectro é atribuído para uso de sistemas de RFID (26 MHZ versus 3 MHz). Esta parte do espectro pode, portanto, ser dividida num número maior de canais e com uma maior largura de banda por canal.

**Número de Canais** – A largura de banda atribuída nos EUA é dividido em 50 canais contra os 10 normalmente usados na Europa o que, em situações em que a densidade de leitores é elevada, provoca uma probabilidade de ocorrência de colisões entre leitores cinco vezes maior na Europa.

**Largura de Banda por Canal** – Cada canal nos EUA tem uma largura de banda de 500 KHz contra os 200 KHz da Europa o que proporciona uma maior velocidade de transferência de dados nos EUA.

**Método de Transmissão** – Enquanto na Europa se usa o LBT, nos EUA é utilizado o FHSS (Frequency Hopping Spread Spectrum). O FHSS é uma tecnologia de transmissão em que o leitor salta de canal numa sequência pseudo-aleatória para evitar colisões entre leitores e pode transmitir durante um intervalo máximo de 0,4 segundos. Após esse tempo tem que saltar para um novo canal.

**Potência de Emissão** – Nos EUA a potência máxima de emissão fixada pela FCC é de 4 W EIRP (Effective Isotropically Radiated Power). Embora as unidades de medida usadas pelos dois reguladores sejam diferentes é possível convertê-las, já que $P_{EIRP} = P_{ERP} \times 1,64$ pelo que a potência máxima de radiação nos EUA é 1,22 vezes maior que na Europa.

### 5.4.3 Dense-Reader Mode (DRM)

Em ambientes em que existe um elevado número de leitores a funcionar próximos uns dos outros e devido às limitações da largura de banda/número de canais para RFID existentes na Europa, os problemas de interferência entre leitores são muito maiores que nos EUA. O modo de funcionamento Dense-Reader pretende evitar este problema.

Os leitores não podem funcionar no mesmo canal porque, após a solicitação de um leitor a tag responde nesse canal e se um outro leitor estiver a funcionar no mesmo canal o seu sinal colide com a resposta da tag impedindo a sua recepção pelo destinatário. Para tentar resolver estas limitações foi proposto o 4-channel DRM (TR 102 649-1).

O 4-channel DRM tem como princípio de funcionamento a separação entre os canais de emissão do sinal pelos leitores e os canais em que as tags respondem. Nesta forma de funcionamento os leitores podem colidir uns com outros, mas não com as tags. Os leitores emitem nos canais 4,7,10 e 13, as tags respondem nos restantes canais e a obrigatoriedade de LBT para os leitores é abandonada.

O leitor emite num canal e a tag responde usando um processo de backscatter modulation usando um canal adjacente (e.g. um leitor transmitindo no canal 4 provoca uma resposta da tag no canal 3 ou 5). Como a potência do sinal de resposta da tag é, normalmente, muito menor que o sinal do leitor os canais de baixa potência podem ser usados para este fim.

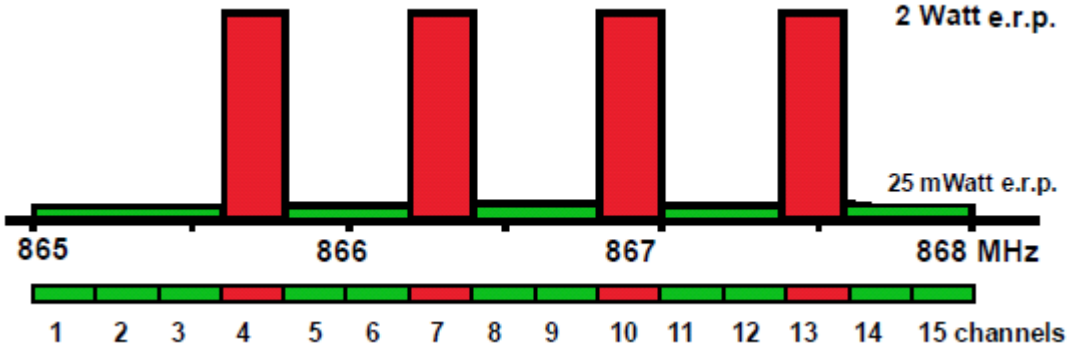


**Figura 5.4** – Canais e Respectivas Potências máximas de emissão modo DRM [35]

### 5.4.4 TAG UHF Class 1 Gen 2 Memory

As especificações EPCglobal definem que a tag deve possuir quatro bancos de memória separados logicamente e, cujo endereçamento, é do tipo MSB (Most Significant Bit) First:

- **Memória Reservada;**
- **Memória EPC;**
- **Memória TID;**
- **Memória do Utilizador (Opcional).**

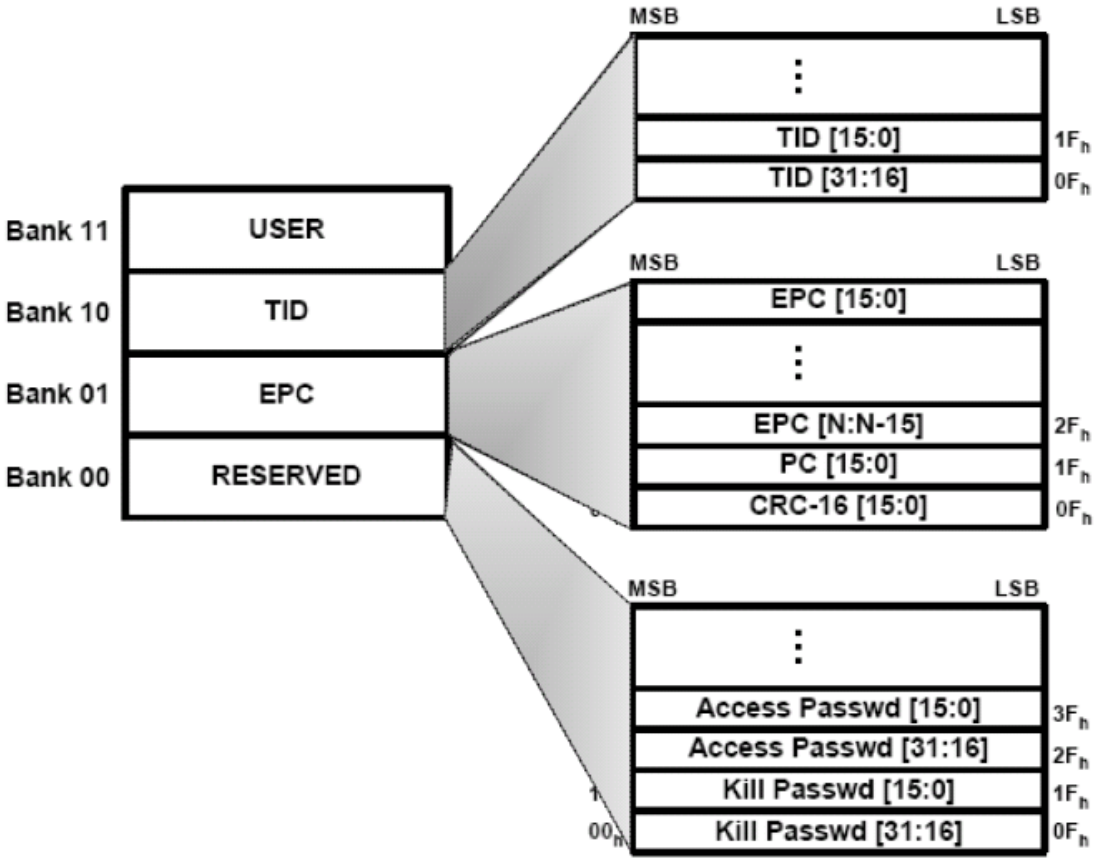


**Figura 5.5** – Estrutura Lógica da Memória de uma tag [36]

**A memória reservada** contém a(s) password(s) de Kill e/ou acesso se existirem.

A password de Kill tem um tamanho de 32 bits e está armazenada nos endereços $00_h$ a $1F_h$. Este comando serve para desactivar permanentemente a tag. Após a execução do comando Kill a tag deixa de responder a qualquer solicitação e nunca mais pode ser reactivada.

A password de acesso tem um tamanho de 32 bits e está armazenada nos endereços $20_h$ a $3F_h$. Um leitor tem que fornecer a password à tag para iniciar um processo de diálogo.

A memória EPC é constituída por:

CRC (Cyclic Redundancy Check) - com um tamanho de 16 bits armazenados nos endereços $00_h$ a $0F_h$. Quando a tag é activada é calculado um CRC-16 função do Protocolo de Controlo e do EPC da tag. Este valor é mapeado no CRC e é usado para proteger alguns comandos enviados pelo leitor para a tag e a resposta da tag para o leitor. Um dos dados protegidos pelo CRC é o envio do EPC da tag para o leitor

- PC (Protocol Control) - com um tamanho de 16 bits armazenado nos endereços de memória $10_h$ a $1F_h$;
- EPC (Electronic Product Code) - que começa no endereço $20_h$ tem um tamanho variável e que, no formato mais usado, tem um tamanho de 96 bits.

EPCglobal/GS1 allocated and managed — Company managed

| Header | Filter Value | Partition Value | Company Prefix | Document Type | Serial Number |
|---|---|---|---|---|---|
| 8 bits | 3 bits | 3 bits | 27 bits | 14 bits | 41 bits |
| 0010 1100 [Static, Binary value] | High-level filter option | Determines Company Prefix length | Equates to eight digits to uniquely identify an organization such as DHS/CBP, DoS, WA State, etc. | Equates to four digits, allowing up to 10,000 document types | Allows for over 2 trillion unique values |

**Figura 5.6** – Lay-out da memória EPC de uma tag Class 1 Gen 2 96 bits [37]

**O Tag IDentifier** é um código atribuído pelo fabricante da tag e que a deveria identificar univocamente, ser gravado no processo de fabrico e não deveria ser passível de alteração constituindo, assim, uma primeira barreira à contrafacção. No entanto, apenas a identificação do fabricante e alguma informação adicional com as características da tag são obrigatórios.

No formato mais aceite o TID é constituído por:

- Identificador da class da tag – 8 bits;
- Fabricante da tag – 12 bits;

- Modelo da tag – 12 bits;
- Número de série da tag – 32 bits.

A User Memory é opcional e, caso exista, as suas características dependem das opções do fabricante.

## 5.5 Tag Data Standards [38]

O Tag Data Standard V 1.3 define um conjunto de identificadores cuja maioria deriva dos sistemas de codificação EAN/UCC:

- GID – General Identifier;
- SGTIN - Serialized Global Trade Item Number;
- SSCC - Serial Shipping Container Code;
- SGLN - Serialized Global Location Number;
- GRAI - Global Returnable Asset Identifier;
- GIAI - Global Individual Asset Identifier;
- DoD – Department of Defense dos EUA.

Os identificadores que vão ser analisados são os de uma tag com um EPC de 96 bits.

### 5.5.1 General Identifier

É o formato genérico de codificação que pode ser utilizado quando os outros formatos não podem ser aplicados e não tem qualquer equivalente na codificação EAN/UCC. O valor do header é $0011\ 0101_b$ e é composto por três campos:

- Código da Entidade Gestora – identifica uma organização (normalmente uma empresa) que é responsável pelo conteúdo dos campos seguintes. O Código da Entidade Gestora é atribuído pela GS1 ou sua legítima representante que garante que ele é único.
- Object Class – é atribuído pela entidade gestora e serve para identificar, dentro da entidade, uma classe, grupo, família ou tipo de objecto e deve ser único.
- Número de Série – é atribuído pela entidade gestora e é único dentro da classe.

### 5.5.2 Serialized Global Trade Item Number

O SGTIN é um identificador baseado no EAN/UCC GTIN-13 que, na perspectiva EPC, não é um verdadeiro identificador já que não identifica univocamente um objecto.

O SGTIN é composto por:

- 8 bits de header com o valor $0011\ 0000_b$ que é comum para todas as tags de 96 bits que contêm um SGTIN;
- 3 bits filter que indica o tipo de objecto em que a tag está colocado (item, embalagem ou palete);

- 3 bits partition que indica como os 44 bits seguintes (prefixo da entidade e referência do item) são divididos;
- 20 a 40 bits (dependendo da partição) para o prefixo da entidade gestora e que é atribuído pela GS1 ou seu representante e é igual à referência da entidade EAN/UCC;
- 24 a 4 bits (dependendo da partição) para a referência do item e é igual à referência do item na codificação EAN/UCC e é atribuído pela entidade gestora;
- 38 bits para o número de série do item.

No formato EAN/UCC o equivalente do SGTIN pode ser obtido no código EAN-128 com a concatenação do GTIN com o número de série através do AI 21

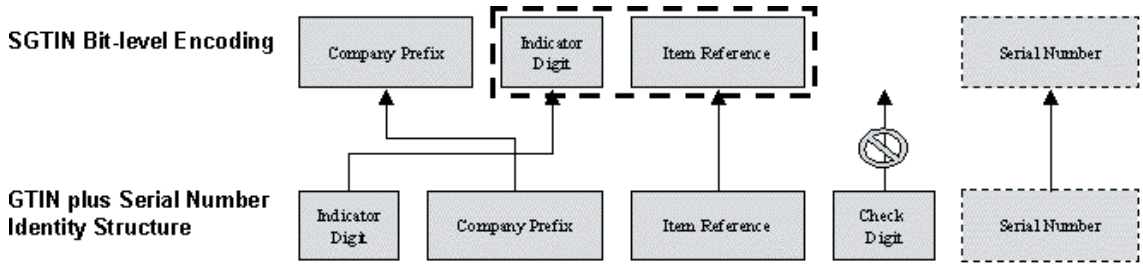


**Figura 5.7** – Conversão de EAN/UCC GTIN mais número de série em SGTIN EPCglobal [38]

### 5.5.3 Serial Shipping Container Code

O SSCC como definido pela EAN/UCC é considerado um verdadeiro identificador na perspectiva EPC já que identifica univocamente um objecto e é composto pelos seguintes campos:

- 8 bits de header com o valor 0011 $0001_b$ que é comum para todas as tags de 96 bits que contêm um SSCC;
- 3 bits filter cujo valor normal é $010_b$ e que indica tratar-se de uma unidade logística/expedição;
- 3 bits partition que indicam como os 58 bits seguintes (prefixo da entidade e número de sequência) são divididos;
- 20 a 40 bits (dependendo da partição) para o prefixo da entidade gestora e que é atribuído pela GS1 ou seu representante e é igual à referência da entidade EAN/UCC;
- 38 a 18 bits (dependendo da partição) para o número de sequência da unidade logística/expedição que é o resultado da concatenação entre o dígito suplementar e a sequência. O dígito suplementar não tem qualquer significado e serve para codificação interna da entidade gestora
- 24 bits não utilizados. Deve conter zeros para estar conforme com a V 1.3.

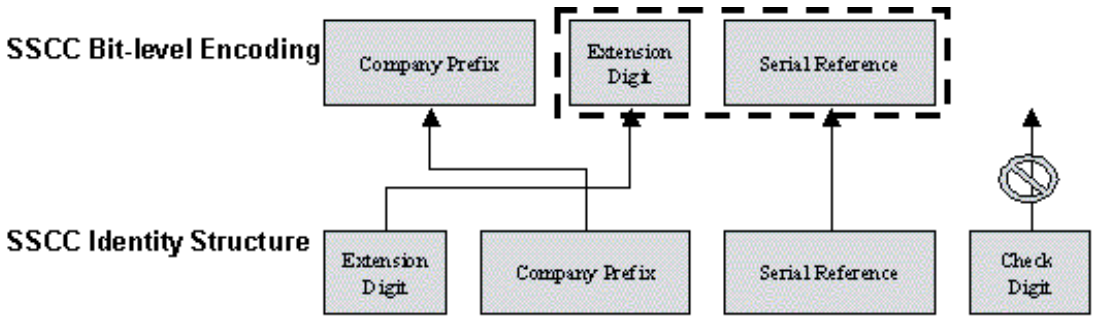


**Figura 5.8** – Conversão do SSCC de EAN/UCC para SSCC EPCglobal [38]

### 5.5.4 Serialized Global Location Number

O SGLN é a implementação pela EPCglobal do EAN/UCP GLN AI (Application Identifier) 414 que identifica a localização física de um local, normalmente um armazém e é composto pelos seguintes campos:

- 8 bits de header com o valor 0011 $0010_b$ que é comum para todas as tags de 96 bits que contêm um SGLN;
- 3 bits filter cujo valor normal é $001_b$ e que indica tratar-se de uma localização fixa;
- 3 bits partition que indicam como os 41 bits seguintes (prefixo da entidade e referência da localização) são divididos;
- 20 a 40 bits (dependendo da partição) para o prefixo da entidade gestora e que é atribuído pela GS1 ou seu representante e é igual à referência da entidade EAN/UCC;
- 21 a 1 bits (dependendo da partição) para a referência da localização;
- 41 bits para a extensão que no formato SGLN-96 deve conter zeros binários.

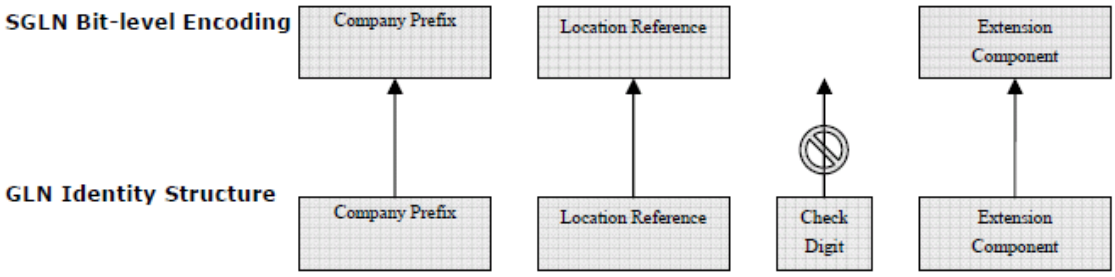


**Figura 5.9** – Conversão do GLN de EAN/UCC mais extensão para SGLN EPCglobal [38]

### 5.5.5 Global Returnable Asset Identifier

O GRAI, como definido pela EAN/UCC, é considerado um verdadeiro identificador na perspectiva EPC, já que identifica univocamente um objecto e é composto pelos seguintes campos:

- 8 bits de header com o valor 0011 $0011_b$ que é comum para todas as tags de 96 bits que contêm um GRAI;
- 3 bits filter que não têm qualquer significado neste identificador;
- 3 bits partition que indicam como os 44 bits seguintes (prefixo da entidade e tipo de activo retornável) são divididos;
- 20 a 40 bits (dependendo da partição) para o prefixo da entidade gestora e que é atribuído pela GS1 ou seu representante e é igual à referência da entidade EAN/UCC;
- 24 a 4 bits (dependendo da partição) para a identificação do tipo de activo retornável;
- 38 bits para identificar univocamente o activo retornável dentro do tipo de activo retornável.

Um activo retornável é uma embalagem ou unidade de transporte que possui valor comercial e pode ser reutilizada para armazenamento de mercadorias normalmente designada como tara retornável.

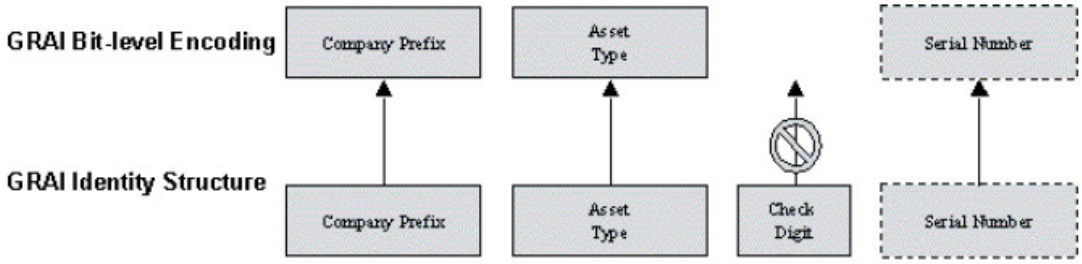


**Figura 5.10** – Conversão do GRAI de EAN/UCC e número de série para GRAI EPCglobal [38]

### 5.5.6 Global Induvidual Asset Identifier

O GIAI, como definido pela EAN/UCC, é considerado um verdadeiro identificador na perspectiva EPC, já que identifica univocamente um objecto e é composto pelos seguintes campos:

- 8 bits de header com o valor 0011 $0100_b$ que é comum para todas as tags de 96 bits que contêm um GIAI;
- 3 bits filter que não têm qualquer significado neste identificador;
- 3 bits partition que indicam como os 82 bits seguintes (prefixo da entidade e activo individual) são divididos;

- 20 a 40 bits (dependendo da partição) para o prefixo da entidade gestora e que é atribuído pela GS1 ou seu representante e é igual à referência da entidade EAN/UCC;
- 62 a 42 bits (dependendo da partição) para a identificação do activo individual.

Um activo individual é um bem com carácter duradouro de uma empresa que deve ser identificado individualmente para controlo do imobilizado corpóreo.

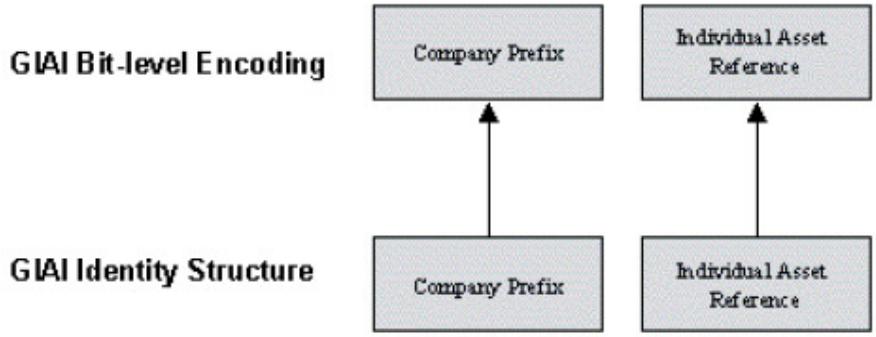


**Figura 5.11** – Conversão do GIAI de EAN/UCC e número de série para GIAI EPCglobal [38]

### 5.5.7 Especificação DoD [39]

O Departamento de Defesa dos EUA tem sido um forte dinamizador da tecnologia RFID ao obrigar que todas as paletes e outras embalagens de um elevado número de produtos, entregues pelos seus fornecedores nas suas bases logísticas, sejam identificados com uma tag RFID e, para isso, criaram uma especificação própria de acordo com os standards EPCglobal.

Os objectos individuais de elevado valor devem ser identificados com um identificador único fornecido pelo DoD o UID (Unique Identification) que é o equivalente do SGTIN usado pela GS1.

A especificação DoD-96 define a codificação da informação a ser fornecida numa tag UHF Class 1 Gen 2 com EPC de 96 bits. Esta especificação define quatro campos:

- 8 bits de header com o valor 0011 $1111_b$ que é comum para todas as tags de 96 bits destinadas ao DoD;
- 4 bits filter que identificam o tipo de embalagem em que as mercadorias fornecidas estão contidas (palete, caixa, contentor, etc);
- 48 bits para identificação do fornecedor. Este campo tanto pode conter o código de empresa atribuído pela GS1, como o código CAGE (Commercial and Government Entity) atribuído pelo DoD;
- 36 bits para o número de série da embalagem que é entregue pelo fornecedor e que com o respectivo código a identificam univocamente.

| Header | Filter | Government Managed Identifier | Serial Number |
|---|---|---|---|
| 8 bits | 4 bits | 48 bits | 36 bits |

**Figura 5.12** – Especificação DoD – 96 [39]

# Capítulo 6

# Privacidade e Segurança

O direito à privacidade está consignado na lei e é considerado um dos direitos básicos de cada indivíduo, mas o seu enquadramento legal difere de país para país, tendo evoluído ao longo do tempo e muito basicamente pode ser definido como o direito a poder estar só.

Quando uma nova tecnologia é introduzida no mercado, os principais critérios de avaliação são, normalmente, as novas funcionalidades que introduz e o preço. Se a nova tecnologia é aceite e se começa a massificar os problemas de standardização, segurança e privacidade passam a ser encarados como fundamentais para a sua aceitação global.

Algumas características intrínsecas a esta tecnologia tornam-na particularmente vulnerável e podem configurar uma ameaça à privacidade entre os sistemas de informação:

- A comunicação entre a tag e o leitor;
- O fraco poder computacional e a pouca energia disponível na generalidade das tags impede a implementação de medidas de segurança mais eficazes;
- As reduzidas dimensões e o local em que são aplicadas algumas tags fazem com que as pessoas as possam transportar sem o seu conhecimento.

## 6.1 Preocupações com o uso de RFID

A possibilidade de a tecnologia de RFID poder permitir uma invasão da privacidade individual tem sido um dos argumentos esgrimidos, por algumas associações, que apelam ao boicote das lojas e dos produtos que usam esta tecnologia de que a norte-americana CASPIAN (Consumers Against Supermarket Privacy Invasion and Numbering) é um exemplo. Os receios prendem-se com a possibilidade de identificar os objectos que uma pessoa transporta e poder, assim, seguir todos os seus passos, conhecer os seus hábitos e gostos pessoais. Além desta potencial invasão da privacidade, a possibilidade de acesso a informação pessoal e confidencial que se encontra em vários documentos electrónicos que as pessoas possuem e, muitas vezes transportam, (passaporte, BI, documento único, etc.) e cujo uso se vai massifican-

do, levantam problemas sobre a segurança (confidencialidade, integridade e disponibilidade) dessa informação já que ela pode ser acedida sem o conhecimento do seu legítimo proprietário.

A preocupação quanto a uma possível invasão da privacidade deve-se a uma característica específica que esta tecnologia implementa ao identificar univocamente um objecto e as correlações que podem ser estabelecidas entre o objecto e o seu proprietário.

As principais preocupações levantadas quanto à privacidade são:

- As dimensões de algumas tags que as tornam difíceis de detectar e a possibilidade de estarem embebidas no produto o que as torna invisíveis;
- A informação transmitida pela tag pode fornecer dados sobre a identificação, localização e características do objecto em que estão colocadas;
- A tag pode fornecer a informação que contém ao longo de toda a sua vida sobre o objecto em que está colocada e permitir assim seguir os hábitos e comportamentos de quem a transporta;
- A possibilidade de ligar uma tag a um pagamento efectuado com um cartão de crédito ou de fidelização e, assim, chegar à identidade do comprador;
- A quantidade de informação gerada é de uma granularidade tão elevada que permite detectar qualquer mudança nos hábitos de consumo e traçar um perfil muito pormenorizado do consumidor. Analisando o perfil do consumidor as empresas podem tirar conclusões sobre os seus rendimentos, estilo de vida, estado de saúde, hábitos de consumo, etc;
- Apesar do raio de acção actual dos leitores ser bastante limitado as associações de consumidores temem que os rápidos avanços tecnológicos não sejam acompanhados pelas respectivas medidas legais de protecção dos direitos individuais quanto ao volume e tipo de informação que pode ser armazenada.

Estas preocupações, apresentadas por alguns sectores da sociedade, podem constituir um forte estímulo ao desenvolvimento de tecnologias de baixo custo que aumentem a privacidade e a segurança da informação veiculada por esta tecnologia.

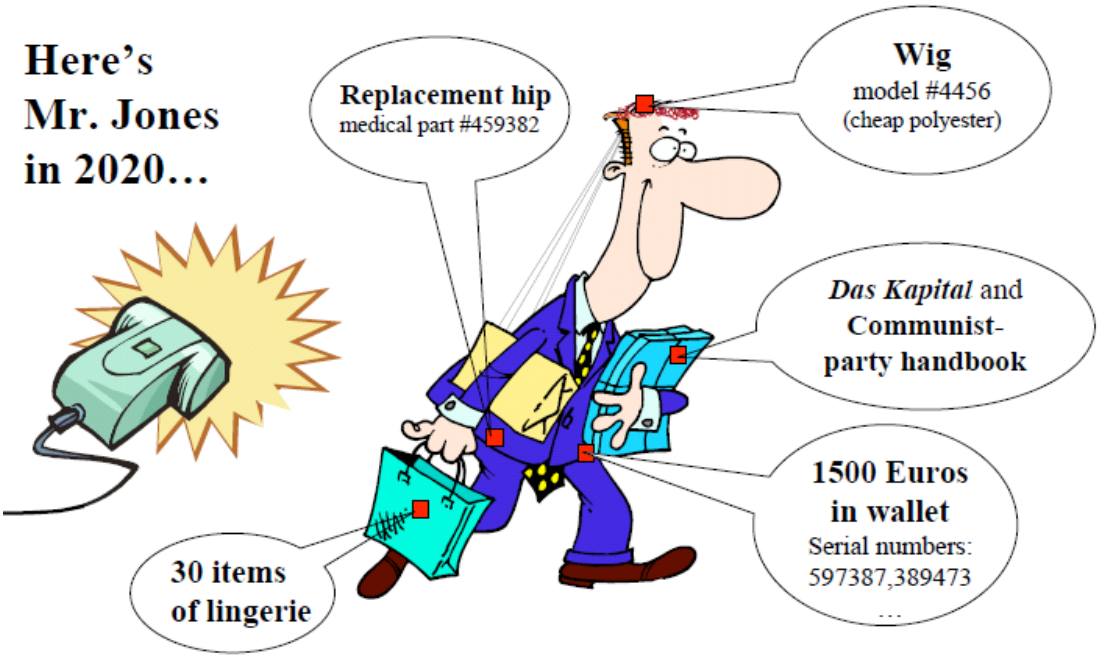


**Figura 6.1** – Ameaças à privacidade do consumidor [40]

## 6.2 Recomendações sobre o uso de RFID

Preocupados com o uso que pode ser dado a esta tecnologia e ao protagonismo que tem sido dado a grupos que se opõem à sua utilização, os governos, em colaboração com fabricantes de equipamentos, associações comerciais, organizações de cidadãos e outros interessados no processo, começam a dar indicações e a legislar sobre o seu uso.

Em 12 de Maio de 2009, a UE, publicou ***'RFID Privacy and Data Protection Recommendation'*** que além de um conjunto de recomendações a adoptar pelos estados membros contém, também, indicações precisas às entidades que usam ou desenvolvem aplicações de RFID sobre o modo como fazê-lo de forma amigável e garantindo privacidade e segurança *by design*.

Algumas das recomendações feitas pelos diversos governos são:

- Implementação pelas organizações de medidas inequívocas de garantia da privacidade;
- Ampla divulgação dessas medidas pelos seus funcionários, clientes, associações de defesa do consumidor e outros interessados;
- Os consumidores devem ser avisados sobre a existência de tags colocadas ou embebidas nos objectos;
- Os consumidores devem ser avisados da existência de leitores que podem ler as tags que transportam;

- As tags devem ser desactivadas ou removidas gratuitamente, no ponto de venda, excepto se o cliente, depois de devidamente informado dos riscos potenciais, desejar a sua manutenção. Devem também ser disponibilizados ao cliente os meios necessários para confirmar a desactivação ou remoção da tag;
- Os retalhistas devem disponibilizar gratuitamente os meios para desactivar ou remover a tag caso o cliente o decida *a posteriori;*
- A desactivação ou remoção da tag não pode ter como consequência a perda ou redução das obrigações do vendedor/fabricante;
- Os retalhistas que não usam a tecnologia RFID não são obrigados a desactivar as tags;
- Divulgação dos benefícios da adopção da tecnologia de RFID;
- Restrições à interligação entre a informação contida na tag e as bases de dados que contêm informação confidencial;
- Restrições no acesso e uso da informação confidencial contida nas tags;
- Assegurar a exactidão e segurança da informação pessoal contida nas tags.

Uma ênfase muito especial deverá ser posta no esclarecimento dos benefícios da adopção da tecnologia RFID e na desmistificação de muitas ameaças que lhe são imputadas no comércio a retalho, já que essa contestação não existiu aquando da sua implementação noutras áreas de actividade, nem com a adopção de outras tecnologias que violam o direito à privacidade como a videovigilância, hoje omnipresente, e que foi apresentado como uma forma de aumentar a nossa segurança e proteger os nossos bens.

A generalidade dos animais domésticos possuem hoje uma tag que os identifica e não é por essa razão que os donos deixam de passear os seus cães.

Os cartões de acesso a determinados locais como edifícios, parques de estacionamento, instalações desportivas ou meios de transporte que permitem saber quando determinada pessoa/viatura lá entrou e saiu não levantam qualquer polémica.

A adesão voluntária de muitos portugueses à via verde é uma realidade e a sua introdução não provocou qualquer contestação, sendo pelo contrário, enaltecidas as suas vantagens.

Portugal prepara-se para adoptar um Dispositivo Electrónico de Matrícula (DEM) que vai permitir identificar a passagem da viatura por determinados pontos, o que pode permitir o seu seguimento e os protestos contra a adopção da tecnologia não têm por base a violação da privacidade, mas o pagamento que vai provocar.

## 6.3 Medidas de Segurança

Além da implementação das recomendações governamentais outras medidas têm sido propostas:

- Evitar que a tag seja alimentada. Esta técnica baseia-se na gaiola de Faraday para interceptar o sinal electromagnético que iria fornecer alimentação à tag.

Este método muito simples já está a ser adoptado em bolsas para guardar documentos, como passaportes e bilhetes de identidade electrónicos ou cartões de débito/crédito. Há, também, estabelecimentos comerciais que fornecem as suas mercadorias dentro de sacos forrados por uma película metálica que impede a leitura por rádio frequência do respectivo conteúdo;

- Uso de dispositivos que emitem um sinal de RF que interfere com o sinal do leitor impedindo, assim, que as tags que se encontram no seu raio de acção sejam lidas;
- Uso de uma função de hash para controlar o estado da tag. Quando a tag é bloqueada é-lhe atribuída uma *meta-id*, com a qual passa a responder a todas as solicitações no estado de bloqueada. A tag só muda de estado se lhe for enviado um valor ***x*** tal que *meta-id=h(x)*. Para evitar a identificação através da sua *meta-id,* esta deve ser alterada no fim de todas as sessões de comunicação. [41]
- Uso de um dispositivo bloqueador que simula a existência de um elevado número de tags impedindo, desta forma, o leitor de identificar as tags que realmente se encontram no seu raio de acção. O número de tags simuladas é no mínimo $2^{64}$ mesmo para os modelos mais simples. [42]

## 6.4 Ataques mais Frequentes e Respectivas Contra medidas

Todos os sistemas de informação estão sujeitos a ataques ao seu conteúdo e integridade. Devido à sua natureza e ao meio de propagação utilizado os sistemas de RFID estão sujeitos a alguns ataques específicos de difícil detecção e localização.

### 6.4.1 - Eavesdropping

Este tipo de ataque passivo consiste em monitorizar as transmissões entre o leitor e a tag ou vice-versa, interceptando o canal de comunicação utilizado e obtendo, desta forma, informação sobre os intervenientes. Como o atacante não interfere nas comunicações a sua presença é muito difícil de detectar pela vítima.

As contra medidas mais usadas consistem em encriptar a informação transmitida impedindo, assim, a fácil compreensão da mensagem pelo atacante. Usando os standards disponíveis limitar a potência de emissão dos leitores ao mínimo necessário pela aplicação, dificultando a intersecção das comunicações. Quanto mais baixa a potência, menor é o raio de acção e, portanto, mais próximo o atacante tem que estar. Mesmo usando leitores não homologados, que possuem raios de acção muito grandes, o sinal emitido pela tag tem uma distância de propagação muito pequena, pelo que a acção do atacante pode ser inviabilizada.

### 6.4.2 – Análise de tráfego

Este tipo de ataque passivo baseia-se em métodos de análise do tráfego entre o leitor e a tag, mesmo que o conteúdo esteja encriptado, e a partir dessa análise elaborar um perfil sobre os movimentos efectuados, ligações estabelecidas e transacções financeiras efectuadas. A análise de tráfego é uma invasão clara da privacidade.

As formas de minimizar este tipo de ataque consistem em evitar rotinas e efectuar falsas comunicações no canal de forma a fornecer falsas informações e confundir os dados fornecidos.

### 6.4.3 - Spoofing

Neste tipo de ataque é usada uma tag clonada ou a sua informação para comunicar com um leitor legítimo e, assim, ganhar acesso a determinados locais, bens ou serviços. A informação necessária para clonar física ou logicamente uma tag, pode ter sido obtida, através monitorização (eavesdropping) ou análise de tráfego, de sessões de comunicações entre leitores e tags legítimos.

As formas de minimizar as probabilidades de sucesso deste tipo de ataque são a implementação de protocolos de autenticação mútua e algoritmos de encriptação mais complexos. Contudo, estas medidas esbarram com as capacidades da tag e os custos inerentes à sua implementação.

### 6.4.4 - Relay attack ou Man in the midle attack

Neste tipo de ataque activo o atacante cria uma ligação entre um leitor legítimo e uma tag legítima. Do ponto de vista do sistema parece que o leitor e a tag legítimos estão ligados directamente, quando na realidade todas as comunicações passam pelo canal criado pelo atacante. Após o estabelecimento deste canal os atacados podem autenticar-se em sistemas de controlo de acessos ou pagamentos. Como o atacante apenas retransmite a informação, os protocolos de autenticação não protegem contra este tipo de ataque.

Este tipo de ataque pode ser evitado se protegermos as tags (normalmente cartões) de ser contactadas, quando não estão a ser usadas, transportando-as numa bolsa que as isole de potenciais solicitações. Este tipo de ataque está limitado pela distância entre o leitor e a tag. Quando a distância entre o leitor e a tag legítimos aumenta, o tempo de retransmissão também aumenta. De acordo com o standard ISO 18000 – 6C (air interface protocol) o leitor espera pela resposta da tag a um *query* durante um intervalo máximo de 77 μs. Se não obtiver uma resposta durante este intervalo de tempo o leitor termina a tentativa de comunicação. Uma forma de minimizar este tipo de ataque consiste em diminuir o tempo de resposta de acordo com as características da instalação em concreto.

### 6.4.5 – Clonagem da Tag

Neste ataque o objectivo é obter uma cópia de uma tag, tanto do ponto de vista físico, como do seu conteúdo. Esta cópia é depois usada para ser colocada em artigos contrafeitos que são introduzidos no mercado, aceder a áreas reservadas ou efectuar transacções em nome da vítima.

A implementação de um protocolo de autenticação pode evitar a clonagem da tag. Se for usado um protocolo do tipo desafio-resposta a informação obtida através do canal de comunicação é insuficiente para duplicar a tag. O TID, que é único e vem gravado de fábrica numa memória não regravável, é a implementação pelo fabricante de um mecanismo anti-clonagem.

As organizações devem também implementar procedimentos de detecção de tags clonadas que se não evitam a clonagem permitem detectar os locais e datas da sua ocorrência e tomar as medidas tendentes à sua eliminação.

### 6.4.6 – Replay attack

Neste tipo de ataque é usada informação obtida anteriormente, durante uma sessão entre um leitor e uma tag legítimos. Para o efeito, é usada uma cópia da tag original ou é enviada para o leitor a informação obtida através de *eavesdropping* com o auxílio de um PC equipado com uma placa e antena apropriadas.

A forma de prevenir este ataque é impedir a obtenção da informação necessária à sua efectivação. Para isso, devem ser implementados protocolos de autenticação, encriptação da informação e tags que implementam mecanismos de protecção contra clonagem *by design*.

### 6.4.7 – Alteração de conteúdo

Se a tag é regravável, um atacante pode alterar ou eliminar a informação que contém, alterar as permissões de acesso de forma a rejeitar o acesso de entidades autorizadas.

Para evitar a alteração de conteúdos, o acesso à memória deve ser controlado por password e as permissões de escrita devem, também, ser protegidas através da colocação da tag num estado em que temporária ou permanentemente não permite gravação.

### 6.4.8 – Destruição da Tag

Este é um processo muito simples de tornar um sistema de RFID inoperativo. Desde quebrar a ligação da antena ao chip, aquecer a tag num microondas ou a destruição pura e simples com um martelo. Estes métodos são utilizados, essencialmente, quando as tags são usadas não só para identificação mas também para protecção contra roubo. Pessoas preocupadas com a invasão de privacidade que certos documentos que incorporam uma tag podem provocar podem também recorrer a estes métodos

### 6.4.9 – Denial of Service attack

Um ataque de DoS sobre uma implementação de RFID pode ser efectuado usando um dispositivo bloqueador que, como já foi referido, simula a existência de um número muito elevado de tags num ambiente, impossibilitando dessa forma, o normal funcionamento do leitor. Neste ataque, um dispositivo é usado com fins completamente diferentes daqueles para que foi criado. Uma outra forma de provocar DoS é criar ruído electromagnético na mesma frequência de funcionamento do sistema (*jamming*). Para as tag activas é possível torná-las inactivas interrogando-as durante longos períodos até que a sua bateria se descarregue. Os ataques através de bloqueadores ou congestionamento são de fácil detecção e localização, pelo que podem ser anulados. Podem ser implementados mecanismos de monitorização e aviso da sua ocorrência.

## 6.5 Outras Vulnerabilidades

Além das vulnerabilidades específicas das tags e do seu protocolo de comunicações com o leitor, estes elementos, fazem parte de uma infra-estrutura de RFID que inclui outros componentes além de leitores e tags e que usam outros protocolos e meios de comunicação.

A infra-estrutura de RFID está normalmente interligada à rede da organização a que pertence, para a qual envia a informação recebida das tags, da qual recebe a informação a enviar às tags, ou, de que necessita para manter o diálogo com as tags.

Estas infra-estruturas e respectivos equipamentos estão, também, sujeitas a todos os tipos de ataques existentes, tanto ao nível da rede, como ao nível dos respectivos sistemas, pelo que, as medidas necessárias à sua protecção devem ser implementadas e monitorizadas para que qualquer possível ataque possa ser evitado, a sua tentativa detectada ou os seus efeitos minimizados.

A implementação de medidas de prevenção, detecção e recuperação de ataques devem fazer parte da política geral da organização e devem ser objecto de análises e melhorias constantes.

**Tabela 6.1** – Ameaças e elementos do sistema RFID atacado [43]

| | Tag | Air interface | Reader | Network | Back end |
|---|---|---|---|---|---|
| Eavesdropping | • | • | | • | |
| Relay attack | | • | | | |
| Unauthorized tag reading | • | • | • | | |
| Tag cloning | • | • | | | |
| People tracking | • | • | | | |
| Replay attack | • | • | | | |
| Tag content changes | • | | | | |
| Malware | • | | • | | • |
| RFID system breakdown | | | | • | • |
| Tag destruction | • | | | | |
| Blocking | | • | | | |
| Jamming | | • | | | |
| Back-end attacks | | | | • | • |

**Tabela 6.2** – Ameaças a um sistema de RFID e potenciais consequências [43]

| Threat \ Consequence | Relay attack* | Tag cloning* | Tracking* | Replay attack* | Tag content changes | RFID system breakdown | Back-end attacks | Malware* | Unauthorized access to secret/private data | Spoofing access-control systems | Material damages | Theft of goods |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Eavesdropping | | × | • | • | | | | | × | • | • | • |
| Relay attack | | | | | | | | | | × | × | × |
| Unauthorized tag reading | × | × | × | • | • | | | | × | • | • | • |
| Tag cloning | | | | × | | | | | | × | • | • |
| Tracking | | | | | | | | | × | | | |
| Replay attack | | | | | | | | | × | × | • | • |
| Tag content changes | | | | | | • | • | × | • | × | × | × |
| RFID system breakdown | | | | | | | | | | × | × | × |
| Malware | | | | | × | × | × | | | • | × | × |
| Blocking | | | | | | × | | | | • | × | × |
| Physical tag destruction | | | | | | | | | | | × | × |
| Jamming | | | | | | × | | | | • | × | × |
| Back-end attacks | | | | | • | × | | × | × | × | × | × |

An "×" indicates direct relationship between the threat and its consequence; "•" indicates an indirect relationship. An "+" indicates consequences that are also threats.

## 6.6 Áreas de Investigação

O estado actual e as perspectivas de crescimento da tecnologia RFID provocam um dinamismo muito elevado de todos os intervenientes neste mercado e novas abordagens estão a ser efectuadas, tanto ao nível dos mecanismos de defesa, como das ameaças.

### 6.6.1 Novas Tendências dos Mecanismos de Defesa

Os resultados da investigação e suas tendências pode ser obtido analisando os anúncios que vão sendo efectuados:

- Investigadores da Universidade do Arcansas anunciaram em 19NOV09 o desenvolvimento de um método de detecção de falsas tags e que parte de um princípio completamente diferente na abordagem que efectuaram ao problema. Estes investigadores dirigiram o seu trabalho não há protecção do conteúdo da tag, mas às características físicas individuais da própria tag e descobriram que cada tag é única devido a diferenças de fabrico e reacções que apresenta. No seu trabalho eles mediram o estímulo mínimo a que uma tag responde a diferentes frequências. Usaram um algoritmo que enviava repetidamente um sinal do leitor à tag começando com um sinal de potência muito baixa e que ia sendo aumentando até obter uma resposta da tag. Variaram, então, a frequência desde 903 MHz até 927 MHz com incrementos de 2,4 MHz e reiniciaram o processo. As medições efectuadas revelaram que cada tag tem um limiar mínimo de resposta único nas diferentes frequências e que esse limiar é muito diferente mesmo entre tags do

mesmo fabricante e do mesmo modelo. Esta resposta é uma das várias características únicas de cada tag. Com as diversas características analisadas criaram aquilo a que chamaram *'Fingerprinting RFID Tags'*. Este método poderá permitir identificar com grande probabilidade cada tag e detectar os seus possíveis clones. Este método tem a grande vantagem de não usar os recursos de memória e computacionais da tag o que permite a sua aplicação a todos os tipos de tags; [44]

- A implementação de criptografia simétrica e assimétrica, o uso de funções de hash e de protocolos de autenticação em tags passivas indicam, também, que um grande investimento está a ser efectuado na segurança, integridade e privacidade da informação contida nas tags de menores recursos. O uso da criptografia é caracterizada pela existência de algoritmos conhecidos e globalmente aceites pelo que a sua implementação em tags de baixo custo pode aumentar em muito a confiança dos utilizadores nesta tecnologia, contudo as implementações efectuadas até à data resistem muito mal a ataques de força bruta, já que possuem chaves muito pequenas. [45]

### 6.6.2 Novas tendências dos Mecanismos de Ataque

As novas funcionalidades e capacidades que as tags de baixo custo apresentam e que permitem a implementação de novas medidas de segurança e privacidade permitem, também, o aparecimento de novas ameaças. O aparecimento de vários tipos de malware com origem na tag e que exploram as debilidades do middleware, que não foi em muitos casos projectado para resistir a ataques com esta origem, e que podem atacar toda a infra-estrutura da organização é uma nova fonte de preocupação. Embora os mecanismos usados não sejam novos, a sua origem na tag é recente. De entre essas ameaças destacam-se: [46]

- Buffer Overflow – Este ataque baseia-se no armazenamento de dados para além dos limites do buffer provocando, assim, um erro na execução do software e pode ser efectuado a partir de uma tag com capacidade muito limitada, já que o mesmo bloco pode ser enviado repetidas vezes até provocar o efeito pretendido;
- Injecção de Código Malicioso – Este ataque baseia-se na introdução de código malicioso no sistema a partir da tag. O código malicioso, tanto pode ser um vírus, como um verme que vai ser transmitido a outros componentes do sistema;
- Injecção de SQL – Este ataque baseia-se na execução de um comandos de sql a partir da informação lida em tags de capacidade muito limitada. O código de sql tanto pode afectar o conteúdo da base de dados, como lançar um comando de sistema como o shutdown.

# Capítulo 7

# Implementação de uma Infra-estrutura de RFID

Os procedimentos a observar na implementação de uma infra-estrutura de RFID, numa organização, não diferem muito dos utilizados na adopção de outras áreas tecnológicas.

Os objectivos, impactos e métricas a usar para avaliar o sucesso do projecto devem estar perfeitamente definidos, bem como, o montante de dinheiro e os meios humanos e materiais a alocar ao projecto, o tempo de duração do projecto, a possibilidade de expandir o projecto a outras áreas de actividade da organização e a capacidade de crescimento da tecnologia adoptada.

A compreensão das vantagens da tecnologia e o empenho na sua adopção pelos mais altos responsáveis da organização não podem ser menosprezados.

A criação de uma *checklist,* tão pormenorizada quanto possível, com a indicação de todos os pontos a abordar na implementação do projecto, respectivos custos, tempo, meios necessários e retorno esperado, deve ser efectuada.

A formação dos utilizadores e os manuais de instalação, configuração e operação devem também ser contemplados.

Os custos de manutenção dos equipamentos e de assistência à instalação devem também ser equacionados.

Dispõe a organização das competências necessárias e estão essas competências disponíveis para liderar, acompanhar e controlar o projecto?

Se estas condições se verificarem o processo pode ter início, caso contrário, deverá ser contratado um consultor externo para a auxiliar a organização nessa tarefa.

Após uma análise aos requisitos, aos meios necessários, ao impacto na actividade normal da empresa e aos benefícios esperados, se a conclusão for continuar com o projecto, deverá ser elaborado um caderno de encargos e efectuado o respectivo concurso, para o fornecimento dos diversos componentes que podem ser adquiridos a um único fornecedor num contrato

tipo ‘chave na mão’ ou efectuadas adjudicações parciais a diferentes entidades. Em qualquer das situações o fornecedor é um dos componentes fundamentais do processo.

A maximização do retorno do investimento deve estar sempre presente em qualquer projecto e deve ser quantificado antes do seu início, já que é a métrica final pela qual o projecto vai ser avaliado. Se os ganhos directos são facilmente mensuráveis os ganhos indirectos são subjectivos, pelo que um projecto não pode estar alavancado em ganhos indirectos.

Uma estreita colaboração entre o consultor externo, caso exista, os responsáveis da organização e outros intervenientes/interessados no processo deve ser estimulada e as respectivas competências perfeitamente definidas para evitar futuros conflitos.

## 7.1 Selecção de Fornecedores

Na selecção de fornecedores, além dos aspectos normais de dimensão, situação financeira e qualidade de serviço devemos ter em conta:

- Lista de referências – É importante determinar se nessa lista existem implementações de projectos idênticas ao nosso, em organizações da mesma área de actividade e de dimensão e meios semelhantes;
- Experiência efectiva em projectos de RFID. Esta experiência é tanto mais importante quanto menores forem as competências internas;
- Experiência na instalação dos equipamentos e/ou serviços que propõe;
- Integração da tecnologia proposta nos sistemas actuais;
- Formação;
- Garantia dos equipamentos e/ou serviços fornecidos;
- Tipo, nível e custos do suporte pós-venda/instalação;
- Adopção de standards, produtos homologados, arquitectura aberta e conformidade com a legislação local.

## 7.2 Selecção da Frequência

A tag e o leitor usam ondas rádio de uma determinada frequência para comunicarem entre si. A escolha da frequência vai afectar as performances do sistema em áreas como velocidade de transferência, alcance e absorção ou reflexão por determinados materiais, que podem ser críticos para a aplicação pretendida.

Outros serviços já instalados na organização, como serviços de comunicações rádio, televisão, telefones móveis e vigilância electrónica, devem ser tidos em conta para que não haja interferências entre os equipamentos instalados e os equipamentos a instalar, para que todos funcionem correctamente.

Os sistemas de RFID funcionam numa das quatro radiofrequências principais do espectro:

- Low Frequency (LF) – Esta gama de frequências estende-se dos 30KHz aos 300 KHz. Os sistemas de RFID, nesta gama de frequências, operam a 125 ou 135 KHz e possuem um alcance inferior a meio metro, velocidade de transferência inferior a 1 kbit/s, baixa interferência com o meio ambiente, muito bom comportamento na leitura de tags em objectos contendo líquidos e metais. São usadas tipicamente em controlo de acessos, identificação animal e imobilização de veículos;
- High Frequency (HF) – Esta gama de frequências estende-se dos 3Mhz aos 30 MHz. Os sistemas de RFID, nesta gama de frequências, operam a 13,56 MHz, que é a única frequência usada em RFID aceite em todo o mundo. Possuem um alcance inferior a dois metros, velocidade de transferência de aproximadamente 25 kbit/s e bom comportamento na leitura de tags em objectos contendo líquidos ou metais. São usadas tipicamente em smart cards, localização e identificação de artigos, livros e controlo de bagagens;
- Ultra High Frequency (UHF) – Esta frequência estende-se dos 300 MHz aos 3 GHz. Os sistemas de RFID, nesta gama de frequências, operam a 433 MHz e, em qualquer frequência, entre os 860 e os 960 MHz dependendo da legislação da região ou país. Possuem um alcance da ordem dos dez metros, velocidade de transferência de aproximadamente 30kbits/s, está sujeita a interferências com os muitos dispositivos que funcionam nesta gama de frequências, fraco comportamento com líquidos e metais e problemas de portabilidade devido à regulamentação específica de cada país. São usadas tipicamente na identificação e localização de artigos, gestão de armazéns e inventários e pagamentos automáticos de portagens;
- Microondas – Esta frequência estende-se de 1 GHz a 300 GHz. Os sistemas de RFID, nesta gama de frequências, operam a 2,45 GHze 5,8 GHz. Possuem uma velocidade de transferência de aproximadamente 100 Kits/s, boa distância de leitura e mau comportamento perante água ou metal. Sujeita a interferência de equipamentos de WLAN que adoptam os standards 802.11x, são usadas tipicamente na identificação de veículos e pagamento automático de portagens.

## 7.3 Selecção de Tags

Na escolha das tags a usar por uma aplicação devem ser considerados alguns aspectos tais como:

- Tipo de Tag – Activa, passiva, semi-activa ou semi-passiva;
- Tipo de Memória – Read Only, Write One Read Many ou Read Write, dependendo das necessidades da aplicação, da quantidade de informação a ser guardada e das necessidades de actualização dessa informação;
- Tamanho, forma e material de suporte da tag;

- Sistema de fixação/colagem;
- Conformidade com standards e legislações, de forma a permitir a sua aceitação e interoperabilidade com outros sistemas;
- Alcance – Distância a que a tag pode ser lida. Este parâmetro deve satisfazer as necessidades da aplicação e não deve ser maximizado evitando assim possíveis interferências;
- Eficiência de leitura – Razão entre o número de leituras correctas e o número total de leituras efectuadas. Este parâmetro é crítico, já que o objectivo é obter uma leitura válida de 100% das tags e dele depende grande parte do sucesso da implementação;
- Capacidade de Memória – De acordo com as necessidades da aplicação. Maior capacidade de memória pode permitir uma maior flexibilidade, mas aumenta em muito o preço da tag e, como a quantidade de tags a usar é normalmente muito elevada, os custos aumentam muito;
- Segurança – O nível de segurança fornecido pela tag deve estar de acordo com as necessidades da aplicação de forma a impedir a clonagem e garantir a confidencialidade e integridade dos dados sempre que necessário;
- Compatibilidade entre a tag, o objecto em que vai ser colocada e o ambiente em que vai ser usada;
- Quantidade de tags gastas por ano;
- Tempo de vida útil esperado e condições de armazenamento.

As tags são aplicadas em objectos com diferentes características electromagnéticas e nas mais diversas localizações. Com a finalidade de melhorar as comunicações entre as tags e os leitores, os fabricantes de tags têm investido meios muito consideráveis no desenho das respectivas antenas, pelo que um dos parâmetros mais importantes a considerar na escolha da tag é a sua antena.

## 7.4 Selecção de Leitores

Na escolha dos leitores a usar por uma aplicação devem ser considerados alguns aspectos tais como:

- Tipos de leitores a usar: fixos, móveis e handheld;
- A robustez do leitor em relação às condições em que vai funcionar deve ser analisada principalmente nos leitores móveis e handheld, já que estão sujeitos a vibrações, quedas e outros embates pelo que esta característica pode ser crítica;
- Confirmar que o leitor funciona na gama de frequência seleccionada, se está homologado para essa frequência e cumpre a legislação do país em que vai ser usado;

- Confirmar que o leitor funciona em Dense Reader Mode ou multi-leitor de acordo com as necessidades da implementação;
- Analisar os interfaces disponíveis para ligação à rede ou a outros dispositivos. Os leitores, dependendo do tipo, apresentam vários interfaces como Ethernet, Serie, USB, Wireless, etc;
- Os leitores fixos podem possuir duas, quatro ou oito portas de ligação de antenas. A escolha do número de portas vai permitir uma maior flexibilidade na definição da área de cobertura do leitor;
- O leitor deve permitir efectuar a actualização do seu firmware/software de uma forma simples e gratuita;
- De acordo com a aplicação pode haver necessidade de monitorização e gestão remota dos leitores, pelo que esta possibilidade deverá ser considerada.

## 7.5 Selecção de Antenas

Os leitores e as tags usam antenas para comunicar que podem ser de vários tipos, possuir diversas orientações e polarizações e serem fabricadas em diversos materiais.

Na selecção das antenas dos leitores, o tipo de leitor (fixo, móvel ou handheld) deve ser tido em conta. Outros factores a ter em conta são o ambiente e o local onde a antena vai ser instalada, dado o impacto que vão ter nas performances e tempo de vida das antenas.

Os tipos de antenas mais usados em RFID são:

- Dipolo – É a antena mais simples e prática. É constituída por um condutor eléctrico rectilíneo dividido ao meio. As duas extremidades centrais constituem os dois pólos. O comprimento do dipolo é função do comprimento de onda que se deseja captar. Muitas tags EPC Gen 2 usam como antena um dipolo de meio comprimento de onda (λ/2);
- Monopolo ou Antena Vertical – A mais usada é a λ/4 e pode ser obtida a partir do dipolo de λ/2 substituindo metade do dipolo por uma superfície condutora chamada plano de terra de onde deriva a sua polarização;
- Antena Omnidireccional – É uma antena que radia uniformemente num plano;
- Antena Helicoidal – É uma antena em que o elemento condutor é enrolado em forma de hélice. Estas antenas são usadas para localização animal, em situações em que o emissor ou o receptor não podem ser facilmente controlados ou a polarização varia com o tempo;
- Antenas Múltiplas – Um leitor pode estar ligada a várias antenas. O uso de várias antenas aumenta e melhora a cobertura do espaço, contudo o seu uso implica um sistema de multiplexagem, já que apenas uma antena pode ser utilizada de cada vez.

Antenas polarizadas linearmente emitem um feixe muito estreito o que aumenta o seu alcance. Contudo, a polarização linear da antena do leitor é sensível à orientação da tag, pelo que as duas antenas devem estar alinhadas. Este tipo de antena é útil para ler tags, cuja orientação é fixa e previsível, pelo que o alinhamento pode ser efectuado e, desta forma, maximizar a eficiência de leitura.

Antenas polarizadas circularmente imitem um feixe mais largo mas de menor alcance. A polarização circular da antena do leitor é menos sensível à orientação da antena da tag pelo que este tipo de polarização deve ser usado quando a orientação da tag é desconhecida.

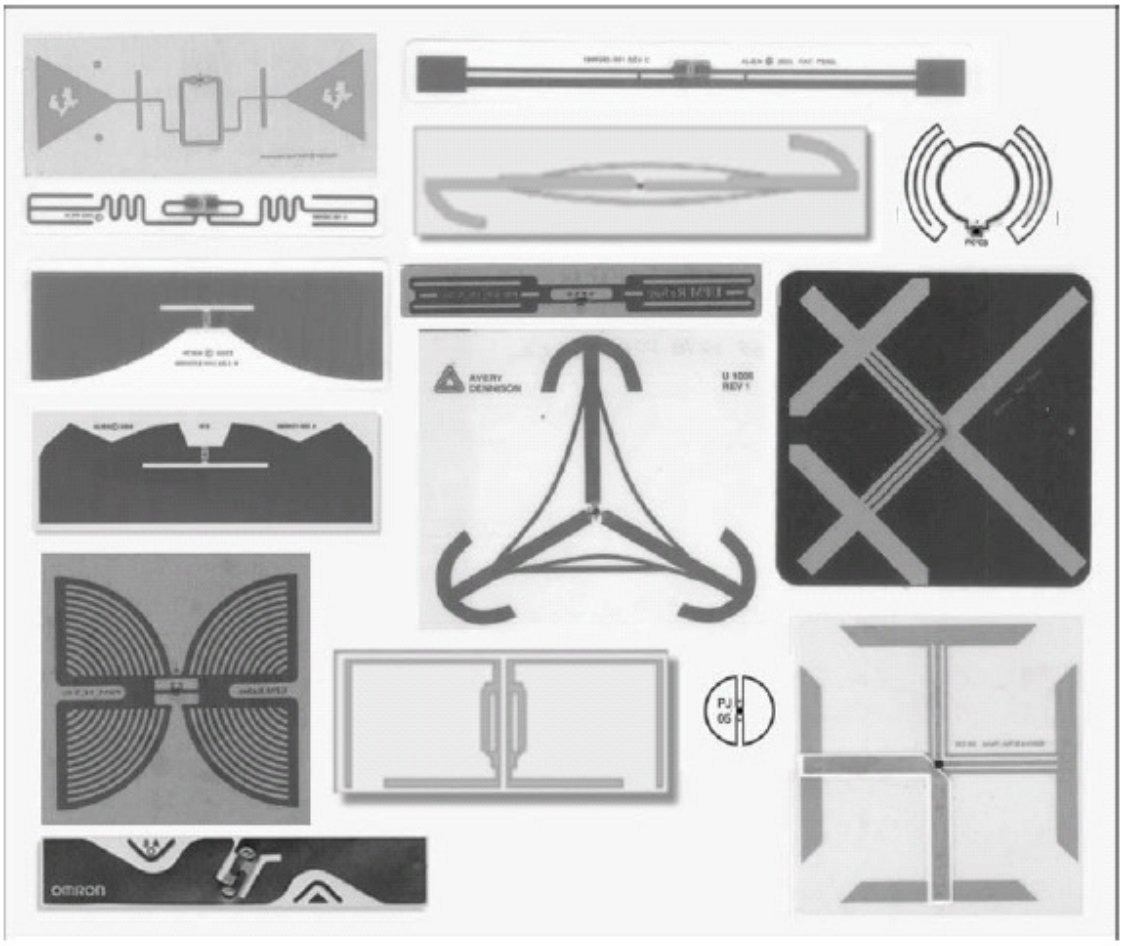


**Figura 7.1** – Diferentes desenhos de antenas de tags (sem escala) [47]

## 7.6 Site Survey

O principal objectivo do site survey é garantir que as zonas de leitura das tags funcionem correctamente, com boa performance e sem interferência nos serviços existentes. Se forem usadas equipamentos com ligações sem fios deverá, também, ser utilizado para identificar a colocação dos AP's (Access points) e respectiva cobertura das instalações.

Um levantamento dos equipamentos existentes no local deve ser efectuado para detectar possíveis fontes de ruído e interferência nas comunicações, determinar a quantidade, tipo e localização das antenas, leitores e outros equipamentos a instalar.

Além das suas características próprias, não podemos esquecer que a infra-estrutura de RFID se deve interligar com a já existente e que vai, também, utilizar partes dessa estrutura como a rede Ethernet, com ou sem fios, e a rede eléctrica.

Na planta das instalações devem ser identificados os equipamentos existentes e respectivas características electromagnéticas.

Os principais aspectos a analisar no site survey são:

- Condições Ambientais – Ambientes corrosivos, elevadas temperaturas ou grande humidade podem danificar as tags e os equipamentos usados;
- Equipamentos – A existência de equipamentos como motores, sistemas de comunicações rádio, fornos de microondas, sistemas industriais de arrefecimento e outros, são potenciais fontes de ruído e interferência electromagnética;
- Estruturas que possam absorver ou reflectir os sinais de RF.

Com recurso a um analisador de espectro devem ser identificadas e caracterizadas as fontes de possíveis interferências.

A recolha da informação necessária para uma efectiva caracterização das condições de funcionamento deve decorrer durante um período relativamente amplo de tempo (24 a 48 horas), durante o horário normal de funcionamento, de forma que todos os equipamentos sejam usados, já que num ambiente industrial há equipamentos que raramente são ligados/desligados e que nessas situações podem provocar consequências inesperadas.

Com o conhecimento efectivo das condições de funcionamento devem ser decididas as características, quantidades e localizações dos novos equipamentos a instalar.

Após a instalação dos novos equipamentos devem ser avaliadas as suas condições de funcionamento, possíveis alterações introduzidas no funcionamento de outros equipamentos e efectuados os ajustes necessários a um bom funcionamento de todos os sistemas.

Os equipamentos a usar no site survey são normalmente:

- Analisador de espectro;
- Tripés;
- Antenas dipolo de ½ ou ¼ de comprimento de onda;
- Placas de terra (Ground plates);
- Computador portátil.

## 7.7 Outros Elementos

Se a opção de usar smart labels for tomada, um especial cuidado deve ser posto na escolha das impressoras/codificadoras que passam a constituir um ponto crítico de todo o processo. Deve ser assegurada a compatibilidade entre a impressora, o tipo e dimensões da tag

seleccionada. As impressoras devem efectuar testes que confirmem o estado da tag e validem a informação nela gravada.

O uso de smart labels levanta o problema da sua aplicação pelo que o uso de aplicadores automáticos deve ser equacionado, já que garantem uma colocação e orientação da tag muito mais precisa que uma aplicação manual.

A implementação de um sistema de RFID, numa organização, implica a instalação de equipamentos que precisam de ser alimentados, interligados entre si e ligados à rede existente.

Alguns equipamentos podem ser alimentados através da rede Ethernet (PoE) e esta possibilidade deve ser analisada, principalmente, no caso de antenas montadas em locais de difícil acesso. O ambiente fabril e a sensibilidade de alguns equipamentos aconselham o uso de circuitos de alimentação independentes com tomadas protegidas por encravamento para evitar o seu uso indevido e protecção da alimentação através do uso de UPS devidamente dimensionada.

Estas situações devem ser devidamente analisadas e os respectivos custos ponderados.

## 7.8 Integração da RFID na Organização

Um sistema de RFID é uma tecnologia automática de aquisição de dados. Após a aquisição dos dados é preciso resolver a questão fundamental do sistema, que é, a utilização a dar aos dados capturados.

O sistema de RFID não é, na generalidade das implementações, uma ilha dentro da organização em que foi implementado, mas um componente de um todo coerente e deve contribuir para uma melhor gestão dos recursos disponíveis.

Os sistemas de RFID são potenciais geradores de uma quantidade de informação muito elevada e um cuidado muito especial deve ser posto na selecção da informação a processar e guardar, de modo a não sobrecarregar o sistema com uma enorme quantidade de dados de utilidade duvidosa e cujo benefício, para a organização, é mínimo.

Os dados fornecidos pelos leitores devem ser filtrados e agregados de forma a evitar duplicações e eliminar dados que não fazem parte do processo. Só os dados considerados relevantes devem ser tratados, integrados e disponibilizados pelos sistemas de gestão. Quanto mais próxima da fonte esta filtragem for efectuada, melhor, já que o seu impacto no sistema é minimizado.

Estas funções são normalmente efectuadas pelo middleware, pelo que um cuidado especial deve existir na sua selecção, instalação e configuração.

Devido ao grande volume de informação gerado pelo sistema de RFID, uma degradação dos tempos de resposta do sistema de gestão da organização pode ocorrer e, desta forma, a necessidade de upgrades das capacidades de armazenamento, backup, processamento e tráfego devem ser equacionadas.

# Capítulo 8

# RFID da Produção à Expedição

## 8.1 Breve Caracterização do Sector

A grande maioria das empresas do sector agro-industrial introduz no mercado grandes quantidades de um número muito limitado de produtos e não tem uma política activa de venda ao consumidor final. A produção é introduzida no mercado nacional através das centrais de compras e distribuidores regionais e no mercado internacional através de representantes nos diversos países.

A gestão de stocks de produtos acabados caracteriza-se por uma situação mista de produção para stock e produção por encomenda.

A produção por encomenda destina-se, normalmente, ao mercado internacional para que a mercadoria respeite a legislação específica de cada país e os requisitos do importador ou a satisfazer a política de implantação de marcas próprias levadas a cabo pelos grandes grupos de distribuição alimentar, cujo peso tem crescido nos últimos anos.

Além do exposto anteriormente, a imposição pela generalidade dos grupos de distribuição alimentar aos seus fornecedores da implementação de sistemas de EDI (Ectronic Data Interchange), a obrigatoriedade de implementação do sistema HACCP (Hazard Analisys and Critical Control Points) e as exigências dos sistemas de garantia da qualidade têm levado a alterações no planeamento da produção e na gestão de stocks das matéria-primas, dos produtos acabados e dos materiais subsidiários.

## 8.2 Metodologia de Identificação

O processo de identificação das mercadorias tem origem na linha de produção. Ao longo da linha, os itens individuais são normalmente identificados com um código de barras EAN – 13 (GTIN), com uma identificação do lote produzido e respectivo prazo de validade. Os itens individuais são, depois, agrupados em caixas ou outras embalagens que são identificadas

através de um código de barras EAN-14 ou ITF-14. As caixas são normalmente agrupadas numa palete que é identificada através de um código de barras EAN-128, cuja última linha contém o SSCC da palete. Além do código SSCC, a etiqueta colada na palete pode conter outros dados como o código do artigo, quantidade e lote tanto sob a forma de código de barras como em formato humanamente legível.

A palete é a unidade normalmente utilizada para armazenamento e expedição de mercadorias, dada a facilidade com que pode ser manipulada pelos equipamentos de manuseamento de cargas e à relativa standardização.

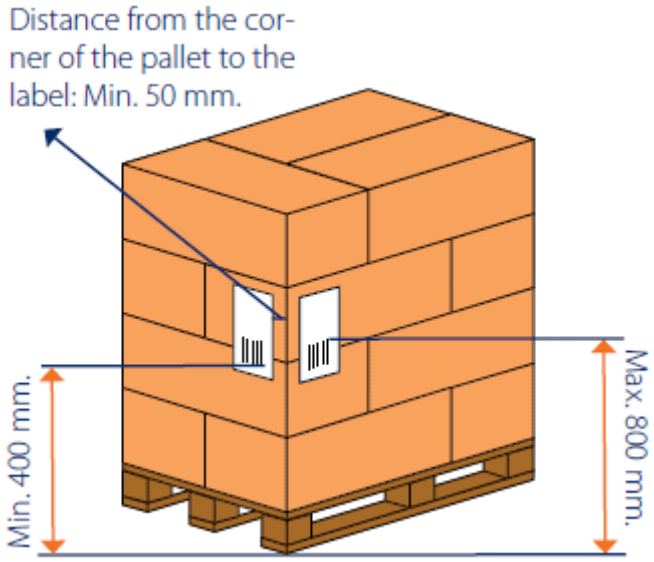


**Figura 8.1** – Colocação das etiquetas GS1-128 na palete [48]

## 8.3 Modo de Funcionamento

O processo administrativo tem o seu início com a aceitação da encomenda do cliente pelo fornecedor. Dependendo dos produtos encomendados e dos stocks existentes a nível de produtos acabados, das matérias-primas e dos materiais subsidiários são despoletados os procedimentos necessários à satisfação da encomenda aceite.

A mercadoria é normalmente entregue a uma transportadora que a leva para uma plataforma logística do cliente onde é controlada. Posteriormente, as mercadorias são introduzidas no consumo através dos diferentes pontos de venda.

Em todo o processo só dois documentos são normalmente impressos, a guia de carga e a guia de transporte ou a guia de remessa.

A guia de carga destina-se ao operador do armazém para que possa seleccionar e carregar as mercadorias.

A guia de transporte ou de remessa é o documento que legalmente deve acompanhar a mercadoria, desde o armazém de carga até ao armazém de descarga, e que é entregue ao

transportador. Uma cópia assinada pelo motorista serve de comprovativo da entrega da mercadoria pelo fornecedor.

Este modo de operação é o resultado da evolução de toda a cadeia de abastecimento e da adopção de sistemas de EDI que hoje controlam, de forma automática, as transacções comerciais entre empresas e tem como consequência a não-aceitação de qualquer diferença entre os diversos documentos intervenientes no processo:

- Encomenda de Cliente/Encomenda aceite;
- Guia de Carga (documento interno);
- Guia de Transporte/Guia de Remessa;
- Factura.

Sempre que é detectada uma diferença entre qualquer dos documentos envolvidos é aberto um processo de não conformidade de resolução muito demorada e que tem como consequência o não pagamento da respectiva factura até que todo o processo seja devidamente esclarecido e corrigido.

À relativa complexidade do processo de fornecimento das mercadorias acresce o modo de funcionamento de cada cliente, os dados necessários ao seu ERP (Enterprise Resource Planning) e à implementação de EDI efectuada. O uso de diferentes aplicações e implementações de software, pelos diversos grupos presentes na grande distribuição em Portugal, e o fraco poder negocial da generalidade das empresas do sector agro-industrial face às centrais de compras, já que são muito poucas as que possuem um produto de difícil substituição no mercado, acabam por dar origem a processos administrativos pouco standardizados.

### 8.3.1 – Expedição da Mercadoria

A guia de carga é um documento que identifica os artigos a carregar, respectivas quantidades e lotes e que é entregue ao operador do armazém para que proceda à expedição das respectivas mercadorias.

Na posse da guia de carga o operador do armazém selecciona os artigos a carregar, normalmente baseado na sua experiência, conhecimento das embalagens e na organização do armazém.

O recurso ao controlo das mercadorias através de terminais portáteis com leitura do código de barras de identificação da palete, pelo operador do empilhador, é um procedimento moroso e que obriga à existência de uma infra-estrutura de comunicações, hardware e software que suporte esse procedimento, cujo custo de implementação se aproxima do custo de uma solução de RFID e que não dá qualquer garantia de que o que foi lido foi efectivamente carregado.

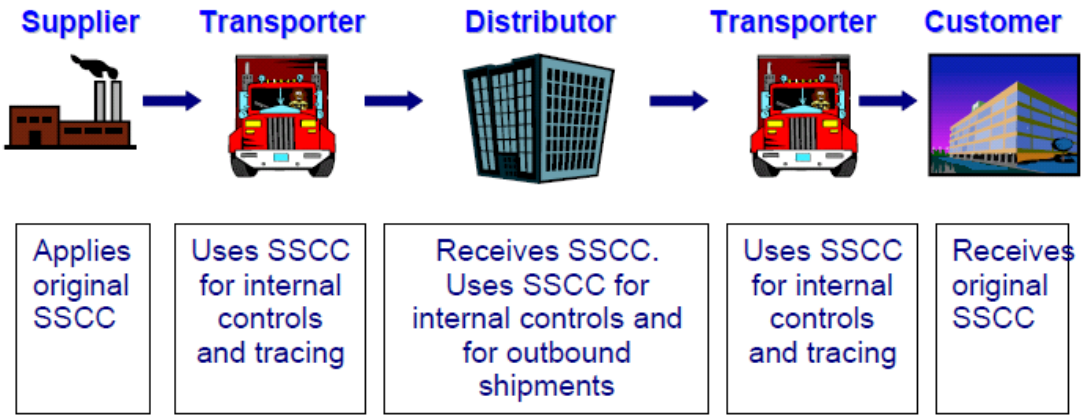


**Figura 8.2** – SSCC na cadeia de abastecimento [49]

## 8.4 Principais Vulnerabilidades do Sistema Actual

A generalidade dos sistemas actualmente usados é baseada em procedimentos operativos exclusivamente manuais ou com recurso ao código de barras e apresentam as seguintes vulnerabilidades:

- Movimentação indevida de mercadorias;
- Troca de mercadorias na expedição;
- Troca de lotes na expedição;
- Quantidades erradas nas mercadorias expedidas;
- Troca de destinatários;
- Desaparecimento de mercadorias;
- Erros no inventário;
- Controlo deficiente de stocks;
- Dificuldades na rastreabilidade das mercadorias.

Algumas destas vulnerabilidades, que ainda há pouco tempo não tinham qualquer relevância ou eram de fácil resolução, são hoje um foco de conflitos, tanto internos como externos, devido à forma como a legislação e toda a cadeia de abastecimento têm vindo a evoluir. A identificação dos lotes fornecidos é hoje um requisito para uma efectiva rastreabilidade e, cuja não implementação pode ter consequências graves para a empresa devido às consequências legais que pode provocar.

Algumas das vulnerabilidades apresentadas foram objectos de várias tentativas de resolução com a implementação de novos procedimentos dos quais se destacam:

- Adopções de procedimentos operativos, quanto ao manuseamento de mercadorias, consignados nos manuais do sistema de garantia da qualidade, adoptados pela generalidade das empresas do sector;
- Reorganização dos processos de armazenamento. Estes procedimentos têm em vista um melhor e mais racional aproveitamento do espaço de armazenamento, um bem cada vez mais caro e escasso, com a diferenciação das áreas de armaze-

namento por artigo e lote, com diversos tipos de caracterização e diferenciação das áreas de armazenamento;

- A separação das diferentes áreas de armazenamento por artigo, lote e condições de manuseamento, pode ser efectuada, com a utilização de áreas fixas para artigos, a sua subdivisão por lote e possibilidade de manuseamento, com a respectiva identificação e caracterização efectuada por painéis, fitas coloridas ou outros meios de identificação, que separam os diversos artigos pelas suas características e que podem fornecer dados preciosos ao sistema de gestão de stocks, mas não podemos esquecer que, um dos pontos críticos da gestão de stocks de produtos acabados na área agro-industrial é o seu prazo de validade. Este condicionalismo leva a que o sistema de gestão de stocks de produtos acabados seja o FIFO (First In First Out) quando o fornecimento pode ser feito através do stock de produto acabado existente. Este procedimento deve ser implementado também, na selecção da matéria-prima e dos materiais subsidiários, na generalidade dos casos, já que a validade do produto final é o prazo de validade do seu componente com menor prazo de validade, o que implica uma estrutura de gestão de stocks para a qual as generalidades das PME´s nacionais não estão sensibilizadas nem preparadas para implementar.

## 8.5 Proposta de Solução

A tecnologia de RFID veio proporcionar uma nova abordagem a todo o controlo de stocks dentro de uma organização, quer na vertente das existências de produtos acabados em armazém, quer na gestão dos stocks de matérias-primas e materiais subsidiários e em todos os processos de entrada, saída e movimentação, dentro dos respectivos armazéns.

A abordagem a efectuar baseia-se numa tag Smart Label, UHF EPC Class 1 Gen 2, com o recurso a uma infra-estrutura de RFID e pretende efectuar um controlo automático das entradas e saídas de mercadorias num armazém de produtos acabados em tempo real.

Esta abordagem, apesar de parecer minimalista, tem a grande vantagem de poder preparar a organização para procedimentos que podem aparecer por imposição externa e proporcionar grandes ganhos no controlo interno de stocks.

Numa empresa produtora, a origem do produto acabado são as suas linhas de produção. As saídas do armazém de produtos acabados são a expedição das mercadorias para os seus clientes. Entre estes dois pontos, as mercadorias podem sofrer um conjunto de movimentações dentro do armazém, normalmente provocadas pela necessidade de gestão de espaço, que introduz novas variáveis no processamento das mercadorias, efectuado muitas vezes de uma forma mecânica pelos operadores dos equipamentos de manuseamento de cargas, baseado na sua experiência e no conhecimento empírico da situação.

A etiqueta GS1-128, actualmente utilizada pela generalidade das empresas e que se destina essencialmente a uso externo, deve ser substituída por uma smart label, EPC Class 1 Gen 2, de dimensões idênticas, (A5 ou A6), com a informação já hoje fornecida e com a  o SSCC da palete gravado na tag.

Além do SSCC, outras informações podem ser gravadas na tag, dependendo das necessidades da organização, do nível de informação pretendido e do tempo de acesso a essa informação desejado.

A opção, quanto às capacidades de memória da tag e informação nela contida, pode ser deixada para uma fase posterior se todo o processo for projectado com essa perspectiva, já que o custo a considerar é unicamente o da tag e, entretanto, todo o processo foi validado.

### 8.5.1 – Entrada em Stock da Produção

Partindo do lay-out estilizado de uma fábrica vamos agora analisar os procedimentos a efectuar.

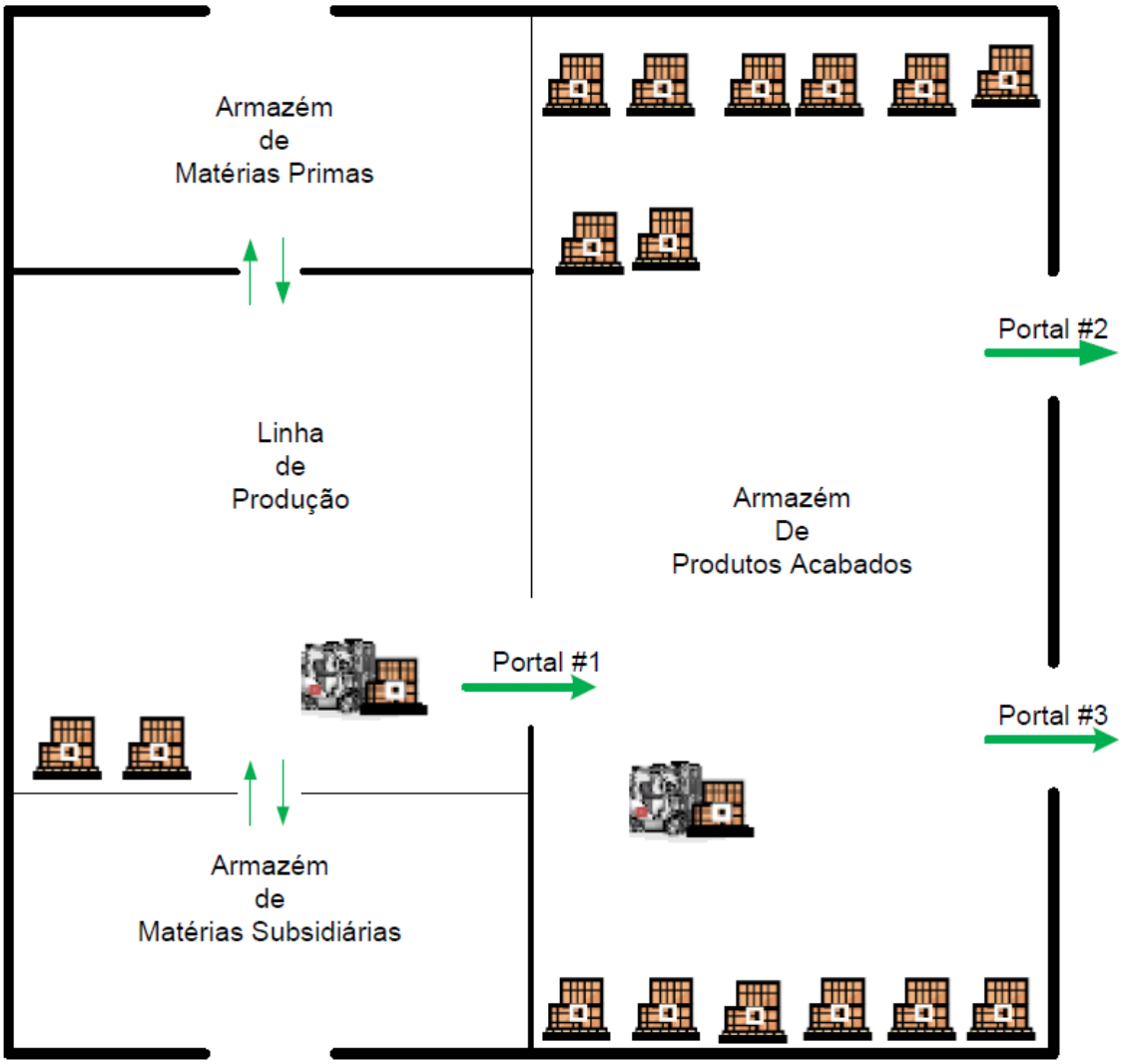


**Figura 8.3** – Lay-out estilizado de uma unidade produtiva

No fim da linha de produção são impressas duas smat labels EPC  Class 1 Gen 2 iguais, com o mesmo SSCC e que são coladas na palete conforme as recomendações da GS1. Este procedimento destina-se a que pelo menos uma das etiqueta esteja sempre visível e permita uma boa leitura de, pelo menos, uma das smart labels. Além do SSCC, a etiqueta pode conter outras informações, mas a chave primária de acesso ao sistema informático é o SSCC.

A localização e a precisão com que as etiquetas são colocadas devem ser devidamente ponderadas, pois estes factores são importantes para que a taxa de leitura seja a pretendida (100%).

Cada empilhador deve possui uma tag com o seu GIAI colada no seu lado direito. Esta tag vai servir para identificar o empilhador/operador e o sentido do movimento quando o empilhador passar num portal. Em cada portal só serão consideradas leituras válidas as que englobarem a leitura da tag do empilhador e a leitura da tag da palete.

O sentido do movimento é dado pela antena (direita ou esquerda) que efectua a leitura da tag do empilhador. A possibilidade de leitura simultânea da tag do empilhador pelas duas antenas do portal deve ser testada, mas devido ao material de que grande parte do empilhador é feito, a uma escolha correcta da tag e a um correcto ajuste das antenas essa possibilidade pode ser eliminada. Caso os procedimentos indicados não resultem, devem ser implementados outros procedimentos de detecção do sentido do movimento como sensores ópticos, de pressão ou outros.


**Figura 8.4** – Empilhador com tag GIAI do lado direito – Permite identificar o sentido

O posto de trabalho existente na linha de produção manda efectuar a impressão das etiquetas. Esta ocorrência é comunicada ao servidor/controlador do portal da linha estando as etiquetas num estado 'Aguarda Confirmação'.

A passagem do empilhador com a palete no Portal #1 dá origem a um conjunto de eventos que vão ser capturados e tratados de forma a validar a informação obtida e despoletar os procedimentos respectivos de acordo com as regras do negócio. A leitura da tag do empilhador e de pelo menos uma das tags da palete constituem a base do procedimento de entrada em stock dos produtos acabados. Além destes eventos outros podem ocorrer com a ajuda de

sensores que activam os leitores, controlam semáforos, sirenes ou outros dispositivos auxiliares e que se destinam a fornecer, aos operadores, informação sobre o procedimento efectuado. Se o processo for considerado correcto é confirmada a entrada em stock da palete e o estado da tag no sistema passa de 'Aguarda Confirmação' a 'Confirmada'.

**Tabela 8.1** – Eventos no Portal #1

| **Portal** | Antena L | Antena R | Estado | Empilhador | Palete | Leitura | Data/Hora |
|---|---|---|---|---|---|---|---|
| **#1** | | | Aguarda | | 001001 | | 2010:05:30-09:08:08 |
| **#1** | Sim | Sim | Confirmada | 00002 | 001003 | Sim | 2010:05:30-09:10:10 |
| **#1** | Não | Sim | Confirmada | 00001 | 001002 | Sim | 2010:05:30-09:14:15 |
| **#1** | Sim | Sim | Confirmada | 00001 | 001005 | Sim | 2010:05:30-09:18:33 |

Os eventos capturados no portal #1 são tratados pelo software de gestão de eventos que os vai filtrar, validar e enviar as informações necessárias ao ERP/WMS para que sejam processadas. O processamento dos dados enviados pelo gestor de eventos tem como consequência a entrada em stok das paletes: 001003, 001002 e 001005.

Na base de dados do sistema deve ser gravado um registo com os seguintes dados mínimos por palete:

- Código da palete (SSCC);
- Data e Hora da criação da etiqueta da palete;
- Ordem de fabrico que originou a palete;
- Artigo contido na palete;
- Quantidade do artigo contida na palete. Só paletes monoproduto;
- Lote de fabrico.
- Data e hora da entrada em stock (confirmação);
- Código do empilhador.

Esta informação vai servir para facilitar as interligações a estabelecer, quer a montante quer a jusante deste processo, de acordo com as regras do negócio.

### 8.5.2 – Saída de Stock - Expedição

O responsável pela expedição das mercadorias selecciona as encomendas a satisfazer, os artigos, quantidades e lotes a fornecer e imprime as respectivas guias de carga e transporte/remessa.

Este procedimento tem subjacente um controlo on-line dos stocks de produtos acabados. Qualquer diferença entre as existências do inventário informático e as existências reais no

armazém é um foco potencial de conflitos, razão pela qual o controlo de stocks é uma das áreas prioritárias da gestão.

A guia de carga é entregue ao operador do empilhador com indicação do cais de carga em que deve ser efectuada a entrega das mercadorias e o respectivo procedimento iniciado.

A indicação do cais de carga serve para evitar que o empilhador possa entregar mercadoria no cais errado, já que, um empilhador só pode carregar mercadoria para uma guia enquanto o respectivo processo estiver em aberto.

A passagem do empilhador pelo portal despoleta a leitura das tags do empilhador e da palete. Os eventos capturados no portal são filtrados, validados e registados. Os dados gerados por estes eventos são enviados ao ERP que os integra nas respectivas aplicações.

Os resultados deste processo são transmitidos ao operador através de mecanismos de aviso como semáforos, cancelas, sirenes, monitores ou outros.

O controlo entre o previsto e o realizado é efectuado on-line e, se for detectada qualquer diferença, são automaticamente despoletados os respectivos procedimentos de correcção.

Com a finalização do processo de carga pode ser enviado por EDI um ASN (Advance Shipping Notice) para os respectivos interessados com todos os detalhes da mercadoria expedida podendo estes preparar a sua recepção on-line.

### 8.5.3 – Outros movimentos no Stock

Devem ser implementados procedimentos que contemplem as seguintes situações:

- Entrada de mercadorias por devolução;
- Saída de mercadorias por quebras/perdas no manuseamento e que podem dar origem a paletes incompletas;
- Apesar de uma palete completa comportar uma quantidade fixa de um determinado artigo as linhas de produção produzem, muitas vezes, paletes incompletas com o resto da produção que não chega para completar uma palete;
- Saída de mercadoria por desagregação da palete. Apesar do procedimento normal ser o fornecimento de paletes completas, às vezes são fornecidas quantidades diferentes.

### 8.5.4 – Análise de Logs

Uma análise dos logs dos portais deve ser efectuada, principalmente, na fase de teste e nos primeiros tempos de implementação, já que ela permite obter muita informação sobre os procedimentos adoptados e detectar possíveis erros, estrangulamentos e pontos críticos. Com base na informação obtida podem ser efectuadas as correcções necessárias e introduzidas novas funcionalidades e melhorias a todo o sistema.

**Tabela 8.2** – Log de Eventos

| Seq | SSCC | Data-Hora | P#1 | P#2 | P#3 | Emp | Stock | Status | Confer |
|---|---|---|---|---|---|---|---|---|---|
| 001 | 001023 | 2010:05:20-9:00:00 | X | | | 00001 | Entrada | OK | OK |
| 002 | 001024 | | | | | | | Aguarda | |
| 003 | 001000 | 2010:05:20-9:03:00 | | X | | 00002 | Saída | OK | OK |
| 004 | 000930 | 2010:05:20-9:03:33 | | | X | 00001 | Saída | OK | OK |
| 005 | 001024 | 2010:05:20-9:05:00 | X | | | 00001 | Entrada | **ERRO** | **ERRO** |
| 006 | 000750 | 2010:05:20-9:05:00 | | X | | 00002 | Saída | | OK |
| 007 | 000888 | 2010:05:20-9:07:00 | | X | | 00002 | Saída | **ERRO** | OK |

Algumas das conclusões que podemos tirar da análise do log apresentado são:

- Seq 1 – Ocorreu uma entrada em armazém da palete 001023 efectuada pelo empilhador 00001;
- Seq 2 – A etiqueta 001024 já foi impressa;
- Seq 3 – Ocorreu uma saída de stock da palete 001000 no Portal #2 efectuada pelo empilhador 00002;
- Seq 4 - Ocorreu uma saída de stock da palete 000930 no Portal #3 efectuada pelo empilhador 00001;
- Seq 5 – Ocorreu um movimento indevido no Portal #1 com a palete 001024, efectuado pelo empilhador 00001 e que ainda não foi justificado. Este movimento pode ter sido provocado porque o operador deu entrada da palete em marcha atrás. Este movimento provoca uma diferença entre o inventário físico e o informático;
- Seq 6 - Ocorreu uma saída de stock da palete 000750 no Portal #2 efectuada pelo empilhador 00002;
- Seq 7 – Foi detectado um movimento indevido no Portal #2, efectuado pelo empilhador 00002 e que já foi resolvido. O movimento indevido pode ter sido provocado porque aquele artigo não se encontrava no stock, não fazia parte daquela guia de carga, a quantidade total daquele artigo já tinha sido carregada ou aquela palete não podia ser movimentada.

Além do controlo da movimentação das paletes, a movimentação dos empilhadores deve ser também controlada de forma a evitar trocas nos cais de carga.

Todas as situações devem ser previstas e tratadas ao nível do respectivo componente, seja ele físico ou lógico. Uma boa compreensão das regras do negócio, dos procedimentos

implementados e um bom trabalho de equipa entre as diferentes entidades envolvidas na implementação do projecto são fundamentais para o respectivo sucesso.

A escolha do responsável pelo projecto é, normalmente, um ponto crítico de uma implementação, sendo muitas vezes mais importantes as suas capacidades de coordenação e liderança que os conhecimentos técnicos.

## 8.6 Portal RFID

Um portal RFID é uma estrutura fixa constituída por um leitor fixo, antenas e sensores cuja função é captar eventos que, depois de devidamente tratados, permitem identificar as mercadorias que transitaram por esse portal e detectar possíveis violações das regras do negócio.

Todos os equipamentos constituintes do portal devem ser seleccionados de forma a constituírem um todo coerente e optimizar as condições de funcionamento.

Uma das características de funcionamento que tem que ser garantida é a taxa de leitura, que deve ser de 100%, e mecanismos de detecção da ocorrência de não leitura devem ser implementados. O recurso a sensores complementares deve ser equacionado para que a redundância do sistema seja garantida.

Os sensores, além de fornecerem informações complementares às do leitor, servem também para despoletar mecanismos de aviso aos operadores dos equipamentos e activar o mecanismo de leitura. Desta forma, os leitores só estão activos durante um curto período de tempo diminuindo, assim, as probabilidades de ocorrência de interferências.

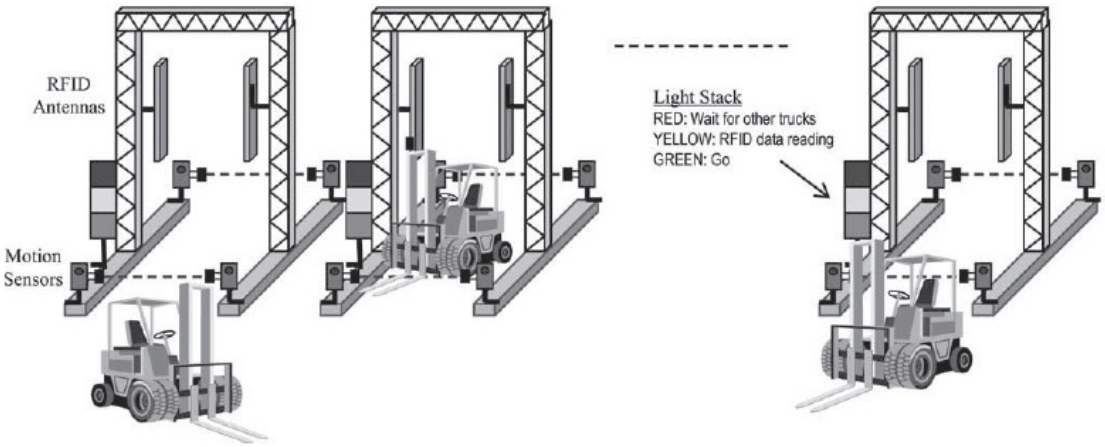


**Figura 8.5** – Portais e seus Componentes [50]

## 8.7 Justificação da Solução Proposta

A solução apresentada já foi testada em várias situações e com diferentes tecnologias, mas todas altamente dependentes do elemento humano que é fundamental para o bom funcionamento de qualquer solução, mas cujo comportamento é de difícil controlo e rastreabilidade e que introduz erros e estrangulamentos nas soluções testadas, sejam elas procedimentos escritos de cumprimento obrigatório ou os mesmos procedimentos adoptados ao uso da tecnologia de código de barras.

O elemento humano é fundamental ao bom funcionamento de qualquer sistema mas, neste tipo de actividade, a presença do mesmo elemento é muito aleatória, seja porque está de férias, porque é transferido em determinados períodos para outras funções ou por abstenção.

A falta dos operadores habituais provoca situações cada vez mais difíceis de resolver e cujas consequências são cada vez mais gravosas para a organização.

A introdução de meios automáticos de captura e controlo de toda a informação é uma exigência dos processos actuais que a gestão pretende cada vez mais independentes do factor humano.

A tecnologia de código de barras, que pode ler o SSCC, para ser credível a este nível implica a existência de uma infra-estrutura quase tão dispendiosa como a de RFID, quer ao nível das comunicações, dos leitores e do software que integra essas leituras no respectivo ERP. Para que não sejam introduzidos atrasos na expedição das mercadorias é necessário um aumento do pessoal afecto ao manuseamento de cargas, já que a leitura do código de barras da palete pelo operador do empilhador é inviável.

As dificuldades apresentadas pela tecnologia de código de barras em implementar controlos automáticos e a sua dependência do factor humano, que além de ser uma fonte potencial de erros é também, normalmente, um ponto de estrangulamento em sistemas que se pretendem de alto débito, podem ser facilmente ultrapassadas com o recurso à tecnologia de RFID, que possui grande independência do factor humano e permite a implementação de mecanismos automáticos de controlo, de forma a melhorar a performance de todo o sistema. O tempo de espera é um parâmetro muito importante na expedição de mercadorias e pode ser um dos factores determinantes para que a identificação por radiofrequência seja adoptada em muitas situações, já que a generalidade das cargas se concentram em curtos espaços de tempo: início e fim da manhã e início e fim da tarde.

## 8.8 Custos da Solução Proposta

Vamos agora apresentar uma estimativa dos custos de implementação da solução apresentada. Os preços do hardware e respectivos custos de manutenção foram obtidos no representante dos equipamentos em Portugal. Os preços de software e serviços baseiam-se na informação fornecida por vários intervenientes no sector, na experiência pessoal e no acesso

às bases de dados de alguns fabricantes e distribuidores que a disponibilizam aos seus parceiros comerciais.


**Figura 8.6** – Leitor Fixo Motorola FX7400 [51]


**Figura 8.7** – Antena Motorola AN480 [52]

**Figura 8.8** - Impressora Zebra RZ 400 [53]

| Custos da Solução € | | | |
|---|---|---|---|
| **Descrição** | **Preço Un** | **Qtd** | **Valor €** |
| Leitor Motorola FX7400 4 Portas [51] | 900,00 | 3 | 2.700,00 |
| Antena Motorola AN480 [52] | 230,00 | 6 | 1.380,00 |
| Cabo Ligação Antena | 100,00 | 6 | 600,00 |
| Pórtico | 2.000,00 | 3 | 6.000,00 |
| Sensores | 600,00 | 3 | 1.800,00 |
| Impressora RZ400 [53] | 2.900,00 | 2 | 5.800,00 |
| Servidor | 5.000,00 | 1 | 5.000,00 |
| **Total de Hardware** | | | **23.280,00** |
| | | | |
| Site Survey | 1.000,00 | 1 | 1.000,00 |
| Software | 5.000,00 | 1 | 5.000,00 |
| Instalação, Configuração e Formação | 2.500,00 | 1 | 2.500,00 |
| Cablagem e Outros trabalhos | 2.500,00 | 1 | 2.500,00 |
| **Total Software e Serviços** | | | **11.000,00** |
| **Total do Investimento** | | | **34.280,00** |
| | | | |
| **Encargos Anuais a Suportar** | | | |
| Tags /ano [54] | 0,25 | 20.000 | 5.000,00 |
| Consumiveis Impressora/ano | 150,00 | 1 | 150,00 |
| Manutenção Hardware /ano | 1.000,00 | 1 | 1.000,00 |
| Manutenção Software/ano | 1.500,00 | 1 | 1.500,00 |
| **Encargos/Ano** | | | **7.650,00** |

**Tabela 8.3** – Custos da Solução

Esta solução foi pensada para uma PME que introduz no mercado 10.000 paletes/ano, factura 15 milhões de euros/ano e o lay-out da unidade produtiva apresentado na figura 8.3.

Para uma amortização do investimento em cinco anos a empresa teria um encargo de aproximadamente 15 mil euros/ano com o seu sistema de RFID.

Analisando os custos apresentados, o retorno do investimento ocorre com a recuperação de 10 paletes/ano ou 1‰ do volume de vendas.

Os ganhos do sistema não devem ser analisados apenas pela óptica do desaparecimento de mercadorias, mas também pelos ganhos de eficiência em todos os procedimentos da gestão de stocks que não são contabilizados directamente. Entre os ganhos indirectos que podem ser obtidos estão as situações criadas pela deficiente comunicação da informação entre os departamentos da empresa, a informação prestada aos diferentes intervenientes na cadeia de abastecimento e os erros cometidos na expedição da mercadoria. Estas ocorrências são, em muitos casos, a causa de um grande dispêndio de tempo e energia na sua solução com a inerente degradação das relações entre os intervenientes.

O relatório da KPMG '*Global Retail Loss Prevention Survey 2009*' conclui que as perdas do stock representam 3% do volume de vendas da organização. As principais causas destas perdas na EMEA são: [55]

- Erros no processo – 37%;
- Roubo por entidades exteriores – 27%;
- Roubo por entidades internas – 26%;
- Fraude entre empresas – 10%.

Comparando os valores apresentados pelo relatório da KPMG com os valores necessários para rentabilizar o investimento proposto podemos concluir que o investimento numa solução de controlo de stocks de produtos acabados baseado na tecnologia de RFID pode ser altamente rentável para a empresa.

# Capítulo 9

# Conclusões e Trabalho Futuro

## 9.1 Conclusões

Após este trabalho podemos concluir que:

- O mercado de RFID está em crescimento e apresenta, segundo os analistas, um elevado potencial de crescimento para a próxima década;
- Existe um grande investimento das empresas e centros de investigação nesta tecnologia;
- Os principais entraves à adopção da tecnologia de RFID são o custo elevado da tecnologia e a falta de standardização;
- Em muitas situações as tecnologias de código de barras e de RFID são complementares e não concorrentes;
- A tecnologia de código de barras vai continuar a ser largamente usada durante muito tempo;
- A passagem do carro de compras pelo check-out do supermercado com a emissão automática da respectiva factura é, actualmente, mais um sonho que uma realidade, apesar de todos os esforço que estão a ser efectuados;
- A etiquetagem da generalidade das mercadorias com uma tag ao nível do item ainda está muito distante;
- A tecnologia de RFID vai continuar a sua penetração nos mercados em que já está presente e a conquistar novos nichos de mercado;
- Cada implementação de RFID é única e deve ser sempre analisada sob esse prisma para evitar surpresas desagradáveis;
- A adopção de regulamentação adequada e a evolução tecnológica, irão colmatar, algumas das limitações/vulnerabilidades apresentadas pelo estado actual da tecnologia de RFID;

- Os custos de implementação e manutenção da tecnologia de RFID em algumas áreas de actividade, quando comparados com os benefícios que pode trazer para a organização, justificam perfeitamente o investimento efectuado;
- O grande esforço que está a ser efectuado na criação de standards para as várias frequências de funcionamento e diversas áreas de actividade são um incentivo à disseminação da tecnologia de RFID;
- A evolução tecnológica e a standardização provocam uma diminuição dos custos da tecnologia, o que é sempre um incentivo à sua adopção, já que facilita o retorno do investimento;
- Dependendo da quantidade e do valor das mercadorias introduzidas no mercado, acreditamos que o uso da tecnologia de RFID para controlo de stocks de paletes de produtos acabados numa empresa do sector agro-industrial, pode ser uma solução muito vantajosa.

## 9.2 Trabalho Futuro

Os conhecimentos adquiridos na realização deste trabalho, os dados fornecidos por empresas do sector agro-industrial e pelos fornecedores de equipamentos e serviços para a tecnologia de RFID, as perspectivas de crescimento do mercado de RFID apresentadas pelos analistas, a evolução tecnológica que está a ocorrer e o reduzido número de fornecedores de soluções de RFID para PME's existentes no mercado nacional, levam-nos a acreditar, que esta é uma área de elevado potencial de crescimento, pelo que é nossa intenção apresentar a algumas empresas, uma solução de gestão do stock de produtos acabados, baseada no modelo apresentado neste trabalho.

# Referências


[1] http://www.nationalbarcode.com/History-of-Barcode-Scanners.htm acesso em Abril de 2010

[2] http://www.gs1pt.org/produtos_solucoes/produtos_solucoes.htm acesso em Abril de 2010

[3] http://www.gs1.org/barcodes/technical/idkeys/gtin acesso em Abril de 2010

[4] The History of RFID Techenology http://www.rfidjournal.com/article/articleview/1338/1/129/ acesso em Abril de 2010

[5] Genesis of the Versatile RFID Tag http://www.rfidjournal.com/article/view/392/1/2 acesso em Abril de 2010

[6] Raghu, Das e Harrop, P – RFID Forcasts, Players & Opportunities 2009 – 2019 – IDTe-chEX2010 http://media2.idtechex.com/pdfs/en/R9034K8915.pdf download em Março 2010

[7] The Bridge Project. www.bridge-project.eu acesso Abril 210

[8] Mark Van Eeghem – EPC Advanced Business Aspects Student's Handbook V1.3 pag 14 http://www.bridge-project.eu/index.php/Training/en/ download em Outubro 2009

[9] VDC Research inc - Barcode and RFID – Market Update & 2010 Outlook apresentado em 20 Janeiro 210 disponível em http://www.slideshare.net/vdcresearch/barcode-and-rfid-market-update-2010-outlook acesso em Abril 2010

[10] Roberti, Mark – Saluting the RFID Pioneers in DoD, RFID Journal de 13 de Abril de 2009 disponível em http://www.rfidjournal.com/article/view/4777 acesso em Abril 2010

[11] EPCglobal Us: Report on the 2009 EPC/RFID Tagging Survey for the Retail / CPG Supply Chain disponível em http://www.gs1us.org/DesktopModules/Bring2mind/DMX/Download.aspx?EntryId=2932&Command=Core_Download&PortalId=0&TabId=73 Acesso em Abril 2010

[12] http://www.rfidjournal.com/article/view/7339/ acesso em Abril de 2010

[13] http://www.rfidjournal.com/article/view/7339 acesso em Abril de 2010

[14] http://www.rfidjournal.com/article/view/7352 acesso em Abril de 2010

[15] http://www.rfidjournal.com/article/view/7255 acesso em Abril de 2010

[16] http://www.rfidjournal.com/article/view/7271 acesso em Abril de 2010

[17] http://www.rfidjournal.com/article/purchase/2472 acesso em Abril de 2010

[18] http://www.rfidjournal.com/article/articleview/2075/1/1/ acesso em Abril 2010

[19] http://www.rfidjournal.com/article/articleview/2950/1/1/ acesso em Abril de 2010-

[20] RFID Case Studies http://www.aimglobal.org/casestudies/RFID.asp acesso Abril 2010

[21] Chia-hung Huang - An Overview of RFID Technology, Application, and Security/Privacy Threats and Solutions – George Mason University – 2009 – download em cryptography.gmu.edu/~jkaps/download.php?docid=1287 acesso Abril 2010

[22] Tom Karigiannis, Bernard Eydt, Greg Barner, Lynn Bunn e Ted Phillips , Nist; Guidelines for Securing Radio Frequency Identification (RFID) Systems Special Publication 800-98

[23] A Summary of RFID Standards – RFID Journal 1335 http://www.rfidjournal.com/article/articleview/1335/1/129/ accesso em Abril 2010

[24] Tao Cheng, Li Jin - Analysis and Simulation of RFID Anti-collision Algorithms - ISBN 978-89-5519-131-8 93560 ; Feb. 12-14, 2007 ICACT2007 ; pag 697

[25] Hugo Albuquerque, Luiz Correia e Onildo Ferraz – Protocolos Anti-Colisão Para Etiquetas RFID; download em www.cin.ufpe.br/~pasg/if740/**Protocolosanticolisao**detags.pptx acesso em Maio 2010

[26] Jihoon Myung, Wonjun Lee - Adaptive Splitting Protocols for RFID Tag Collision Arbitration ; *MobiHoc'06*, May 22–25, 2006, Florence, Italy. Download em http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.103.4252

[27] Michael Wack, Bernd.Schmidt - Embedded RFID Middleware **The interface between RFID systems and enterprise applications, download em** http://www.embeddedinnovation.de/pdf/RFID-EmbeddedWorld2007.pdf

[28] Mark Van Eeghem, Basics of EPC – Student's Handbook V2.0 pag 70 http://www.bridge-project.eu/index.php/Training/en/ download em Outubro 2009

[29] Mark Van Eeghem, EPC Advanced Technical – Student's Handbook V1.4 pag 60 http://www.bridge-project.eu/index.php/Training/en/ download em Outubro 2009

[30] Klaus Finkenzeller, RFID Handbook: Fundamental and Applications in contactless Smart Cards and Identification, pag 42

[31] Xiaoyong Su, Chi-Cheng Chu, B.S. Prabhu, Rajit Gadh- On The Creation of Automatic Identification and Data Capture Infrastructure via RFID, download em http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.92.2317 acesso em Maio 2010

[32] http://pffc-online.com/mag/mastering_rfid_1005/ acesso em Maio 2010

[33]The History of EPCglobal http://www.epcglobalus.org/AboutUs/History/tabid/191/Default.aspx acesso em Abril 2010

[34]Standars EPCglobal - http://www.epcglobalinc.org/standards acesso em Abril 2010

[35] ETSI TR 102 649-1 V1.1.1 (2007-04), download em http://www.etsi.org/deliver/etsi_tr/102600_102699/10264901/01.01.01_60/tr_10264901v010101p.pdf

[36] EPCglobal - Specification for RFID Air Interface V1.0.9 pag 35 http://www.epcglobalinc.org/standards/uhfc1g2/uhfc1g2_1_0_9-standard-20050126.pdf download em Fevereiro 2010

[37] Paul Mangus - Enhanced Driver's License and Lessons Learned – U.S. Departement of Homeland Security – Junho 2008 download em http://www.ncai.org/ncai/2008annual/EDL%20Native%20Americans%20Presentation.ppt

[38] EPCglobal – Tag Data Standards – V1.4 - Junho 2008, download em http://www.epcglobalinc.org/standards/tds/tds_1_4-standard-20080611.pdf

[39] United States Department of Defense Suppliers' Passive RFID Information Guide V14.0 download em http://www.acq.osd.mil/log/rfid/r_suppliers_guide.html

[40] Ari Juels – RFID Security and Privacy: A Reserche Survey, Setembro 2005, download em http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.94.5249&rep=rep1&type=pdf

[41] Stephen A. Weis , Sanjay E. Sarma_ , Ronald L. Rivest and Daniel W. Engels - Security and Privacy Aspects of Low-Cost Radio Frequency Identification Systems , download em http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.129.7578&rep=rep1&type=pdf

[42] Ari Juels, Ronald Rivest e Michael Szydlo - The Blocker Tag: Selective Blocking of RFID Tags for Consumer Privacy, download em http://www.google.com/url?q=http://citeseerx.ist.psu.edu/viewdoc/download%3Fdoi%3D10.1.1.1.7036%26rep%3Drep1%26type%3Dpdf&sa=U&ei=MSAiTJqwA8KYOO_zmBs&ved=0CBMQFjAA&usg=AFQjCNEV5igi0bRGZuhvi1TYFFOT8qD-ag

[43] Paweł Rotter - A Framework for Assessing RFID System Security and Privacy Risks - Published by the IEEE CS n 1536-1268/08

[44] http://dailyheadlines.uark.edu/16260.htm acesso em Maio de 2010

[45] Hee-Bok Kang e tal - Crypto Based EPC C1G2 UHF (860 MHz–960 MHz) Passive RFID Tag Chip

[46] Melanie R. Rieback, Bruno Crispo e Andrew S. Tanenbaum - Is Your Cat Infected with a Computer Virus?, download em http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.64.1391&rep=rep1&type=pdf

[47] Daniel Dobkin – The RF in RFID – pag 306

[48] Quickguide to the GS1-128 pallet label - GS1 Denmark's ServiceCenter, download em http://www.supergros.com/2007/pdf/logistik/GS1_128_quick_guide_UK.pdf

[49] The GS1 Logistics Label – GS1 Austrália, download em http://www.gs1au.org/assets/documents/industry/fresh_produce/mis_fprod_logistics_label.pdf

[50] A. Soylemezoglu et al. – A testbed architecture for Auto-Id Techenologies, Assembly Automation, Vol.26, No.2, pp.127-136, 2006

[51] FX Series RFID Readers Integrator Guide http://support.symbol.com/support/search.do?cmd=displayKC&docType=kc&externalId=12249001apdf&sliceId=&dialogID=178698938&stateId=0%200%2022536903

[52] Antena AN480 http://www.motorola.com/business/v/index.jsp?vgnextoid=ea2b3acf35e95110VgnVCM1000008406b00aRCRD acesso em Maio de 2010

[53] Impressora Zebra RZ400 acesso em Maio de 2010 http://www.zebra.com/id/zebra/na/en/index/products/printers/rfid/rz400.html

[54] Tag - http://www.fastrfid.com/raflatac/UHF/tech_speck_3001488_letter.pdf

[55] KPMG - Global Retail Loss Prevention Survey 2009 - Este relatório está disponível em http://www.kpmginstitutes.com/insights/2009/pdf/global-retail-loss-prevention.pdf